Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aanbiedingsformulier
Overheidsbreed Beleidsoverleg Digitale Overheid

Agendapunt **Onderwerp**	5a Standaardisatie: Meting Informatieveiligheidsstandaarden medio 2023
Datum behandeling	30 november 2023
Sponsors **Betrokken partijen**	
Contactgegevens	Organisatie : Forum Standaardisatie Contactpersoon : Bart Knubben (adviseur)/ Ludwig Oberendorff (hoofd BFS) Telefoonnummer : 06-21162373/ 06-52311217 E-mailadres :
Doel van de behandeling (dubbelklikken op vakje en 'ingeschakeld' aanvinken)	☐ Ter bespreking/discussie/meningvormend ☒ Ter besluitvorming ☐ Hamerstuk ☐ Ter advies naar eigenaar/OBDO/staatssecretaris/… ☐ Ter informatie, agendapunt wordt toegelicht ☐ Ter kennisname, agendapunt wordt niet behandeld
Eerder behandeld in Datum behandeling: Uitkomst behandeling: Resultaat toets: Gemaakte afspraken:	☐ Directeurenoverleg DO ☐ IDO ☐ Programmeringsraad GDI ☐ Anders:SO OBDO en Forum Standaardisatie ☐ MT DO|DS|CIO Rijk ☐ Overeenstemming ☐ Geen overeenstemming N.a.v. eerdere Informatie Veiligheid (IV)-Metingen maakte OBDO de volgende afspraken: • 1 december 2022: CIO-Rijk (trekker) i.s.m. BZK, VNG en Manifestgroep maken plan van aanpak waarbij nader bekeken wordt wat de meest impactvolle maatregel is. Hierbij kan als uitgangspunt de best practice VWS worden gebruikt. Vervolgens wordt het wederom ter bespreking geagendeerd. Dit maakt dat er collectief gestuurd worden. • 7 april 2022: - Verzoek aan MinBZK om een verdergaande verplichting van IPv6 voor websites en e-mail te realiseren, bijv. op basis van de Wet digitale overheid (Wdo) - IPv6 na 12 jaar pas-toe-of-leg-uit beleid en streefbeeld afspraak (eind 2021) onvoldoende om achterblijvers over de streep te trekken. Voorafgaand aan verplichting middels Wdo de tussenstap: de voorzitter neemt contact op met de ADR (voor de Rijksonderdelen), en er komt een 'naming & shaming' volgorde in de rapportage van achterblijvers. • 19 november 2020: Opdracht geven binnen eigen cirkel voor compliance aan alle standaarden (informatieveiligheid én IPv6), bijzondere aandacht voor de veilige configuratie van TLS (HTTPS) en STARTTLS.

	26 november 2019: Aanspreken achterblijvers binnen eigen cirkel t.a.v. de eerdere streefbeeldafspraken (deadlines eind 2017 en 2018).
Discussiepunten **Beslispunten**	Het OBDO neemt kennis van de 'Meting Informatieveiligheidstandaarden medio 2023', en neemt besluitvorming over de onderstaande adviezen van Forum Standaardisatie. Omdat – ondanks de wettelijke verplichting van 1 juli 2023 – geen significante voortgang te zien is, wordt voorgesteld deze adviezen over te nemen. **Advies 1**: Stuur als OBDO op de adoptie bij achterblijvers, door het gezamenlijke Plan van Aanpak (CIO-Rijk in afstemming met VNG en Manifestgroep) af te ronden en uit toe voeren, waartoe in de decembervergadering werd besloten. Neem een planning met deadlines op in dat plan. **Advies 2:** Maak duidelijk dat de organisaties zelf aan de slag moeten (eigen mandaat), maar benoem telkens op 'koepel-niveau' ook een programmamanager van formaat. Een voorbeeld kan genomen worden aan de aanpak van de ministeries van AZ, SZW, VWS, BZK, en EZK. Zo'n aanpak leidt telkens tot zeer grote verbeteringen. **Advies 3:** Organiseer regie op internetdomeinen binnen individuele overheidsorganisaties. Zet in op een groeistop van het domeinnaamportfolio en stuur idealiter op een inkrimping. **Advies 4:** Zorg ervoor dat de ondersteuning van verplichte open standaarden onderdeel zijn van het leveranciersmanagement van individuele overheidsorganisaties. Vraag leveranciers periodiek naar de planning voor ondersteuning van standaarden. Overweeg om over te stappen als een leverancier onvoldoende meebeweegt. **Advies 5:** Gebruik de collectieve slagkracht van de overheid om grotere leveranciers en techgiganten te bewegen naar adoptie van alle verplichte standaarden, bijvoorbeeld via Strategisch Leveranciersmanagement (SLM) Rijk.
Financiële consequenties Kosten: Dekking:	 Eenmalige kosten : Jaarlijks terugkerende kosten : ☐ Ja ☐ Nee ☐ Gedeeltelijk
Leeswijzer	
Toelichting Ruimte voor aanleiding, voorgeschiedenis, samenvatting, relevante context, zoals betrokken (inter)nationale wet- en regelgeving, vervolgproces.	[bijlage 1a. rapport meting informatie veiligheid standaarden medio 2023. In het rapport is een link opgenomen naar bijlage 1b. met individuele detailresultaten] **Overheidsbreed zijn afspraken gemaakt om moderne internetstandaarden voor websites en e-mail versneld te adopteren**. Forum Standaardisatie meet op verzoek van het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) halfjaarlijks de implementatievoortgang van deze afspraken. De afgesproken uiterlijke implementatiedata zijn voor alle standaarden (met uitzondering van RPKI) al verstreken, waardoor verwacht mag worden dat alle webapplicaties en e-mailsystemen deze standaarden correct toepassen. De vorige IV-meting was van januari 2023 (25 mei in OBDO). In dit document wordt gerapporteerd over de stand van zaken per 1 juli 2023.

	In de zomer van 2023 is de analyse uitgevoerd. In aanloop naar het OBDO worden deze resultaten gedeeld, inclusief de mogelijkheid om (desgewenst) opmerkingen over oorzaak of context integraal als citaat in de definitieve rapportage op te laten nemen, waarna deze openbaar wordt. **Overheden die internetdomeinen niet veilig configureren nemen onnodige risico's**. Het gaat daarbij om een verhoogde kans op phishing, fake-news en ransomware uit naam van overheidsorganisaties, en een verhoogde kans op manipulatie en afluisteren van web- en e-mailverkeer. Zonder toepassing van de standaarden is het bijvoorbeeld een fluitje van een cent om een e-mail te versturen vanaf het mail-adres van een bestuurder of bewindspersoon. Een prominent voorbeeld van de gevolgen van onveilige configuratie van standaarden is een incident van e-mailphishing namens @overheid.nl in het verleden, toen van 200 burgers DigiD-inloggegevens zijn buitgemaakt. Hoe meer domeinnamen voldoen aan de standaarden, hoe kleiner de kans is dat dergelijke incidenten zich voordoen. **Verzwaring regime: HTTPS/HSTS wettelijk verplicht per 1 juli** Twee informatieveiligheidstandaarden, die de authenticiteit en vertrouwelijke communicatie met een website regelen ('het slotje op de website': HTTS/HSTS), zijn sinds 1 juli 2023 wettelijke verplicht. Het afzenderschap van rapportages over compliance van deze wettelijke verplichting komt bij BZK te liggen. Mede om de verzwaring van het regime te onderstrepen. Deze meting kan daarvan als 0-meting worden gezien. Om de voortgang ten opzichte van vorige IV-metingen in kaart te brengen, zijn de metingen over deze standaarden op geaggregeerd niveau in deze meting meegenomen. Gelet op het organisatorisch- en functioneel werkingsgebied van de wettelijke verplichting zijn er dit keer meer internetdomeinen in de meting meegenomen: 5206 in plaats van 2654 (zowel het domein met, als zonder "www"). Nota bene: het betreft nog steeds niet alle internetdomeinen van de overheid waarvoor de wettelijke verplichting geldt (daar is geen goed overzicht van, en loopt in de 10-duizenden). **Samenvattende bevinding:** Ondanks de lichte verbetering van enkele procentpunten is er een aanzienlijk deel (namelijk een derde deel tot de helft) van de domeinnamen dat achterblijft en de IV-standaarden nog niet goed toepast. Voor de standaarden die sinds 1 juli 2023 wettelijk verplicht zijn, blijft ongeveer een kwart van de domeinnamen achter.

Forum Standaardisatie
Standaard Samenwerken

Meting Informatieveiligheidstandaarden overheid medio 2023

Inclusief IPv6

Datum document: 09-11-2023

Status document: versie OBDO

Inhoudsopgave

Leeswijzer

Dit rapport is piramidaal gestructureerd en begint in hoofdstuk 1 met de conclusies, adviezen, en het totaalbeeld.

Hoofdstuk 2 en 3 gaan in op het algehele beeld rond de adoptie van respectievelijk websitebeveiligingsstandaarden en e-mailbeveiligingsstandaarden.

Hoofdstuk 4 gaat in op de adoptie van IPv6 voor websites en e-mail.

Hoofdstuk 5 gaat in op de adoptie van RPKI voor websites en e-mail.

Hoofdstuk 6 en 7 gaan dieper in op de adoptiegraad per standaard van respectievelijk de verschillende overheidscategorieën en ministeries.

Hoofdstuk 8 beschrijft de achtergrond van de meting, waaronder de beleidsmatige afspraken, desbetreffende standaarden en de methodiek.

De bijlage geeft een detailinzicht per internetdomein, gecategoriseerd naar overheidscategorie of ministerie.

1. Samenvatting

Overheidsbreed zijn afspraken gemaakt om moderne internetstandaarden voor websites en e-mail versneld te adopteren. Forum Standaardisatie meet op verzoek van het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) halfjaarlijks de implementatievoortgang van deze afspraken. De afgesproken uiterlijke implementatiedata zijn voor alle standaarden al verstreken, waardoor verwacht mag worden dat alle webapplicaties en e-mailsystemen deze standaarden correct toepassen. In dit document wordt gerapporteerd over de stand van zaken per 1 juli 2023. In juli en augustus van 2023 is de analyse uitgevoerd en zijn eventuele correcties doorgevoerd. Bij de totstandkoming van dit rapport lag de focus op het automatiseren van de rapportage en het verhogen van datakwaliteit. Zo is de ordening van de gemeten domeinnamen sterk verbeterd en zijn de meetresultaten extra gecontroleerd. Daardoor is de meting op dit moment nog niet via de samenwerkingsverbanden en koepels teruggelegd bij de organisaties van wie de domeinnamen zijn gemeten. Terugleggingen bij eerdere metingen waren vooral waardevol ter stimulering van de adoptie en zorgden in een klein aantal gevallen tot correcties, maar hebben toen niet geleid tot grote wijzigingen van de geaggregeerde resultaten. Ook deze meting zal nog worden teruggelegd. Eventuele correcties en ontvangen motivaties voor afwijking zullen in de uiteindelijke te publiceren versie van het rapport worden opgenomen.

Overheden die internetdomeinen niet veilig configureren nemen onnodige risico's. Het gaat daarbij om een verhoogde kans op phishing uit naam van overheidsorganisaties, en een verhoogde kans op manipulatie en afluisteren van web- en e-mailverkeer. Een prominent voorbeeld van de gevolgen van onveilige configuratie van standaarden is een incident van e-mailphishing namens *@overheid.nl* in 2018, toen van 200 burgers DigiD-inloggegevens zijn buitgemaakt. Hoe meer domeinnamen voldoen aan de standaarden, hoe kleiner de kans is dat dergelijke incidenten zich voordoen.

De meting laat zien dat bij 65% van de in vorige meting gemeten internetdomeinen alle verplichte website internetveiligheidstandaarden correct zijn toegepast (excl. IPv6 en RPKI). Dit is een stijging van 3 procentpunt ten opzichte van de vorige meting. Het gaat om belangrijke beveiligingsstandaarden voor vertrouwelijk webverkeer. Inclusief IPv6 voor duurzame bereikbaarheid van online diensten voldoet 59%, ook hier is de toename 3 procentpunt. RPKI laat een grote stijging van 8 procentpunt zien, 57% voldoet al aan de implementatieafspraken voor eind 2024 (excl IPv6, 52% incl. IPv6).

Bij 52% van de in vorige meting gemeten internetdomeinen zijn alle verplichte e-mailstandaarden correct toegepast (excl. IPv6 en excl. RPKI). Dit is hetzelfde percentage als de vorige meting. Hier gaat het om belangrijke beveiligingsstandaarden om e-mailvervalsing uit naam van de overheid te voorkomen en het e-mailverkeer vertrouwelijk te houden. Inclusief IPv6 voor duurzame bereikbaarheid van online diensten voldoet 50%, ook dit is hetzelfde percentage als de vorige meting. RPKI laat ook bij email een grote stijging

zien van 11 procentpunt, 59% voldoet al aan de implementatieafspraken voor eind 2024 (excl IPv6, 48% incl. IPv6).

