Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aanbiedingsformulier Overheidsbreed Beleidsoverleg Digitaal Overheid

1. Korte titel	Duiding en maatregelen Monitor open standaarden 2019 (incl. Monitor 2019, eindmeting IV-standaarden, streefbeeldafspraak IPv6 en concept-opdracht DMARC) + plaatsing GWSW op de 'pas toe of leg uit'-lijst en OID op de lijst aanbevolen standaarden
2. Datum behandeling	Strategisch Vooroverleg: 3 maart 2020 | OBDO: 18 maart 2020
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. ☒ Anders: Forum Standaardisatie Uitkomst behandeling in bovenstaand gremium: ☐ Overeenstemming *(geen toelichting vereist)*
5. Voorgeschiedenis / context: *6. Samenvatting/toelichting*	**1.** A) Monitor open standaarden 2019 (bijlage 1a): hieruit blijkt dat de uitvraag van één of meer relevante 'pas toe of leg uit'-standaarden (ptolu) in aanbestedingen verder is gegroeid naar 89%, maar dat slechts in 6% álle verplichte standaarden worden gevraagd. 'Leg uit' in jaarverslagen ontbreekt geheel als niet gekozen is voor open standaarden. Toepassing van open standaarden in voorzieningen gaat goed, maar enkele voorzieningen en standaarden verdienen extra aandacht. Tot slot is over het gebruik grofweg van de helft van de ptolu-standaarden veel bekend en over de andere helft weinig. Als jaar op jaar weinig (meer) naar voren komt over het gebruik van een standaard, dan kan dit aanleiding zijn om nut en noodzaak van de ptolu-status nader ter discussie te stellen. B) IV-meting eind 2019 (bijlage 1b): uit de eindmeting gebruik informatieveiligheidsstandaarden (IV-standaarden), onderdeel van de Monitor, blijkt dat de toepassingsgraad nog toeneemt maar dat het groeitempo afvlakt. Het risico op schade door phishing/spoofing, afluisteren en manipulatie van overheidsmail is daarom nog aanzienlijk. De IV-meting laat zien of overheidsorganisaties voldoen aan de in het OBDO (en voorheen in het Nationaal Beraad) gemaakte streefbeeldafspraken voor de implementatie van IV-standaarden. Strategisch Leveranciersmanagement Rijk is i.s.m. Forum Standaardisatie in gesprek met Microsoft over toepassing van anti-afluisterstandaarden (DANE) op Office 365 Exchange Online. Microsoft heeft toegezegd eind februari met meer duidelijkheid te komen. Vanwege het belang hiervan zal het Forum Standaardisatie deze informatie met het OBDO delen zodra deze beschikbaar is. C) Streefbeeldafspraak IPv6 (bijlage 1c): uit de Monitor blijkt ook dat het aantal overheidswebsites en -mailsystemen dat IPv6 (de toekomstbestendige standaard voor netwerkadressen op internet)

	gebruikt toeneemt, maar een extra impuls nodig heeft. Het nagenoeg uitgeputte en nog veel gebruikte IPv4 belemmert groei en innovatie, en bemoeilijkt fraudedetectie en -preventie. Een overheidsbrede overstap naar IPv6 volgt de markt-beweging en houdt de digitale overheid in de toekomst bereikbaar. Een overheidsbrede streefbeeldafspraak voor IPv6 is nodig om dit te ondersteunen (vgl. de streefbeeldafspraken voor IV-standaarden). D) Strikte DMARC policy (bijlage 1d): tot slot laat de Monitor zien dat slechts 53% van de emaildomeinen binnen het Rijk actieve DMARC policies heeft ingesteld. *Phishing mails namens overheidsorganisaties (inclusief bewindspersonen, burgemeesters etc.) komen in die gevallen dus nog steeds bij burgers en bedrijven aan*. Een juiste instelling van DMARC voorkomt phishing, geeft blijkt van goed huisvaderschap en voorkomt uiteindelijk kosten en onrust bij eindgebruikers (zoals in het recente geval bij de universiteit van Maastricht). Met bijgaand stappenplan kan de eigen ICT-dienstverlener helpen een verscherpte DMARC-policy te implementeren. <u>Mutaties lijsten open standaarden</u> **2.** Het Forum adviseert het OBDO de standaard **GWSW** (standaard voor eenduidige uitwisseling en hergebruik van gegevens in stedelijk waterbeheer) te plaatsen op de 'pas toe of leg uit'-lijst'. Het Forum adviseert het OBDO de standaard **OIDC** (open en gedistribueerde standaard om één authenticatiedienst naar keuze te kunnen hergebruiken) te plaatsen op de lijst aanbevolen standaarden.
7. Beslispunten/discussiepunten	**1.** Agenderen van Monitor open standaarden 2019 (inclusief de IV-meting) in eigen gremia (zie tabel bijlage 1a, graag evt. PM's aanvullen): hoe *conform toezegging Minister van BZK aan Tweede Kamer* de 'pas toe of leg uit'-standaarden te vervlechten in eigen bedrijfsvoering (ICT-opdrachtgeverschap en contractmanagement, aanschaf en inkoop, informatiebeveiliging en bedrijfsvoering, toezicht en handhaving) Opdracht geven binnen eigen cirkel van invloed aan de hiervoor verantwoordelijke afdelingen om het nalaten van het gebruik van relevante open standaarden in jaarverslag 2020 uit te leggen Instemmen met het maken van de **streefbeeldafspraak IPv6**; Opdracht geven aan eigen ICT-dienstverlener om verscherpte **DMARC**-policy te implementeren om phishingmails te stoppen. **2.** Instemmen met plaatsing van **GWSW** op de 'pas toe of leg uit'-lijst. Instemmen met plaatsing van **OIDC** op de lijst aanbevolen standaarden.
8. Contactgegevens	**1.** Désirée Castillo Gosker (Monitor en jaarverslag) 06-52504226, Bart Knubben (IPv6 en DMARC) 06-21162373 **2.** Redouan Ahaloui ('pas toe of leg uit' & aanbevolen lijst) 06-15642325

Notitie

FORUM STANDAARDISATIE
Duiding en maatregelen Monitor Open standaarden 2019

Versie 6 maart 2020

Waarom open standaarden en wat betekenen de laatste cijfers over het gebruik volgens het Forum Standaardisatie?

Open standaarden zorgen voor interoperabiliteit. Dat wil zeggen een vloeiende uitwisseling van vindbare, toegankelijke en begrijpelijke gegevens. Verder zijn leveranciersonafhankelijkheid, kostenbesparingen, innovatie en inclusie, belangrijke doelen waaraan open standaarden bijdragen.

Forum Standaardisatie beheert de 'pas toe of leg uit'-lijst van open standaarden. Sinds 2008 zijn de standaarden op deze lijst voor overheidsorganisaties verplicht. Afwijken van deze verplichting mag, mits met een geldige reden die terug te vinden is in het jaarverslag.

Jaarlijks onderzoekt ICTU in opdracht van het Forum Standaardisatie hoe het staat met het gebruik van deze 'pas toe of leg uit'- standaarden en de uitleg als gebruik achterwege blijft. Bijgaand treft u het rapport van het laatste onderzoek aan: de Monitor Open Standaarden 2019[1].

Hieruit blijkt dat de adoptie van de 'pas toe of leg uit'- standaarden groeit. Er wordt toegepast maar nog niet voldoende. Correct uitleggen gebeurt niet tot zelden.

Forum Standaardisatie waarschuwt met klem voor informatiebeveiligingsrisico's rond het nalaten van de verplichte e-mailstandaarden

De belangrijkste conclusie die uit de Monitorcijfers getrokken mag worden is dat het gebruik nog steeds geen volledige naleving laat zien van de 'pas toe of leg uit'- verplichting én de aanvullende streefbeeldafspraken die het OBDO gemaakt heeft voor een aantal informatiebeveiligingsstandaarden. Met name de standaarden voor e-mailbeveiliging blijven achter. Forum Standaardisatie waarschuwt daarom met klem voor de risico's hiervan. Phishing kan bijvoorbeeld tot forse schade leiden. Zoals onlangs bij de Universiteit van Maastricht: https://nos.nl/artikel/2321749-hoe-een-phishingmail-in-oktober-met-kerst-de-universiteit-platlegde.html. *Phishing e-mail* uit naam van overheidsorganisaties die de standaarden nog niet streng hebben afgesteld komt nog steeds bij burgers en bedrijven aan, terwijl dat issue eind 2017 al het acht-uur journaal haalde, toen ondermeer de e-mail van de Tweede Kamer en de AIVD

[1] https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS-191211.5A1_Rapport_Monitor_Open_standaarden_2019_v1.0.pdf

onvoldoende beveiligd bleek te zijn en de relevante standaarden niet geïmplementeerd waren[2].
https://www.security.nl/posting/536615/E-mail+Tweede+Kamer+was+kwetsbaar+voor+spoofing

Vertrouwensbeginsel

Nalaten van het gebruik van de 'pas toe of leg uit'- standaarden staat verder op gespannen voet met het vertrouwensbeginstel, voor zover burgers en bedrijven erop mogen vertrouwen dat de overheid zich aan zijn eigen afspraken houdt. Denk aan leveranciers die zien dat de uitvraag van open standaarden vaak wel met de mond wordt beleden, maar dat - er als het erop aankomt- te vaak gekozen wordt voor aanbiedingen van concullega's die de standaarden niet of niet allemaal ondersteunen. Het is wachten op de dag dat hierop bij de rechter met succes beroep op wordt gedaan.

Leeswijzer voor de rest van de notitie.
- Onder het kopje "Duiding" de conclusies van het Forum Standaardisatie per onderdeel van de Monitor Open Standaarden 2019.
-Onder het kopje "Maatregelen", *ter besluitvorming*, welke maatregelen het Forum Standaardisatie aan het OBDO adviseert, opdat het gebruik van deze standaarden moge toenemen.

Duiding

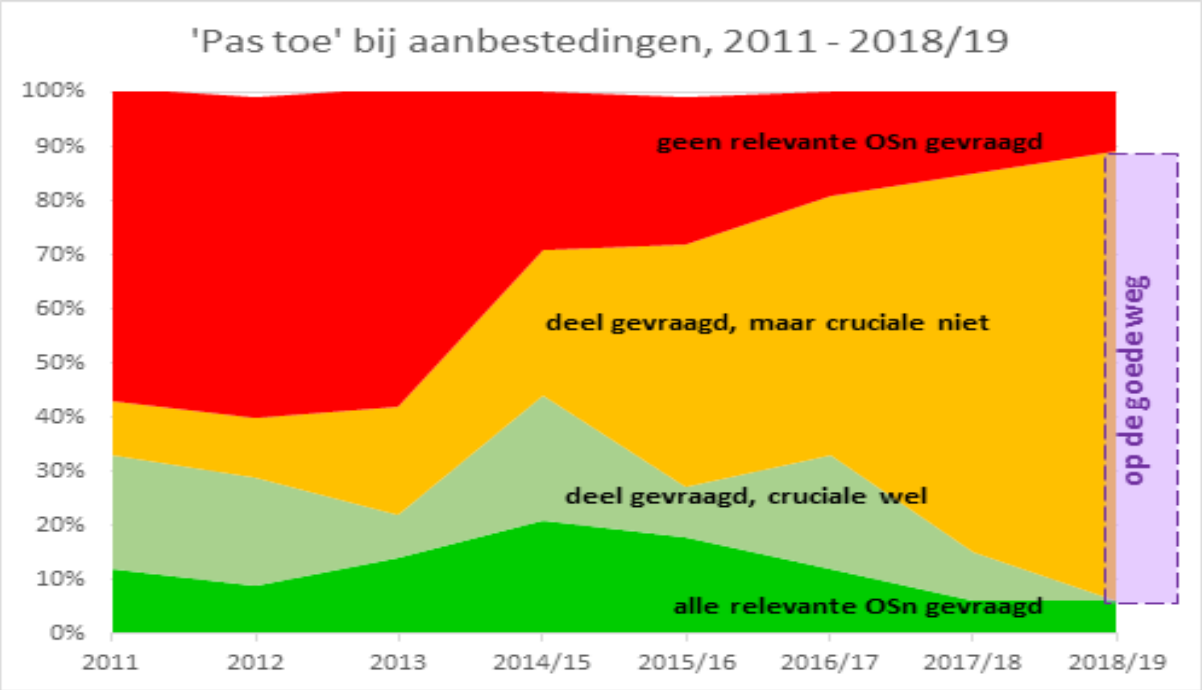
De Monitor Open Standaarden 2019 bestaat uit vier onderdelen. Hieronder per onderdeel de onderzoeksvraag, het onderzoeksresultaat en de duiding van Forum Standaardisatie (Duiding FS). Voor meer gedetailleerde informatie, zoals grafieken, tabellen, de methode of over het hoe en waarom: zie (de managementsamenvatting van) het rapport en de bijlagen[3].

1. **Vragen overheidsorganisaties om de relevante open standaarden in aanbestedingen?**
   Uit de Monitor Open Standaarden 2019 blijkt nu dat:
   - in 6% van de aanbestedingen *alle* Open Standaarden (in de figuur afgekort met OSn) worden uitgevraagd;
   - in 83% procent van de aanbestedingen *een deel* van de relevante aanbestedingen, vanaf 2019 aangeduid met "op de goede weg";
   - In totaal wordt dus in 89% minstens om een van de relevante standaarden uitgevraagd (was 85%), dat percentage is dus weer verder gegroeid.

In de figuur hiernaast bovenstaande resultaten vergeleken met voorgaande jaren.
In de Monitor Open Standaarden 2019 staat een overzicht van de onderzochte aanbestedingen, met daarbij aangegeven het percentage waarin om de relevante open standaarden is gevraagd. Maar in 6% van de onderzochte aanbestedingen worden alle relevante open standaarden van de 'pas toe of leg uit' –lijst uitgevraagd.

[2] Voor die organisaties is dat toen binnen een week opgelost.
[3] https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS-191211.5A1_Rapport_Monitor_Open_standaarden_2019_v1.0.pdf;
https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS-191211.5A2_PBLQ_Monitor_Open_Standaarden_Voorzieningen_2019_v1.00.pdf

Duiding FS: In combinatie met de overige percentages levert dit de conclusie op dat een standaard gemiddeld 50% kans maakt om in een aanbesteding daadwerkelijk gevraagd te worden. Dat is nog steeds te weinig.



Figuur: uitvraag percentages in opeenvolgende versies van de Monitor Open Standaarden[4]

2. Leggen overheidsorganisaties afwijkingen correct uit in het jaarverslag?

Monitor Open Standaarden 2019: *Nee, dit gebeurt structureel niet of nauwelijks.*

Duiding FS: Uitleggen moet, vooral daar waar niet is uitgevraagd (zie punt 1).

3. *Passen beheerorganisaties de relevante open standaarden toe in generieke overheidsvoorzieningen?*

https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS-191211.5A2_PBLQ_Monitor_Open_Standaarden_Voorzieningen_2019_v1.00.pdf

Monitor Open Standaarden 2019: *In de meeste gevallen voldoen de onderzochte voorzieningen aan de meeste ervoor relevante standaarden: aan 69% wordt voldaan, aan 15% voldoet de voorziening deels of is dit gepland en in 16% van de gevallen wordt op dit moment niet voldaan aan een relevante open standaard.*

Duiding FS: Een paar voorzieningen en standaarden verdienen extra aandacht (zie maatregelen).

[4] Het eerder gemaakte onderscheid “cruciaal en niet-cruciaal” komt vanaf 2019 niet meer voor in de weergave van de resultaten.

4. ***Wat is, bezien per standaard, verder nog bekend over het gebruik van de standaarden op de 'pas toe of leg uit'- lijst?***
   Monitor Open Standaarden 2019: *Dat verschilt per standaard of per domein standaarden. Grofweg is van de helft van de standaarden over het gebruik veel bekend en over de andere helft weinig.*
   Duiding FS: Als over een standaard of over een set standaarden jaar op jaar weinig (meer) naar voren komt over het gebruik, dan ligt hierin een aanleiding om nut en noodzaak van de 'pas toe of leg uit'- status nader ter discussie te stellen. Wellicht is het dan tijd om de standaard van de 'pas toe of leg uit'-lijst te halen.

5. Een speciale categorie in dit onderdeel van het Monitoronderzoek zijn de informatieveiligheidsstandaarden, die onder ander helpen om phishing tegen te gaan. Over het gebruik van deze standaarden zijn in het OBDO streefbeeld afspraken gemaakt; drie overheidsbrede afspraken over uiterste implementatiedata. Het Forum Standaardisatie voert medio 2015 metingen uit naar het gebruik van de afgesproken standaarden op 550 overheidsdomeinnamen.
   Uit de laatste IV-meting (winter 2020) blijkt dat het gebruik van de meeste standaarden enorm is toegenomen; de toepassingsgraad van de meeste standaarden is inmiddels ruim boven de 90%. Opvallend is dat de webstandaarden gemiddeld beter worden toegepast dan de mailstandaarden (92% vs 77%).
   Duiding FS: Voor een paar standaarden blijft de adoptie echter rond circa de helft steken, terwijl het streefbeeld was om die eind 2019 op orde te hebben*. Forum standaardisatie waarschuwt met klem voor risico op schade door phishing/spoofing en afluisteren en manipulatie van e-mail van de overheid.*

Maatregelen ter besluitvorming

Gelet op bovenstaande duiding, adviseert Forum Standaardisatie aan het OBDO:

1. Agendering van de Monitor Open Standaarden 2019 - inclusief de IV-meting (bijlage 1b)- in de gremia in onderstaande tabel;

2. Dat via deze gremia (conform de toezegging van de Minister van BZK aan de Kamer) gesproken wordt over de manier waarop de pas-toe-of-leg-uit standaarden vervlochten kunnen worden in reeds bestaande processen en kaders rond:
   a. ICT-opdrachtgeverschap en contractmanagement;
   b. Aanschaf en inkoop;
   c. Informatiebeveiliging en bedrijfsvoering
   d. Toezicht en handhaving

	ICT opdrachtgeverschap en contractmanagement	**Aanschaf en inkoop**	**Informatiebeveiliging en bedrijfsvoering**	**Toezicht en handhaving**
Gemeenten	College van dienstverleningszaken: x/x/2020	VNG Taskforce Samen Organiseren: x/x/2020	VNG Adviesraad IBD: x/x/2020	VNG Taskforce Samen Organiseren: x/x/2020
Rijk	CIO-beraad: 11/7/2019, 3/6/2020 CTO-raad: 22/5/2019, 16/9/2020 EZK/LNV CIO-raad: x/x/2020	ICIA (strategie rijkinkoopbeleid): 28/11/2019	SIB / CISO overleg (Strategisch Informatiebeveiligings Beraad): x/x/2020, eTIB: 10/10/2019	ADR - loopt
Provincies	SIO (Strategisch Informatie Overleg): Voorzitter is Frank Ossewaarde, en was CIO Noord-Holland, maar sinds 1 maart bij het IPO. fossewaarde@ipo.nl, 06 – 53 25 05 05	Centraal Platform van Inkopers: voorzitter is Maarten Raauws, maarten.raauws@provincie-utrecht.nl, 06 – 52 76 98 08	CIBO: voorzitter is Pieter de Ruiter, ruiterp@noord-holland.nl, 06 – 31 68 81 37	Ambtelijke Adviescommissie MTH (Milieu, Toezicht en Handhaving). Secretaris in Hugo van de Baan, hvdbaan@ipo.nl, 06 28 90 12 05
Uitvoeringsorganisaties	Manifestgroep: x/x/2020 Programmeringsraad: Logius x/x/2020	IMO (directeuren inkoop uitvoeringsorganisaties Rijk): 6/2/2020 en daarna over een half jaar	PM	PM
Waterschappen	iPlatform Waterschapshuis: x/x/2020	PM	Coördinatoren Informatieveiligheid Waterschappen (CIW): x/x/2020	PM
Alle	OBDO: 23/4/2019, x/x/2020 NORA gebruikersraad 26 maart 2020			

Tabel: spreken over vervlechting, monitor & iv-meting

3. Dat de leden van het OBDO binnen hun cirkel van invloed opdracht geven aan de hiervoor verantwoordelijke afdelingen om het nalaten van het gebruik van de relevante open standaarden uit te leggen in het jaarverslag vanaf 2020;

4. Dat de leden van het OBDO om het gebruik van standaarden te vergroten
   - instemmen met het streefbeeld rond de bereikbaarheid van overheidsdienstverlening via IPv6 (bijlage 1c);
   - binnen hun cirkel van invloed opdracht geven om phishingmails te stoppen voordat het de eindgebruiker bereikt, door hun ICT-dienstverlener opdracht te geven een invoeringstraject in te zetten om een verscherpte DMARC policy te implementeren. Hierbij kan desgewenst gebruik gemaakt worden van de voorbeeldopdracht (bijlage 1d).

TER KENNISNAME AAN HET OBDO

Het Forum Standaardisatie vraagt het OBDO kennis te nemen van:

1. De Monitor Open Standaarden 2019 (bijlage 1a2) inclusief het rapport van PBLQ over het gebruik van open standaarden in voorzieningen als laatste bijlage;

   Met betrekking tot sommige onderzoeksresultaten van de Monitor Open Standaarden en de duiding en voorgestelde maatregelen van het Forum Standaardisatie is het goed om te weten wat al aanpalend aan acties is ingezet en waarover dus niet meer besloten hoeft te worden. Het gaat hierbij met name om de volgende toezeggingen in de Kabinetsreactie op het rapport Inventarisatie Standaardisatie.

2. De acties die volgen uit de aanbiedingsbrief van de Minister van BZK van het rapport Inventarisatie Standaardisatie aan de Tweede Kamer, die met het achterblijven van de adoptie van open standaarden verband houden, te weten:
   a. Dat in 2020 de minister van BZK met inkopers en opdrachtgevers verkent hoe open standaarden meer en beter vervlecht kunnen worden in reeds bestaande processen rond het moment van inkoop en aanbesteding van IT;
   b. Dat in 2020 de minister van BZK verkent hoe de vervlechting van het gebruik van open standaarden in bedrijfsvoerings- en controlprocessen kan plaatsvinden;
   c. Dat de minister van BZK in gesprek gaat met de Audit Dienst Rijk over toezicht op naleving van ‘pas toe of leg uit’. Door bijvoorbeeld door de jaarverslagen te controleren op geldige redenen op grond waarvan het gebruik van relevante standaarden achterwege is gelaten, ‘leg uit’;
   d. Dat de minister van BZK aan het Forum Standaardisatie gevraagd heeft om een onderzoek uit te voeren naar de bottlenecks voor de adoptie van open standaarden.

Meting Informatieveiligheidstandaarden overheid maart 2020

Datum 9 maart 2020
Status Definitief t.b.v. OBDO

Forum Standaardisatie

Standaard Samenwerken

Managementsamenvatting

Achtergrond
Het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) en het Nationaal Beraad hebben voor een aantal informatieveiligheidsstandaarden, in aanvulling op pas-toe-of-leg-uit, overheidsbrede streefbeeldafspraken met uiterlijke implementatiedata gemaakt. De Meting Informatieveiligheidstandaarden laat zien of overheidsorganisaties voldoen aan de gemaakte afspraken en wat de voortgang is.

Door toepassing van de informatieveiligheidstandaarden wordt:
- de verbinding met overheidswebsites beter beveiligd, zodat criminelen niet zomaar uitgewisselde gegevens kunnen onderscheppen of manipuleren;
- e-mailverkeer met de overheid beter beveiligd, zodat criminelen niet zomaar
    - e-mails kunnen onderscheppen of manipuleren;
    - overheidsdomeinen kunnen misbruiken als afzenddomein voor bijvoorbeeld phishing-aanvallen.

Resultaten
De toepassingsgraad van informatieveiligheidstandaarden blijft toenemen maar het groeitempo vlakt af. Een significant deel van de gemeten websites en vooral e-mailservers voldoet nog niet (volledig) aan de afgesproken standaarden. Met name gelet op de achterblijvende mailstandaarden waarschuwt het Forum Standaardisatie voor risico op schade door phishing/spoofing, afluisteren en manipulatie van e-mailverkeer van de overheid.[1]

Streefbeelden
De toepassing van de standaarden van de eerste twee streefbeeldafspraken stagneert (respectievelijk 94% en 92%). De derde streefbeeldafspraak, die eind 2019 afliep, laat meer groei zien (van 71% naar 75%). Tegelijkertijd vlakt het groeitempo van de derde streefbeeldafspraak wel af (van 7%-punt, naar 5%-punt en nu naar 4%-punt per half jaar).

Mailstandaarden
Voor mailstandaarden is de gemiddelde toepassingsgraad het afgelopen half jaar toegenomen van 77% naar 81%. Het groeitempo is daarmee met 1%-punt gestegen ten opzichte van het halfjaar daarvoor. De toepassing van mailstandaarden is beduidend lager dan die van webstandaarden. Tegelijkertijd is de groei voor mailstandaarden wel sterker.

Bij de mailstandaarden is met name het gebruik van DMARC-policy (anti-phishing) en DANE (vertrouwelijkheid) zorgelijk. Beide groeien nog wel maar worden pas op de helft van de gemeten domeinnamen toegepast, terwijl de derde streefbeeldafspraak ten doel had dat alle overheden deze eind 2019 op orde zouden hebben. Dat betekent bijvoorbeeld dat mails van fraudeurs die afzenderadressen van de overheid misbruiken nog steeds bij burgers en bedrijven aankomen. Op die plekken waar DMARC nog steeds niet streng is afgesteld, kunnen bijvoorbeeld ook de mailadressen van bewindspersonen en bestuurders worden misbruikt.

[1] Phishing blijft een groot probleem. Recente phishing voorbeeld is de aanval op de universiteit van Maastricht. Ook de Betaalvereniging prioriteert phishing bestrijding in haar recente jaarverslag.

Webstandaarden
De toepassingsgraad voor webstandaarden is relatief hoog, maar de groei vlakt af. Uit de laatste meting blijkt dat de gemiddelde toepassing van webstandaarden het laatst gemeten half jaar is toegenomen van 92% naar 94%. Het groeitempo nam af van 3%- punt naar 2%-punt per half jaar.

Per overheidslaag
De gemeenten blijven koploper qua gemiddelde gebruik van de veilige webstandaarden (96%). De waterschappen staan op een tweede plaats maar zijn ten opzichte van de vorige meting niet verbeterd (92%). Het laagst scoren de uitvoerders met 87%. Bij veilige mailstandaarden is het Rijk koploper met een gemiddeld gebruik van 88%. Waterschappen en provincies blijven het meest achter (respectievelijk 72% en 73%). Als enige bestuurslaag gaan de provincies gemiddeld achteruit (van 75% naar 73%).

Handelingsperspectief
Hoewel de gemiddelde adoptie van informatieveiligheidstandaarden in de afgelopen drie jaar sterk is gegroeid zijn we er nog niet. De volgende aanvullende inspanningen zijn noodzakelijk om de gemaakte afspraken voor de geteste set domeinnamen alsnog na te komen.

1. Overheden die nog niet voldoen aan de afgesproken standaarden dienen dringend (opnieuw) hun leverancier formeel te verzoeken om ondersteuning, en daarbij te wijzen op beschikbare howto's[2] en te vragen om een concrete planning.
2. Overheden wordt verzocht om de ontvangen leveranciersplanningen ter informatie te delen met het Forum Standaardisatie. Forum Standaardisatie is bereid om desgewenst het gesprek met grotere overheidsleveranciers die nog niet te voldoen te coördineren.
3. Als de huidige leverancier te weinig medewerking verleent, dienen overheden te overwegen om over te stappen naar een leverancier die wel voldoet aan de afgesproken standaarden. Om geschikte leveranciers te vinden kan geleerd worden van collega-overheden die wel de afgesproken standaarden ondersteunen.
4. Forum Standaardisatie zal overheidsorganisaties, in samenwerking met koepelorganisaties, individueel aanspreken en helpen.
5. Het ministerie van BZK is voornemens om HTTPS, TLS geconfigureerd volgens de aanbevelingen van het NCSC en HSTS verdergaand te verplichten door middel van een algemene maatregel van bestuur (AMvB) op basis van het wetsvoorstel Wet digitale overheid. Deze AMvB is tussen 2 september 2019 en 20 oktober 2019 in openbare consultatie geweest. Het ministerie van Binnenlandse Zaken zal onderzoeken of dit ook voor andere informatieveiligheidstandaarden een goede optie is.

Strategisch Leveranciersmanagement Rijk (onderdeel van het Ministerie van Justitie en Veiligheid) is in samenwerking met Forum Standaardisatie in gesprek met Microsoft om ondersteuning van DANE in het product Microsoft Office 365 Exchange Online te krijgen. Microsoft heeft toegezegd eind februari met meer duidelijkheid te komen. Vanwege het belang hiervan zal het Forum Standaardisatie deze informatie met het OBDO delen zodra deze beschikbaar is.

[2] Voor how-to's over DANE en DMARC+DKIM+SPF zie: https://github.com/internetstandards/toolbox-wiki

Inhoudsopgave

1. Inleiding

Burgers en ondernemers moeten erop kunnen vertrouwen dat gegevensuitwisseling met de overheid en tussen overheden veilig verloopt. Recente phishing-incidenten waarin e-mails en websites van de overheid werden nagemaakt onderstrepen het belang van overheidsbrede adoptie van informatieveiligheidstandaarden. Binnen de overheid zijn daarom implementatieafspraken gemaakt over standaarden voor het beveiligen van mail en websites.

Om de voortgang van deze afspraken bij te houden voert het Forum Standaardisatie op verzoek van het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) twee keer per jaar een meting naar het gebruik van informatieveiligheidstandaarden door overheidsorganisaties.

Voorliggende meting dateert van maart 2020, waarbij 548 domeinnamen zijn getoetst. Uit deze meting blijkt dat het stijgende gebruik van de standaarden doorzet maar wel afvlakt. Tegelijkertijd is duidelijk dat de doelstelling van de derde streefbeeldafspraak die per eind 2019 afliep slechts door ongeveer de helft van de overheden is behaald. Dit betekent dat de e-mail van de andere helft van overheden nog altijd kwetsbaar is voor de risico's waartegen de afgesproken standaarden beschermen, namelijk phishing/spoofing en afluisteren van mailverkeer.

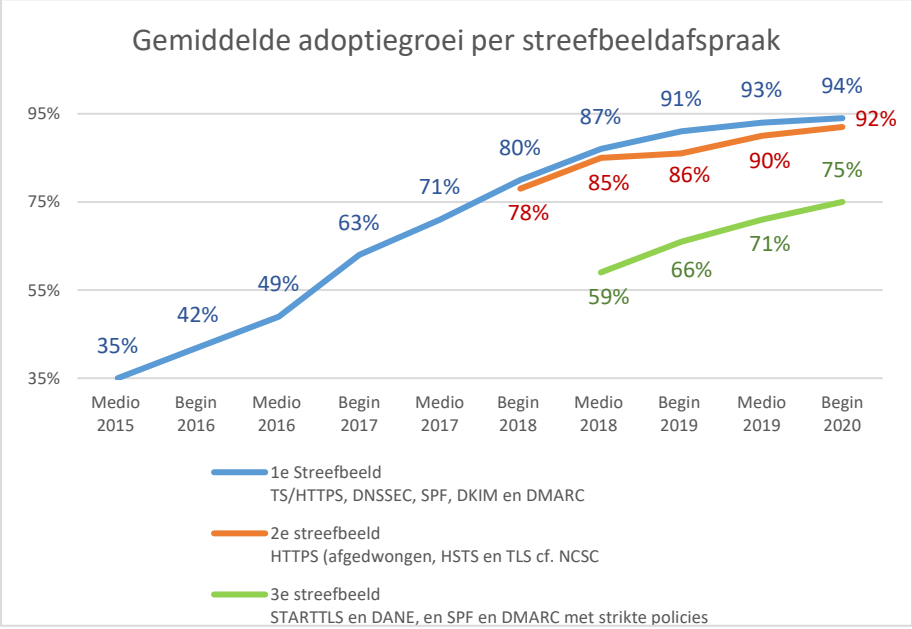
2. Conclusie

Het gebruik van de informatieveiligheidstandaarden is afgelopen half jaar wederom gegroeid. De webstandaarden worden gemiddeld veel beter toegepast dan de mailstandaarden (94% tegenover 81%). Het gemiddelde groeitempo van de webstandaarden vlakt af. Die groei was de vorige meting 3%-punt en nu 2%-punt. Het gemiddelde groeitempo in gebruik van mailstandaarden is met 4%-punt licht gestegen ten opzichte van de groei van 3%-punt in de vorige meting.

2.1. Streefbeeldafspraken

Eind 2019 is de uiterste realisatiedatum van de derde overheidsbrede streefbeeldafspraak verlopen. Deze streefbeeldafspraak gaat over zowel het implementeren van STARTTLS en DANE (om vertrouwelijkheid van mailverkeer te borgen) als het voldoende strikt configureren van SPF en DMARC (om mailspoofing tegen te gaan). In het afgelopen half jaar is de adoptiegraad van deze standaarden met gemiddeld 4% gegroeid. Daarmee vlakt het groeitempo verder af ten opzichte van de voorgaande metingen, die nog 7%-punt en 5%-punt groei lieten zien.

De onderstaande grafiek toont de overheidsbrede voortgang in het voldoen aan deze en eerdere streefbeeldafspraken. Opvallend is dat eerste twee streefbeeldafspraken beide nog maar licht groeien met respectievelijk 1%-punt en 2%-punt.



2.2. Webstandaarden

De gemiddelde adoptie van alle webstandaarden is inmiddels **94%**. Dat is 1%-punt hoger dan bij de vorige meting. De groei wordt veroorzaakt doordat de achterblijvers (provincies en uitvoerders) in beweging zijn gekomen. Bij de koplopers (gemeenten, waterschappen en rijk) stagneert de adoptie.

De gemeenten blijven het beste van alle overheidslagen scoren met een adoptiegraad van gemiddeld 96% van de webstandaarden, een stijging van 1%. De waterschappen en het Rijk stagneren met een adoptiegraad van respectievelijk 92% en 90%.

Bij provincies (van 84% naar 88%) is wel groei zichtbaar. Dat geldt ook voor de uitvoerders (van 84% naar 87%) die nu wel hekkensluiter zijn qua toepassing van webstandaarden.

Overheidsbreed groeien alle webstandaarden (DNSSEC, HTTPS, TLS, TLS cf NCSC) met 1%, behalve HSTS waarvan de adoptiegraad met 3% is gegroeid.

2.3. E-mailstandaarden

De gemiddelde adoptie van de mailstandaarden ligt met **81%** lager dan de webstandaarden. Dit is niet vreemd aangezien er meer mailstandaarden zijn, en er voor een deel van de standaarden pas sinds begin 2018 een streefbeeldafspraak was die eind 2019 is afgelopen. Het groeitempo is 4%-punt en licht daarmee iets hoger dan het groeitempo van het voogaande half jaar (3%-punt).

De adoptie groeit bij alle bestuurslagen, behalve bij provincies waar een lichte achteruitgang zichtbaar is (van 75% naar 73%).

De waterschappen hebben opnieuw de grootste groei in gebruik van mailstandaarden doorgemaakt met 5%-punt. Toch doen de waterschappen het met een gemiddelde adoptie van 72% nog steeds het minst goed van alle overheidslagen.

Bij gemeenten en uitvoerders is na de achteruitgang bij de vorige meting weer groei zichtbaar. Het Rijk doet het nog steeds het beste van alle bestuurslagen en de gemiddelde adoptie is behoorlijk gestegen (van 84% naar 88%).

In algemene zin ligt de uitdaging met name bij het strikt configureren van de DMARC policy (58%), het toepassen van DANE (50%), en DNSSEC MX (67%). De adoptie van deze standaarden is wel gegroeid, maar de groei van DNSSEC MX is gestagneerd. DNSSEC MX is een randvoorwaarde voor het kunnen toepassen van DANE.

We zien met name bij provincies een sterke achteruitgang voor DNSSEC op de mailservers (MX). Bij Rijks en uitvoerders is er sprake van een lichte achteruitgang. Bij de meeste bestuurslagen groeit het gebruik van DANE, behalve bij de waterschappen en provincies waar een stagnatie zichtbaar is. Er is nog extra groeipotentieel voor DANE, gezien de adoptiegraad van DNSSEC op de mailservers met 67% nog wel hoger ligt dan dat van DANE (50%).

De oorzaak van de trend rondom DNSSEC MX en DANE is dat een aantal overheden de overstap naar Microsoft Office 365 Exchange Online heeft gemaakt. Dit product biedt vooralsnog geen ondersteuning voor DNSSEC, en daarmee ook geen ondersteuning voor DANE. Dit is een duidelijk zorgpunt voor de betrouwbaarheid van overheidsmail, omdat deze gemeenten en provincies niet altijd een versleuteld mailtransport kunnen afdwingen en tevens niet aan de streefbeeldafspraak omtrent het gebruik van DANE kunnen voldoen.

Strategisch Leveranciersmanagement Rijk (onderdeel van het Ministerie van Justitie en Veiligheid) is in samenwerking met Forum Standaardisatie in gesprek met Microsoft om ondersteuning van DANE in het product Microsoft

Office 365 Exchange Online te krijgen. Microsoft heeft toegezegd eind februari met meer duidelijkheid te komen. Vanwege het belang hiervan zal het Forum Standaardisatie deze informatie met het OBDO delen zodra deze beschikbaar is. Tegelijkertijd is het van belang dat overheden die zelf Office365-klant zijn hier ook zelf formeel om (blijven) verzoeken bij Microsoft.

2.4. Handelingsperspectief

Hoewel de gemiddelde adoptie van informatieveiligheidstandaarden in de afgelopen 3 jaar sterk is gegroeid zijn we er nog niet. De volgende aanvullende inspanningen zijn noodzakelijk om de gemaakte afspraken voor de geteste set domeinnamen alsnog na te komen.

1. Overheden die nog niet voldoen aan de afgesproken standaarden dienen dringend (opnieuw) hun leverancier formeel te verzoeken om ondersteuning, en daarbij te wijzen op beschikbare howto's[3] en te vragen om een concrete planning.
2. Overheden wordt verzocht om de ontvangen leveranciersplanningen ter informatie te delen met het Forum Standaardisatie. Forum Standaardisatie is bereid om desgewenst het gesprek met grotere overheidsleveranciers die nog niet te voldoen te coördineren.
3. Als de huidige leverancier te weinig medewerking verleent, dienen overheden te overwegen om over te stappen naar een leverancier die wel voldoet aan de afgesproken standaarden. Om geschikte leveranciers te vinden kan geleerd worden van collega-overheden die wel de afgesproken standaarden ondersteunen.
4. Forum Standaardisatie zal overheidsorganisaties, in samenwerking met koepelorganisaties, individueel aanspreken en helpen.
5. Het ministerie van BZK is voornemens om HTTPS, TLS geconfigureerd volgens de aanbevelingen van het NCSC en HSTS verdergaand te verplichten door middel van een algemene maatregel van bestuur (AMvB) op basis van het wetsvoorstel Wet digitale overheid. Deze AMvB is tussen 2 september 2019 en 20 oktober 2019 in openbare consultatie geweest. Het ministerie van Binnenlandse Zaken zal onderzoeken of dit ook voor andere informatieveiligheidstandaarden een goede optie is.

Meer specifiek met betrekking tot de mailstandaarden:

- Het instellen van een voldoende strikte DMARC-policy is een kwestie van een goed, zorgvuldig configuratie-traject door de ICT-dienstverlener[4]. SPF en DKIM zijn noodzakelijk randvoorwaarden voor DMARC-policy. De meting laat zien dat die standaarden al zeer veel worden toegepast (op tenminste 90% van de domeinen). Er ligt dus een duidelijk groeipotentieel voor DMARC-policy.
- Het toepassen van DANE is een actie die ligt bij de beheerder van de mailserver. DNSSEC MX is een randvoorwaarde voor DANE en wordt al toegepast op 67% van de domeinnamen. Als een mailserver al DNSSEC doet, dan is het ondersteunen van DANE een relatief kleine stap ('laaghangend fruit'). Een aantal overheidsorganisaties maakt gebruik van cloud mailservers die nog geen DNSSEC MX en DANE ondersteunen.

[3] Voor how-to's over DANE en DMARC+DKIM+SPF zie: https://github.com/internetstandards/toolbox-wiki

[4] Een concept opdrachtomschrijving is als bijlage toegevoegd. Daarnaast is er het periodiek BOM-overleg (Betrouwbare Overheids Mail), waarin best-practices en tools worden uitgewisseld, waarop overheidsorganisaties kunnen aansluiten (bart.knubben@forumstandaardisatie.nl).

Het gaat o.a. om Microsoft Office 365. Het is van belang dat overheden ook bij deze leveranciers formele ondersteuningsverzoeken indienen.

2.5. Toekomstige metingen

De streefbeeldafspraken en bijbehorende metingen hebben gelet op de adoptiegroei gedurende de afgelopen jaren duidelijk effect gehad. Tegelijkertijd voldoen nog niet alle overheidsdomeinnamen aan de gemaakte afspraken. Het Forum Standaardisatie wil daarom de metingen de komende twee jaar voortzetten.

In toekomstige metingen zullen de volgende aanpassingen en uitbreidingen worden doorgevoerd:

1. Als de overheidsbrede streefbeeldafspraak voor IPv6 wordt vastgesteld, dan zal voortaan IPv6 ook onderdeel uitmaken van de metingen.
2. De set aan domeinnamen zal worden uitgebreid, mede op basis van het websiteregister van Dienst Publiek en Communicatie en de Staatsalmanak.
3. De test of TLS is geconfigureerd conform de TLS-richtlijnen van NCSC zal worden aangepast aan de laatste versie van deze richtlijnen.

In de huidige metingen wordt getest of een overheidsorganisatie zelf DMARC-, DKIM-, SPF- en DANE-kenmerken publiceert. In de loop van 2020 zal naar verwachting ook voor het eerst getest kunnen worden of een overheidsorganisatie dit soort kenmerken van anderen valideert.

3. Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden[5] de mogelijkheid om via de website Internet.nl domeinen te toetsen op het gebruik van verschillende 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[6]. 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[7].

De eerste streefbeeldafspraak is eind 2017 afgelopen. Begin 2018 is een eindmeting voor deze afspraak gepubliceerd. Ondanks een grote stijging de afgelopen twee jaar was volledige adoptie nog niet bereikt. Daarom zijn deze afspraken in april 2018 herbevestigd en aangevuld door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO), de opvolger van het Nationaal Beraad. De metingen vanaf 2018 zijn daarom uitgebreider (meer standaarden) dan voorgaande metingen. Daarnaast was het een goed moment om de lijst met de te toetsen domeinnamen te herijken en is besloten om het tijdstip van meten beter te laten aansluiten op de bestaande overlegcycli.

3.1. Om welke standaarden gaat het

Het Nationaal Beraad en het OBDO hebben streefbeeldafspraken gemaakt met betrekking tot de volgende standaarden[8]:

[5] Platform Internet Standaarden is een gezamenlijk initiatief van de Internetgemeenschap en de Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en NCSC). Zie https://internet.nl/about/

[6] http://www.binnenlandsbestuur.nl/digitaal/nieuws/nationaal-beraad-wil-sneller-moderne-e.9540822.lynkx

[7] Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. De halfjaarlijkse IV-meting is ook onderdeel van de jaarlijkse Monitor Open standaarden beleid.

[8] Voor meer informatie ga naar: https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken

Implementatie-deadline	Betreffende standaarden
uiterlijk EIND 2017	TLS/HTTPS: beveiligde verbindingen van (transactie)websites DNSSEC: domeinnaambeveiliging SPF: anti-phishing van email DKIM: anti-phishing van email DMARC: anti-phishing van email
uiterlijk EIND 2018	HTTPS, HSTS en TLS conform de NCSC richtlijn (externe link): beveiligde verbindingen van alle websites
uiterlijk EIND 2019	STARTTLS en DANE: encryptie van mailverkeer SPF en DMARC: het instellen van strikte policies voor deze emailstandaarden

3.2. Om welke domeinnamen gaat het

In totaal zijn in deze meting 548 domeinnamen van overheidsorganisaties getoetst, bestaande uit:

- Domeinen die horen bij de deelnemers van het OBDO;
- De domeinen die horen bij voorzieningen van de basisinfrastructuur (GDI);
- De 30 best bezochte domeinen van Rijksoverheden (en uitvoerders);
- De domeinen van de andere overheidsorganisaties die direct of indirect vertegenwoordigd zijn in het OBDO, zoals:
    - Uitvoerders (de Manifestpartijen);
    - Partijen die behorend tot Klein LEF;
    - Gemeenten;
    - Provincies;
    - Waterschappen.

Bij de selectie van de relevante domeinnamen is telkens gekozen voor het hoofddomein waarop de website van de overheidsorganisatie bereikbaar is. Daarnaast is gekozen voor het hoofddomein dat de desbetreffende overheidsorganisatie gebruikt voor e-mail (vaak dezelfde als voor web). Bij uitzondering zijn ook subdomeinen geselecteerd, bijvoorbeeld voor bekende inlogportalen of op verzoek van de beheerder.

De lijst betreft een selectie van alle overheidsdomeinnamen. De lijst is niet volledig en kan dat ook niet zijn omdat de overheid momenteel geen overzicht heeft over alle domeinnamen. De gemeten domeinen zijn bij lange na niet alle domeinen waar het OBDO direct en indirect voor verantwoordelijk is. Zo beheert het ministerie van AZ al meer dan 6000 domeinnamen. Een 100%-score op de gemeten domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn tegen bijvoorbeeld phishing. Indien uwer inziens een relevante domeinnaam ontbreekt, dan verzoeken we om deze aan ons door te geven.

3.3. Hoe wordt gemeten

De meting geeft de stand van zaken weer op de peildatum 3 maart 2020. De meting laat zien of op een domeinnaam de standaarden worden toegepast.

De meting wordt uitgevoerd middels een bulktoets via de API van Internet.nl. Voor de web-standaarden wordt het hoofddomein getoetst met de toevoeging www. (dus: www.forumstandaardisatie.nl), omdat het gebruikelijk is dat de website daarop bereikbaar is. Voor de maildomeinen wordt getoetst zonder enig voorvoegsel omdat dat doorgaans gebruikt wordt als e-maildomein (dus @forumstandaardisatie.nl).

Op Internet.nl is eenvoudig te testen of een website of e-mail een aantal moderne internetstandaarden ondersteunen, ook de standaarden waarover streefbeeldafspraken zijn gemaakt zijn onderdeel van de test. Overigens heeft de score die een domeinnaam op Internet.nl kan halen (namelijk max. 100%) geen relatie met het resultaat uit deze meting, aangezien deze meting een subset omvat van de standaarden waar Internet.nl op test.

De website Internet.nl is een initiatief van het Platform Internetstandaarden. In het platform participeren verschillende partners uit de internetgemeenschap (zoals Internet Society, RIPE NCC, SIDN en SURFnet) en Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en NCSC). Het uitgangspunt is dat Internet.nl de adviezen van Forum Standaardisatie en NCSC met betrekking tot de Internetstandaarden volgt.

De meting geeft geen inzicht in het risiconiveau van een bepaald domein. Zo is het aannemelijk dat de aantrekkelijkheid van misbruik hoger is bij domeinen van grote uitvoerders (zoals *phishing* met aanmaningen) dan bij domeinen van kleine gemeenten.

3.4. Wat wordt niet gemeten

In de meting wordt alleen gekeken naar de toepassing van standaarden op domeinnamen. Er wordt in de meting (nog) niet gekeken naar de validatie op de standaarden. Dat betekent dat de volgende zaken niet worden gemeten:

1. validatie van DNSSEC door de DNS-resolver van een overheidsorganisatie;
2. validatie van de DMARC-, DKIM- en SPF-kenmerken door ontvangende mailservers van een overheidsorganisatie;
3. validatie van DANE-kenmerken door verzendende mailservers van een overheidsorganisatie.

In de loop van 2020 zal naar verwachting de functionaliteit van Internet.nl worden aangepast zodat het mogelijk zal zijn om te controleren of DMARC-, DKIM-, SPF- en DANE-validatie wordt toegepast.

3.5. Over de standaarden

Er worden zowel web- als mailstandaarden gemeten. Hieronder per standaard een korte uitleg over wat deze doet. Overigens is meer (technische) informatie over wat er wordt getoetst te vinden op Internet.nl.

3.5.1. Webstandaarden

Wij meten het gebruik van de beveiligingsstandaarden voor het web ook op domeinen die alleen gebruikt worden voor mail omdat dit vaak wel domeinnamen zijn die re-directen naar het hoofddomein. Ook hiervoor moeten de standaarden juist worden toegepast en burgers weten vaak niet hoe deze domeinen worden gebruikt. Als redirects worden toepast dan moeten ook de doorverwijzende domeinen met HTTPS beveiligd zijn, anders is de beginschakel niet veilig en daarmee is ook de gehele keten onveilig. Dit geldt ook wanneer een zogenaamde 'parking page' wordt getoond. Alleen als een geregistreerd domein geen webpagina bevat dan is HTTPS niet nodig (en niet mogelijk).