Er zijn zeer kleine verbeteringen zichtbaar ten opzichte van de vorige meting. Dat komt slechts deels de toevoegingen van domeinnamen. Domeinnamen die niet eerder werden gemeten scoren slechter dan waarop al werd gemeten, er zijn veel misconfiguraties in niet hoofddomeinnamen, of domeinnamen die enkel doorverwijzen. Het consequent meten en publiceren van de compliance van internetdomeinen helpt dus.

In deze meting zijn in totaal 5206 overheidsdomeinen gecontroleerd. In de vorige meting waren dit 2654 overheidsdomeinen. Deze bijna verdubbeling komt voornamelijk door het toevoegen van alle domeinnamen met en zonder 'www'. Daarnaast is er een stijging van nieuw geregistreerde domeinnamen en oudere domeinnamen die pas later aan de domeinnaamportfolio's zijn toegevoegd. Dit zijn nog niet alle overheidsdomeinnamen, het totaalportfolio heeft vele duizenden meer domeinen. De overheid heeft als geheel geen zicht op het totaalportfolio. Dit rapport toont met diverse doorsnedes inzicht in de stand van zaken per overheidscategorie en per ministerie. De mate van adoptie kan gezien worden als een indicator voor de effectiviteit van sturing op kwaliteit van de informatievoorziening.

1.1. Adviezen

Net als in de vorige meting is de conclusie dat geen van de streefbeeldafspraken voor de overheid als geheel gehaald is. Het ontbreekt aan effectieve sturingsmechanismen om overheidsbrede afspraken eenduidig te laten landen en nageleefd te krijgen binnen alle individuele overheidsorganisaties. De op 1 juni 2023 van kracht zijnde Wet Digitale Overheid die de standaarden HTTPS en HSTS middels een AMvB wettelijk verplicht laat nog geen significante verandering in de adoptie van deze standaarden zien.

Advies 1: stuur als OBDO op de adoptie bij achterblijvers, door het gezamenlijke Plan van Aanpak (CIO-Rijk in afstemming met VNG en Manifestgroep) af te ronden en uit toe voeren, waartoe in de decembervergadering van december 2022 werd besloten. Neem een planning met deadlines op in dat plan (websites worden daarna afgesloten; dat leidt in 99% van de gevallen tot implementatie).

Advies 2: maak per individuele overheidsorganisatie een plan van aanpak om de streefbeeldafspraken effectief te laten landen in de uitvoering zodat de verplichte standaarden worden geïmplementeerd. Organisaties moeten zelf aan de slag (mandaat), maar benoem telkens op 'koepel niveau' ook een programmamanager van formaat. Een voorbeeld kan genomen worden aan de aanpak van de ministeries van AZ, BZK, EZK, SZW en VWS.

Advies 3: om de adoptieopgave behapbaar te maken en te houden, kan ook gekeken worden naar het beperken van het domeinnaamportfolio. Samenvoeging van verschillende websites, of het vaker inzetten van subdomeinen in plaats van nieuwe domeinnamen, verkleinen het digitale oppervlak waar de standaarden geïmplementeerd moeten worden. Het advies is in ieder geval om de registratie van nieuwe domeinnamen zoveel als mogelijk te beperken.

Als handreiking voor het beheersbaar maken van domeinnamen heeft Forum Standaardisatie vijf basisprincipes voor regie op internetdomeinen op een rij gezet. Voor de Rijksoverheid heeft het Rijksprogramma voor Duurzaam Digitale Informatiehuishouding (RDDI), in samenwerking met Forum Standaardisatie, in 2021 de Handreiking Beheer Internetdomeinen Rijksoverheid gepubliceerd. Deze informatie is ook in 2023 nog steeds actueel en kan helpen bij deze opgave.

Organiseer regie op internetdomeinen binnen individuele overheidsorganisaties. Zet in op een groeistop van het domeinnaamportfolio en stuur idealiter op een inkrimping.

Advies 4: Overheden besteden hun e-mailvoorzieningen steeds vaker uit aan clouddienstverleners. Een aantal van dit soort dienstverleners ondersteunen niet alle verplichte standaarden. Conform het open-standaardenbeleid zou formeel moeten worden gekozen voor dienstverlening die de standaarden wel ondersteunt. Indien hiervan is afgeweken is het belangrijk dat overheden hun dienstverleners alsnog blijven vragen om ondersteuning van verplichte standaarden. Diverse dienstverleners geven in informele gesprekken aan dat een gebrek aan klantvraag een reden is om niet te investeren in ondersteuning van de voor overheid verplichte standaarden.

Tegelijkertijd kan ook gezien worden dat grotere leveranciers moeilijk in beweging te krijgen zijn. Dit terwijl steeds meer overheidsonderdelen overstappen naar cloudoplossingen, zoals Microsoft 365 voor e-maildiensten. Deze beweging kan leiden tot een afname in adoptiegraad, wanneer de cloudoplossingen de verplichte standaarden niet ondersteunen.

Zorg ervoor dat de ondersteuning van verplichte open standaarden onderdeel zijn van het leveranciersmanagement van individuele overheidsorganisaties. Vraag leveranciers periodiek naar de planning voor ondersteuning van standaarden. Overweeg om over te stappen als een leverancier onvoldoende meebeweegt.

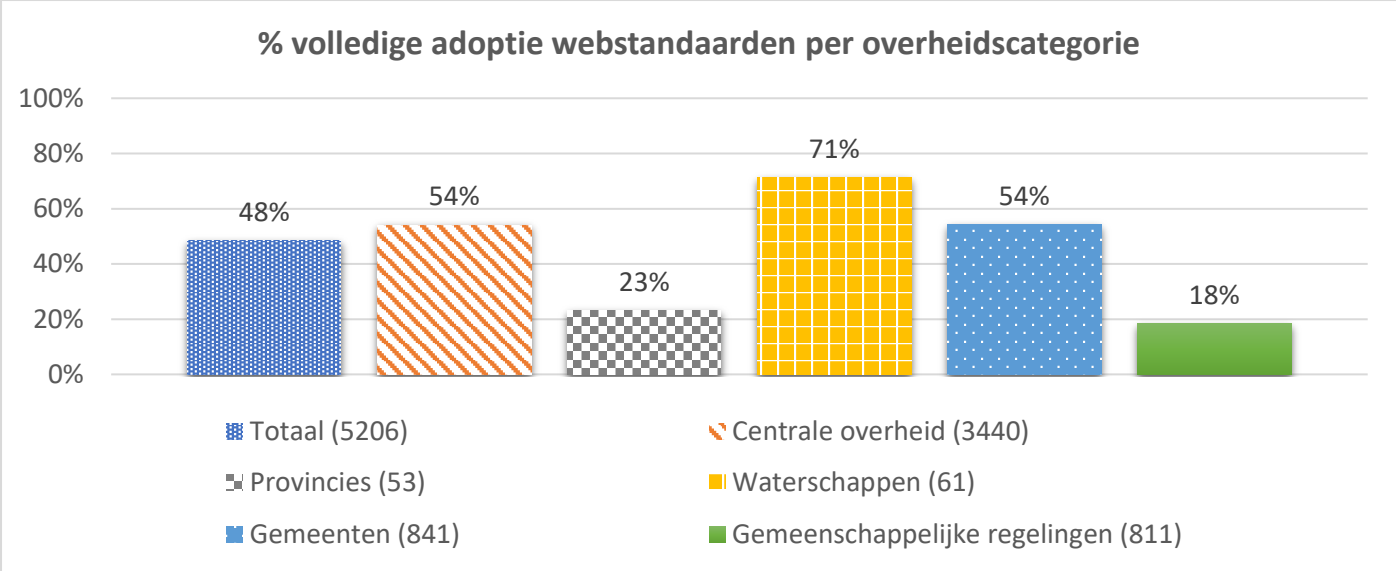
Advies 5: gebruik de collectieve slagkracht van de overheid om grotere leveranciers en techgiganten te bewegen naar adoptie van alle verplichte standaarden, bijvoorbeeld via Strategisch Leveranciersmanagement (SLM) Rijk.

1.2. Websitestandaarden

1.2.1. Totaalbeeld websites per overheidscategorie (incl. IPv6 en incl. RPKI)

Onderstaande cijfers laten zien in welke mate de domeinnamen van verschillende overheidscategorieën de afgesproken websitestandaarden voor veilig en modern webverkeer toepassen (exclusief IPv6 en RPKI). Gemeenten en waterschappen lopen gemiddeld gezien ver voor op de andere categorieën. De gemeenschappelijke regelingen lopen ver achter.

Hoofdstuk 2 gaat in meer detail in op de specifieke websitebeveiligingsstandaarden, hoofdstuk 4 gaat in op IPv6 en hoofdstuk 5 op RPKI.



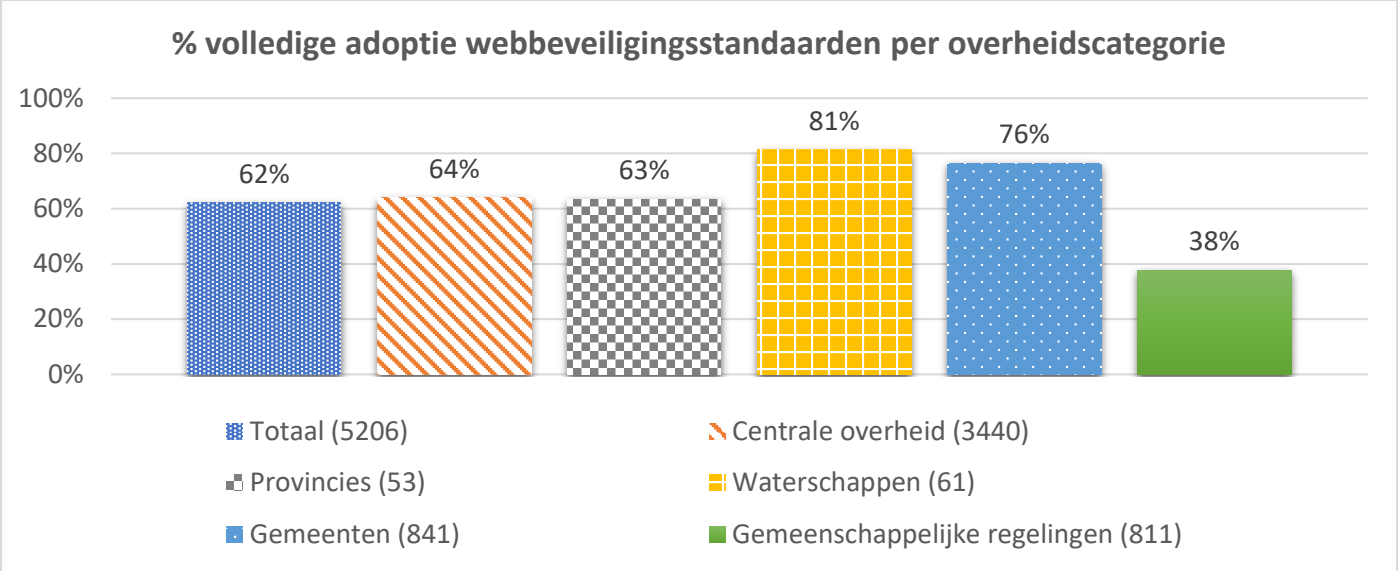
1.2.2. Websitebeveiligingsstandaarden (excl. IPv6 en excl. RPKI)

Door toepassing van websitebeveiligingsstandaarden wordt de verbinding met overheidswebsites beter beveiligd, zodat criminelen niet zomaar uitgewisselde gegevens kunnen onderscheppen of manipuleren.

Deze paragraaf laat het totaalbeeld per overheidscategorie en het totaalbeeld per ministerie zien (zonder IPv6 en zonder RPKI).