DNSSEC	Domain Name System (DNS) is het registratiesysteem van namen en bijbehorende internetnummers en andere domeinnaaminformatie. Het is vergelijkbaar met een telefoonboek. Dit systeem kan worden bevraagd om namen naar nummers te vertalen en omgekeerd. Er is getest of de domeinnaam ondertekend is met DNSSEC, zodat de integriteit van de DNS-informatie is beschermd. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
TLS	Als een bezoeker een onbeveiligde HTTP-verbinding heeft met een website, dan kan een kwaadwillende eenvoudig gegevens onderweg afluisteren of aanpassen, of zelfs het contact volledig overnemen. Getest wordt of TLS is toegevoegd aan HTTP om de verbinding te beveiligen. Op Internet.nl heet deze subtest 'HTTPS available'. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
TLS cf. NCSC	We maken een onderscheid tussen 'TLS' en 'TLS conform NCSC'. In het eerste geval wordt gebruik gemaakt van TLS en in het tweede geval is TLS bovendien zodanig geconfigureerd dat deze voldoet aan de aanbevelingen van het Nationaal Cyber Security Center (NCSC)[9]. Zodat de vertrouwelijkheid, de authenticiteit en integriteit van een bezoek aan een website is gegarandeerd. De streefbeeldafspraak was om hier voor 2019 aan te voldoen.
HTTPS	Er wordt getest of een webserver bezoekers automatisch doorverwijst van HTTP naar HTTPS op dezelfde domeinnaam óf dat deze ondersteuning biedt voor alleen HTTPS en niet voor HTTP. Op Internet.nl heet deze subtest 'HTTPS Redirect'. De streefbeeldafspraak was om hier voor 2019 aan te voldoen.
HSTS	HSTS zorgt ervoor dat een browser eist dat een website altijd HTTPS blijft gebruiken na het eerste contact over

[9] Zie https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html. Een wijziging ten opzichte van de vorige meting is dat in de huidige meting ook de vertrouwensketen van het certificaat wordt meegenomen in de test voor TLS conform NCSC.

	HTTPS. Dit helpt voorkomen dat een derde -bijvoorbeeld een kwaadaardige WiFi hotspot- een browser kan omleiden naar een valse website. Door HTTPS samen met HSTS te gebruiken wordt het gebruik van beveiligde verbindingen zoveel mogelijk afgedwongen. De streefbeeldafspraak was om hier voor 2019 aan te voldoen.

3.5.2. Mailstandaarden

Wij meten het gebruik van e-mailbeveiligingsstandaarden ook op domeinen waarvan een organisatie geen e-mail verstuurt. Dit is relevant omdat ook die domeinen worden misbruikt (burgers weten vaak niet dat deze domeinen niet door de organisatie worden gebruikt), en juist domeinen waarvandaan niet gemaild wordt, makkelijk kunnen worden geblokkeerd met behulp van SPF en DMARC (met de policies –all en p=reject).

DMARC	Met DMARC kan een e-mailprovider kenbaar maken hoe andere (ontvangende) mailservers om dienen te gaan met de resultaten van de SPF- en/of DKIM-controles van ontvangen e-mails. Dit gebeurt door het publiceren van een DMARC beleid in het DNS-record van een domein. In deze test wordt alleen gekeken of DMARC beschikbaar is, niet of er beleid is ingesteld. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
DMARC Policy	Zolang er geen beleid is ingesteld weet de ontvanger nog niet wat te doen met verdachte e-mail. De configuratie moet op orde zijn. (Opm: Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC) Er wordt gecontroleerd of de syntax van de DMARC-record correct is en of deze een voldoende strikte policy bevat. De streefbeeldafspraak was om hier voor 2020 aan te voldoen
DKIM	Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven. Getest wordt of de domeinnaam DKIM ondersteunt. Voor non-mail domeinen waar dit goed is ingesteld heeft DKIM verder geen toegevoegde waarde. In de meting wordt dit weergegeven middels de score “NVT” (niet van toepassing) voor DKIM. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF	SPF heeft als doel spam te verminderen. SPF controleert of een verzendende mailserver die e-mail namens een domein wil versturen, ook daadwerkelijk gerechtigd is om

	dit te mogen doen. Getest wordt of de domeinnaam een SPF-record heeft. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF Policy	Aanvullend op bovenstaande test wordt gecontroleerd of de syntax van de SPF-record geldig is en of deze een voldoende strikte policy bevat om misbruik van het domein door phishers en spammers tegen te gaan. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
STARTTLS	STARTTLS in combinatie met DANE gaan het afluisteren of manipuleren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers op basis van certificaten met TLS te beveiligen. Er wordt getest of de ontvangende mailservers (MX) ondersteuning bieden voor STARTTLS. De streefbeeldafspraak is om hier voor 2020 aan te voldoen. Als er geen mailservers aanwezig is voor het domein dan wordt dit weergeven met NVT. Dit geldt ook voor STARTTLS CF. NCSC, DANE en DNSSEC MX.
STARTTLS CF. NCSC[10]	Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies van het TLS en verschillende versleutelingsstandaarden (ciphers). Aangezien niet alle versies en combinaties als voldoende veilig worden beschouwd, is het belangrijk om hierin de juiste keuze te maken en ook regelmatig te controleren of de gebruikte instellingen nog veilig zijn. Getest wordt of STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
DANE	DANE, dat voortbouwt op DNSSEC, zorgt er in combinatie met STARTTLS voor dat een verzendende e-mailserver de authenticiteit van een ontvangende e-mailserver kan controleren en het kan het gebruik van TLS bovendien afdwingen. Getest wordt of de nameservers van de mailservers één of meer TLSA-records voor DANE bevatten. De streefbeeldafspraak was om hier voor 2020 aan te voldoen
DNSSEC MX	DNSSEC is een randvoorwaarde voor het instellen van DANE. Daarom wordt getest of de domeinnamen van de mailservers (MX) ondertekend zijn met DNSSEC. Dit in het kader van de streefbeeldafspraak om voor 2020 STARTTLS en DANE te ondersteunen.

[10] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

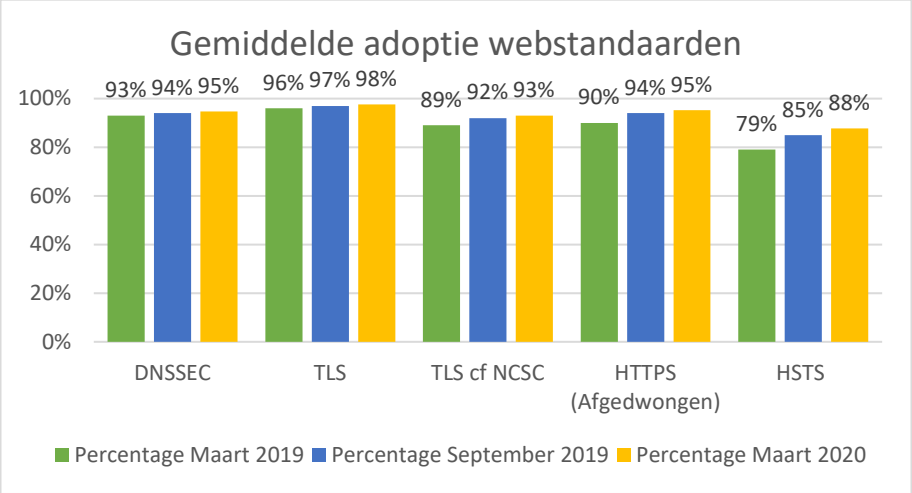
4. Resultaten meting maart 2020

Op 3 maart 2020 heeft het Bureau Forum Standaardisatie de meting uitgevoerd. De resultaten zijn voorgelegd aan een aantal koepelorganisaties en stakeholders en geactualiseerd indien nodig. Naast de resultaten per standaard en per “overheidslaag” zoals bij voorgaande metingen, bevat deze meting tevens het perspectief van de verschillende streefbeelden. Dit laat duidelijk zien hoe het met de adoptie van de standaarden per streefbeeld is gesteld.

4.1. Per standaard

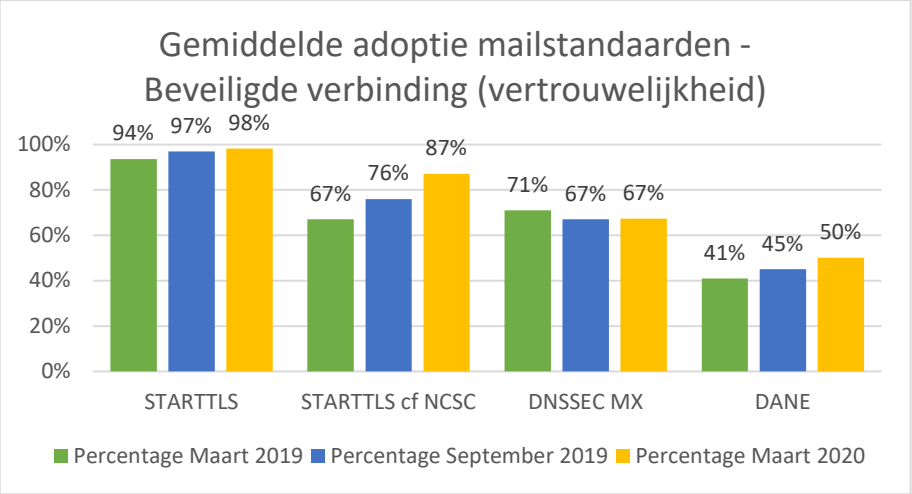
De onderstaande grafiek toont de adoptiestatus van de individuele standaarden voor zowel de webstandaarden als de mailstandaarden. Daar waar mogelijk is er een vergelijking gemaakt met de voorgaande metingen.

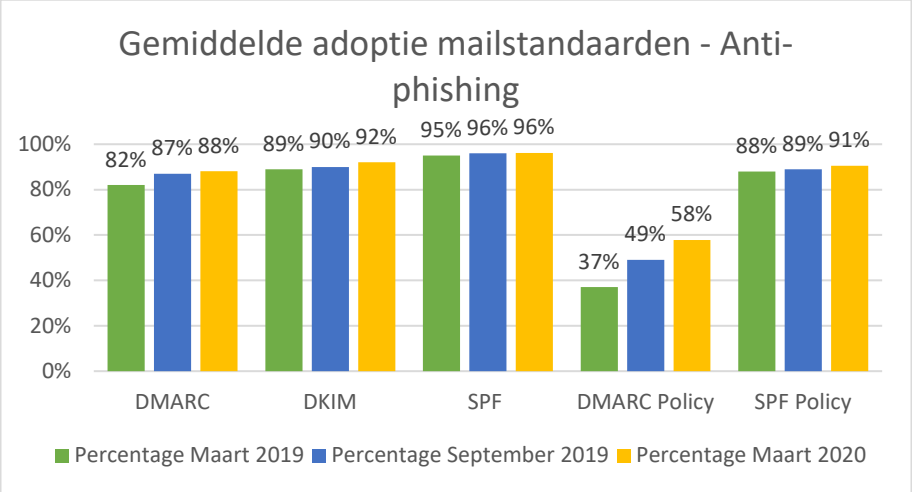
De gemiddelde adoptie van de webstandaarden is hoog. Het gemiddelde van alle webstandaarden samen is inmiddels 94% De toepassing van HSTS trekt dit gemiddelde omlaag met 88%, evenals de toepassing van TLS conform de NCSC TLS-richtlijnen met 93%. Positief is dat we deze meting weer een hogere groei in toepassing van webstandaarden zien ten opzichte van het voorgaande halfjaar. Om de adoptie van deze standaarden verder te stimuleren is een ‘één op één’ benadering nodig om dichter bij de 100% te komen.



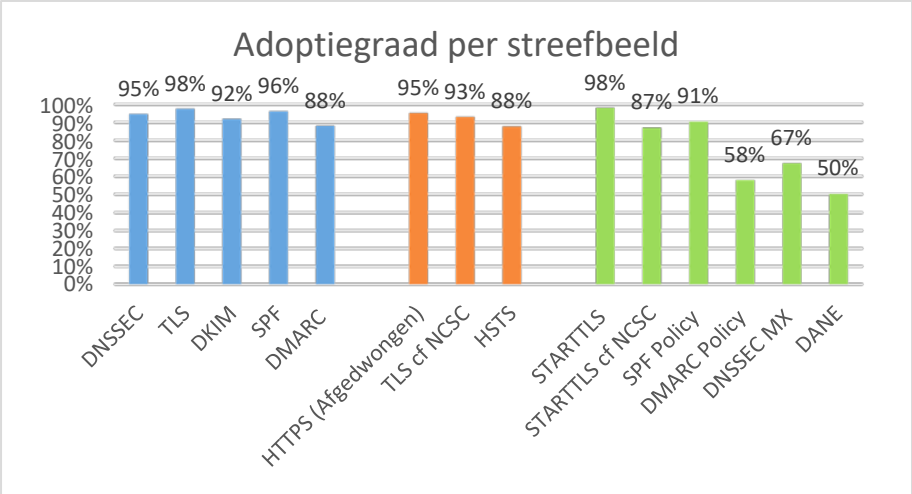
De gemiddelde adoptie van de mailstandaarden (visualisatie op de volgende pagina) ligt met 81% lager dan de webstandaarden. Dit is enerzijds te verklaren door de grotere hoeveelheid standaarden waaraan voldaan moet worden en anderzijds geldt voor een deel van de standaarden pas sinds begin 2018 een streefbeeldafspraak die liep tot eind 2019. Het groeitempo is met 4% licht gestegen ten opzichte van het vorige half jaar toen het groeitempo 3% was.

Met name het achterblijven van DMARC policy en DANE is zorgwekkend, omdat dit overheidsmail die niet voldoet onnodig kwetsbaar maakt voor spoofing en afluisteren.


Gemiddelde adoptie mailstandaarden - Beveiligde verbinding (vertrouwelijkheid)
100%
80%
60%
40%
20%
0%
94%
97%
98%
67%
76%
87%
71%
67%
67%
41%
45%
50%
STARTTLS
STARTTLS cf NCSC
DNSSEC MX
DANE
Percentage Maart 2019
Percentage September 2019
Percentage Maart 2020


Gemiddelde adoptie mailstandaarden - Anti-phishing
100%
80%
60%
40%
20%
0%
82%
87%
88%
89%
90%
92%
95%
96%
96%
37%
49%
58%
88%
89%
91%
DMARC
DKIM
SPF
DMARC Policy
SPF Policy
Percentage Maart 2019
Percentage September 2019
Percentage Maart 2020

4.2. Per streefbeeldafspraak



Bovenstaande grafiek verdeelt de standaarden over de drie streefbeeldafspraken van het OBDO. De eerste set standaarden (blauw) uit het streefbeeld dat eind 2017 afliep worden gemiddeld het meest toegepast (94%), maar ook begin 2020 is voor deze standaarden de gewenste 100% adoptie nog niet gehaald. Bovendien is de groei vrijwel gestagneerd.

De deadline voor tweede streefbeeldafspraak (oranje) was eind 2018. Ook voor deze standaarden geldt dat de gemiddelde adoptie hoog is (91%), maar de 100% nog niet is behaald. Ook hier is opvallend dat de groei vrijwel stagneert.

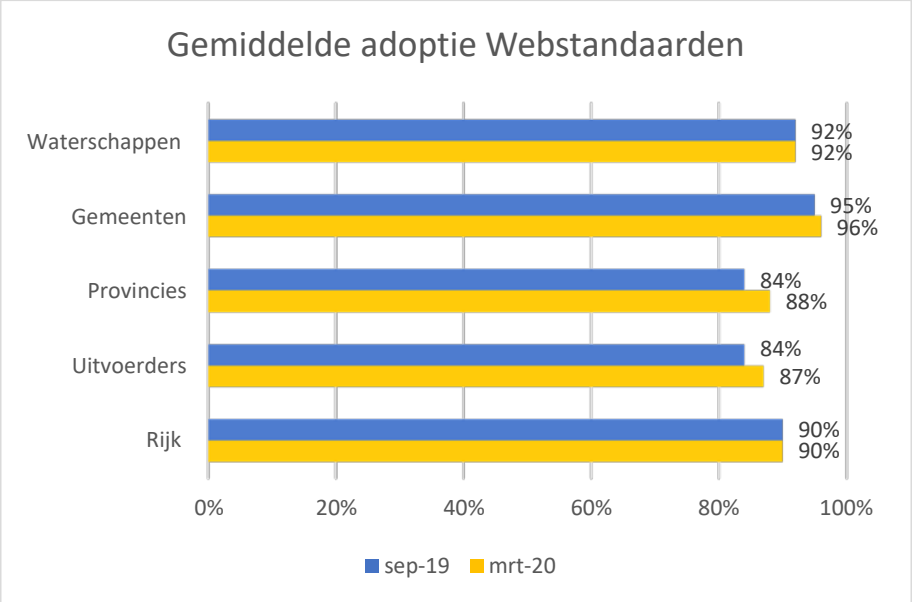
Voor deze laatste standaarden (HTTPS, 'TLS conform NSCS' en HSTS) is er het voornemen een Algemene Maatregel van Bestuur (AMvB) op te stellen[11]. Deze AMvB is naar verwachting in de tweede helft van 2020 van kracht en dwingt partijen die ondanks de streefbeeldafspraken de standaarden nog steeds niet toepassen, dat alsnog te doen.

De gemiddelde adoptie van de standaarden uit de derde streefbeeldafspraak (groen) is het laagst. Deze streefbeeldafspraak liep tot eind 2019. Voor dit streefbeeld is afgelopen halfjaar progressie (gemiddeld 4%-punt) geboekt, maar de doelstelling van de streefbeeldafspraak is overduidelijk niet behaald (75%). Daardoor is een aanzienlijk deel van de overheden kwetsbaar voor spoofing en afluisteren van mailverkeer.

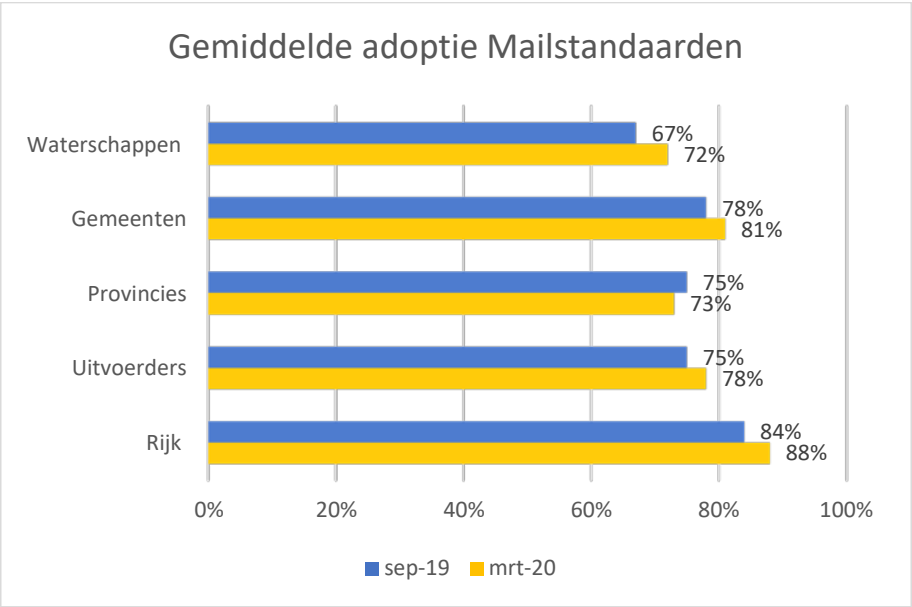
4.3. Per overheidslaag

Een uitsplitsing van de resultaten van de webstandaarden naar overheidslaag (zie volgende pagina) laat zien dat de adoptiegraad bij waterschappen en het Rijk is gestagneerd. De gemeenten zijn koploper met 96%, een lichte groei van 1% ten opzichte van een half jaar daarvoor. De provincies en uitvoerders hebben als achterlopers afgelopen halfjaar de grootste groei doorgemaakt met respectievelijk 4% en 3%.

[11] Op basis van artikel 2 van het wetsvoorstel Wet digitale overheid.



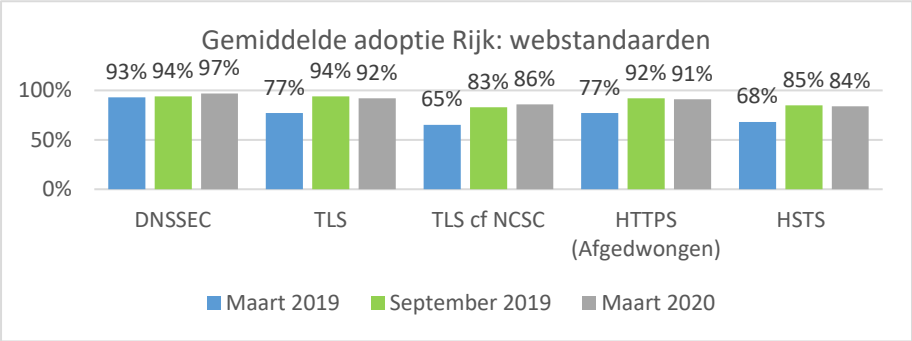
Het beeld is anders bij de mailstandaarden. Hier blijven de waterschappen gemiddeld iets achter op de andere overheidslagen. Het Rijk heeft bij de mailstandaarden gemiddeld de hoogste adoptiegraad. Verderop in de rapportage wordt per overheidslaag toegelicht welke standaarden gemiddeld veel worden toegepast en welke minder.



4.3.1. Het Rijk

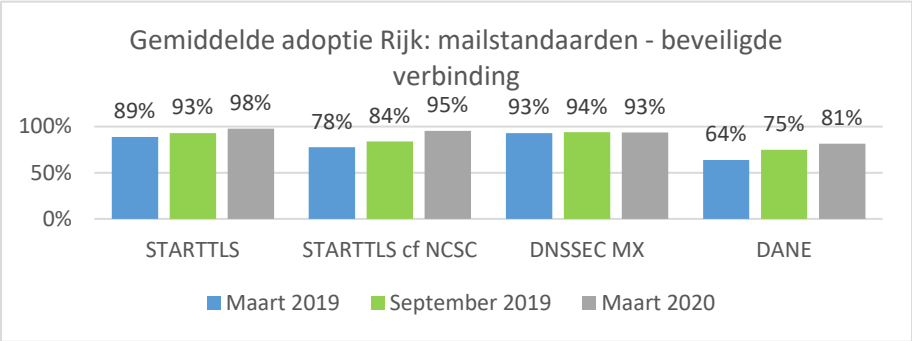
Na een flinke inhaalslag gemaakt met betrekking tot de standaarden voor het versleutelen van webverkeer (HTTPS en HSTS) in de vorige meting, zien we nu bij TLS, het afdwingen van HTTPS en HSTS een lichte terugval.

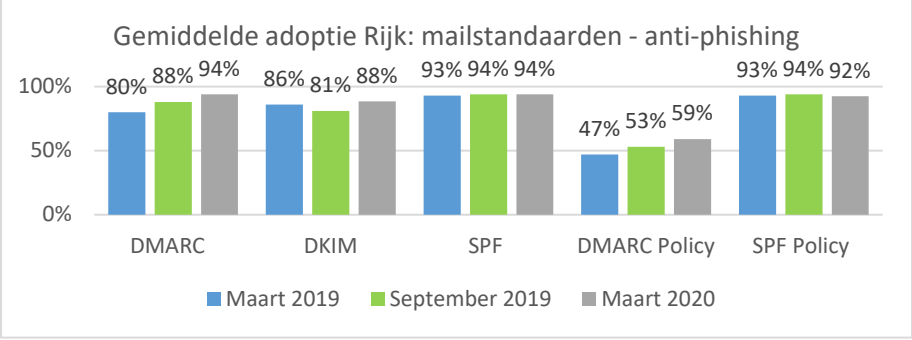
Er valt nog winst te behalen bij het veilig configureren van TLS en het toepassen van HSTS.



Het Rijk scoort goed als het gaat om de mailstandaarden. Met name DMARC en DANE scoren hier hoog t.o.v. de andere overheidslagen. Dit komt waarschijnlijk doordat het beheer van de mailservers bij een relatief klein aantal partijen belegd is. Een aanpassing bij die partijen heeft daarom grote impact op de score van het Rijk.

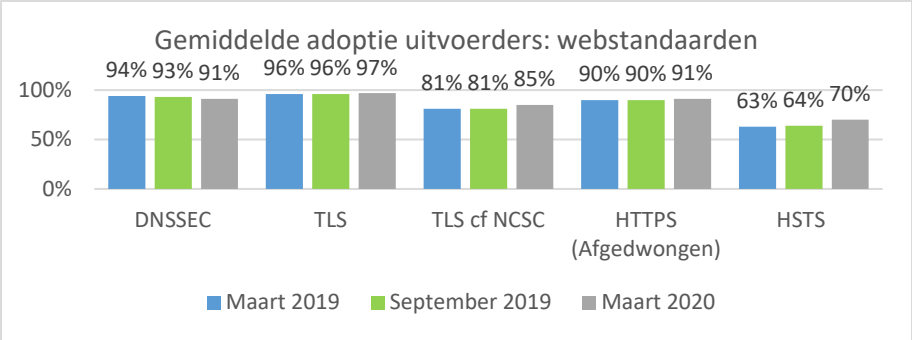
STARTTLS conform de TLS-richtlijnen van het NCSC en DMARC laten significante voortuitgang zien. Daarnaast toont DKIM een sprong voorwaarts na een achteruitgang in de vorige meting. Er valt nog winst te behalen bij het strikt configureren van de DMARC policy en het toepassen van DANE.



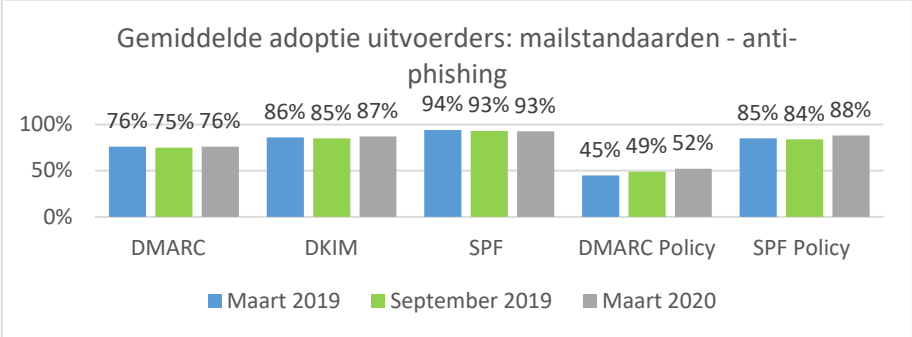


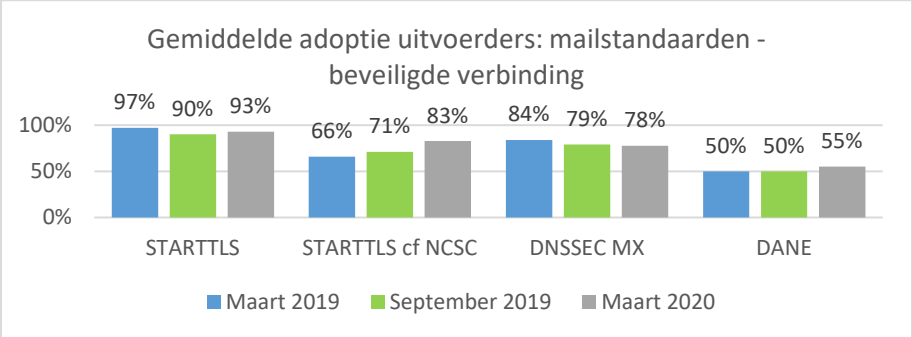
4.3.2. Uitvoering

De uitvoerders vormen een middenmoter. Bij de webstandaarden zien we een dalende trend ontstaan bij het toepassen van DNSSEC. Hoewel we groei zien valt er nog winst te behalen bij het veilig configureren van TLS en het toepassen van HSTS.



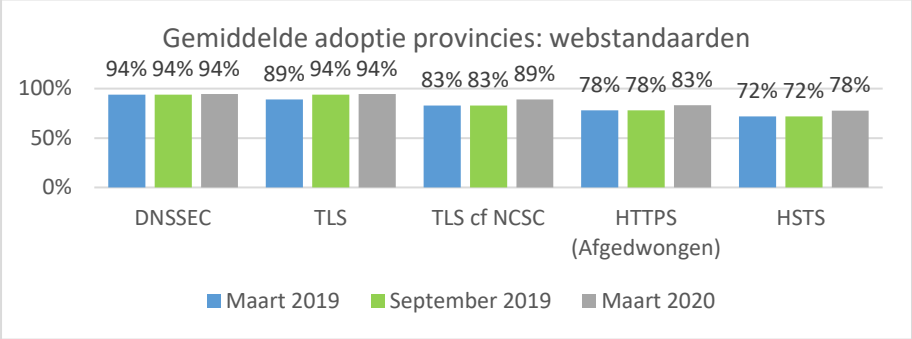
Naast significante groei in de adoptiegraad van het toepassen van STARTTLS conform de TLS-richtlijnen van het NCSC en de toepassing van DANE, zien we veelal stagnatie in het toepassen van de mailstandaarden en in een enkel geval een lichte achteruitgang (DNSSEC MX). Er is over de hele linie nog genoeg ruimte voor verbetering.





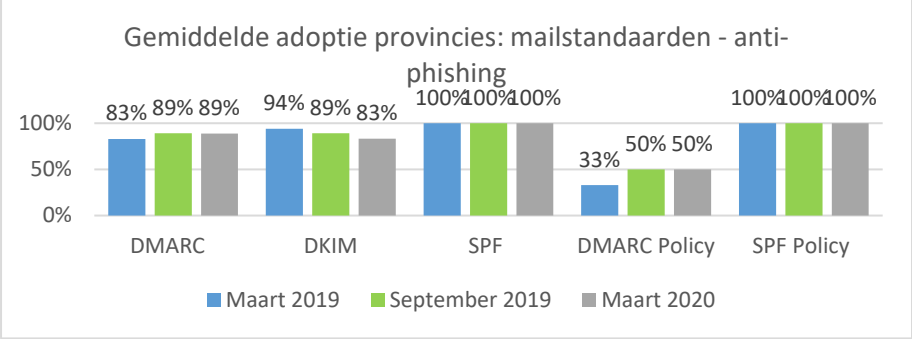
4.3.3. Provincies

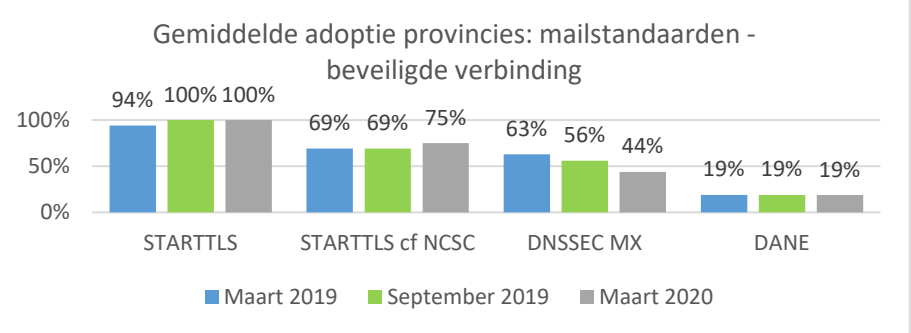
De provincies laten ten aanzien van de webstandaarden gemiddeld groei zien na stagnatie in de vorige meting. De adoptiegraden van DNSSEC en TLS zijn gelijk gebleven met 94%. Er valt nog winst te behalen bij het veilig configureren van TLS, het afdwingen van HTTPS, en het toepassen van HSTS.



Ten aanzien van e-mail zien we helaas voornamelijk stagnatie en daling in de toepassing van de standaarden. Enkel de toepassing van STARTTLS conform de TLS-richtlijnen van het NCSC is gestegen. Het gebruik van DKIM en DNSSEC zijn wederom gedaald en tonen een negatieve trend. Positief is dat alle provincies gebruik maken van SPF en bovendien de juiste policy toepassen, daarnaast passen zij ook allen STARTTLS toe, hoewel niet altijd voldoende veilig geconfigureerd.

De neerwaartse trend van DNSSEC op de mailservers (MX) is doorgezet omdat opnieuw twee maildomeinen overgestapt zijn op clouddienst Microsoft Office 365 Exchange. Dit product biedt vooralsnog geen ondersteuning voor DNSSEC, en daarmee ook geen ondersteuning voor DANE. Dit is een duidelijk zorgpunt voor de provincies, omdat zij hierdoor niet aan de overheidsbrede afspraken omtrent het gebruik van DANE kunnen voldoen.

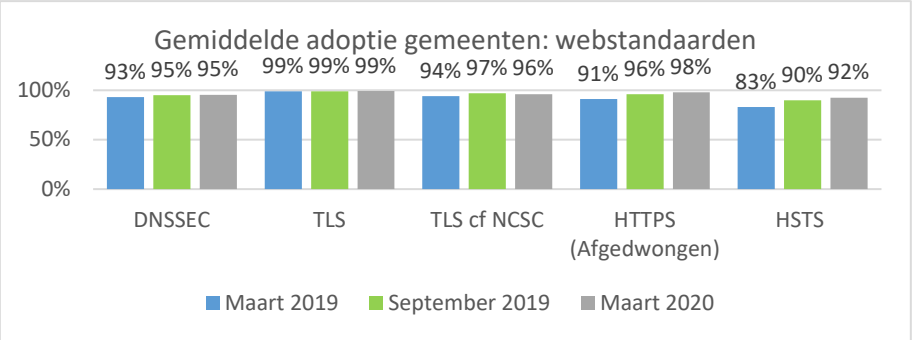




4.3.4. Gemeenten

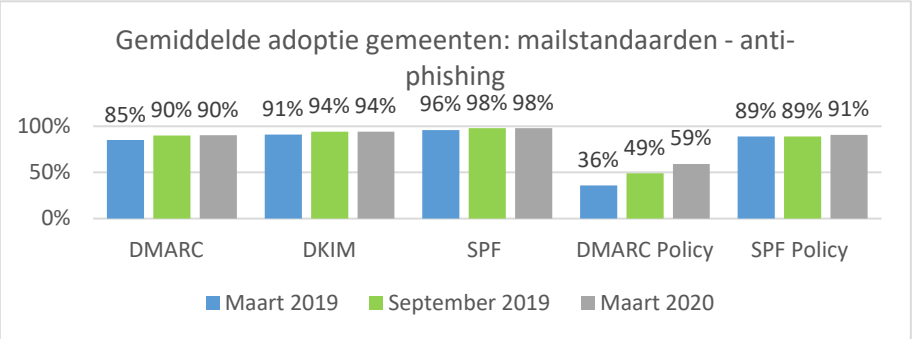
De gemeenten scoren het beste op het gebruik van de webstandaarden. Positief is dat we ondanks de al hoge statistieken uit de vorige meting er wederom een zichtbare groei is. Met name het afdwingen van de HTTPS verbinding met onder meer HSTS wordt beter toegepast.

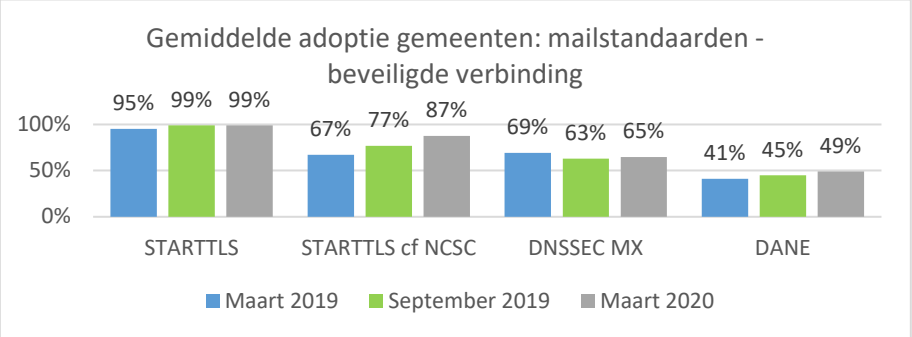
Het feit dat de gemeenten met afstand de meeste domeinen bezitten in onze test (365 van de 548) maakt de hoge scores nog indrukwekkender.



Ten aanzien van de mailstandaarden zien we over het algemeen ook groei. Het strikt afstellen van de DMARC policy is gegroeid, hoewel er voldoende ruimte is voor meer groei.

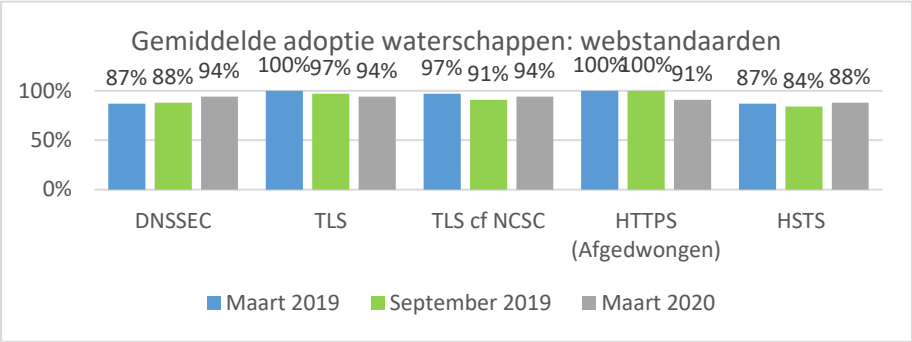
STARTTLS word steeds vaker volgens de TLS-richtlijnen van het NCSC geconfigureerd; we zien in de toepassing van STARTTLS conform NCSC een groei van 10%. Wel is er nog voldoende ruimte voor groei in de toepassing van DANE, waarmee de beveiligde verbinding kan worden afgedwongen en zogenaamde 'downgrade attacks' kunnen worden voorkomen.



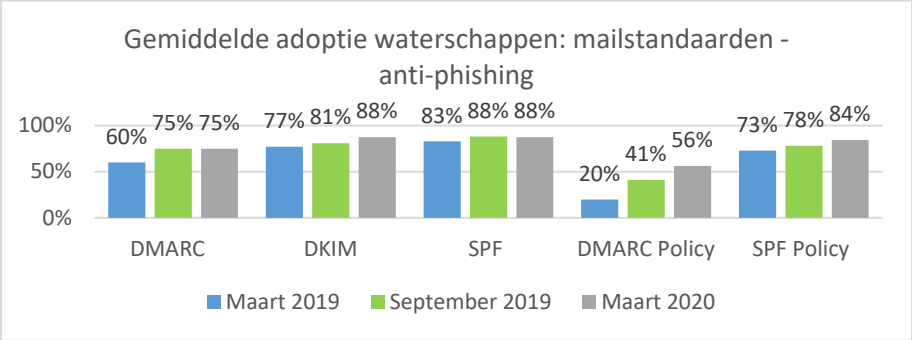


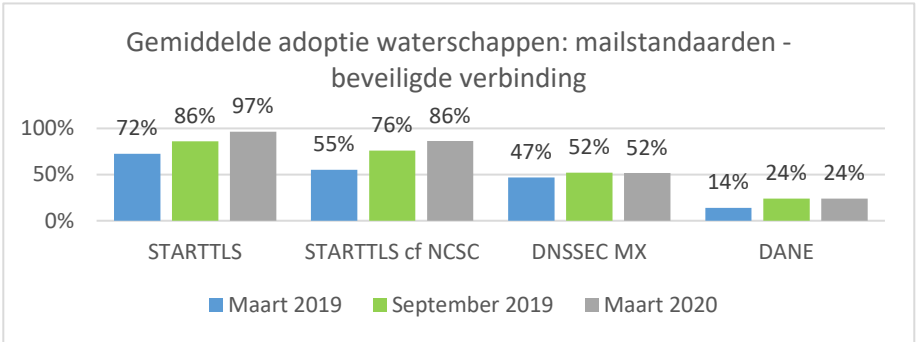
4.3.5. Waterschappen

De waterschappen scoren al enkele metingen achter elkaar relatief hoog op het toepassen van webstandaarden. Ook dit keer scoren zij in verhouding nog redelijk hoog. Helaas zien we bij TLS en het afdwingen van HTTPS een achteruitgang, wat een zorgpunt is voor de waterschappen. De achteruitgang lijkt procentueel fors, maar valt mee in de wetenschap dat het gaat om 32 domeinen, waar 1 domein al voor meer dan 3% meetelt.



Ten aanzien van de mailstandaarden hebben de waterschappen een gemiddelde groei van 5% doorgemaakt, de grootste groei in verhouding met andere overheidslagen. Toch blijven de waterschappen met een gemiddelde adoptie van 72% achter lopen op de andere overheidslagen. Met name het toepassen van DMARC met de juiste strikte policy en DANE blijft achter.





Bijlage: Individuele resultaten per domeinnaam

Op de volgende pagina's staan de onderliggende individuele testresultaten van de Meting Informatieveiligheidstandaarden van maart 2020. De resultaten zijn ter afstemming naar de koepelorganisaties van de verschillende overheidslagen verzonden. Hierop zijn 23 reacties binnengekomen die in enkele gevallen hebben geleid tot verbetering. Eventuele onvolkomenheden of testfouten kunnen worden doorgegeven via **info@forumstandaardisatie.nl** en kunnen, indien tijdig ontvangen, voor online publicatie van het digitaal magazine nog worden aangepast.

Toelichting resultaten:
WAAR = de betreffende standaard is geïmplementeerd op het geteste domein.
ONWAAR = de betreffende standaard is niet (correct) geïmplementeerd op het geteste domein.
NVT = geen mailserver geconfigureerd waardoor bepaalde standaarden niet van toepassing zijn.
NIETTESTBAAR = wel mailserver geconfigureerd, maar door de specifieke configuratie van de mailserver was de betreffende standaard tijdens de meting niet testbaar.

Resultaten beveiligingsstandaarden voor web

Resultaten web Rijk

Domein	DNSSEC	TLS available	TLS NCSC web	HTTPS enforced	HSTS
crl.pkioverheid.nl	1	1	1	1	1
machtigen.digid.nl	1	1	1	1	1
mijn.digid.nl	1	1	1	1	1
mijn.overheid.nl	1	1	1	1	1
portaal.digikoppeling.nl	1	0	0	0	0
portaal.digimelding.nl	1	1	1	1	1
www.berichtenbox.antwoordvoorbedrijven.nl	1	1	0	1	1
www.consuwijzer.nl	1	1	1	1	1
www.crisis.nl	0	1	1	1	1
www.daarkunjemeethuiskomen.nl	1	1	1	1	1
www.defensie.nl	1	1	1	1	1
www.dictu.nl	1	1	1	1	1
www.digid.nl	1	1	1	1	1
www.digitaleoverheid.nl	1	1	1	1	1
www.digitoegankelijk.nl	1	1	1	1	1
www.dji.nl	1	1	1	1	1
www.dsta.nl	1	1	1	1	1
www.eherkenning.nl	1	1	1	1	1
www.energielabelvoorwoningen.nl	1	1	1	1	1
www.fmhaaglanden.nl	1	1	1	1	1
www.forensischinstituut.nl	1	1	1	1	1
www.forumstandaardisatie.nl	1	1	1	1	1
www.government.nl	1	1	1	1	1
www.helpdesk-efactureren.nl	1	1	1	1	1
www.ictu.nl	1	1	1	1	1
www.idensys.nl	1	1	1	1	1
www.internetconsultatie.nl	1	1	0	1	0

www.koninklijkhuis.nl	1	1	1	1	1
www.logius.nl	1	1	1	1	1
www.mijnoverheidvoorondernemers.nl	1	0	0	0	0
www.minaz.nl	1	1	1	1	1
www.minbuza.nl	1	1	1	1	1
www.minbzk.nl	1	1	1	1	1
www.mindef.nl					
www.minez.nl	1	1	1	1	1
www.minfin.nl	1	1	1	1	1
www.minienm.nl	1	1	1	1	1
www.minjus.nl	1	0	0	0	0
www.minlnv.nl	1	1	1	1	1
www.minocw.nl	1	1	1	1	1
www.minszw.nl	1	1	1	1	1
www.minvenj.nl	1	0	0	0	0
www.minvws.nl	1	1	1	1	1
www.ncsc.nl	1	1	1	1	1
www.nctv.nl	1	1	1	1	1
www.nederlandwereldwijd.nl	1	1	1	1	1
www.nfi.nl	1	1	1	0	1
www.noraonline.nl	1	1	1	1	0
www.officielebekendmakingen.nl	1	1	0	1	1
www.ondernemersplein.nl	1	1	1	1	1
www.overheid.nl	1	1	1	1	1
www.p-direkt.nl	1	1	1	1	1
www.rechtspraak.nl	1	1	1	1	1
www.rijkshuisstijl.nl	1	1	1	1	1
www.rijksoverheid.nl	1	1	1	1	1
www.rijksvastgoedbedrijf.nl	1	1	1	1	1
www.rvig.nl	1	1	1	1	1
www.rvo.nl	1	1	1	1	1
www.sbr-nl.nl	1	1	1	1	1
www.ssc-ict.nl	1	1	1	1	1
www.stelselcatalogus.nl	1	0	0	0	0
www.tenderned.nl	1	1	0	1	0
www.ubrijk.nl	1	1	1	1	1
www.werkenbijdefensie.nl	1	1	1	1	0
www.werkenvoornederland.nl	0	1	1	1	0

Resultaten web uitvoerders

Domein	DNSSEC	TLS available	TLS NCSC web	HTTPS enforced	HSTS
mijn.belastingdienst.nl	1	1	1	1	0
mijn.toeslagen.nl	1	1	1	0	1
www.acm.nl	1	1	1	1	1
www.acvz.org	0	1	1	0	0
www.agentschaptelecom.nl	1	1	1	1	1
www.amberalert.nl	0	1	1	1	0
www.autoriteitpersoonsgegevens.nl	1	1	1	1	1
www.belastingdienst.nl	1	1	1	1	1
www.bkwi.nl	1	1	1	1	1
www.bureauft.nl	1	1	1	1	1
www.burgernet.nl	1	1	0	1	1
www.c2000.nl	1	1	1	1	1
www.cbg-meb.nl	1	1	1	1	1
www.cbr.nl	1	1	0	1	1
www.cbs.nl	1	1	1	1	1
www.cibg.nl	1	1	1	1	1
www.ciz.nl	1	1	1	1	1
www.cjib.nl	1	1	1	1	1
www.ctgb.nl	1	1	1	1	1
www.cultureelerfgoed.nl	1	1	1	1	1
www.cvdm.nl	1	1	1	1	0
www.doc-direkt.nl	1	1	1	1	1
www.duo.nl	1	1	1	1	1
www.dus-i.nl	1	1	1	1	1
www.emissieautoriteit.nl	1	1	1	1	1
www.fiu-nederland.nl	1	1	0	1	1
www.halt.nl	0	1	0	1	0
www.hetcak.nl	1	1	1	1	1
www.huisvoorklokkenluiders.nl	1	1	1	1	1
www.huurcommissie.nl	1	1	1	1	1
www.ilent.nl	1	1	1	1	1
www.inburgeren.nl	1	1	1	1	1
www.ind.nl	1	1	1	1	0
www.inspectie-jenv.nl	1	1	1	1	1
www.justid.nl	1	1	1	1	1
www.justis.nl	1	1	1	1	1
www.kadaster.nl	1	1	1	1	0
www.kansspelautoriteit.nl	0	1	0	1	0
www.kleinlef.nl	1	1	0	0	0
www.knmi.nl	1	1	1	1	0
www.kvk.nl	1	1	1	1	1

www.manifestgroep.nl	1	0	0	0	0
www.mensenrechten.nl	1	1	0	1	0
www.mijnsvb.nl	1	0	0	0	0
www.nationaalarchief.nl	1	1	1	1	0
www.niwo.nl	1	1	0	1	0
www.nrgd.nl	1	1	1	1	1
www.nuffic.nl	1	1	1	1	0
www.nvao.net	0	1	1	1	0
www.nvwa.nl	1	1	1	1	1
www.om.nl	1	1	1	1	1
www.onderzoeksraad.nl	1	1	1	1	1
www.politie.nl	1	1	1	1	1
www.rdw.nl	1	1	1	1	1
www.rijkswaterstaat.nl	1	1	1	1	1
www.rivm.nl	1	1	1	1	1
www.rsj.nl	1	1	1	1	1
www.rws.nl	1	1	1	0	1
www.schadefonds.nl	1	1	1	1	1
www.stab.nl	0	1	1	1	0
www.svb.nl	1	1	1	1	1
www.uitvoeringvanbeleidszw.nl	1	1	1	1	1
www.uwv.nl	1	1	1	1	1
www.vananaarbeter.nl	1	1	1	1	0
www.werk.nl	1	1	1	1	0
www.zinl.nl					
www.zorginstituutnederland.nl	1	1	1	1	1