1.2.2.1. Adoptie per overheidscategorie

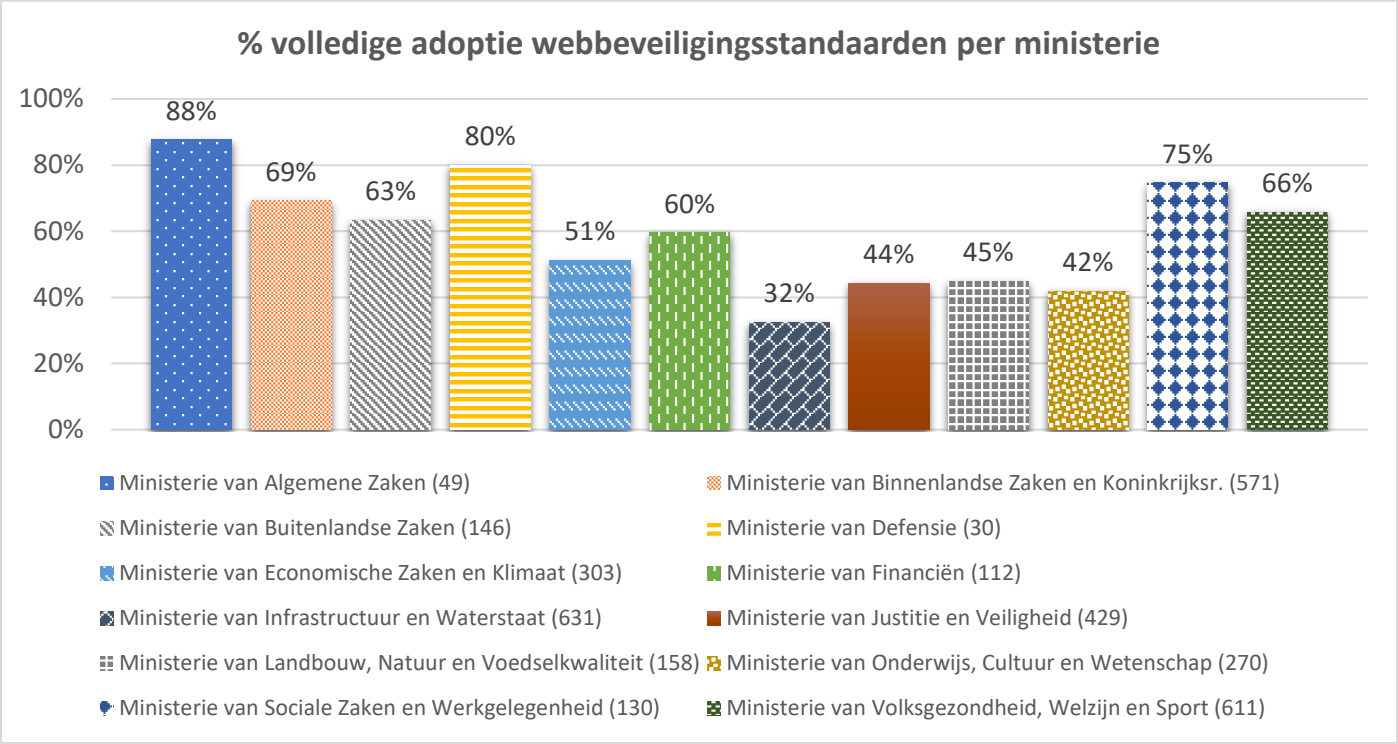
De achterblijvers zijn met name te vinden bij de centrale overheid en de gemeenschappelijke regelingen. De centrale overheid is getalsmatig oververtegenwoordigd in de meting doordat er veel secundaire internetdomeinen (campagnesites, projectsites, etc.) zijn meegenomen. Er is geen goed beeld van secundaire internetdomeinen van decentrale overheden, hoewel we weten dat gemeenten wel honderden websites in beheer kunnen hebben.



Voor meer details per overheidscategorie zie hoofdstuk 6.

1.2.2.2. Adoptie per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan vallen de ministeries van Algemene Zaken (88%), Defensie (80%) en Sociale Zaken en Werkgelegenheid (75%) in positieve zin op. De achterblijvers zijn de ministeries van Infrastructuur en Waterstaat (32%) en Onderwijs, Cultuur en Wetenschap (42%).

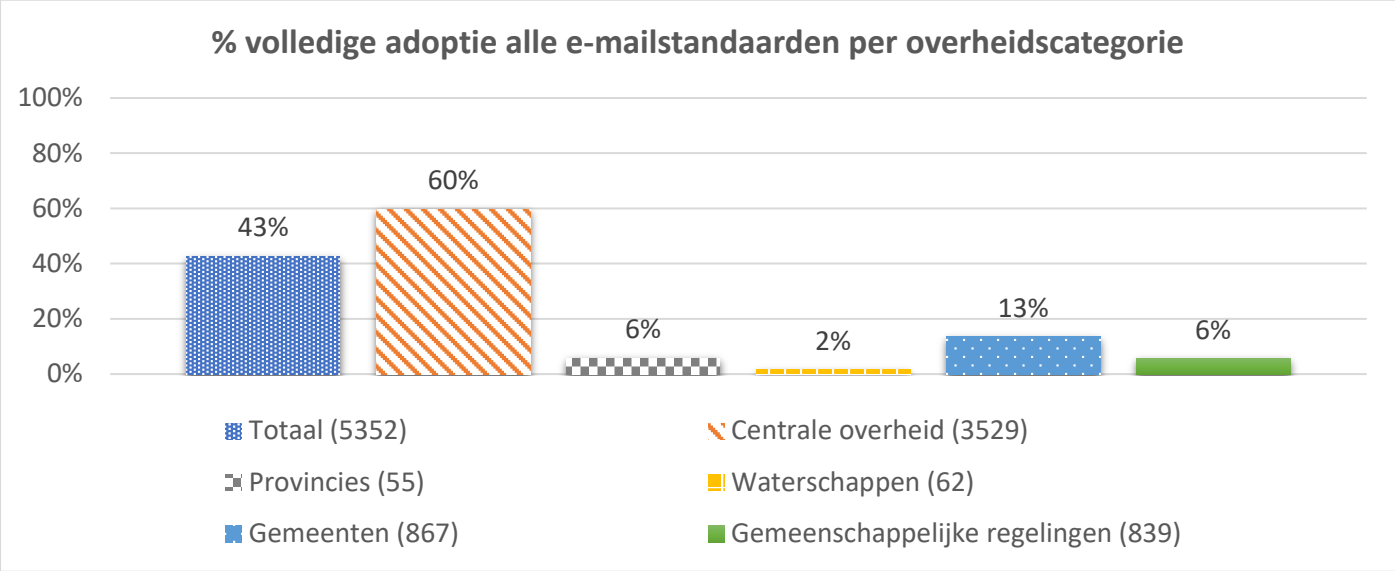


Voor meer details per ministerie zie hoofdstuk 7.

1.3. E-mailstandaarden

1.3.1. Totaalbeeld e-mail per overheidscategorie

Onderstaande cijfers laten zien in welke mate de verschillende overheidscategorieën alle afgesproken websitestandaarden voor veilig en modern e-mailverkeer (inclusief IPv6 en RPKI) toepassen. De centrale overheid (60%) loopt ruim voorop in de toepassing van deze standaarden. Dat komt met name door een hoge mate van gebruik van gemeenschappelijke dienstverleners die de standaarden correct toepassen. Decentrale overheden lopen achter, in het bijzonder de waterschappen (2%). Enerzijds komt dit door een hogere mate van gebruik van clouddiensten die niet alle standaarden ondersteunen, anderzijds zal bij gemeenschappelijke regelingen het gebrek aan bewustzijn mogelijk een rol spelen.



Hoofdstuk 3 gaat in meer detail in op de specifieke e-mailbeveiligingsstandaarden, hoofdstuk 4 gaat in op IPv6 en 5 op RPKI.

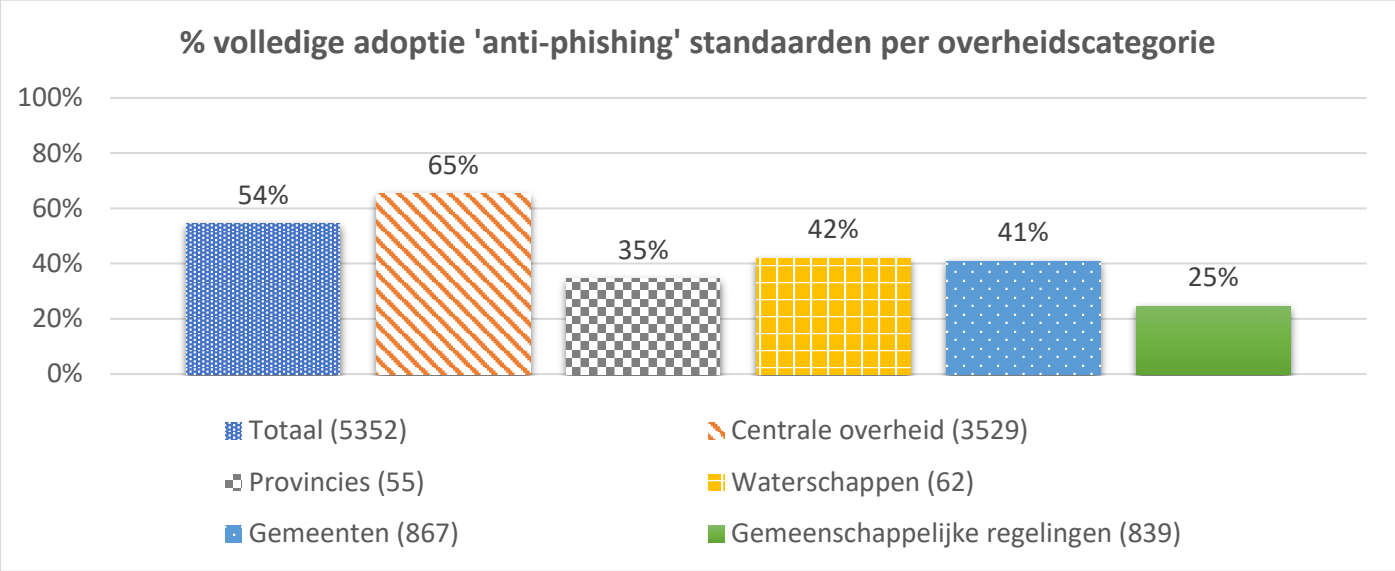
1.3.2. E-mailstandaarden voor bestrijding van phishing (excl. IPv6 en excl. RPKI)

Door toepassing van e-mailstandaarden voor het bestrijden van phishing wordt e-mailverkeer met de overheid beter beveiligd, zodat criminelen niet zomaar overheidsdomeinen kunnen misbruiken als afzenddomein voor bijvoorbeeld phishing-aanvallen. Deze standaarden zijn relevant voor alle domeinnamen, ook diegene waarvan normaliter geen e-mail wordt verzonden.

Deze paragraaf laat het totaalbeeld per overheidscategorie en het totaalbeeld per ministerie zien (zonder IPv6 en zonder RPKI).

1.3.2.1. Adoptie per overheidscategorie

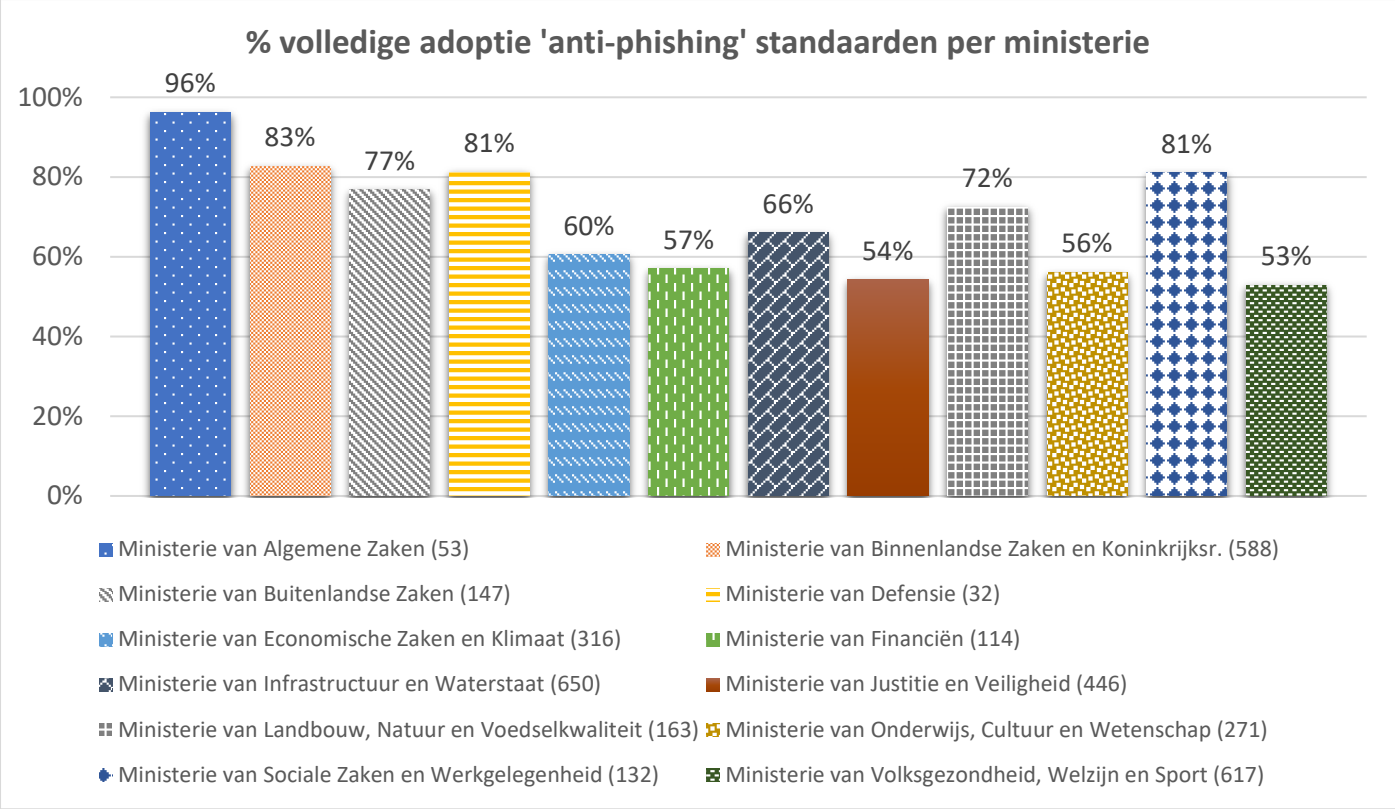
Doordat alle secundaire bekende domeinnamen nu ook zijn meegenomen vallen deze cijfers vooral voor de decentrale overheden slecht uit, veelal zijn de secundaire domeinnamen niet afdoende beschermd. Positief valt de centrale overheid op, in het grotendeels centrale DNS beheer worden de anti-phishing standaarden ook voor secundaire domeinnamen meegenomen.