Resultaten web provincies

Domein	DNSSEC	TLS available	TLS NCSC web	HTTPS enforced	HSTS
www.bij12.nl	1	1	1	1	0
www.brabant.nl	1	1	1	1	1
www.drenthe.nl	1	1	1	1	1
www.flevoland.nl	1	1	0	1	0
www.fryslan.frl	1	1	1	1	1
www.fryslan.nl	1	0	0	0	0
www.gelderland.nl	1	1	1	1	1
www.ipo.nl	0	1	1	1	0
www.limburg.nl	1	1	1	1	1
www.noord-holland.nl	1	1	1	1	1
www.overijssel.nl	1	1	1	0	1
www.provincie.drenthe.nl	1	1	1	1	1
www.provinciegroningen.nl	1	1	1	1	1
www.provincie-utrecht.nl	1	1	1	1	1
www.prvlimburg.nl	1	1	1	0	1
www.pzh.nl	1	1	1	1	1
www.zeeland.nl	1	1	1	1	1
www.zuid-holland.nl	1	1	1	1	1

Resultaten web waterschappen

Domein	DNSSEC	TLS available	TLS NCSC web	HTTPS enforced	HSTS
www.aaenmaas.nl	1	1	1	1	1
www.agv.nl	0	1	1	1	1
www.brabantsedelta.nl	1	1	1	1	1
www.derbg.nl	1	1	1	1	1
www.dommel.nl	1	1	1	1	1
www.hdsr.nl	1	1	1	1	1
www.hetwaterschapshuis.nl	1	1	1	1	1
www.hhdelfland.nl	1	1	1	1	1
www.hhnk.nl	1	1	1	1	1
www.hhsk.nl	1	0	0	0	0
www.hunzeenaas.nl	1	1	1	1	1
www.ihw.nl	1	1	1	1	1
www.informatiehuiswater.nl	1	1	1	1	1
www.noorderzijlvest.nl	1	1	1	1	1
www.rijnland.net	1	1	1	1	1
www.scheldestromen.nl	1	1	1	1	1
www.schielandendekrimpenerwaard.nl	1	0	0	0	0
www.stowa.nl	1	1	1	1	0
www.uvw.nl	1	1	1	1	1
www.vallei-veluwe.nl	1	1	1	1	1
www.vechtstromen.nl	1	1	1	1	1
www.waternet.nl	0	1	1	1	1
www.waterschaplimburg.nl	1	1	1	1	1
www.waterschappen.nl	1	1	1	1	1
www.waterschaprivierenland.nl	1	1	1	1	1
www.wbl.nl	1	1	1	0	0
www.wdodelta.nl	1	1	1	1	1
www.wetterskipfryslan.nl	1	1	1	1	1
www.wrij.nl	1	1	1	1	1
www.wshd.nl	1	1	1	1	1
www.wsrl.nl	1	1	1	1	1
www.zuiderzeeland.nl	1	1	1	1	1

Resultaten web gemeenten

Domein	DNSSEC	TLS available	TLS NCSC web	HTTPS enforced	HSTS
gemeente.groningen.nl	0	1	1	1	1
gemeente.leiden.nl	1	1	1	1	1
www.aaenhunze.nl	1	1	1	1	1
www.aalsmeer.nl	1	1	1	1	1
www.aalten.nl	1	1	1	1	1
www.achtkarspelen.nl	1	1	1	1	1
www.alblasserdam.nl	1	1	1	1	1
www.albrandswaard.nl	1	1	1	1	1
www.alkmaar.nl	1	1	1	1	1
www.almelo.nl	1	1	1	1	1
www.almere.nl	1	1	1	1	0
www.alphenaandenrijn.nl	1	1	1	1	1
www.alphen-chaam.nl	1	1	1	1	1
www.ameland.nl	1	1	1	1	1
www.amersfoort.nl	0	1	1	1	1
www.amstelveen.nl	1	1	1	1	1
www.amsterdam.nl	1	1	1	1	1
www.apeldoorn.nl	1	1	1	1	1
www.appingedam.nl	1	1	1	1	1
www.arnhem.nl	1	1	1	1	1
www.assen.nl	0	1	1	1	0
www.asten.nl	1	1	1	1	1
www.baarle-nassau.nl	1	1	1	1	1
www.baarn.nl	1	1	1	1	1
www.barendrecht.nl	1	1	1	1	1
www.barneveld.nl	1	1	1	1	1
www.beekdaelen.nl	1	1	1	1	1
www.beemster.net	1	1	1	1	0
www.beesel.nl	1	1	1	1	1
www.bergeijk.nl	1	1	1	1	1
www.bergen.nl	1	1	1	1	1
www.bergendal.nl	1	1	1	1	1
www.bergen-nh.nl	1	1	1	1	1
www.bergenopzoom.nl	1	1	0	0	0
www.bernheze.org	1	1	1	1	1
www.beuningen.nl	1	1	0	1	1
www.beverwijk.nl	1	1	1	1	1
www.bladel.nl	1	1	1	1	1
www.blaricum.nl	1	1	1	1	1
www.bloemendaal.nl	1	1	1	1	1
www.bodegraven-reeuwijk.nl	1	1	0	0	1

www.boekel.nl	1	1	1	1	1
www.borger-odoorn.nl	1	1	1	1	1
www.borne.nl	0	1	1	1	0
www.borsele.nl	1	1	1	1	1
www.boxmeer.nl	1	1	1	1	1
www.boxtel.nl	1	1	1	1	1
www.breda.nl	1	1	1	1	1
www.brielle.nl	1	1	1	1	1
www.bronckhorst.nl	1	1	1	1	1
www.brummen.nl	1	1	1	1	1
www.brunssum.nl	1	1	1	1	1
www.bunnik.nl	1	1	1	1	1
www.bunschoten.nl	1	1	1	1	1
www.buren.nl	1	1	1	1	1
www.capelleaandenijssel.nl	1	1	1	1	1
www.castricum.nl	1	1	1	1	1
www.coevorden.nl	1	1	1	1	1
www.cranendonck.nl	1	1	1	1	1
www.cuijk.nl	1	1	1	1	1
www.culemborg.nl	1	1	1	1	1
www.dalfsen.nl	1	1	1	1	1
www.dantumadiel.frl	1	1	1	1	1
www.debilt.nl	1	1	1	1	1
www.defryskemarren.nl	1	1	1	1	1
www.delft.nl	1	1	1	1	1
www.delfzijl.nl	1	1	1	1	1
www.denhaag.nl	1	1	1	1	1
www.denhelder.nl	1	1	1	1	1
www.derondevenen.nl	1	1	1	1	1
www.deurne.nl	1	1	1	1	1
www.deventer.nl	1	1	1	1	1
www.dewolden.nl	1	1	1	1	1
www.diemen.nl	1	1	1	1	1
www.dinkelland.nl	1	1	1	1	1
www.doesburg.nl	1	1	1	1	1
www.doetinchem.nl	1	1	1	1	1
www.dongen.nl	1	1	1	1	1
www.dordrecht.nl	1	1	1	1	0
www.drechterland.nl	1	1	1	1	1
www.drimmelen.nl	1	1	1	1	1
www.dronten.nl	1	1	1	1	1
www.druten.nl	1	1	1	1	1
www.duiven.nl	1	1	1	1	1
www.echt-susteren.nl	1	1	1	1	1

www.edam-volendam.nl	1	1	1	1	1
www.ede.nl	1	1	1	1	1
www.eemnes.nl	1	1	1	1	1
www.eersel.nl	1	1	1	1	1
www.eijsden-margraten.nl	1	1	1	1	1
www.eindhoven.nl	1	1	1	1	1
www.elburg.nl	1	1	1	0	1
www.emmen.nl	1	1	1	1	1
www.enkhuizen.nl	1	1	1	1	1
www.enschede.nl	0	1	1	1	0
www.epe.nl	1	1	1	1	1
www.ermelo.nl	1	1	1	1	1
www.etten-leur.nl	1	1	1	1	1
www.geertruidenberg.nl	1	1	1	1	1
www.geldrop-mierlo.nl	1	1	1	1	1
www.gemeentealtena.nl	1	1	1	1	1
www.gemeentebeek.nl	1	1	1	1	1
www.gemeenteberkelland.nl	1	1	1	1	1
www.gemeentebest.nl	1	1	1	1	1
www.gemeentehulst.nl	0	1	1	1	0
www.gemeentehw.nl	1	1	1	1	1
www.gemeentelangedijk.nl	1	1	1	1	1
www.gemeentemaasgouw.nl	1	1	1	1	1
www.gemeentemaastricht.nl	1	1	1	1	1
www.gemeente-mill.nl	1	1	1	1	1
www.gemeentenoordenveld.nl	1	1	1	1	1
www.gemeente-oldambt.nl	0	1	1	1	0
www.gemeentesluis.nl	1	1	0	1	1
www.gemeente-steenbergen.nl	1	1	1	1	1
www.gemeentestein.nl	1	1	1	1	1
www.gemeentesudwestfryslan.nl	1	1	1	1	0
www.gemeentewesterveld.nl	1	1	1	1	1
www.gemeentewestland.nl	1	1	1	1	1
www.gemert-bakel.nl	0	1	1	1	1
www.gennep.nl	1	1	1	1	1
www.gilzerijen.nl	1	1	1	1	1
www.goeree-overflakkee.nl	1	1	1	1	1
www.goes.nl	1	1	1	1	1
www.goirle.nl	1	1	1	1	1
www.gooisemeren.nl	1	1	1	1	1
www.gorinchem.nl	1	1	1	1	1
www.gouda.nl	1	1	1	1	1
www.grave.nl	1	1	1	1	1
www.groningen.nl	1	1	1	1	0

www.gulpen-wittem.nl	1	1	1	1	1
www.haaksbergen.nl	1	1	1	1	1
www.haaren.nl	1	1	1	1	1
www.haarlem.nl	1	1	1	1	1
www.haarlemmermeer.nl	1	1	1	1	1
www.haarlemmermeergemeente.nl	1	1	1	1	0
www.halderberge.nl	1	1	1	1	1
www.hardenberg.nl	1	1	1	1	1
www.harderwijk.nl	1	1	1	1	1
www.hardinxveld-giessendam.nl	1	1	1	1	1
www.harlingen.nl	1	1	1	1	1
www.hattem.nl	1	1	1	1	1
www.heemskerk.nl	1	1	1	1	1
www.heemstede.nl	1	1	1	1	1
www.heerde.nl	1	1	1	1	1
www.heerenveen.nl	1	1	1	1	1
www.heerhugowaard.nl	1	1	1	1	1
www.heerlen.nl	1	1	1	1	1
www.heeze-leende.nl	1	1	1	1	1
www.heiloo.nl	1	1	1	1	1
www.hellendoorn.nl	1	1	1	1	1
www.hellevoetsluis.nl	1	1	1	1	1
www.helmond.nl	1	1	1	1	1
www.hengelo.nl	1	1	1	1	1
www.hethogeland.nl	1	1	1	1	1
www.heumen.nl	1	1	1	1	1
www.heusden.nl	1	1	1	1	1
www.heuvelrug.nl	1	1	1	1	1
www.h-i-ambacht.nl	1	1	1	1	1
www.hillegom.nl	1	1	1	1	1
www.hilvarenbeek.nl	1	1	1	1	1
www.hilversum.nl	1	1	1	1	1
www.hofvantwente.nl	1	1	1	1	1
www.hollandskroon.nl	1	1	1	1	1
www.hoogeveen.nl	1	1	1	1	1
www.hoorn.nl	1	1	1	1	1
www.horstaandemaas.nl	1	1	1	1	1
www.houten.nl	1	1	1	1	1
www.huizen.nl	1	1	1	1	1
www.ijsselstein.nl	1	1	1	1	1
www.informatiebeveiligingsdienst.nl	1	1	1	1	1
www.kaagenbraassem.nl	1	1	1	1	1
www.kampen.nl	0	1	1	1	1
www.kapelle.nl	1	1	1	1	1

www.katwijk.nl	1	1	1	1	1
www.kerkrade.nl	1	1	1	1	1
www.koggenland.nl	1	1	1	1	1
www.krimpenaandenijssel.nl	1	1	1	1	1
www.krimpenerwaard.nl	1	1	1	1	1
www.laarbeek.nl	0	1	1	1	1
www.landerd.nl	1	1	1	1	1
www.landgraaf.nl	1	1	1	1	1
www.landsmeer.nl	1	1	1	1	1
www.lansingerland.nl	1	1	1	1	1
www.laren.nl	1	1	1	1	1
www.leeuwarden.nl	1	1	1	1	1
www.leiden.nl	1	1	1	1	1
www.leiderdorp.nl	1	1	1	1	1
www.leidschendam-voorburg.nl	1	1	0	0	1
www.lelystad.nl	1	1	1	1	1
www.leudal.nl	1	1	1	1	1
www.leusden.nl	1	1	1	1	1
www.lingewaard.nl	1	1	1	1	1
www.lisse.nl	1	1	1	1	1
www.lochem.nl	1	1	1	1	1
www.loonopzand.nl	1	0	0	0	0
www.lopik.nl	1	0	0	0	0
www.loppersum.nl	1	1	1	1	1
www.losser.nl	1	1	1	1	1
www.lv.nl	1	1	1	1	1
www.maasdriel.nl	1	1	1	1	1
www.maassluis.nl	1	1	1	1	1
www.maastricht.nl	1	1	1	1	1
www.medemblik.nl	1	1	1	1	1
www.meerssen.nl	1	1	1	1	1
www.meierijstad.nl	1	1	1	1	1
www.meppel.nl	1	1	1	1	1
www.middelburg.nl	1	1	1	1	0
www.middendelfland.nl	1	1	1	1	1
www.middendrenthe.nl	1	1	1	1	1
www.midden-groningen.nl	1	1	1	1	1
www.moerdijk.nl	1	1	1	1	1
www.molenlanden.nl	1	1	1	1	1
www.montferland.info	1	1	1	1	1
www.montfoort.nl	1	1	1	1	1
www.mookenmiddelaar.nl	1	1	1	1	1
www.nederbetuwe.nl	1	1	1	1	1
www.nederweert.nl	1	1	1	1	1

www.nieuwegein.nl	1	1	1	1	1
www.nieuwkoop.nl	1	1	1	1	1
www.nijkerk.eu	1	1	1	1	1
www.nijmegen.nl	1	1	1	1	1
www.nissewaard.nl	1	1	1	1	1
www.noardeast-fryslan.nl	1	1	1	1	1
www.noord-beveland.nl	1	1	1	1	1
www.noordoostpolder.nl	1	1	1	1	1
www.noordwijk.nl	1	1	1	1	0
www.nuenen.nl	1	1	1	1	1
www.nunspeet.nl	1	1	1	1	1
www.oegstgeest.nl	1	1	1	1	1
www.oirschot.nl	1	1	1	1	1
www.oisterwijk.nl	1	1	1	1	1
www.oldebroek.nl	1	1	1	1	1
www.oldenzaal.nl	0	1	1	1	0
www.olst-wijhe.nl	1	1	1	1	1
www.ommen.nl	1	1	1	1	1
www.oosterhout.nl	1	1	1	1	1
www.oostgelre.nl	0	1	1	1	1
www.ooststellingwerf.nl	1	1	1	1	1
www.oostzaan.nl	1	1	1	1	1
www.opmeer.nl	1	1	1	1	1
www.opsterland.nl	1	0	0	0	0
www.oss.nl	1	1	1	1	1
www.oude-ijsselstreek.nl	1	1	1	1	1
www.ouder-amstel.nl	1	1	1	1	1
www.oudewater.nl	1	1	1	1	1
www.overbetuwe.nl	1	1	1	1	0
www.papendrecht.nl	1	1	1	1	1
www.peelenmaas.nl	1	1	1	1	1
www.pekela.nl	1	1	1	1	1
www.pijnacker-nootdorp.nl	0	1	1	1	1
www.purmerend.nl	1	1	1	1	1
www.putten.nl	1	1	0	1	1
www.raalte.nl	0	1	1	1	1
www.reimerswaal.nl	1	1	1	1	1
www.renkum.nl	1	1	1	1	1
www.renswoude.nl	1	1	1	1	1
www.reuseldemierden.nl	1	1	1	1	1
www.rheden.nl	1	1	1	1	1
www.rhenen.nl	1	1	1	1	1
www.ridderkerk.nl	1	1	1	1	1
www.rijssen-holten.nl	1	1	1	1	1

www.rijswijk.nl	1	1	1	1	1
www.roerdalen.nl	1	1	1	1	1
www.roermond.nl	0	1	1	1	1
www.roosendaal.nl	1	1	1	1	1
www.rotterdam.nl	1	1	1	1	1
www.rozendaal.nl	1	1	0	1	0
www.rucphen.nl	1	1	1	1	1
www.schagen.nl	1	1	1	1	1
www.scherpenzeel.nl	1	1	1	1	1
www.schiedam.nl	1	1	1	1	1
www.schiermonnikoog.nl	1	1	1	1	1
www.schouwen-duiveland.nl	1	1	1	1	1
www.s-hertogenbosch.nl	1	1	1	1	1
www.simpelveld.nl	1	1	1	1	1
www.sintanthonis.nl	1	1	1	1	1
www.sint-michielsgestel.nl	1	1	1	1	1
www.sittard-geleen.nl	1	1	1	1	1
www.sliedrecht.nl	1	1	1	1	1
www.smallingerland.nl	1	1	1	1	1
www.soest.nl	1	1	1	1	1
www.someren.nl	1	1	1	1	1
www.sonenbreugel.nl	1	1	1	1	1
www.stadskanaal.nl	1	1	1	1	1
www.staphorst.nl	1	1	1	1	1
www.stedebroec.nl	1	1	1	1	1
www.steenwijkerland.nl	1	1	1	1	1
www.stichtsevecht.nl	1	1	1	1	0
www.sudwestfryslan.nl	1	1	1	1	0
www.t-diel.nl	1	1	1	1	1
www.terneuzen.nl	1	1	1	1	1
www.terschelling.nl	1	1	1	1	1
www.texel.nl	1	1	1	1	1
www.teylingen.nl	1	1	1	1	1
www.tholen.nl	1	1	1	1	1
www.tiel.nl	1	1	1	1	1
www.tilburg.nl	1	1	1	1	1
www.tubbergen.nl	1	1	1	1	1
www.twenterand.nl	1	1	1	1	1
www.tynaarlo.nl	1	1	1	1	1
www.tytsjerksteradiel.nl	1	1	1	1	1
www.uden.nl	1	1	1	1	1
www.uitgeest.nl	1	1	1	1	1
www.uithoorn.nl	1	1	1	1	1
www.urk.nl	1	1	1	1	1

www.utrecht.nl	1	1	1	1	1
www.vaals.nl	1	1	1	1	1
www.valkenburg.nl	1	1	0	0	1
www.valkenswaard.nl	1	1	1	1	1
www.veendam.nl	1	1	1	1	1
www.veenendaal.nl	1	1	1	1	1
www.veere.nl	1	1	1	1	1
www.veldhoven.nl	1	1	1	1	1
www.velsen.nl	0	1	1	1	0
www.venlo.nl	1	1	1	1	1
www.venray.nl	1	1	1	1	1
www.vijfheerenlanden.nl	1	1	1	1	1
www.vlaardingen.nl	1	1	0	1	1
www.vlieland.nl	1	1	1	1	1
www.vlissingen.nl	1	1	1	1	1
www.vng.nl	1	1	0	1	0
www.vngrealisatie.nl	1	1	1	1	1
www.voerendaal.nl	1	1	1	1	1
www.voorschoten.nl	1	1	1	1	1
www.voorst.nl	1	1	1	1	1
www.vught.nl	1	1	1	1	0
www.waadhoeke.nl	1	1	1	1	1
www.waalre.nl	1	1	1	1	1
www.waalwijk.nl	1	1	1	1	1
www.waddinxveen.nl	1	1	1	1	1
www.wageningen.nl	1	1	1	1	1
www.wassenaar.nl	1	1	1	1	1
www.waterland.nl	1	1	1	1	1
www.weert.nl	1	1	1	1	0
www.weesp.nl	1	1	1	1	1
www.westbetuwe.nl	1	1	1	1	1
www.westerkwartier.nl	1	1	1	1	1
www.westervoort.nl	1	1	1	1	1
www.westerwolde.nl	1	1	1	1	1
www.westmaasenwaal.nl	1	1	1	1	1
www.weststellingwerf.nl	1	1	1	1	1
www.westvoorne.nl	1	1	1	1	1
www.wierden.nl	1	1	1	1	1
www.wijchen.nl	1	1	1	1	1
www.wijdemeren.nl	1	1	1	1	0
www.wijkbijduurstede.nl	1	1	1	1	1
www.winterswijk.nl	1	1	1	1	1
www.woensdrecht.nl	1	1	1	1	1
www.woerden.nl	1	1	1	1	1

www.wormerland.nl	1	1	1	1	1
www.woudenberg.nl	1	1	1	1	1
www.zaanstad.nl	1	1	0	1	0
www.zaltbommel.nl	1	1	1	1	1
www.zandvoort.nl	1	1	1	1	1
www.zeewolde.nl	1	1	1	1	1
www.zeist.nl	1	1	1	1	1
www.zevenaar.nl	1	1	1	1	1
www.zoetermeer.nl	1	1	1	1	1
www.zoeterwoude.nl	1	1	1	1	1
www.zuidplas.nl	1	1	1	1	1
www.zundert.nl	1	1	1	1	1
www.zutphen.nl	1	1	1	1	1
www.zwartewaterland.nl	1	1	1	1	1
www.zwijndrecht.nl	1	1	1	1	1
www.zwolle.nl	0	1	1	1	1

Resultaten beveiligingsstandaarden voor mail

Resultaten mail Rijk

Domein	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC MX	DANE
aansluiten.procesinfrastructuur.nl	0	0	0	0	0	NVT	NVT	NVT	NVT
berichtenbox.antwoordvoorbedrijven.nl	1	1	1	1	1	NIETTESTBAAR	NIETTESTBAAR	1	NIETTESTBAAR
consuwijzer.nl	0	1	1	0	1	1	1	1	0
crisis.nl	1	1	1	1	1	NVT	NVT	NVT	NVT
crl.pkioverheid.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
daarkunjemeethuiskomen.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
defensie.nl	1	1	0	0	0	1	1	1	1
dictu.nl	1	1	1	1	1	1	1	1	1
digid.nl	1	1	1	1	1	1	1	1	1
digitaleoverheid.nl	1	1	1	1	1	1	1	1	1
digitoegankelijk.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
dji.nl	1	1	1	0	1	1	1	1	0
dsta.nl	1	NVT	1	1	1	1	1	1	0
eherkenning.nl	1	1	1	0	1	1	1	1	1
energielabelvoorwoningen.nl	0	0	1	0	1	NVT	NVT	NVT	NVT
fmhaaglanden.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
forensischinstituut.nl	1	1	0	0	0	NIETTESTBAAR	NIETTESTBAAR	1	NIETTESTBAAR
forumstandaardisatie.nl	1	1	1	1	1	1	1	1	1
government.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
helpdesk-efactureren.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
ictu.nl	1	1	1	1	1	1	1	1	1
idensys.nl	1	1	1	0	1	1	1	1	1
internetconsultatie.nl	1	1	1	0	1	1	1	1	1
koninklijkhuis.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
logius.nl	1	1	1	1	1	1	1	1	1
machtigen.digid.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
mijn.digid.nl	1	1	1	1	1	NVT	NVT	NVT	NVT
mijn.overheid.nl	1	1	1	1	1	1	1	1	1
mijnoverheidvoorondernemers.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
minaz.nl	1	0	1	0	1	0	0	0	0
minbuza.nl	1	1	1	0	1	1	1	1	1
minbzk.nl	1	1	1	0	1	1	1	1	1
mindef.nl	1	1	1	1	1	1	1	1	1
minez.nl	1	1	1	1	1	1	1	1	1
minfin.nl	1	1	1	1	1	1	1	1	1
minienm.nl	1	1	1	0	1	1	1	1	1
minjus.nl	1	1	1	1	1	1	1	1	1
minlnv.nl	1	1	1	1	1	1	1	1	1
minocw.nl	1	1	1	0	1	1	1	1	0
minszw.nl	1	1	1	0	1	1	1	1	1

minvenj.nl	1	1	1	1	1	1	1	1	1
minvws.nl	1	1	1	1	1	1	1	1	1
ncsc.nl	1	1	1	1	1	1	1	1	1
nctv.nl	1	1	1	0	1	1	1	1	1
nederlandwereldwijd.nl	1	0	0	0	0	NVT	NVT	NVT	NVT
nfi.nl	1	1	1	0	1	1	1	1	1
noraonline.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
officielebekendmakingen.nl	1	1	1	0	1	1	1	1	1
ondernemersplein.nl	1	1	1	1	1	1	1	0	0
overheid.nl	1	1	1	1	1	1	1	1	1
p-direkt.nl	1	1	1	1	1	1	1	1	1
portaal.digikoppeling.nl	1	0	1	0	1	NVT	NVT	NVT	NVT
portaal.digimelding.nl	1	0	1	0	1	NVT	NVT	NVT	NVT
rechtspraak.nl	1	1	1	1	0	1	1	1	1
rijkshuisstijl.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
rijksoverheid.nl	1	1	1	0	1	1	1	1	1
rijksvastgoedbedrijf.nl	1	NVT	1	1	1	1	1	1	1
rvig.nl	1	1	1	1	1	1	1	1	1
rvo.nl	1	1	1	1	1	1	1	1	1
sbr-nl.nl	0	1	1	0	1	NIETTES TBAAR	NIETTES TBAAR	1	NIETTES TBAAR
ssc-ict.nl	1	1	1	0	1	1	1	1	1
stelselcatalogus.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
tenderned.nl	1	1	1	1	1	1	1	1	1
ubrijk.nl	1	1	1	0	1	NVT	NVT	NVT	NVT
werkenbijdefensie.nl	1	1	1	0	1	1	0	1	0
werkenvoornederland.nl	1	1	1	0	1	1	1	0	0