Voor meer details per overheidscategorie zie hoofdstuk 6.

1.3.2.2. Adoptie per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan vallen de ministeries van Algemene Zaken (96%), Binnenlandse Zaken (83%), Defensie (81%) en Sociale Zaken en Werkgelegenheid (81%) positief op. De ministeries van Volksgezondheid, Welzijn en Sport (53%) en Justitie en Veiligheid (54%) hebben nog veel werk te verzetten om e-mailvervalsing namens haar domeinnamen te voorkomen.



Voor meer details per ministerie zie hoofdstuk 7.

1.3.3. E-mailstandaarden voor vertrouwelijk e-mailverkeer (excl. IPv6 en excl. RPKI)

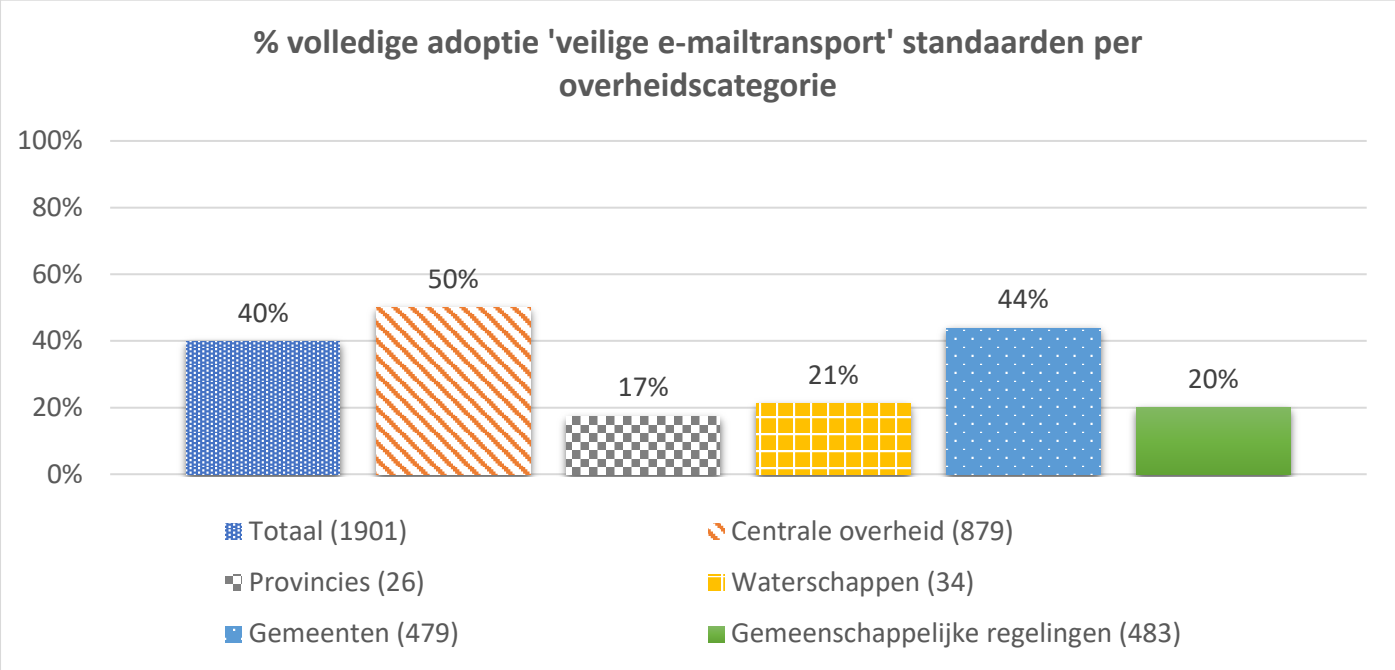
Door toepassing van e-mailstandaarden voor vertrouwelijk e-mailverkeer wordt e-mailverkeer met de overheid beter beveiligd, zodat criminelen niet zomaar e-mails kunnen onderscheppen of manipuleren.

Omdat de test zich beperkt tot een controle of de e-mailontvangst van de betreffende overheden voldoende veilig e-mailverkeer mogelijk maakt, zijn alleen de internetdomeinen met een ontvangende mailserver (MX) meegenomen in de statistieken. Hierdoor is het aantal gecontroleerde domeinen significant lager dan bij de standaarden voor bestrijding van phishing.

Deze paragraaf laat het totaalbeeld per overheidscategorie en het totaalbeeld per ministerie zien (zonder IPv6 en zonder RPKI).

1.3.3.1. Adoptie per overheidscategorie

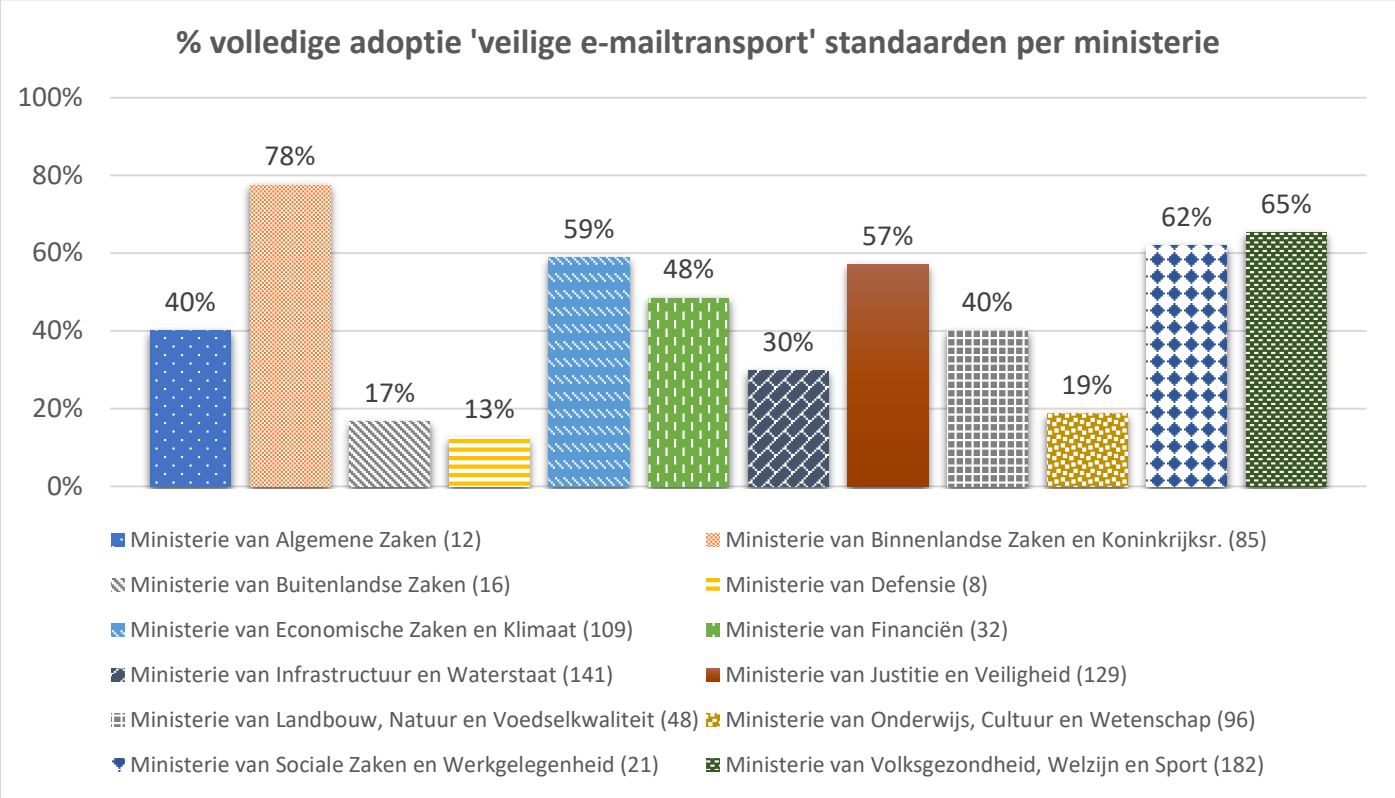
De standaarden op het gebied van veilige e-mailtransport blijken over het algemeen het minst goed geïmplementeerd. De centrale overheid (50%) en gemeenten (44%) scoren relatief het beste op deze standaarden. Het gebruik van gemeenschappelijke e-maildienstverleners geeft daarbij een hefboomeffect. Decentrale overheden maken veel meer gebruik van clouddiensten voor e-mailverkeer, die de standaarden DNSSEC en DANE over het algemeen niet ondersteunen. Dit is duidelijk zichtbaar in de adoptiegraad bij provincies, gemeenschappelijke regelingen en waterschappen.



Voor meer details per overheidscategorie zie hoofdstuk 6.

1.3.3.2. Adoptie per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan valt op dat ministeries die actief sturen op toepassing van standaarden beter scoren, zoals de ministeries van Volksgezondheid, Welzijn en Sport, Sociale Zaken en Werkgelegenheid en Binnenlandse Zaken en Koninkrijksrelaties. Ook het ministerie van Economische Zaken en Klimaat scoort relatief hoger, omdat de meeste e-mail door de huisleverancier wordt verzorgd. Het ministerie van Defensie is een negatieve opvaller met slechts 13% volledige adoptie van standaarden voor veilig e-mailtransport.



Voor meer details per ministerie zie hoofdstuk 7.

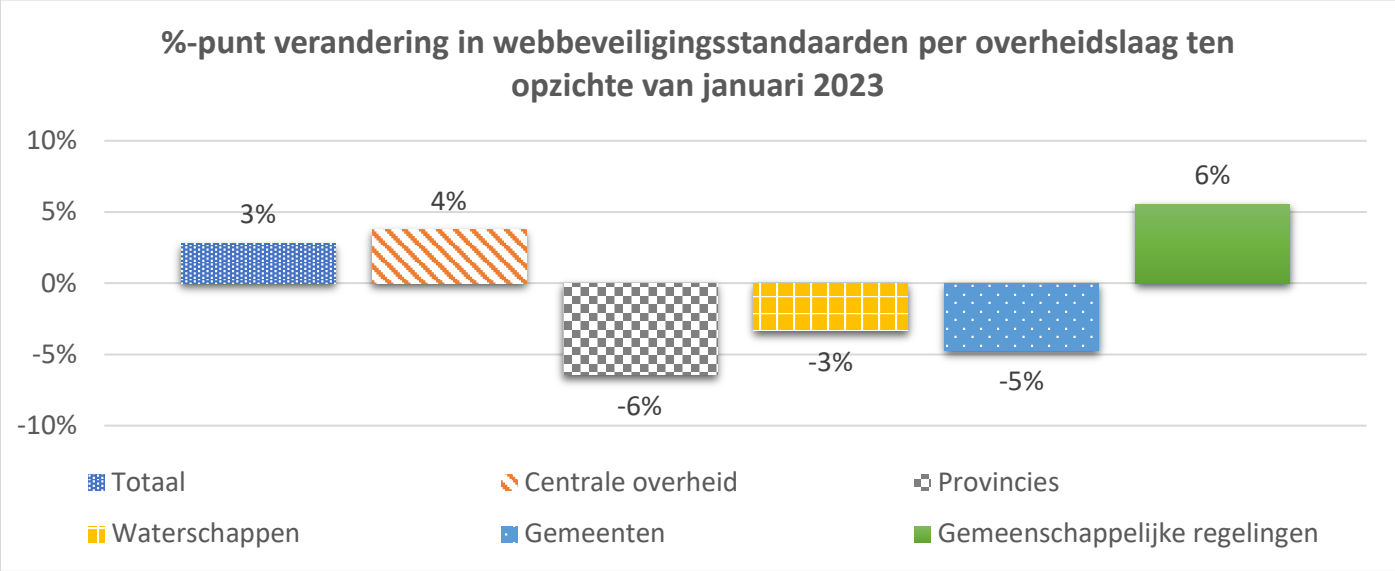
1.4. Vergelijking vorige meting

In de vorige meting van januari 2023 werd gewerkt met een kleinere set aan domeinnamen. Het gevolg hiervan was dat de meetresultaten niet goed te vergelijken zijn met deze metingen. Hierom is hier apart gekeken naar enkel de domeinnamen die in beide metingen voorkomen, wat een vergelijking met voorgaande meting mogelijk maakt.

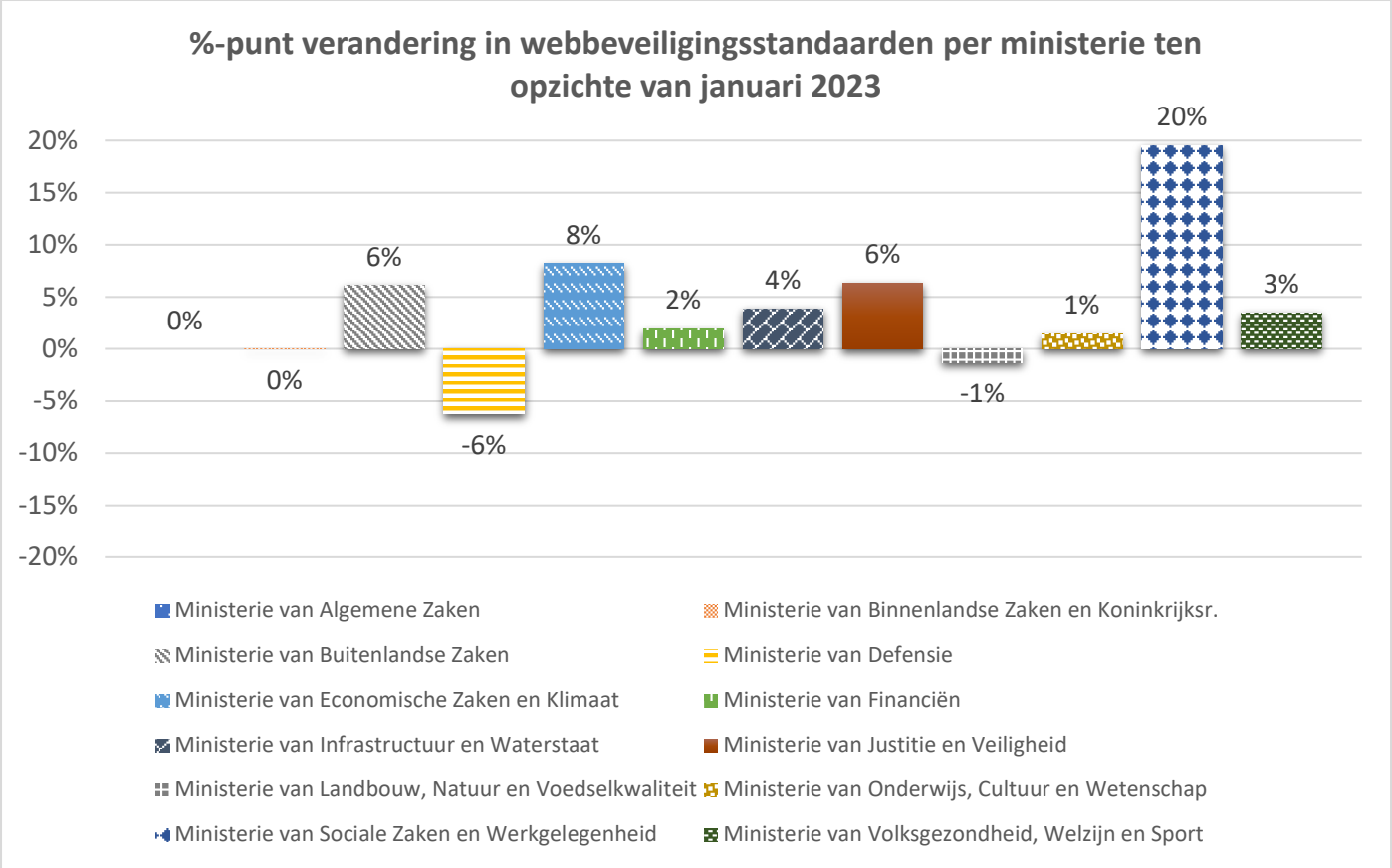
De voorgaande secties laten zien dat adoptie nog steeds verre van volledig is binnen de overheid. Echter is het ook van belang om bewegingen in kaart te brengen. In deze vergelijking worden de verbeteringen en verslechteringen zichtbaar gemaakt door het verschil in procentpunten uit te drukken.

1.4.1. Vergelijking webstandaarden

Kijkende naar de veranderingen in adoptie van webbeveiligingsstandaarden per overheidslaag (excl. IPv6 en excl. RPKI), zien we over de gehele breedte van de domeinnamenset een lichte stijging in het aantal domeinen dat aan alle afspraken voldoet. Helaas is er tegelijkertijd een lichte afname te zien bij de provincies, waterschappen en gemeenten. Bij provincies en waterschappen gaat het om een relatief kleine set aan domeinnamen.

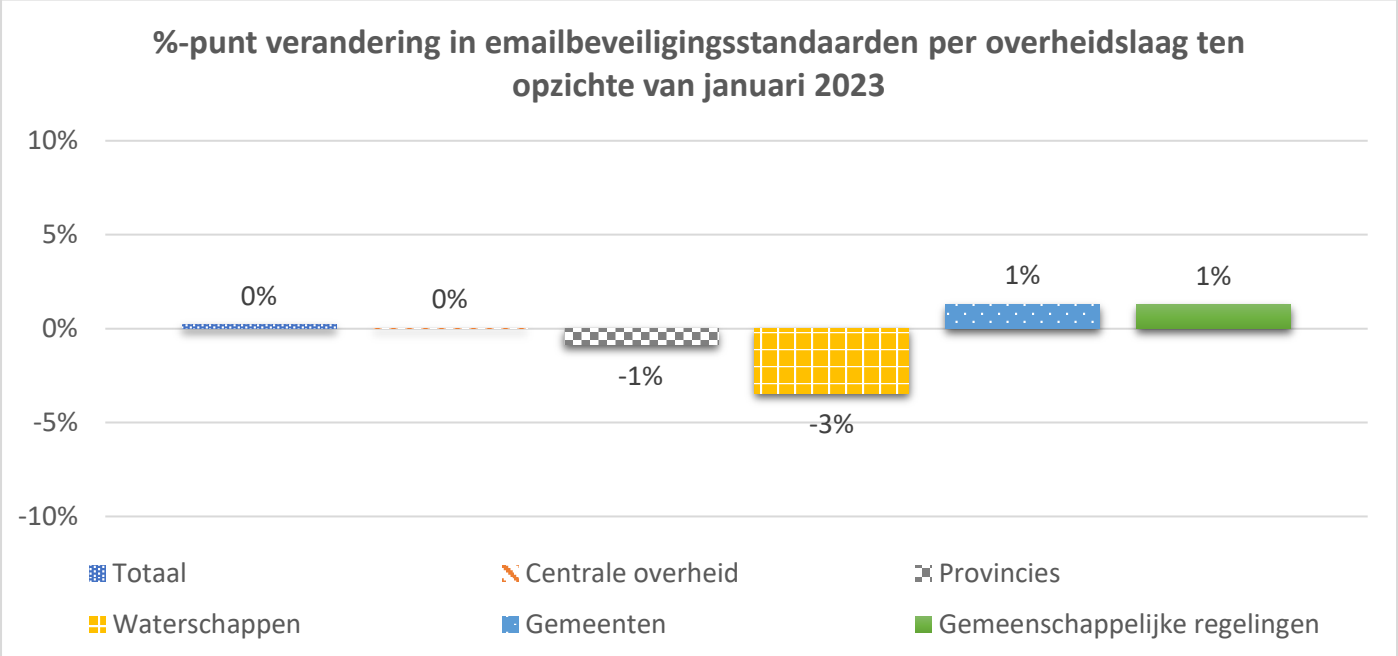


Kijkende naar de centrale overheid, zien we een mooie verbetering in de adoptie van webbeveiligingsstandaarden. In het bijzonder heeft het ministerie van Sociale Zaken en Werkgelegenheid een achterstand ingelopen (verbetering van 20 procentpunt). De ministeries van Defensie en Landbouw, Natuur en Voedselkwaliteit laten een verslechtering zien in de webbeveiligingsstandaarden.

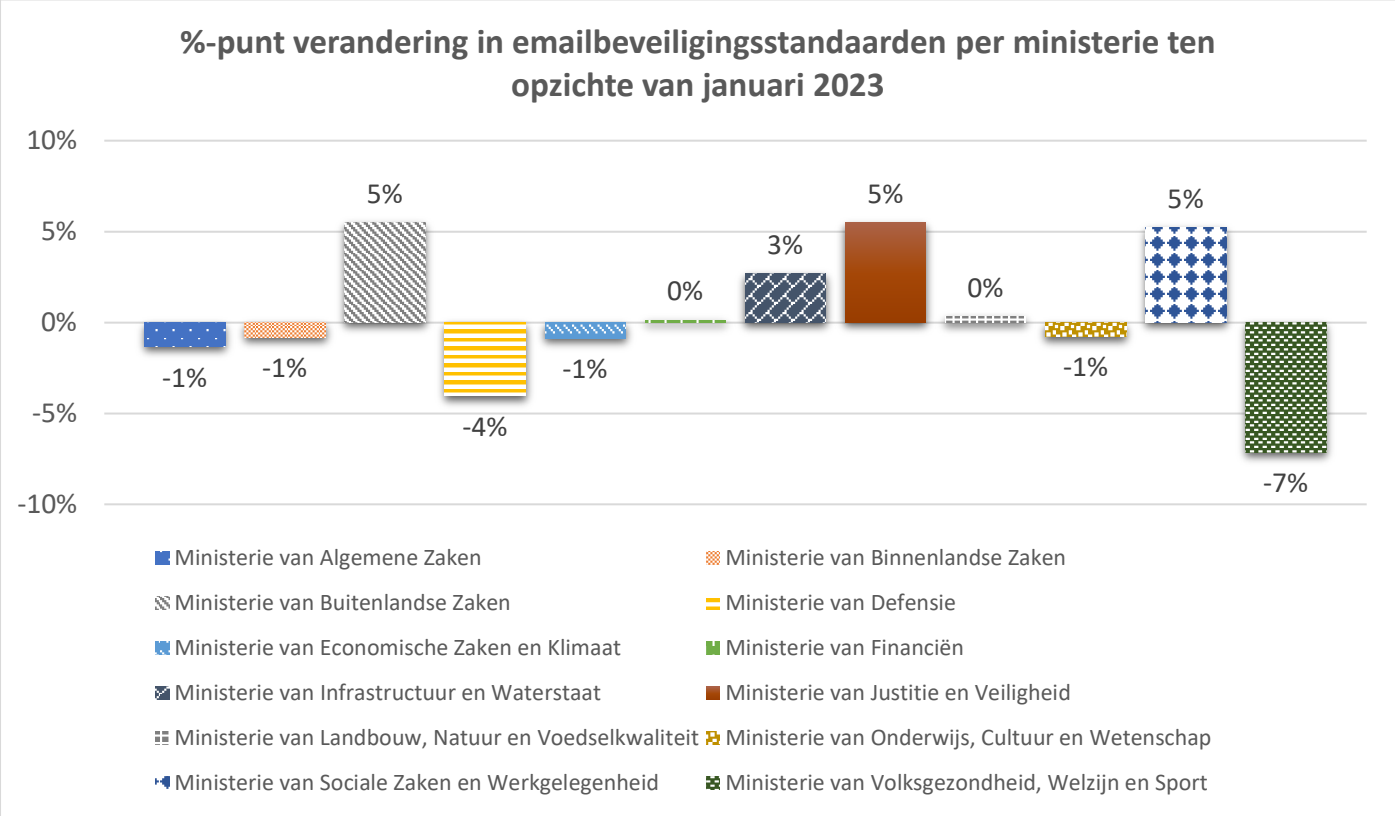


1.4.2. Vergelijking emailstandaarden

Bij de emailbeveiligingsstandaarden is over het totaal geen verbetering te zien ten opzichte van januari 2023.