Resultaten mail uitvoerders

Domein	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC MX	DANE
acm.nl	0	1	1	0	1	1	1	1	0
acvz.org	0	1	1	0	1	1	0	0	0
agentschaptelecom.nl	1	1	1	1	1	1	1	1	1
amberalert.nl	0	1	1	0	1	1	0	0	0
autoriteitpersoonsgegevens.nl	1	1	1	1	1	1	1	1	1
belastingdienst.nl	1	1	1	1	1	1	1	1	1
bkwi.nl	0	0	1	0	1	1	1	1	1
bureauft.nl	0	1	1	0	1	1	1	0	0
burgernet.nl	1	1	1	1	1	1	1	1	0
c2000.nl	1	1	1	1	1	0	0	1	0
cbg-meb.nl	0	0	1	0	1	0	0	0	0
cbr.nl	1	0	1	0	1	1	1	1	1
cbs.nl	1	1	1	1	1	1	1	1	1
cibg.nl	1	1	1	1	1	1	1	1	1
ciz.nl	1	1	1	1	1	1	0	1	1
cjib.nl	1	1	1	1	1	1	1	1	1
ctgb.nl	1	1	1	1	1	1	1	1	1
cultureelerfgoed.nl	1	1	1	0	1	1	1	1	0
cvdm.nl	1	1	1	1	1	1	1	0	0
doc-direkt.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
duo.nl	1	1	1	1	1	1	1	1	0
dus-i.nl	1	1	1	0	1	1	1	1	1
emissieautoriteit.nl	1	1	1	1	0	1	1	1	1
fiu-nederland.nl	1	0	1	1	1	1	1	1	0
halt.nl	0	1	1	0	1	1	1	0	0
hetcak.nl	1	1	1	0	1	1	1	1	1
huisvoorklokkenluiders.nl	1	1	1	0	1	1	1	1	1
huurcommissie.nl	1	1	1	1	1	1	1	0	0
ilent.nl	1	1	1	0	1	1	1	1	1
inburgeren.nl	1	0	1	1	1	NVT	NVT	NVT	NVT
ind.nl	1	1	1	1	1	1	1	1	1
inspectie-jenv.nl	1	1	1	1	1	1	1	1	1
justid.nl	1	1	1	1	1	1	1	1	1
justis.nl	1	1	1	0	1	1	1	1	1
kadaster.nl	1	1	1	1	1	1	1	1	1
kansspelautoriteit.nl	1	1	1	0	0	1	1	1	1
kleinlef.nl	0	1	0	0	0	0	0	0	0
knmi.nl	1	1	1	1	1	1	1	1	1
kvk.nl	1	1	1	1	1	1	1	0	0
manifestgroep.nl	0	0	0	0	0	1	1	1	0
mensenrechten.nl	0	1	1	0	1	1	1	1	1
mijn.belastingdienst.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT

mijn.toeslagen.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
mijnsvb.nl	0	0	0	0	0	1	1	1	0
nationaalarchief.nl	1	1	1	0	0	1	0	1	0
niwo.nl	0	1	1	0	1	1	1	1	0
nrgd.nl	1	1	0	0	0	1	1	1	1
nuffic.nl	1	1	1	1	1	1	1	0	0
nvao.net	1	1	1	1	1	1	1	0	0
nvwa.nl	0	0	1	0	1	1	1	1	1
om.nl	1	1	1	1	1	1	1	1	1
onderzoeksraad.nl	1	1	1	0	1	1	1	1	0
politie.nl	1	1	1	1	1	1	1	1	1
rdw.nl	1	1	1	0	1	1	0	1	1
rijkswaterstaat.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
rivm.nl	1	1	1	0	1	1	1	1	1
rsj.nl	1	1	1	0	1	1	1	1	1
rws.nl	0	1	0	0	0	1	0	1	0
schadefonds.nl	1	1	1	1	1	1	1	1	1
stab.nl	0	1	1	0	1	1	1	0	0
svb.nl	1	1	1	0	1	0	0	0	0
uitvoeringvanbeleidszw.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
uwv.nl	1	1	1	0	1	1	1	1	0
vananaarbeter.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
werk.nl	1	NVT	1	1	1	NVT	NVT	NVT	NVT
zinl.nl	1	1	1	1	1	1	1	1	1
zorginstituutnederland.nl	0	1	1	0	1	NVT	NVT	NVT	NVT

Resultaten mail provincies

Domein	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC MX	DANE
bij12.nl	0	1	1	0	1	1	1	0	0
brabant.nl	1	1	1	1	1	1	1	0	0
drenthe.nl	1	1	1	0	1	1	1	0	0
flevoland.nl	1	1	1	0	1	1	0	1	0
fryslan.frl	1	0	1	1	1	1	1	0	0
fryslan.nl	1	0	1	1	1	1	1	0	0
gelderland.nl	1	1	1	0	1	1	1	0	0
ipo.nl	0	1	1	0	1	1	1	0	0
limburg.nl	1	1	1	1	1	1	1	1	1
noord-holland.nl	1	1	1	0	1	1	0	1	0
overijssel.nl	1	1	1	0	1	1	0	1	0
provincie.drenthe.nl	1	0	1	0	1	NVT	NVT	NVT	NVT
provinciegroningen.nl	1	1	1	0	1	1	1	1	0
provincie-utrecht.nl	1	1	1	1	1	1	0	0	0
prvlimburg.nl	1	1	1	1	1	1	1	1	1
pzh.nl	1	1	1	1	1	1	1	0	0
zeeland.nl	1	1	1	1	1	1	1	1	1
zuid-holland.nl	1	1	1	1	1	NVT	NVT	NVT	NVT

Resultaten mail waterschappen

Domein	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC MX	DANE
aaenmaas.nl	1	1	1	0	1	1	1	0	0
agv.nl	1	1	1	1	1	1	1	1	0
brabantsedelta.nl	1	1	1	1	1	1	1	0	0
derbg.nl	0	1	0	0	0	1	1	1	1
dommel.nl	1	1	1	1	1	1	1	1	1
hdsr.nl	1	1	1	0	1	1	1	1	0
hetwaterschapshuis.nl	0	1	1	0	1	1	1	0	0
hhdelfland.nl	1	1	1	0	1	1	1	0	0
hhnk.nl	0	1	1	0	0	1	1	1	0
hhsk.nl	1	1	1	0	1	1	1	1	1
hunzeenaas.nl	1	1	1	1	1	1	0	0	0
ihw.nl	0	0	1	0	1	1	1	0	0
informatiehuiswater.nl	0	0	1	0	1	NIETTESTBAAR	NIETTESTBAAR	0	NIETTESTBAAR
noorderzijlvest.nl	1	1	1	1	1	1	1	0	0
rijnland.net	1	1	1	0	1	1	1	1	1
scheldestromen.nl	1	1	1	1	1	1	0	1	0
schielandendekrimpenerwaard.nl	0	0	0	0	0	NVT	NVT	NVT	NVT
stowa.nl	1	1	1	1	1	1	1	0	0
uvw.nl	1	1	1	1	1	1	1	0	0
vallei-veluwe.nl	1	1	1	1	1	1	1	0	0
vechtstromen.nl	1	1	1	1	1	1	0	1	0
waternet.nl	1	1	1	1	1	1	1	1	0
waterschaplimburg.nl	1	1	1	1	1	1	1	1	0
waterschappen.nl	0	1	0	0	0	NIETTESTBAAR	NIETTESTBAAR	1	NIETTESTBAAR
waterschaprivierenland.nl	1	1	1	1	1	1	1	1	1
wbl.nl	0	0	0	0	0	0	0	0	0
wdodelta.nl	1	1	1	1	1	1	1	1	0
wetterskipfryslan.nl	1	1	1	1	1	1	1	0	0
wrij.nl	1	1	1	1	1	1	1	0	0
wshd.nl	1	1	1	0	1	1	1	1	1
wsrl.nl	1	1	1	1	1	1	1	1	1
zuiderzeeland.nl	1	1	1	1	1	1	1	0	0

Resultaten mail gemeenten

Domein	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC MX	DANE
aaenhunze.nl	1	1	1	1	1	1	1	1	1
aalsmeer.nl	1	1	1	0	1	1	1	1	1
aalten.nl	1	1	1	1	1	1	1	1	1
achtkarspelen.nl	0	1	1	0	1	1	1	0	0
alblasserdam.nl	1	1	1	1	1	1	1	0	0
albrandswaard.nl	1	1	1	0	1	1	1	1	0
alkmaar.nl	1	1	1	1	1	1	0	1	1
almelo.nl	1	1	1	1	1	1	1	0	0
almere.nl	1	1	1	0	1	1	0	1	1
alphenaandenrijn.nl	1	1	1	1	1	1	1	1	1
alphen-chaam.nl	1	1	1	1	1	1	1	1	1
ameland.nl	1	1	1	1	1	1	1	0	0
amersfoort.nl	1	1	1	1	1	1	1	1	1
amstelveen.nl	1	1	1	0	1	1	1	1	1
amsterdam.nl	1	1	1	0	1	1	1	0	0
apeldoorn.nl	1	1	1	0	1	1	1	1	1
appingedam.nl	1	1	0	0	0	1	1	1	0
arnhem.nl	1	1	1	1	1	1	1	1	1
assen.nl	1	1	1	1	1	1	1	0	0
asten.nl	1	1	1	1	1	1	1	1	1
baarle-nassau.nl	1	1	1	1	1	1	1	1	1
baarn.nl	1	1	1	1	1	1	1	0	0
barendrecht.nl	1	1	1	0	1	1	1	1	0
barneveld.nl	1	1	1	0	0	1	1	1	1
beekdaelen.nl	1	1	1	1	1	1	1	1	1
beemster.net	1	1	1	1	1	1	1	1	1
beesel.nl	1	1	1	1	1	1	1	1	1
bergeijk.nl	1	1	1	1	1	1	1	1	1
bergen.nl	1	1	1	1	1	1	1	1	1
bergendal.nl	1	1	1	0	1	1	1	1	1
bergen-nh.nl	1	1	1	0	1	1	1	0	0
bergenopzoom.nl	1	1	1	0	1	1	1	1	1
bernheze.org	1	1	1	1	1	1	1	1	0
beuningen.nl	1	1	1	1	1	1	1	1	1
beverwijk.nl	1	1	1	1	1	1	1	1	1
bladel.nl	1	1	1	1	1	1	1	1	1
blaricum.nl	1	1	1	1	1	1	1	1	1
bloemendaal.nl	1	1	1	1	1	1	1	1	1
bodegraven-reeuwijk.nl	0	0	1	0	1	1	1	0	0
boekel.nl	1	1	1	0	1	0	0	0	0
borger-odoorn.nl	1	1	1	0	1	1	1	0	0
borne.nl	1	1	1	0	1	1	1	0	0

borsele.nl	1	1	1	1	1	1	1	0	0
boxmeer.nl	1	1	1	0	1	1	0	0	0
boxtel.nl	1	1	1	0	1	1	1	0	0
breda.nl	1	1	1	0	1	1	1	0	0
brielle.nl	0	0	1	0	0	1	1	1	0
bronckhorst.nl	1	1	1	1	1	1	1	1	1
brummen.nl	1	1	1	1	1	1	1	1	1
brunssum.nl	1	1	1	1	1	1	1	1	1
bunnik.nl	1	1	1	1	1	1	1	0	0
bunschoten.nl	1	1	1	1	1	1	1	0	0
buren.nl	1	1	1	0	1	NIETTEST BAAR	NIETTEST BAAR	1	NIETTEST BAAR
capelleaandenijssel.nl	1	1	1	0	1	1	1	1	1
castricum.nl	1	1	1	0	1	1	1	0	0
coevorden.nl	1	1	1	0	1	1	1	0	0
cranendonck.nl	1	1	1	1	1	1	1	1	1
cuijk.nl	0	1	1	0	1	1	0	1	0
culemborg.nl	1	1	1	1	1	1	1	1	1
dalfsen.nl	1	1	1	0	1	1	1	1	1
dantumadiel.frl	1	1	1	1	1	1	1	0	0
debilt.nl	1	1	1	1	1	1	1	0	0
defryskemarren.nl	0	1	1	0	1	1	1	1	1
delft.nl	1	1	1	1	1	1	1	1	1
delfzijl.nl	0	1	1	0	1	1	1	1	0
denhaag.nl	1	1	1	1	1	1	1	1	1
denhelder.nl	1	1	1	0	1	1	1	1	1
derondevenen.nl	1	1	1	1	1	1	1	1	1
deurne.nl	1	1	1	1	1	1	1	0	0
deventer.nl	1	1	1	1	1	1	1	0	0
dewolden.nl	1	1	1	0	1	1	1	1	1
diemen.nl	1	1	1	0	1	1	1	0	0
dinkelland.nl	1	1	1	1	1	1	1	1	0
doesburg.nl	1	1	1	1	1	1	1	1	1
doetinchem.nl	1	1	1	1	1	1	1	1	1
dongen.nl	1	1	1	1	1	1	1	1	1
dordrecht.nl	1	1	1	1	1	1	1	0	0
drechterland.nl	1	1	1	1	1	1	1	1	1
drimmelen.nl	1	1	1	0	1	1	1	0	0
dronten.nl	1	1	1	0	1	1	1	1	1
druten.nl	1	1	1	0	1	1	1	1	1
duiven.nl	0	1	1	0	1	1	1	0	0
echt-susteren.nl	1	1	1	0	1	1	0	1	0
edam-volendam.nl	1	1	1	1	1	1	1	1	1
ede.nl	1	1	1	1	1	NIETTEST BAAR	NIETTEST BAAR	1	NIETTEST BAAR
eemnes.nl	1	1	1	1	1	1	1	1	1

eersel.nl	1	1	1	1	1	1	1	1	1
eijsden-margraten.nl	1	1	1	1	1	1	1	1	1
eindhoven.nl	1	1	1	0	1	1	1	0	0
elburg.nl	1	1	1	1	1	1	1	0	0
emmen.nl	1	1	1	0	1	1	1	0	0
enkhuizen.nl	1	1	1	1	1	1	1	1	1
enschede.nl	1	1	1	0	1	1	1	0	0
epe.nl	1	1	1	1	1	1	1	1	1
ermelo.nl	1	1	1	1	1	1	1	1	0
etten-leur.nl	1	1	1	0	1	1	1	1	1
geertruidenberg.nl	1	1	1	0	1	1	1	1	1
geldrop-mierlo.nl	1	1	1	0	1	1	0	1	1
gemeente.groningen.nl	1	0	0	1	0	NVT	NVT	NVT	NVT
gemeente.leiden.nl	1	0	0	1	0	NVT	NVT	NVT	NVT
gemeentealtena.nl	1	1	1	1	1	1	1	1	0
gemeentebeek.nl	1	1	1	1	1	1	1	1	1
gemeenteberkelland.nl	1	1	1	0	1	1	0	1	0
gemeentebest.nl	1	1	1	1	1	1	1	0	0
gemeentehulst.nl	1	0	1	0	1	1	0	0	0
gemeentehw.nl	0	0	1	0	1	NIETTEST BAAR	NIETTEST BAAR	0	NIETTEST BAAR
gemeentelangedijk.nl	1	1	1	0	0	1	1	0	0
gemeentemaasgouw.nl	1	1	1	0	1	1	0	1	0
gemeentemaastricht.nl	1	1	1	1	1	NVT	NVT	NVT	NVT
gemeente-mill.nl	0	1	1	0	1	1	0	1	0
gemeentenoordenveld.nl	1	1	1	0	1	1	0	1	0
gemeente-oldambt.nl	1	1	1	0	1	1	1	1	1
gemeentesluis.nl	0	1	1	0	1	1	0	0	0
gemeente-steenbergen.nl	1	1	1	1	1	1	1	1	1
gemeentestein.nl	1	1	1	1	1	1	1	1	1
gemeentesudwestfryslan.nl	1	1	1	1	1	1	0	1	0
gemeentewesterveld.nl	1	1	1	1	1	1	1	1	1
gemeentewestland.nl	1	1	1	1	1	1	1	1	1
gemert-bakel.nl	1	1	1	1	1	1	1	1	0
gennep.nl	1	1	1	1	1	1	1	0	0
gilzerijen.nl	1	1	1	1	1	1	1	1	1
goeree-overflakkee.nl	1	1	1	1	1	1	1	0	0
goes.nl	1	1	1	1	1	1	1	0	0
goirle.nl	1	1	1	1	1	1	1	1	1
gooisemeren.nl	1	1	1	1	1	1	1	0	0
gorinchem.nl	1	1	1	1	1	1	1	0	0
gouda.nl	1	1	1	0	1	1	1	1	1
grave.nl	0	1	1	0	1	1	0	1	0
groningen.nl	1	1	1	1	1	1	1	1	0
gulpen-wittem.nl	1	1	1	1	1	1	1	1	1

haaksbergen.nl	1	1	1	1	1	1	1	1	0
haaren.nl	1	1	1	0	1	1	1	0	0
haarlem.nl	1	1	1	1	1	1	1	1	1
haarlemmermeer.nl	1	0	1	1	1	1	1	0	0
haarlemmermeergemeente.nl	0	1	0	0	0	NVT	NVT	NVT	NVT
halderberge.nl	1	1	1	1	1	1	0	0	0
hardenberg.nl	1	1	1	0	1	1	1	0	0
harderwijk.nl	1	1	1	1	1	1	1	1	0
hardinxveld-giessendam.nl	1	1	1	1	1	1	1	0	0
harlingen.nl	1	1	1	0	1	1	0	1	0
hattem.nl	1	1	1	1	1	1	0	0	0
heemskerk.nl	1	1	1	0	1	1	1	1	1
heemstede.nl	1	1	1	1	1	1	1	1	1
heerde.nl	1	1	1	1	1	1	0	0	0
heerenveen.nl	1	1	1	1	1	1	1	1	0
heerhugowaard.nl	1	1	1	0	0	1	1	0	0
heerlen.nl	1	1	1	1	1	1	1	1	1
heeze-leende.nl	1	1	1	1	1	1	1	1	1
heiloo.nl	1	1	1	0	1	1	1	0	0
hellendoorn.nl	1	1	1	1	1	1	1	1	1
hellevoetsluis.nl	1	1	1	1	1	1	1	1	0
helmond.nl	1	1	1	0	1	1	1	1	1
hengelo.nl	1	1	1	1	1	1	0	0	0
hethogeland.nl	1	0	1	0	1	1	1	1	0
heumen.nl	1	1	1	1	1	1	1	1	1
heusden.nl	1	1	1	1	1	1	1	1	1
heuvelrug.nl	1	1	1	1	1	1	1	0	0
h-i-ambacht.nl	1	1	1	1	1	1	1	0	0
hillegom.nl	1	1	1	0	1	1	1	0	0
hilvarenbeek.nl	1	1	1	1	1	1	1	1	1
hilversum.nl	1	1	1	1	1	1	1	1	1
hofvantwente.nl	1	1	1	0	0	NIETTESTBAAR	NIETTESTBAAR	0	NIETTESTBAAR
hollandskroon.nl	1	1	1	0	1	1	1	0	0
hoogeveen.nl	1	1	1	0	1	1	1	1	1
hoorn.nl	1	1	1	1	1	1	1	1	1
horstaandemaas.nl	1	1	1	0	1	1	0	1	0
houten.nl	1	1	1	1	1	1	1	1	1
huizen.nl	0	1	1	0	0	1	1	0	0
ijsselstein.nl	1	0	1	1	1	1	1	1	0
informatiebeveiligingsdienst.nl	1	0	1	1	1	1	1	1	0
kaagenbraassem.nl	1	1	1	1	1	1	1	1	1
kampen.nl	1	1	1	0	0	1	1	1	1
kapelle.nl	1	1	1	1	1	NIETTESTBAAR	NIETTESTBAAR	0	NIETTESTBAAR

katwijk.nl	1	1	1	1	1	1	1	1	0
kerkrade.nl	1	1	1	1	1	1	1	1	1
koggenland.nl	1	1	1	1	1	1	1	1	1
krimpenaandenijssel.nl	1	1	1	0	0	1	1	1	1
krimpenerwaard.nl	1	1	1	1	1	1	0	1	0
laarbeek.nl	1	1	1	1	1	1	1	1	0
landerd.nl	1	1	1	1	1	1	1	1	1
landgraaf.nl	1	1	1	1	1	1	1	1	1
landsmeer.nl	0	0	1	0	0	1	0	0	0
lansingerland.nl	1	1	1	1	1	1	1	1	1
laren.nl	1	1	1	1	1	1	1	1	1
leeuwarden.nl	1	1	1	1	1	1	1	0	0
leiden.nl	1	0	1	1	1	1	1	0	0
leiderdorp.nl	1	1	1	0	1	1	1	0	0
leidschendam-voorburg.nl	1	1	1	1	1	1	1	0	0
lelystad.nl	1	1	1	1	1	1	1	1	1
leudal.nl	1	1	1	1	1	1	1	1	1
leusden.nl	1	1	1	0	1	1	1	0	0
lingewaard.nl	1	1	1	0	1	1	1	1	1
lisse.nl	1	1	1	0	1	1	1	0	0
lochem.nl	1	1	1	1	1	1	1	1	0
loonopzand.nl	1	1	1	1	1	1	1	1	1
lopik.nl	1	1	1	1	1	1	1	1	0
loppersum.nl	0	1	1	0	1	1	1	1	0
losser.nl	1	1	1	0	1	1	1	0	0
lv.nl	1	1	1	0	1	1	1	0	0
maasdriel.nl	1	1	1	0	1	1	1	1	1
maassluis.nl	1	1	1	1	0	1	1	0	0
maastricht.nl	1	1	1	1	1	1	1	1	1
medemblik.nl	1	1	1	1	1	1	1	1	1
meerssen.nl	1	0	1	1	1	1	1	1	1
meierijstad.nl	1	1	1	1	1	1	1	1	1
meppel.nl	1	1	1	1	1	1	1	1	1
middelburg.nl	1	1	1	1	1	1	1	1	1
middendelfland.nl	1	1	1	1	1	1	1	1	1
middendrenthe.nl	1	1	1	0	1	1	1	1	1
midden-groningen.nl	1	0	1	1	1	1	1	1	1
moerdijk.nl	1	1	1	1	1	1	1	1	1
molenlanden.nl	1	0	1	1	1	1	1	0	0
montferland.info	1	1	1	1	1	1	1	1	1
montfoort.nl	1	1	1	1	1	1	1	1	0
mookenmiddelaar.nl	1	1	1	1	1	1	1	1	1
nederbetuwe.nl	1	1	1	1	0	1	1	1	1
nederweert.nl	0	1	1	0	1	1	1	1	1