Verder kijkende naar de veranderingen per ministerie, is wederom een enorme stijging te zien bij de ministeries van Buitenlandse Zaken en Sociale Zaken en Werkgelegenheid, maar ook bij Justitie en Veiligheid. Negatieve uitschieters zijn de ministeries van Defensie en Volksgezondheid, Welzijn en Sport.



1.4.3. Conclusie

De vergelijking laat zien dat er sinds de vorige meting verbeteringen zijn doorgevoerd in de adoptie van de webstandaarden. De voortgang van adoptie bij emailstandaarden is ten opzichte van de vorige meting nihil. In het bijzonder zijn stijgingen waar te nemen bij het ministerie van Sociale Zaken en Werkgelegenheid op zowel web als emailstandaarden.

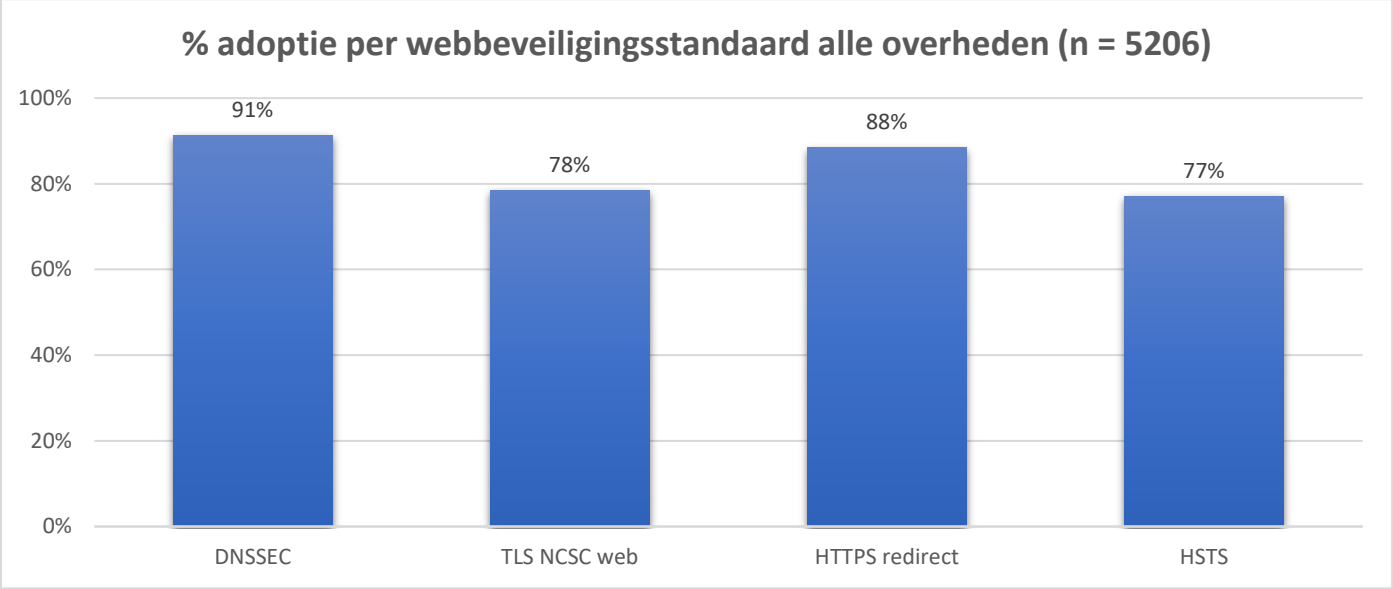
Het is de hoop dat andere overheidsorganisaties dit voorbeeld volgen en inzetten op verbetering van de adoptiecijfers. De voorbeelden laten zien dat verbeteringen mogelijk en uitvoerbaar zijn.

2. Adoptie per websitebeveiligingsstandaard

Dit hoofdstuk toont de algehele adoptiegraad per websitebeveiligingsstandaard.

Hoofdstuk 6 en 7 gaan in meer detail in op de adoptiegraad van specifieke standaarden per respectievelijk overheidscategorie en ministerie.

Onderstaande statistieken tonen onder meer aan dat bij een kwart van de internetdomeinen de TLS- en HSTS-configuraties niet op orde zijn. Overheden moeten HTTPS en HSTS toepassen conform de ICT-beveiligingsrichtlijnen voor webapplicaties, en configureren hun TLS-verbindingen conform de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC.



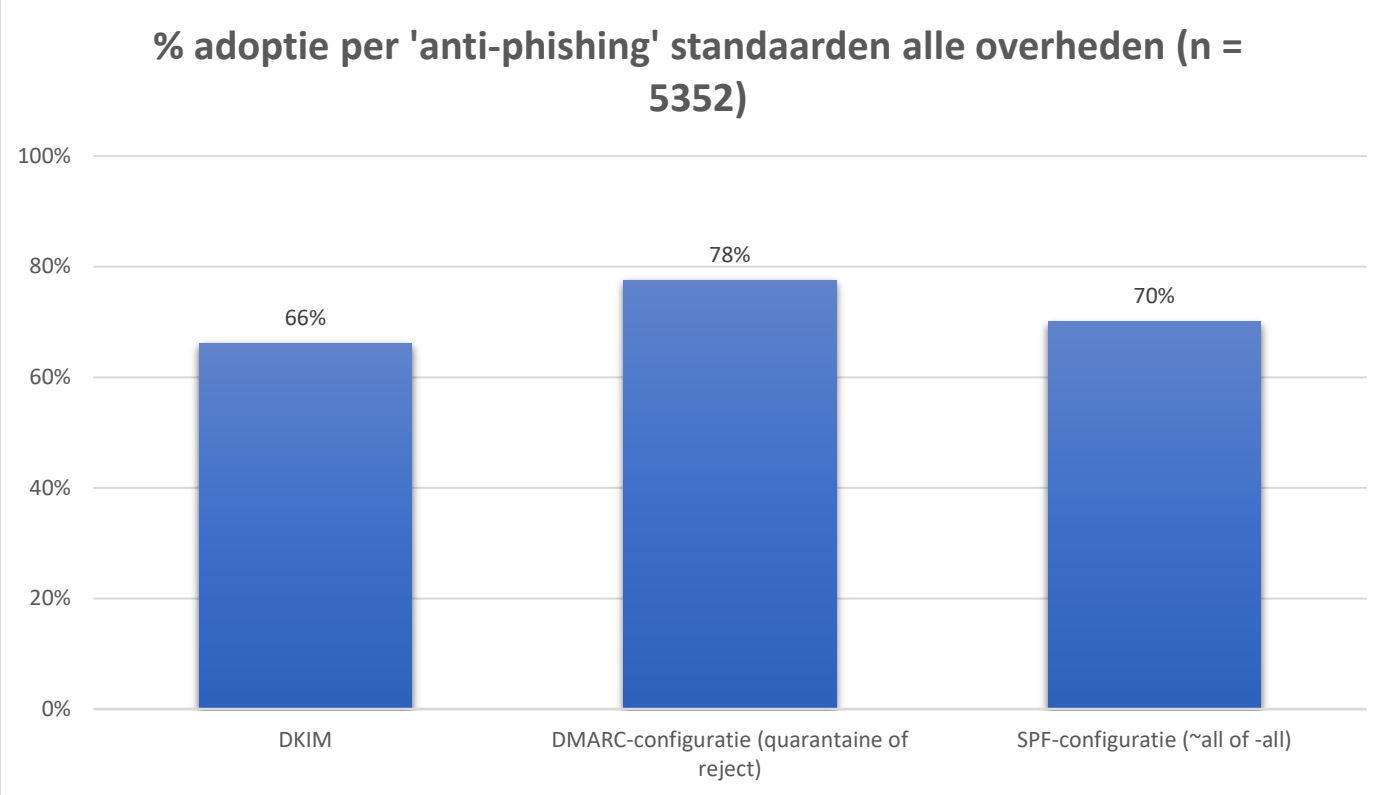
3. Adoptie per e-mailbeveiligingsstandaard

Dit hoofdstuk toont de algehele adoptiegraad per e-mailbeveiligingsstandaard.

Hoofdstuk 6 en 7 gaan in meer detail in op de adoptiegraad van specifieke standaarden per respectievelijk overheidscategorie en ministerie.

3.1. E-mailstandaarden voor bestrijding van phishing

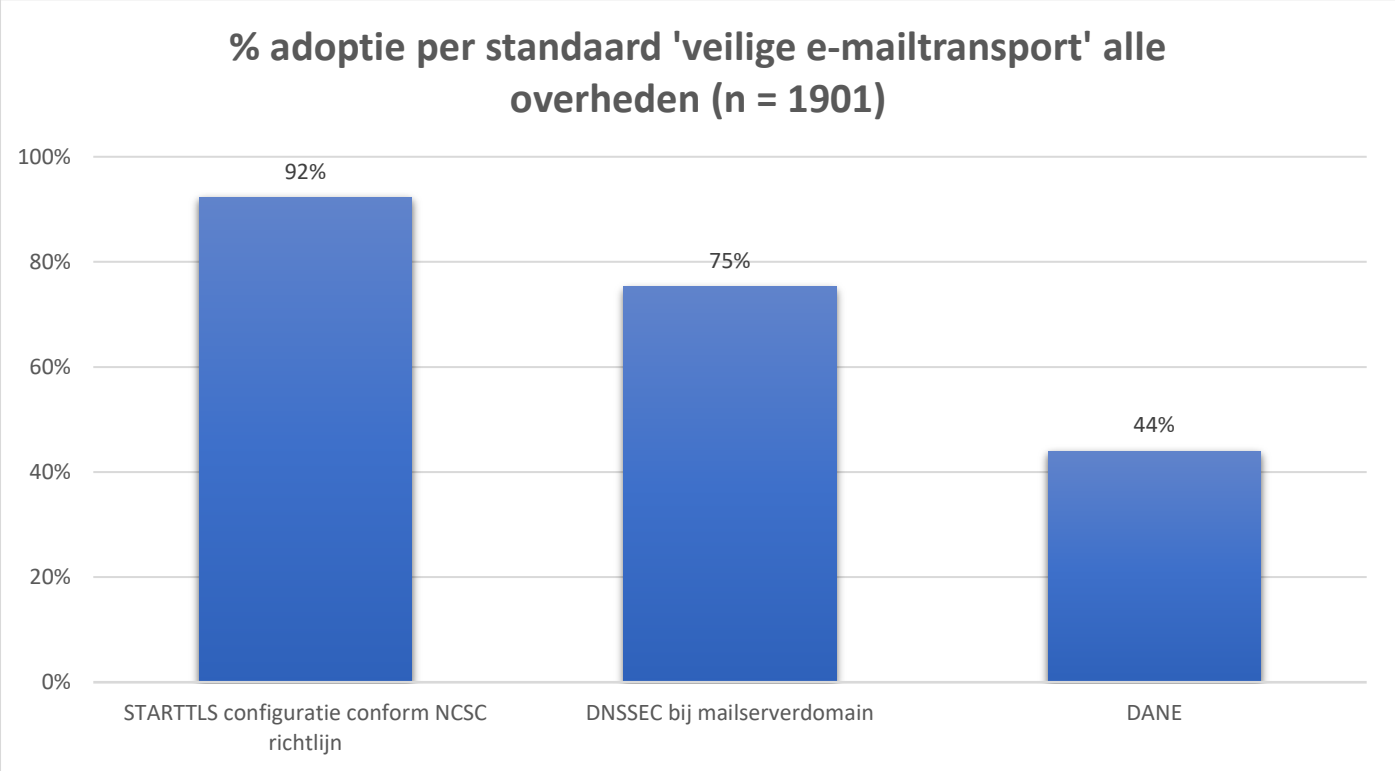
Om phishingmails uit naam van overheidsorganisaties (inclusief bewindspersonen) te voorkomen, moet voor 22% van de internetdomeinen nog een strikt DMARC-beleid worden ingesteld en 30% een strikte SPF. Veelal is te zien dat bij subdomeinen van decentrale overheden SPF in geheel niet aanwezig is. Als de SPF voor deze subdomeinen zo wordt ingesteld dat dit subdomein niet mag mailen, vervalt automatisch ook de DKIM controle en zal dit cijfer meestijgen met de SPF implementatie. Het implementeren van SPF Het streefbeeld was om dit eind 2019 voor elkaar te hebben.



3.2. E-mailstandaarden voor vertrouwelijk e-mailverkeer

Bij nog 8% van de ontvangende e-mailservers is de STARTTLS-configuratie niet toekomstvast geconfigureerd. Overheden dienen hun TLS-verbindingen te configureren op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC.