nieuwegein.nl	1	1	1	0	1	1	1	1	0
nieuwkoop.nl	1	1	1	0	1	0	0	0	0
nijkerk.eu	1	1	0	0	0	1	1	0	0
nijmegen.nl	1	1	1	0	1	1	1	1	1
nissewaard.nl	0	1	1	0	0	1	1	1	0
noardeast-fryslan.nl	1	1	1	1	1	1	1	0	0
noord-beveland.nl	1	1	1	1	1	1	1	0	0
noordoostpolder.nl	1	1	1	1	1	1	1	0	0
noordwijk.nl	1	1	1	1	0	1	1	1	1
nuenen.nl	1	1	1	0	1	1	0	1	1
nunspeet.nl	1	1	1	1	1	1	1	1	1
oegstgeest.nl	1	1	1	1	1	1	1	0	0
oirschot.nl	1	1	1	1	1	1	1	1	1
oisterwijk.nl	1	1	1	1	1	1	1	1	1
oldebroek.nl	1	1	1	1	1	1	0	0	0
oldenzaal.nl	1	1	1	1	1	1	0	0	0
olst-wijhe.nl	1	1	1	1	1	1	1	0	0
ommen.nl	1	1	1	0	1	1	1	0	0
oosterhout.nl	1	1	1	1	1	1	1	1	1
oostgelre.nl	1	1	1	1	1	1	1	1	1
ooststellingwerf.nl	1	1	1	0	1	1	0	1	0
oostzaan.nl	0	0	1	0	1	1	1	0	0
opmeer.nl	1	1	1	1	1	1	1	1	1
opsterland.nl	1	1	1	0	1	1	0	1	0
oss.nl	1	1	1	0	1	1	0	1	1
oude-ijsselstreek.nl	1	1	1	1	1	1	1	1	1
ouder-amstel.nl	1	1	1	0	1	1	1	0	0
oudewater.nl	1	1	1	1	0	1	1	0	0
overbetuwe.nl	1	1	1	0	1	1	1	0	0
papendrecht.nl	1	1	1	1	1	1	1	0	0
peelenmaas.nl	1	1	1	0	1	1	1	1	1
pekela.nl	1	1	1	1	1	1	1	1	1
pijnacker-nootdorp.nl	1	1	1	0	1	1	1	0	0
purmerend.nl	1	1	1	0	0	1	1	1	1
putten.nl	1	1	1	0	1	1	1	0	0
raalte.nl	1	1	1	1	1	1	1	0	0
reimerswaal.nl	1	1	1	1	1	1	1	0	0
renkum.nl	1	1	1	1	1	1	1	1	1
renswoude.nl	1	1	1	0	1	1	1	0	0
reuseldemierden.nl	1	1	1	1	1	1	1	1	1
rheden.nl	1	1	1	1	1	1	1	1	1
rhenen.nl	1	1	1	1	1	1	1	0	0
ridderkerk.nl	1	1	1	0	1	1	1	1	0
rijssen-holten.nl	1	1	1	1	1	1	1	1	1

rijswijk.nl	1	1	1	1	1	1	1	1	1
roerdalen.nl	1	1	0	0	0	1	0	1	0
roermond.nl	0	1	1	0	1	1	1	1	1
roosendaal.nl	1	1	1	0	1	1	1	1	1
rotterdam.nl	1	1	1	1	1	1	1	1	1
rozendaal.nl	1	1	1	0	0	1	0	0	0
rucphen.nl	1	1	1	1	1	1	1	0	0
schagen.nl	0	1	1	0	1	1	1	1	1
scherpenzeel.nl	1	1	1	0	1	1	1	0	0
schiedam.nl	1	1	1	0	1	1	1	1	0
schiermonnikoog.nl	1	1	1	1	1	1	1	0	0
schouwen-duiveland.nl	0	1	1	0	1	1	1	1	1
s-hertogenbosch.nl	1	1	1	1	1	1	1	1	1
simpelveld.nl	1	1	1	1	1	1	1	1	1
sintanthonis.nl	1	1	1	0	0	1	0	0	0
sint-michielsgestel.nl	1	1	1	0	1	1	1	0	0
sittard-geleen.nl	1	1	1	1	1	1	1	1	1
sliedrecht.nl	1	1	1	1	1	1	1	0	0
smallingerland.nl	1	1	1	0	1	1	0	1	0
soest.nl	1	1	1	1	1	1	1	0	0
someren.nl	1	1	1	1	1	1	1	1	1
sonenbreugel.nl	1	1	1	0	1	1	0	1	1
stadskanaal.nl	0	1	1	0	1	1	1	0	0
staphorst.nl	1	1	1	1	1	1	1	1	1
stedebroec.nl	1	1	1	1	1	1	1	1	1
steenwijkerland.nl	1	1	1	0	0	1	1	1	1
stichtsevecht.nl	1	1	1	1	1	1	1	1	0
sudwestfryslan.nl	1	1	1	1	1	1	0	1	0
t-diel.nl	0	1	1	0	1	1	1	0	0
terneuzen.nl	0	1	1	0	1	1	1	1	1
terschelling.nl	1	1	1	1	1	1	1	0	0
texel.nl	1	1	1	0	1	1	0	1	0
teylingen.nl	1	1	1	0	1	1	1	0	0
tholen.nl	1	1	1	1	1	1	1	1	1
tiel.nl	1	1	1	1	1	1	1	1	1
tilburg.nl	1	1	1	1	1	1	1	1	1
tubbergen.nl	1	1	1	1	1	1	1	1	0
twenterand.nl	1	1	1	1	1	1	1	0	0
tynaarlo.nl	1	1	1	1	1	1	1	1	1
tytsjerksteradiel.nl	0	0	0	0	0	NIETTESTBAAR	NIETTESTBAAR	0	NIETTESTBAAR
uden.nl	1	1	1	0	0	1	1	1	1
uitgeest.nl	1	1	1	0	1	1	1	0	0
uithoorn.nl	1	1	1	0	0	1	1	0	0
urk.nl	1	1	1	1	1	1	1	1	1

utrecht.nl	1	1	1	1	1	1	1	0	0
vaals.nl	1	1	1	0	1	1	1	0	0
valkenburg.nl	1	1	1	0	1	1	1	1	0
valkenswaard.nl	1	1	1	1	1	1	1	1	1
veendam.nl	1	1	1	1	1	1	1	1	1
veenendaal.nl	1	1	1	0	1	1	1	0	0
veere.nl	1	1	1	1	1	1	1	0	0
veldhoven.nl	1	1	1	0	1	1	1	1	1
velsen.nl	1	1	1	1	1	0	0	0	0
venlo.nl	0	1	1	0	0	1	1	1	1
venray.nl	1	1	1	0	1	1	0	1	0
vijfheerenlanden.nl	1	1	1	1	1	1	1	1	1
vlaardingen.nl	1	1	1	0	0	NIETTESTBAAR	NIETTESTBAAR	1	NIETTESTBAAR
vlieland.nl	1	1	1	1	1	1	1	0	0
vlissingen.nl	1	1	1	1	1	1	1	1	1
vng.nl	1	0	1	0	1	1	1	0	0
vngrealisatie.nl	0	1	0	0	0	NVT	NVT	NVT	NVT
voerendaal.nl	1	1	1	1	1	1	1	1	1
voorschoten.nl	1	1	1	1	1	1	1	1	1
voorst.nl	0	0	1	0	1	1	1	1	1
vught.nl	1	1	1	1	1	NIETTESTBAAR	NIETTESTBAAR	1	NIETTESTBAAR
waadhoeke.nl	1	1	1	1	1	1	1	0	0
waalre.nl	1	1	1	0	1	1	1	0	0
waalwijk.nl	1	1	1	1	1	1	1	1	1
waddinxveen.nl	1	1	1	0	1	1	1	1	1
wageningen.nl	1	1	1	0	0	NIETTESTBAAR	NIETTESTBAAR	0	NIETTESTBAAR
wassenaar.nl	1	1	1	1	1	1	1	1	1
waterland.nl	0	1	1	0	1	1	1	1	1
weert.nl	0	1	1	0	1	1	0	1	0
weesp.nl	1	1	1	1	1	1	0	1	0
westbetuwe.nl	1	1	1	1	1	1	1	1	1
westerkwartier.nl	1	1	1	1	1	1	1	0	0
westervoort.nl	0	1	1	0	1	1	1	0	0
westerwolde.nl	1	1	1	1	1	1	1	1	1
westmaasenwaal.nl	1	1	1	1	1	1	1	0	0
weststellingwerf.nl	1	1	1	0	1	1	0	1	0
westvoorne.nl	0	0	1	0	1	1	1	1	0
wierden.nl	1	1	1	1	1	1	1	1	1
wijchen.nl	1	1	1	0	1	1	1	1	1
wijdemeren.nl	0	0	1	0	1	1	1	1	1
wijkbijduurstede.nl	1	1	1	1	1	1	1	0	0
winterswijk.nl	1	1	1	1	1	1	1	1	1
woensdrecht.nl	1	1	1	1	1	1	1	1	1
woerden.nl	1	1	1	1	0	1	1	0	0

wormerland.nl	0	0	1	0	1	1	1	0	0
woudenberg.nl	1	1	1	0	1	1	1	1	1
zaanstad.nl	1	1	1	1	1	1	1	1	1
zaltbommel.nl	1	1	1	0	1	1	1	1	1
zandvoort.nl	1	1	1	1	1	1	1	1	1
zeewolde.nl	1	1	1	1	1	1	1	1	0
zeist.nl	1	1	1	1	1	1	1	1	0
zevenaar.nl	0	1	1	0	1	1	1	0	0
zoetermeer.nl	1	1	1	1	0	1	0	0	0
zoeterwoude.nl	1	1	1	1	1	1	1	0	0
zuidplas.nl	1	1	1	0	1	1	1	1	1
zundert.nl	1	1	1	1	1	1	1	1	1
zutphen.nl	1	1	1	1	1	NIETTEST BAAR	NIETTEST BAAR	1	NIETTEST BAAR
zwartewaterland.nl	1	1	1	1	1	1	1	1	1
zwijndrecht.nl	1	1	1	1	1	1	1	0	0
zwolle.nl	1	1	1	0	0	1	0	1	0

notitie

OBDO – 18 maart 2020
Overheidsbrede streefbeeldafspraak IPv6

Nummer:	Bijlage 1C - standaardisatie
Aan:	Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO)
Van:	Forum Standaardisatie (via strategisch vooroverleg OBDO)
Datum:	18 maart 2020
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 IPv6. Het doel is om alle overheidswebsites en e-maildomeinen van de overheid uiterlijk eind 2021, behalve via IPv4, ook volledig bereikbaar te laten zijn via IPv6.

De streefbeeldafspraak sluit aan bij de intentieverklaring die verschillende overheidsorganisaties en leveranciers recentelijk hebben ondertekend. Het gaat o.a. om de volgende partijen: VNG Realisatie, min. BZK, min. EZK, Logius, Equinix, KPN, Microsoft, Simgroep, en VodafoneZiggo.

Met de intentieverklaring spraken de ondertekenaars af om alles te doen wat in hun vermogen ligt om IPv6 te ondersteunen, zodat overheidsorganisaties uiterlijk per 31 december 2021 extern (d.w.z. via website en e-mail) volledig bereikbaar zijn via IPv6. De ondertekenaars riepen ook het Forum Standaardisatie en het OBDO op om te komen tot een overheidsbrede streefbeeldafspraak, en om periodiek te meten en te rapporteren over de implementatievoortgang.

IPv6 is de open internetstandaard die iedere internetgebruiker nodig heeft om ook in de toekomst onbelemmerd gebruik te kunnen maken van internet. Er zijn verschillende goede redenen om voor IPv6 te kiezen, juist ook als overheid: groei en innovatie van internet, directere en snellere dienstverlening, en tegengaan van fraude.

Het Forum Standaardisatie heeft IPv6 in combinatie met IPv4 (‘dual stack’) in 2010 op de ‘pas toe of leg uit-lijst geplaatst. De adoptiestatistieken van Forum Standaardisatie laten zien dat het aantal overheidswebsites en -mailsystemen dat via IPv6 bereikbaar is duidelijk groeit. Momenteel ondersteunt 56% van de websites en 22% van de mailservers IPv6. Ook in de markt is momentum zichtbaar, mede doordat onlangs de laatst beschikbare IPv4-adressen voor Europa zijn uitgegeven.

De bestaande streefbeeldafspraken voor internetbeveiligingsstandaarden die het OBDO heeft gemaakt, hebben voor die standaarden duidelijk een adoptie-impuls gegeven. Gelet op het voorgaande is nu het juiste moment om ook voor IPv6 een streefbeeldafspraak te maken.

Gevraagd besluit

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

A. een streefbeeldafspraak te maken om alle overheidswebsites en e-maildomeinen van de overheid uiterlijk eind 2021, behalve via IPv4, ook volledig bereikbaar te laten zijn via IPv6;
B. door Forum Standaardisatie de implementatievoortgang halfjaarlijks te laten meten en daarover te rapporteren aan OBDO;
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

1. Oproep aan Forum Standaardisatie en OBDO

Op 4 oktober 2019 ondertekenden VNG Realisatie, Logius, verschillende leveranciers, serviceproviders en andere overheidsorganisaties een intentieverklaring om de implementatie van IPv6 te versnellen. Zij focussen zich in eerste instantie op de externe bereikbaarheid. De ambitie is om het mogelijk te maken dat alle overheidsorganisaties eind 2021 via IPv6 bereikbaar zijn. De ondertekenaars roepen Forum Standaardisatie en OBDO op om een overheidsbrede implementatieafspraak voor IPv6 te maken (net als eerder voor de internetbeveiligingsstandaarden is gedaan), en ook om periodiek te meten en te rapporteren over de implementatievoortgang.

Ondertussen is de intentieverklaring, behalve door de initiële ondertekenaars, ook door andere partijen ondertekend. Hieronder volgt een overzicht zoals bijgehouden door VNG Realisatie.

- Overheden: DUO/ODC Noord, Govroam, min. BZK, min. EZK, Logius, Parkstad-ICT, VNG Realisatie.
- Bedrijven:, Equinix, E-Zorg, KPN, Microsoft, Mozard, Muada, Seneca, Simgroep, Steffann, en VodafoneZiggo.

De ondertekening door de volgende organisaties staat nog gepland: BIT, Cisco, min. JenV, Tele2.

Onderstaand kader bevat de tekst van de intentieverklaring.

Intentieverklaring

IPv6 is de open internetstandaard die iedere internetgebruiker nodig heeft om ook in de toekomst onbelemmerd gebruik te kunnen maken van internet. De Nederlandse overheid digitaliseert haar dienstverlening in hoog tempo en om voor alle inwoners en ondernemingen ook in de toekomst bereikbaar te blijven, moeten haar websites en mailservers ook via IPv6 (naast het oude beperktere adresprotocol IPv4) bereikbaar worden gemaakt. IPv6 zorgt bovendien voor betere 'end-to-end'-connectiviteit, hogere snelheid en meer innovatie. De afgelopen jaren heeft een groot aantal overheidsorganisaties IPv6 al ingevoerd voor websites en mailservers.

De ondertekenaars, bestaande uit zowel overheden als leveranciers, willen deze ontwikkeling nu graag gaan versnellen. Zij zullen zelf alles doen wat in hun vermogen ligt om IPv6 te ondersteunen, zodat overheidsorganisaties uiterlijk per 31 december 2021 extern (d.w.z. via website en e-mail) volledig bereikbaar zijn via IPv6. De ondertekenaars roepen daarnaast het Forum Standaardisatie op om een overheidsbrede implementatieafspraak voor IPv6 te maken (net als eerder voor de internetbeveiligingsstandaarden is gedaan), en ook periodiek te meten en te rapporteren over de implementatievoortgang.

2. Over IPv6

2.1 Werking

Het Internet Protocol (IP) vormt de basis onder al het verkeer op Internet. Ieder apparaat dat met het internet is verbonden, heeft een uniek numeriek adres namelijk het IP-adres.

Er bestaan twee versie van het Internet Protocol: versie 4 (IPv4) en versie 6 (IPv6). Deze versies zijn niet compatibel met elkaar. Dit betekent dat een computer met een IPv4-adres niet kan communiceren met een computer die alleen een IPv6-adres heeft. Wel kunnen versie 4 en versie 6 naast elkaar worden gebruikt, maar uiteindelijk zal IPv4 volledig worden vervangen door IPv6. Bijna alle apparatuur en diensten ondersteunen inmiddels zowel IPv4 als IPv6.

2.2 Nut

Er zijn verschillende goede redenen om voor IPv6 te kiezen, ook juist als overheid: groei en innovatie van internet, directere en snellere dienstverlening, en tegengaan van fraude.

Alleen als beide partijen die een verbinding maken IPv6 ondersteunen, zal IPv6 worden gebruikt en kunnen de voordelen worden benut. Het individuele en maatschappelijke nut van IPv6 neemt daardoor toe naarmate IPv6 meer ondersteund wordt. Er is sprake van een ‘first mover disadvantage’ (wel de lasten, niet de lusten). Dit zorgt voor marktfalen waardoor de adoptie niet of traag tot stand komt. De overheid kan onder andere door zelf het goede voorbeeld te geven de adoptie bevorderen. Een ander blijkt ook uit een studie van het Centraal Planbureau naar de “Economische aspecten van internetveiligheid” uit 2013.

Groei en innovatie van internet
IPv6-adressen zijn kosteloos beschikbaar. Voor IPv4-adressen moet ondertussen steeds meer worden betaald. Dit zorgt voor een toetredingsdrempel voor nieuwe (innovatieve) dienstaanbieders. Denk aan een nieuwe internetprovider die om te beginnen veel IPv4-adressen nodig heeft. Uiteindelijk zorgt het ervoor dat eindgebruikers minder keuze hebben en een hogere prijs betalen.

Directere en snellere dienstverlening
Met IPv6 kan ieder apparaat, en daarmee iedere gebruiker, op internet over een eigen adres beschikken. Dit in tegenstelling tot IPv4 waar schaarste providers dwingt om zuinig met deze adressen om te gaan. Gebruikers delen hierdoor vaak één IPv4-adres met elkaar (via zogenaamde CGNAT-techniek). Met IPv6 kunnen diensten die 'end-to-end'-connectiviteit vereisen makkelijker worden geleverd, omdat gebruikers over een eigen IPv6-adres kunnen beschikken. Uit ervaringen van o.a. Facebook en LinkedIn blijkt bovendien dat het met meerdere gebruikers delen van IPv4-adressen ook ten koste gaat van de snelheid.

Tegengaan van fraude
Door het tekort aan IPv4-adressen is het steeds vaker zo dat er meerdere gebruikers schuilgaan achter één IPv4-adres. Dit bemoeilijkt fraudedetectie en -preventie. Maatregelen tegen één IPv4-adres zullen al snel niet alleen de fraudeur, maar ook andere legitieme gebruikers treffen. Dit speelt niet bij IPv6. Voor onder andere de Rabobank was dit een belangrijke drijfveer om IPv6 te implementeren.

2.3 Marktontwikkelingen

IPv6 kende jarenlang een zeer trage adoptie. Nederland deed het slechter dan ons omringende landen. Ondertussen zien we een opgaande trend in de markt.

Steeds meer internet access providers bieden ondersteuning voor IPv6. Ook grote providers zoals KPN en Ziggo doen dat, alhoewel nog niet al hun klanten IPv6 kunnen gebruiken (bijv. door oudere modems). KPN maakte onlangs bekend ook IPv6 aan te gaan bieden aan hun mobiele klanten. Bij iets meer dan 20% van de websitebezoeken wordt nu IPv6 gebruikt. Een jaar geleden was dat nog ongeveer 13%.

Op 25 november 2019 heeft RIPE NCC, de instantie voor IP-nummeruitgiftes in Europa, het Midden-Oosten en delen van Centraal-Azië, bekendgemaakt dat zij geen IPv4-nummers meer heeft om uit te geven. Dat betekent dat IPv4-adressen nu alleen tegen betaling op de markt aangeschaft kunnen worden. Een IPv4-adres heeft momenteel een marktwaarde van tussen de 10 en 20 euro.

3. IPv6 bij de overheid

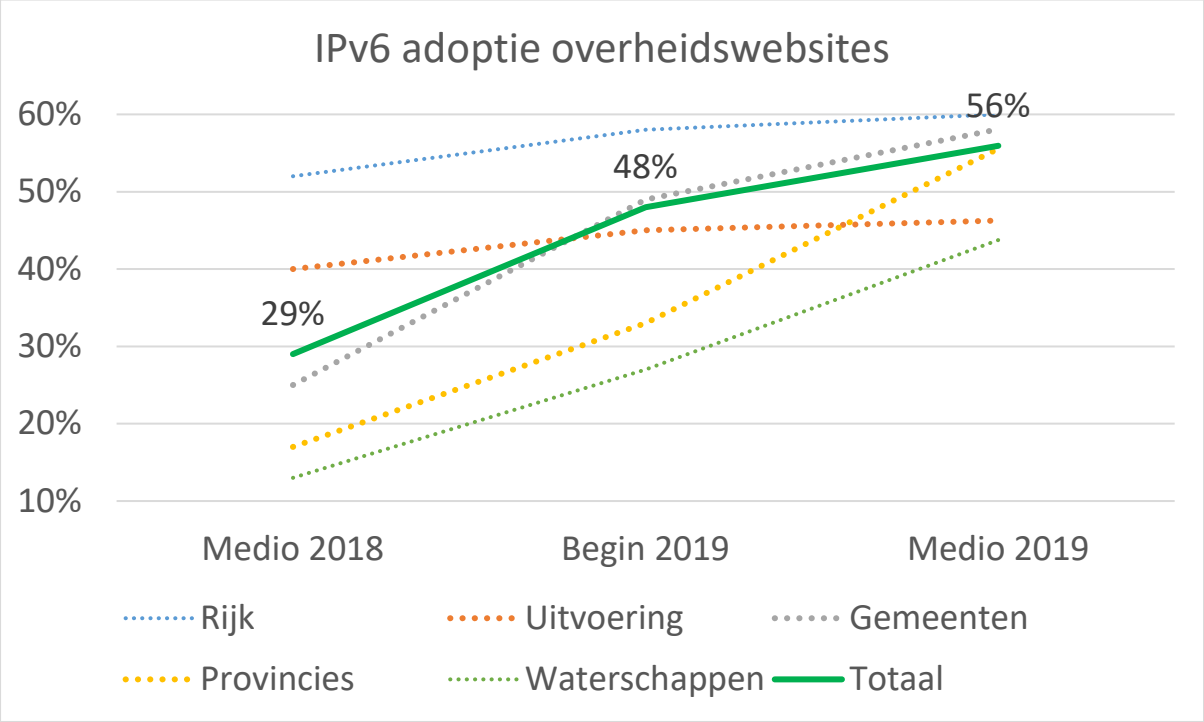
3.1 Pas toe of leg uit

Het Forum Standaardisatie heeft IPv6 in combinatie met IPv4 ('dual stack') in 2010 op de 'pas toe of leg uit-lijst geplaatst. Ondertussen hebben overheden 10 jaar de tijd gehad om websites en mailsystemen aan te schaffen die IPv6 ondersteunen.