DANE is de minst toegepaste standaard uit de meting met een adoptiegraad van 44%. DNSSEC bij mailserverdomein en DANE zorgen in samenhang voor geauthentiseerde versleuteling van e-mailtransport tussen de verzendende en ontvangende mailserver. Dit voorkomt dat een actieve aanvaller zomaar mailverkeer kan afluisteren.



De grootste implementatiedrempel voor DNSSEC en DANE is leveranciersondersteuning door met name clouddienstverleners. Het is belangrijk dat overheden die nog niet voldoen hun leverancier blijven vragen om ondersteuning van deze standaarden.

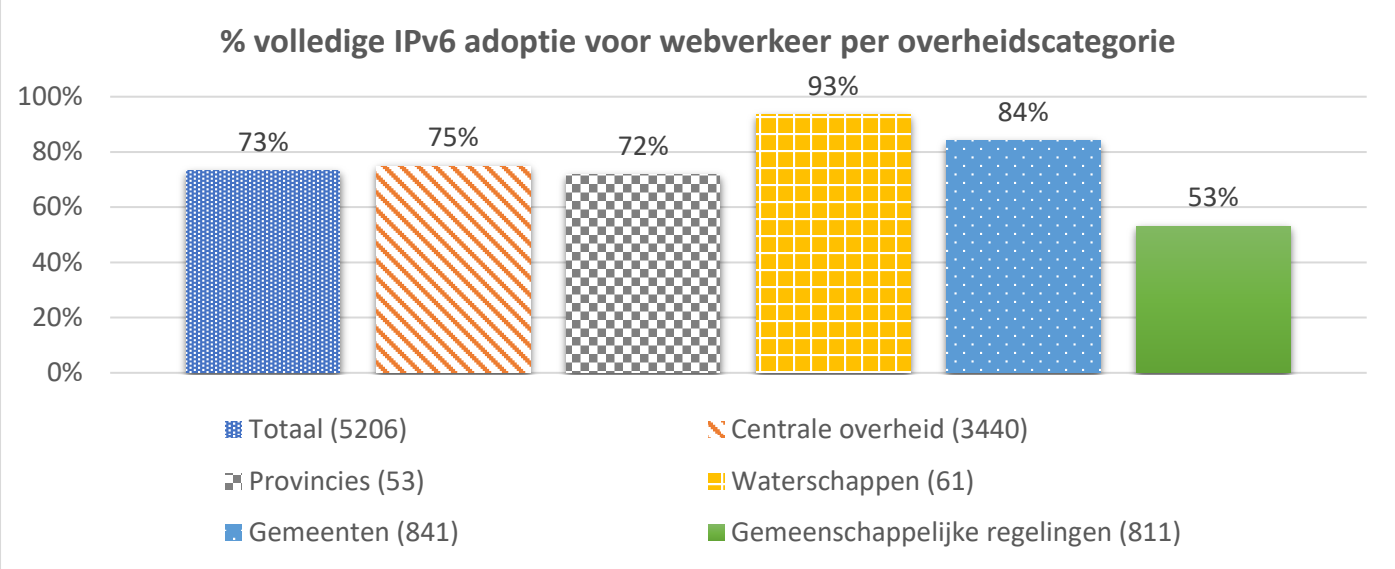
4. Adoptie IPv6 voor websites en e-mail

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.

De overheid heeft ook een voorbeeldfunctie om moderne internetstandaarden zoals IPv6 te gebruiken. Deze standaarden zorgen er namelijk voor dat het internet nu en in de toekomst voor iedereen wereldwijd veiliger en toegankelijker wordt waardoor ook nieuwe innovatie kan plaatsvinden. Brede ondersteuning van IPv6 binnen Nederland is ook belangrijk voor onze mondiale concurrentiepositie.

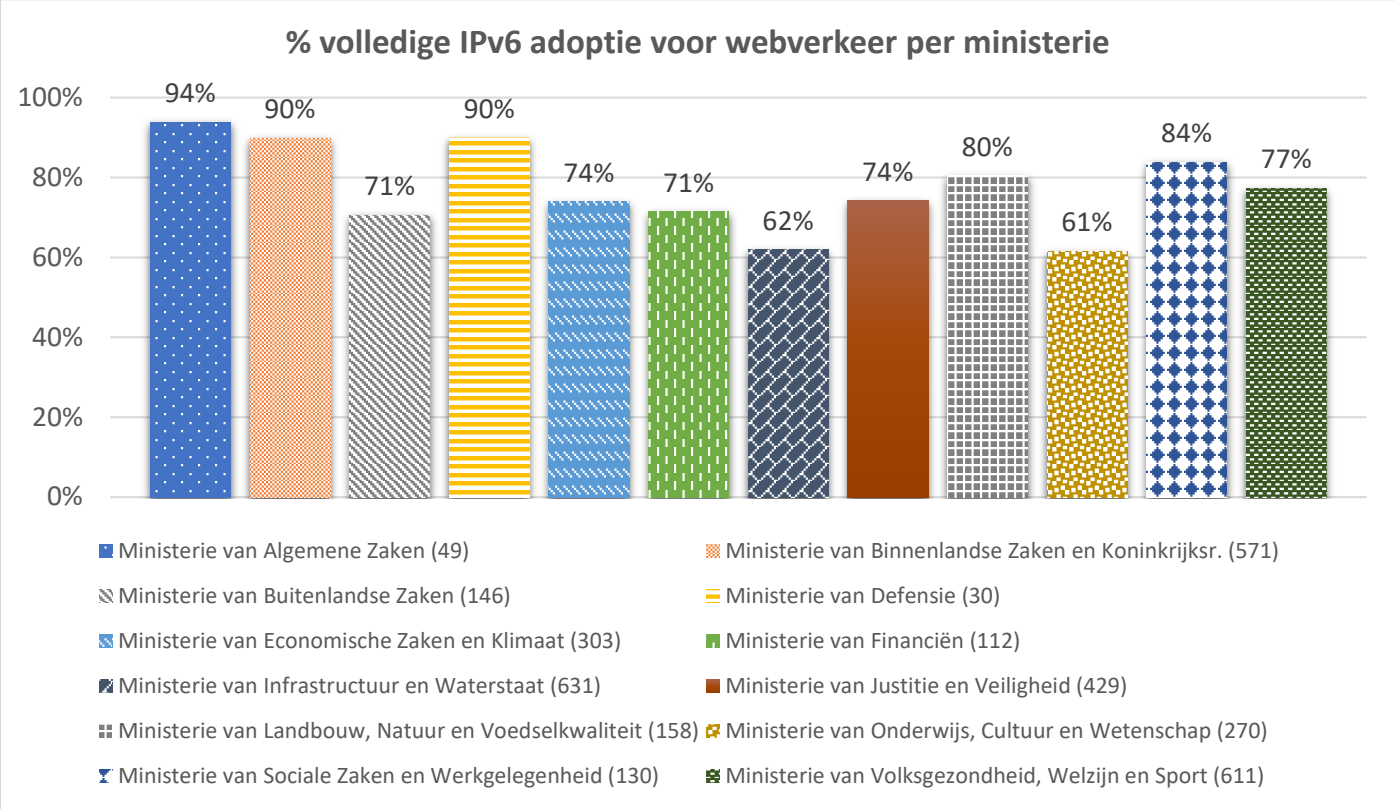
4.1. IPv6 voor webverkeer per overheidscategorie

De gemeenschappelijke regelingen scoren lager bij het gebruik van IPv6 voor webverkeer. De overheidsbrede afspraken hebben onvoldoende doorwerking gehad naar deze instanties, ondanks dat zij meestal gefinancierd worden vanuit de andere overheden.



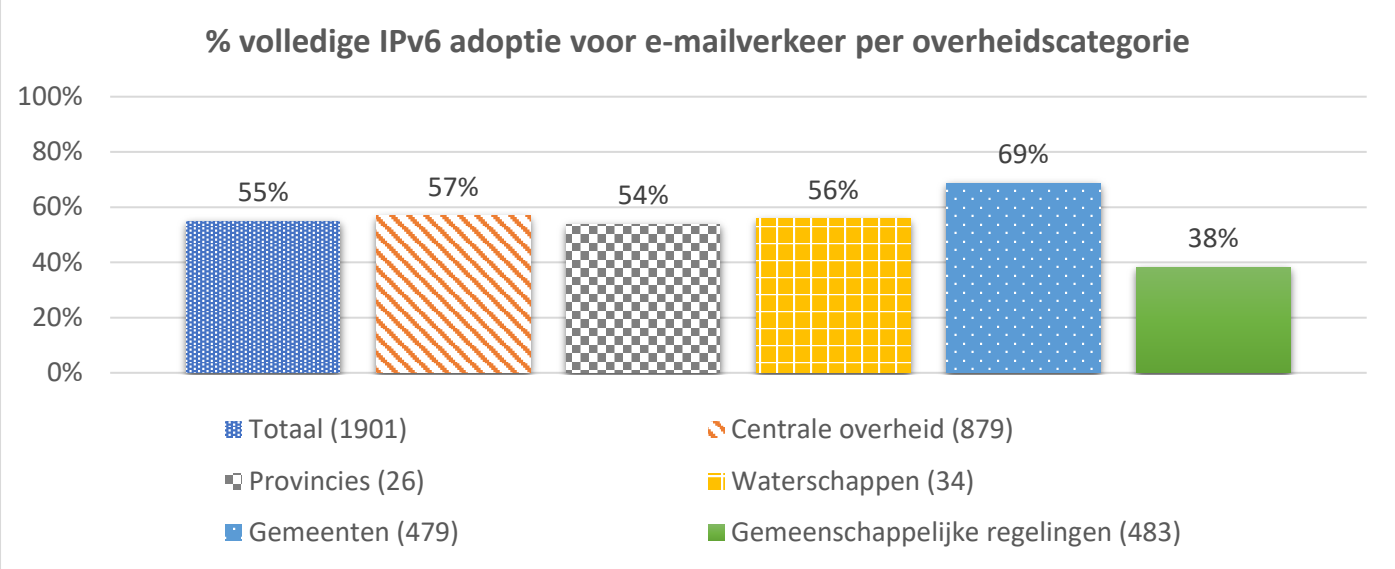
4.2. IPv6 voor webverkeer per ministerie

Positieve uitschieters – met een klein webportfolio – zijn de ministeries van Algemene Zaken (94%), Binnenlandse Zaken (90%) en Defensie (90%). Negatieve opvaller is het ministerie van Onderwijs, Cultuur en Wetenschap (61%) en Infrastructuur en Waterstaat (62%), waarvan de websites het minst bereikbaar zijn via IPv6.



4.3. IPv6 voor e-mailverkeer per overheidscategorie

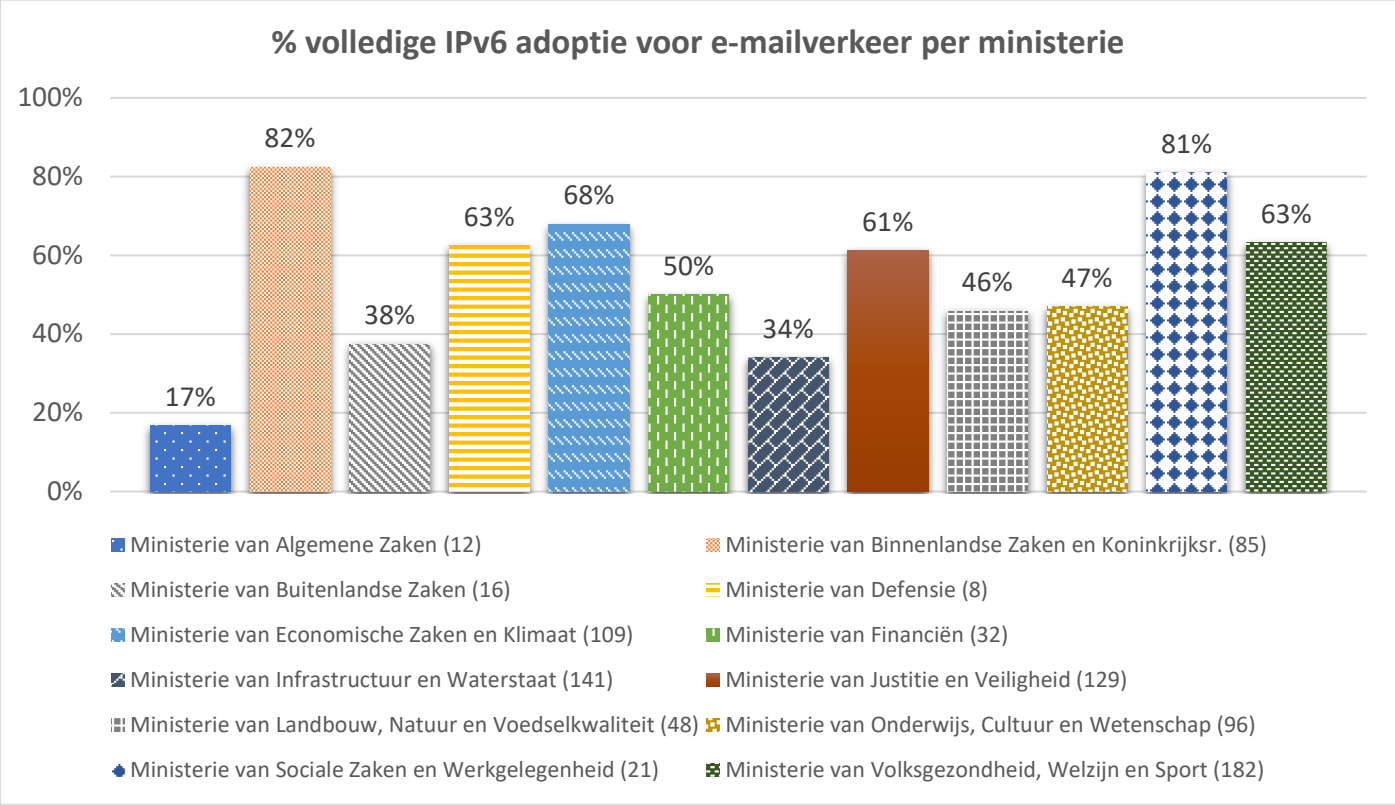
Ook bij het gebruik van IPv6 voor e-mailverkeer scoren de gemeenschappelijke regelingen ver onder de maat met een adoptiegraad van slechts 38%.