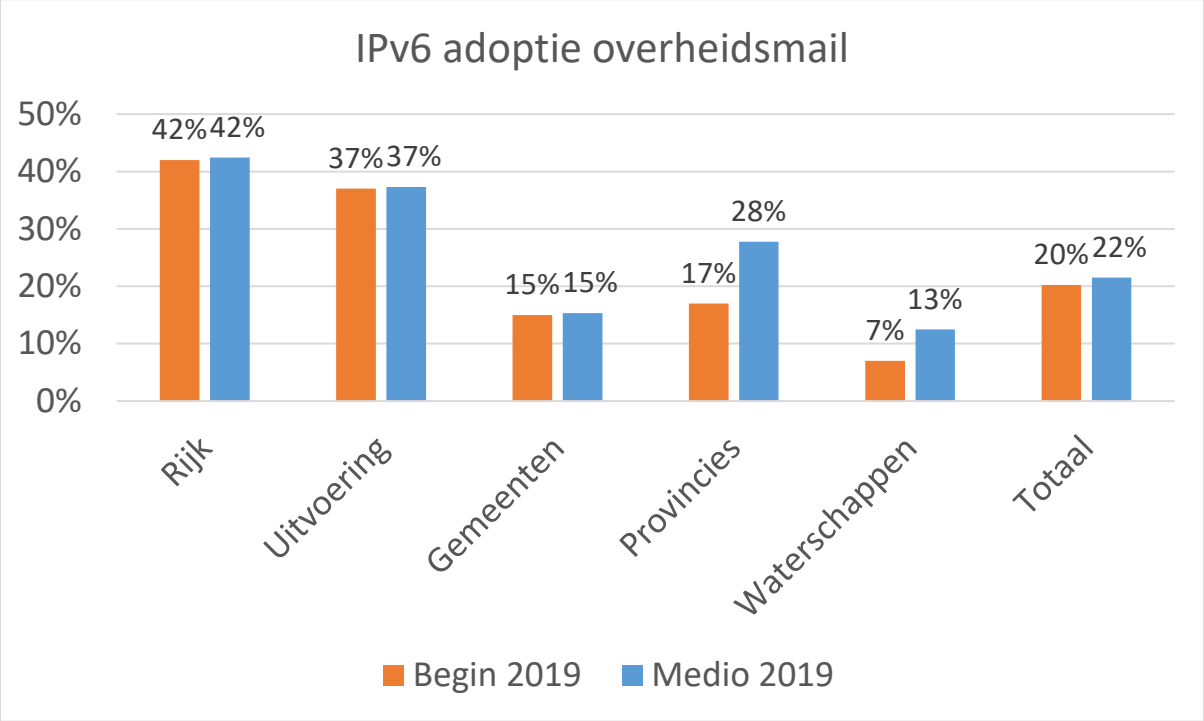
Uit de lopende evaluatie naar IPv6 die het Forum Standaardisatie uitvoert, komt ook het advies naar voren om voor IPv6 een overheidsbrede streefbeeldafspraak te maken. Het evaluatierapport dat daarnaast nog een aantal andere adoptieadviezen zal omvatten zal naar verwachting tijdens de volgende vergadering van het Forum Standaardisatie op de agenda staan.

3.2 Statistieken

IPv6 maakt reeds onderdeel uit van de testtool Internet.nl. Hierdoor zijn er door middel van 'bijvangst' al statistieken bekend van de IPv6 adoptie onder de 548 domeinen die deel uitmaken van de Meting Informatieveiligheidstandaarden. We zien dat er het laatste jaar met name voor overheidswebsites een flinke stijging waarneembaar is in de toepassing van IPv6. Dit laat zien dat de tijd nu rijp is om de adoptie een sterkere impuls te geven middels het maken van een streefbeeldspraak, zodat ook achterblijvers in beweging komen.



Bij overheidsmaildomeinen zien we dat de adoptie wat achterloopt ten opzichte van websites. Bij provincies en waterschappen is wel een duidelijke stijging zichtbaar in het laatste half jaar.



Hoe meten we IPv6 adoptie
De meting wordt uitgevoerd middels een bulktoets via de API van Internet.nl. Voor de webserver wordt het hoofddomein getoetst met de toevoeging www. (dus bijv. www.forumstandaardisatie.nl), omdat het gebruikelijk is dat de website daarop bereikbaar is. Voor de maildomeinen wordt getoetst zonder enig voorvoegsel omdat dat doorgaans gebruikt wordt als e-maildomein (dus @forumstandaardisatie.nl).

- In totaal zijn in deze meting 548 domeinnamen van overheidsorganisaties getoetst, bestaande uit:
- Domeinen die horen bij de deelnemers van het OBDO;
- De domeinen die horen bij voorzieningen van de basisinfrastructuur (GDI);
- De 30 best bezochte domeinen van Rijksoverheden (en uitvoerders);
- De domeinen van de andere overheidsorganisaties die direct of indirect vertegenwoordigd zijn in het OBDO, zoals:
    - Uitvoerders (de Manifestpartijen);
    - Partijen die behorend tot Klein LEF;
    - Gemeenten;
    - Provincies;
    - Waterschappen.

4. Eerdere 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

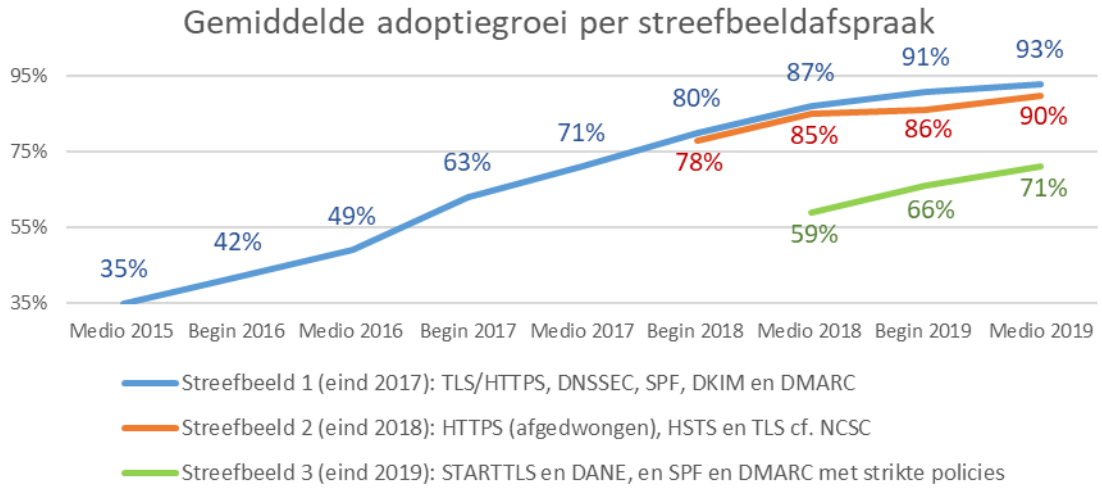
investeringsmoment en dan de standaarden implementeren), maar dat actief wordt ingezet op implementatie van de standaarden op de kortere termijn. Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. De halfjaarlijkse Meting Informatieveiligheidstandaarden is ook onderdeel van de jaarlijkse Monitor Open standaarden beleid.

De eerste streefbeeldafspraak is eind 2017 afgelopen. Begin 2018 is een eindmeting voor deze afspraak gepubliceerd. Ondanks een grote stijging de afgelopen twee jaar 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 werd geconcludeerd dat de streefbeeld-afspraak 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 tweede en derde streefbeeldafspraakis de groei in adoptie van de standaarden duidelijk zichtbaar in de metingen (zie onderstaande grafiek).



bijlage 1D - standaardisatie

Van: Forum Standaardisatie
Aan: ICT opdrachtgevers overheid

Betreft: Concept opdracht aan ICT-mail-leverancier/SSC's om stapsgewijs anti-*phishing* standaard (DMARC) streng af te stellen

Opdrachtomschrijving implementatie strikte DMARC policy aan gemeenschappelijke ICT-dienstverleners

Inleiding

Uit de meest recente Meting Informatieveiligheidstandaarden blijkt dat de anti-spoofing e-mailstandaard DMARC is op slechts 49% van de overheidsdomeinen voldoende strikt is geconfigureerd. Binnen het Rijk gaat het om 53% van de domeinen waarbij DMARC voldoende strikt zijn geconfigureerd. Dat betekent dat de andere helft van die overheidsdomeinen nog steeds kan worden misbruikt door fraudeurs. Phishing mails namens die organisaties (inclusief bewindspersonen) komen daardoor nog steeds bij burgers en bedrijven aan.

Informatieveiligheidstandaarden staan al enkele jaren op de 'pas toe of leg uit'-lijst en zijn daarmee conform de Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten verplicht.

Aanvullend zijn er overheidsbreed adoptieafspraken gemaakt om de adoptie te versnellen: https://www.forumstandaardisatie.nl/thema/meting-informatieveiligheidstandaarden-en-adoptieafspraken

Daarnaast zijn de informatieveiligheidstandaarden verankerd in de Baseline Informatiebeveiliging Overheid (BIO) via maatregel 13.2.3.1. De BIO vervangt de BIR: https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html#d17e150

We zien dat gemeenschappelijke IT-dienstverleners (shared service centers) een versnellend effect kunnen hebben op de adoptie van informatieveiligheidstandaarden. Zo is bij het Rijk een meetbare verbetering in de toepassing van webstandaarden zichtbaar, namelijk van 76% naar 90% in een half jaar tijd, doordat CIO BZK aan SSC-ICT opdracht heeft gegeven een significant aantal webdomeinen in samenhang te laten voldoen aan de informatieveiligheidstandaarden. Om deze reden zien wij een kans om ook in de adoptie van mailstandaarden verschil te maken door aan de gemeenschappelijke IT-dienstverleners opdracht te geven om hun klanten proactief te helpen om domeinnamen te beschermen tegen phishing met een strikte DMARC-policy.

Nut van een strikte DMARC policy

Een strenge configuratie van DMARC voorkomt dat phishing-mail waarbij het afzenderadres van een overheidsorganisatie wordt misbruikt, aankomt bij een eindgebruiker. Naast dat toepassing van informatieveiligheidstandaarden hoort bij goed huisvaderschap, kan een strikte DMARC policy een kwantitatieve besparing opleveren. Via DMARC kan worden ingesteld wat de mailserver moet doen als die een verdachte e-mail ontvangt. Zo zag KPN na activering van actieve DMARC policy naast minder gespoofde e-mails ook een reductie in het aantal helpsdesk calls. PostNL zag het aantal phishing-

gerelateerde vragen bij hun klantenservice met 54% dalen nadat zij hun DMARC policy hadden ingesteld op ‘reject’.

Met actieve DMARC policies kan spoofing van overheidsdomeinen goed worden aangepakt. In onze metingen zien we echter dat slechts 53% van e-maildomeinen binnen het Rijk actieve DMARC policies heeft ingesteld (quarantaine of reject). Gespoofde mails verzonden namens domeinen zonder deze DMARC policies komen dus nog steeds aan.

Rol van gemeenschappelijke ICT-dienstverleners

De overheid heeft een verantwoordelijkheid voor de domeinen waarvoor zij kantoormail beheerd, wat het lastiger maakt is dat er vaak ook andere mailstromen zijn (nieuwsbrieven, facturen, etc.). Klanten hebben in de meeste gevallen zelf niet de kennis om DKIM, SPF en DMARC goed te laten configureren voor haar maildomeinen en mailstromen. SSC’s kunnen aan de hand van DMARC-rapportages de legitieme mailstromen in kaart brengen en er met de klant voor zorgen dat deze netjes SPF en DKIM doen. Zodra dat is gedaan kan er een actieve DMARC policy worden ingesteld waarmee mailspoofing en mailphishing actief wordt bestreden.

Gemeenschappelijks dienstverleners moeten hier centraal de lead in nemen, en proactief aan de slag gaat om de DMARC instellingen voor (en mét) haar klanten veilig in te stellen. Dit kan door opdracht te geven om onderstaand stappenplan uit te voeren voor alle maildomeinen die in beheer zijn bij de shared service organisaties.

Stappen om tot een strikte DMARC policy te komen

Middels onderstaand stappenplan kan een ICT-dienstverlener klanten helpen van een passieve DMARC policy naar een veilige DMARC policy te komen om spoofing te voorkomen. Maak tevens gebruik van de adviezen van het NCSC en de IBD, en eventueel de how-to van Platform Internetstandaarden:

- https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing
- https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/06/20160602_Factsheet_emailauthenticatie_v1.01.pdf
- https://github.com/internetstandards/toolbox-wiki/blob/master/DMARC-how-to.md

1. SPF, DKIM en DMARC (none) records instellen voor zover dat nog niet was gedaan

Overheidsorganisaties dienen een DMARC-record toe te voegen aan hun DNS-systeem met parameter ‘p=none’ om de uitgaande e-mailstromen per domein te kunnen onderzoeken. Configureer het DMARC-record zodanig dat de terugkoppelingen (DMARC-rapportages) van de e-mailproviders verzameld wordt ten behoeve van de analyse. Opmerking: Voor het analyseren van de DMARC-rapportages van de e-mailproviders, bijvoorbeeld voor het identificeren van de e-mailstromen, is specifieke kennis en tooling nodig zodat deze (eenvoudig) geïnterpreteerd kunnen worden.

Technische richtlijnen:

- (Algemeen) Gebruik voor inactieve domeinnamen geen DKIM, maar wel DMARC en SPF.
- (SPF) Controleer of het SPF-beleid al is toegevoegd aan een domeinnaam door het TXT-record in de DNS op te zoeken. Publiceer een SPF-beleid als een TXT-record in de DNS-zone van de desbetreffende domeinnaam. Maak gebruik van een softfail-policy om false positives te voorkomen. Zorg daarnaast dat voor alle domeinnamen waarvandaan in het geheel geen mail wordt verstuurd,

een SPF-beleid is opgenomen met waarde ' v=spf1 –all' om misbruik ervan zoveel mogelijk tegen te gaan.
- (DKIM) Genereer publieke en private sleutels (van minstens 2048 bit RSA). Voeg de publieke sleutel toe als een TXT-record aan de DNS-zone van de desbetreffende domeinnaam. Zorg dat de Signing identity (d=) exact overeenkomt met de From: header-domeinnaam, vergelijkbaar met strikte alignment in DMARC. Gebruik een apart sleutelpaar en een aparte selector per organisatie en genereer regelmatig (bijvoorbeeld twee keer per jaar) een nieuw sleutelpaar om de DKIM-handtekening mee te maken.
- (DMARC) Zorg dat de 'identifiers' op elkaar afgestemd zijn, zodat de 'Identifier Alignment'-controle van DMARC succesvol zal zijn. Dit zijn de velden die gebruikt worden ter authenticatie. De RCF5322.From domain en SPF- en DKIM-domeinnamen moeten overeenkomen. De 'Strict'-modus vereist een exacte overeenkomst, de 'Relaxed'-modus een overeenkomst op basis van domeinnaam.

2. Analyse van de DMARC rapportages om (legitieme) mailstromen te identificeren

In deze stap dient een overzicht te worden gecreëerd van de domeinnamen, e-mailstromen en soorten e-mailberichten. Dit overzicht omvat zowel domeinnamen waarvandaan e-mailberichten worden verstuurd als domeinnamen waarvandaan nooit e-mailberichten worden verstuurd. Om een zo compleet mogelijk beeld te vormen van de e-mailstromen dient de terugkoppeling van de e-mailproviders gedurende een periode van 6 tot 8 weken gelogd en geanalyseerd te worden. Veel van deze informatie zal binnen de gemeente aanwezig zijn. Denk hierbij aan de volgende e-mailstromen: Ketenpartners; Leveranciers; Kantoormail; Afsprakenmodules van klantcontactcentra (KCC) en Nieuwsbrieven.

Identificeer per domein welke e-mailstromen legitiem zijn ten behoeve van opname in het SPF-record. Deze configuratie zal goed gemonitord dienen te worden om mogelijke problemen snel te detecteren en op te lossen.

3. In samenspraak met de klant verbeteren van het SPF record, en implementeren van DKIM bij verzendende mailservers, voor het klantdomein ten behoeve van legitieme mailstromen

Gebruik de rapportages om e-mailstromen die niet voldoen aan het SPF- en DKIM-beleid te verhelpen en 'identifier alignment'-problemen te corrigeren. Dit is ook een gelegenheid om e-mail te herkennen die wel SPF-controles doorkomt, maar niet voldoet aan het DKIM-beleid. Deze e-mails zullen ongetwijfeld problemen opleveren bij forwarding. Om de analyse te vergemakkelijken kunnen tools gebruikt worden.

DKIM dient geïmplementeerd te worden bij alle mailservers die namens het domein mail verzenden. De toepassing van DKIM vergt meer middelen dan de toepassing van SPF. Om DKIM toe te passen dient er vaak aanvullende software geïnstalleerd worden op de e-mailserver.

4. DMARC policies naar quarantaine, en actief blijven monitoren of legitieme mailstromen als spam worden aangemerkt (zo ja, zie 3)

Op het moment dat inzicht is in de legitieme e-mailstromen kan na verloop van tijd het beleid worden aangescherpt van accepteren (p=none) naar als spam markeren (p=quarantaine).

Zijn voor een bepaalde domeinnaam alle mailservers opgenomen in het SPF-beleid en wordt al het e-mailverkeer ondertekend met DKIM, publiceer dan een policy 'quarantine' met een kleine waarde voor 'pct'. Debug false positives (wegens gemiste mailstromen) en schroef de waarde van 'pct' langzaam op. Staat 'pct' op een waarde van 100 zonder nadelige effecten, publiceer dan een policy 'reject' met een kleine waarde voor 'pct'. Herhaal de debugging en pas de waarde aan. Het doel is om uiteindelijk zoveel mogelijk mailstromen te laten authenticeren door ze 'reject' als beleid mee te geven.

5. Bij voldoende zekerheid dat legitieme mail niet als spam wordt aangemerkt DMARC policy naar reject

Uiteindelijk kan het beleid nog verder worden aangescherpt naar NIET accepteren, door voor het betreffende domein het DMARC-beleid in te stellen op ‘p=reject’ op het moment dat er sprake is van afwijkingen.

6. Bij voortduring blijven monitoren van de DMARC rapportages

De implementatie, configuratie en gebruik van de e-mailauthenticatiemiddelen zal gemonitord moeten worden om effectief te zijn. Let onder andere op misbruik van een domeinnaam, problemen met geautoriseerde verzenders en aanpassingen aan e-mailservers.

Domeinen zonder e-mail

Wanneer je voor een domeinnaam geen e-mail wil gebruiken, gebruik dan de volgende instellingen:

- Plaats een zogenaamd “null MX” record in de DNS zone.
- Plaats een “SPF -all” record in de DNS zone.
- Plaats een “DMARC p=reject” record in de DNS Zone.
- Plaats geen DKIM record.

Nadere informatie

https://www.forumstandaardisatie.nl/standaard/dmarc

notitie

Standaardisatie
Bijlage 2 - Mutaties lijsten open standaarden

Hamerstuk
U wordt gevraagd om in te stemmen met het volgende advies / de volgende adviezen.

A. Het OBDO stemt in met de plaatsing van de GWSW op de ‘pas toe of leg uit’-lijst.

B. Het OBDO stemt in met de plaatsing van de OIDC op de lijst van aanbevolen standaarden.

Ad. A) Plaatsing van GWSW op de ‘pas toe of leg uit’-lijst (standaard voor eenduidige uitwisseling en hergebruik van gegevens in het stedelijk waterbeheer)

Het OBDO wordt gevraagd om in te stemmen met de volgende adviezen:
A Het OBDO stemt in met de plaatsing van de GWSW op de ‘pas toe of leg uit’-lijst.

Voor de Nederlandse overheid wordt het beheer van stedelijk water en riolering van digitale gegevensuitwisseling steeds belangrijker. De maatschappelijke opgaven zoals klimaatadaptatie, energietransitie en de bouwopgave vereisen een (digitale) integrale aanpak, waarbij gezamenlijke gegevensdefinities een voorwaarde zijn. Zo zijn er meerdere ketenpartijen betrokken bij het beheer van stedelijk water en riolering, zoals gemeenten, bedrijven en waterschappen. Het doelmatig managen van (afval)watersystemen vereist een gemeenschappelijk taal. De open standaard GWSW (Gegevenswoordenboek Stedelijk Water) is die gezamenlijke taal. Het GWSW geeft significante verbeteringen aan het gegevensbeheer met betrekking tot het gezamenlijk beheren van stedelijke (afval)watersystemen. GWSW maakt het mogelijk om diverse objecten die een rol spelen bij waterbeheer te visualiseren op een gebiedskaart, bijvoorbeeld uitlaten en pompen. Het uitwisselen van gegevens tussen beheersystemen onderling wordt makkelijker en het berekenen van de watercapaciteit gaat spoediger. De standaard draagt daarmee bij aan interoperabiliteit in de benodigde informatievoorziening rondom waterbeheer. GWSW wordt beheerd door Stichting RIONED, een non-profitkoepelorganisatie namens alle belanghebbenden in het stedelijke waterbeheer. Stichting RIONED ziet het meerjarig beheer en doorontwikkeling van GWSW als een van haar kerntaken. Het is een vast onderdeel van de meerjarenbegroting van de Stichting, ook voor de komende jaren. Het Fonds Collectieve Kennis Civiele Techniek erkent en ziet het GWSW als een belangrijk product voor het werkveld. Afgelopen tien jaar hebben Stichting RIONED en het FCK-CT (deelprogramma Objectinformatie) samen het onderzoeks- en ontwikkelprogramma van het GWSW gefinancierd. RIONED voert momenteel ook een onderzoek uit naar hoe er een robuuste (deel)financiering van het GWSW kan komen, zonder daarbij het karakter van een open standaard volgens de richtlijnen van het Forum Standaardisatie en BOMOS aan te tasten. Stichting RIONED heeft tevens recentelijk een kosten-batenanalyse gerealiseerd om de businesscase voor ontwikkeling en implementatie van het GWSW verder te verduidelijken[1].

Advies en gevraagd besluit

Na consultatie van onafhankelijke experts en organisaties die door de standaarden geraakt worden, adviseert het Forum Standaardisatie om de standaard op de ‘pas toe of leg uit’-lijst te plaatsen om daarmee verbetering te geven aan het gegevensbeheer met betrekking tot het gezamenlijk beheren van stedelijke (afval)watersystemen, maar wel beperkt tot de inzameling en het transport van overtollig grondwater (conform de gemeentelijk watertaken, zoals vastgelegd in de Waterwet).

Het volledige Forumadvies van GWSW is te vinden op de website van het Forum Standaardisatie.

[1] Business case voor uniforme gegevensuitwisseling op basis van het GWSW en meerjarig beheer en doorontwikkeling GWSW

Ad. B) Plaatsing van OIDC op de lijst van aanbevolen standaarden (een open en gedistribueerde standaard om één authenticatiedienst naar keuze te kunnen hergebruiken)

Het OBDO wordt gevraagd om in te stemmen met de volgende adviezen:
B) Het OBDO stemt in met de plaatsing van de OIDC op de lijst van aanbevolen standaarden.

De Wet digitale overheid heeft als doel het regelen van het veilig en betrouwbaar kunnen inloggen voor Nederlandse burgers en bedrijven bij de (semi-)overheid. Deze wet beschrijft waaraan digitale publieke diensten en authenticatie voorzieningen moeten voldoen en maakt het voor publieke dienstverleners verplicht authenticatie voor hun elektronische diensten aan te bieden middels DigiD en een privaat alternatief voor DigiD, zoals bijvoorbeeld iDIN. Daarnaast legt de Europese eIDAS-verordening diezelfde partijen de verplichting op om authenticatiemiddelen uit het buitenland (onder voorwaarden) te accepteren. Vanuit het programma eID is voorgesteld om een routeringsvoorziening te realiseren waar alle overheidsorganisaties gebruik van kunnen maken. Dienstverleners in de eID-governance hebben aangedrongen op het in eerste instantie aanbieden van het DigiD-SAML koppelvlak. Het DigiD-SAML koppelvlak volstaat echter niet om de gehele set aan technische en functionele wensen van de publieke dienstverleners in de eID-governance te kunnen bieden op langere termijn. Hiervoor heeft de eID governance opgeroepen om niet een nieuw koppelvlak te baseren op SAML (een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen), maar op de open standaard OpenID Connect (OIDC). OIDC geeft apparaten en programma's de mogelijkheid om de identiteit van een eindgebruiker te controleren gebaseerd op verschillende authenticatieservices (zoals DigiD), waarbij profielinformatie van de eindgebruiker volgens een gestandaardiseerde wijze beschikbaar wordt gesteld aan de daarvoor geautoriseerde apparaten en programma's. OIDC lost een interoperabiliteitsprobleem op dat ligt bij de mobiele apps en machtigen van anderen om in te loggen op digitale publieke diensten en websites.

Advies en gevraagd besluit

Na consultatie van onafhankelijke experts en organisaties die door de standaarden geraakt worden, adviseert het Forum Standaardisatie om de standaard op de lijst van aanbevolen standaarden te plaatsen. Belangrijkste redenen zijn de beperkte doorontwikkeling van de SAML standaard en juist de actieve ontwikkelingen binnen de OIDC standaard. Verder vormen de eenvoud en de ondersteuning van de 'mobile-first' strategie van diverse dienstverleners belangrijke redenen hiervoor. Daarnaast zorgt de plaatsing van OIDC voor een impuls in de ontwikkeling om een breed gedragen Nederlands profiel te ontwikkelen voor OIDC. Dit breed gedragen Nederlands profiel zal dan moeten worden aangedragen voor plaatsing op de 'pas toe of leg uit'-lijst.

Het volledige Forumadvies van OIDC is te vinden op de website van het Forum Standaardisatie.