4.4. IPv6 voor e-mailverkeer per ministerie

Waar het ministerie van Defensie eerder helemaal geen IPv6 e-mailverkeer mogelijk had, heeft het een grote sprong omhoog gemaakt (63%). Het ministerie Algemene Zaken (17%) heeft ondanks een klein portfolio aan ontvangen e-maildomeinen een erg lage adoptiegraad.

De hoogste sores zijn voor ministeries Binnenlandse Zaken (82%) en Sociale Zaken en Werkgelegenheid (81%).



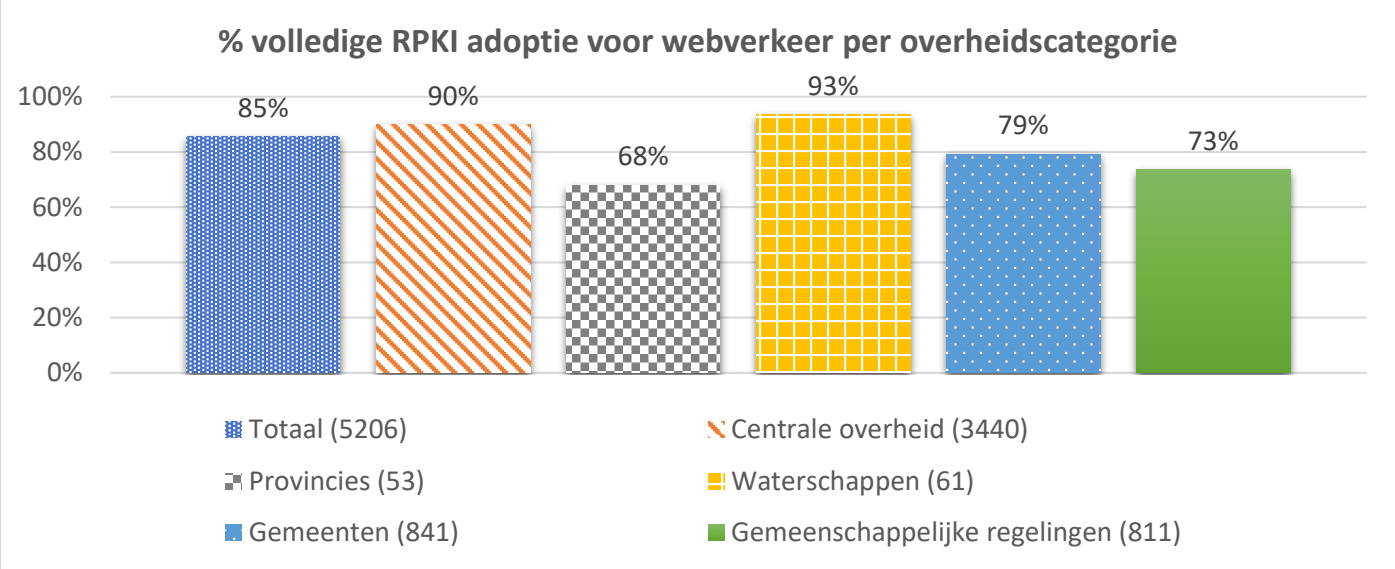
5. Adoptie RPKI voor websites en e-mail

Resource Public Key Infrastructure (RPKI) is een standaard met als doel om zogenaamde route hijacks te voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet geautoriseerd netwerk. Een hijack kan het gevolg zijn van een simpele typefout van een netwerkbeheerder die daarmee onbedoeld internetverkeer omleidt, of het gevolg zijn van een doelgerichte aanval op de infrastructuur van het internet om bijvoorbeeld websites onbereikbaar te maken of om gegevens van internetgebruikers afhandig te maken. In deze meting wordt enkel naar de publicerende Route Origin Authorisation (ROA) kant van RPKI gekeken.

De overheidsbrede afspraak is om RPKI voor het eind van 2024 te implementeren.

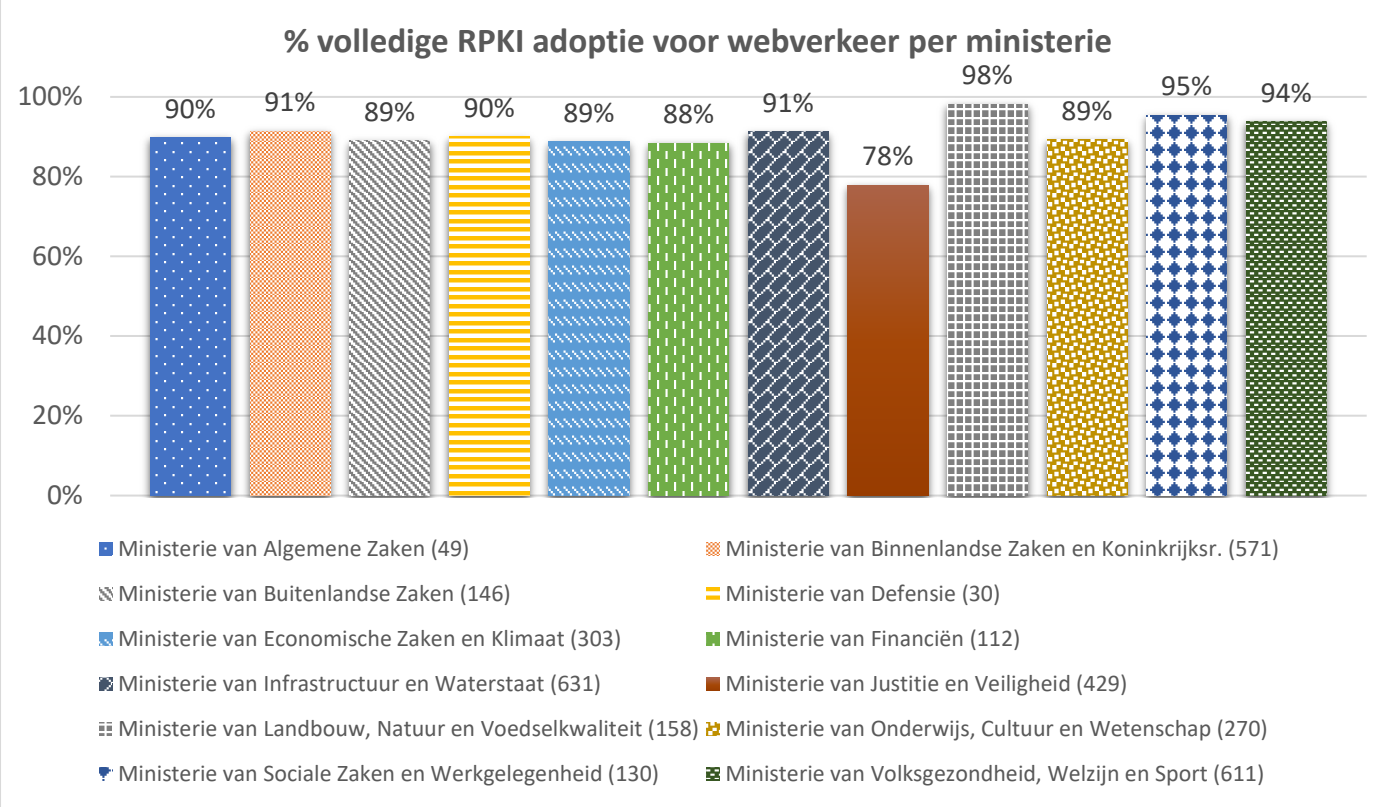
5.1. RPKI voor webverkeer per overheidscategorie

Bij de Waterschappen en de centrale overheid heeft RPKI bij de eerste keer van meten al een adoptie van boven de 90%. Enkel de provincies en gemeenschappelijke regelingen scoren ruim onder de 80%.



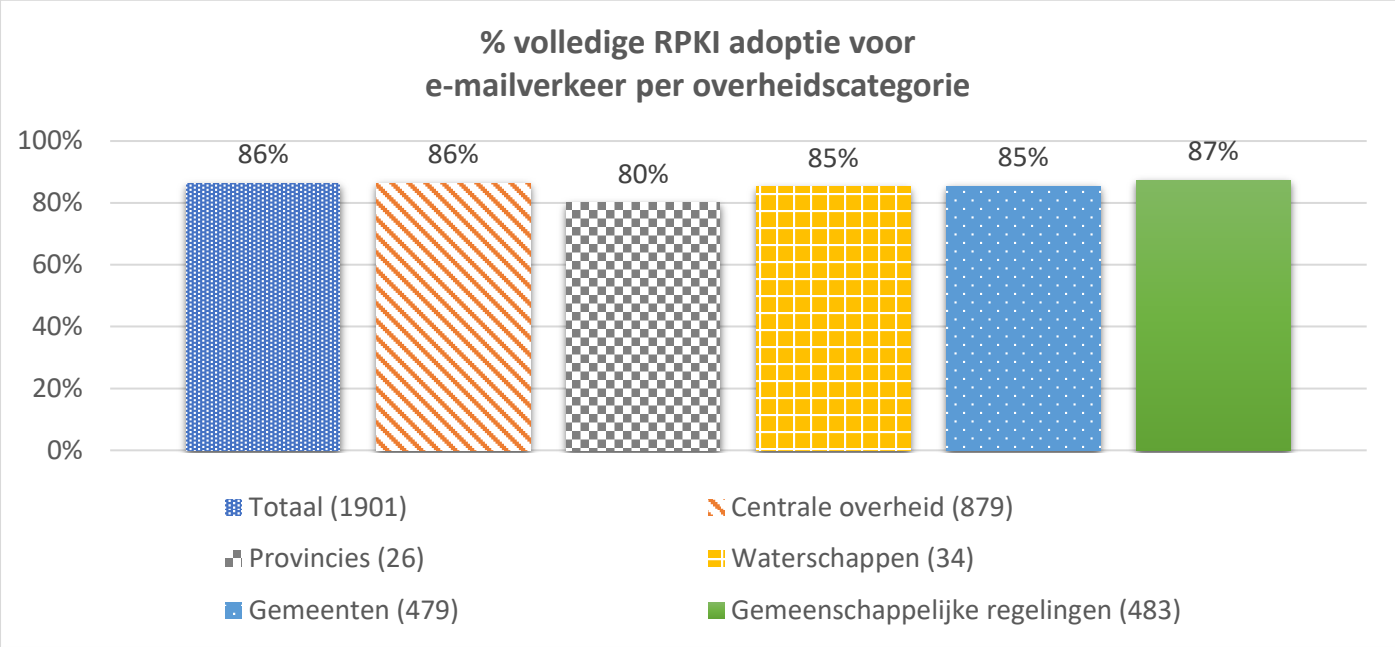
5.2. RPKI voor webverkeer per ministerie

De ministeries hebben bijna allemaal een zeer hoge adoptie rond de 90%. Enige achterblijver is Justitie en Veiligheid (78%) waar een paar niet ondertekende routes zorgt voor een lagere scores dan de overige ministeries. Het ministerie van Landbouw, Natuur en Voedselkwaliteit (98%) heeft al bijna de afspraak behaald voor RPKI op de IP-adressen gebruikt in het webverkeer.



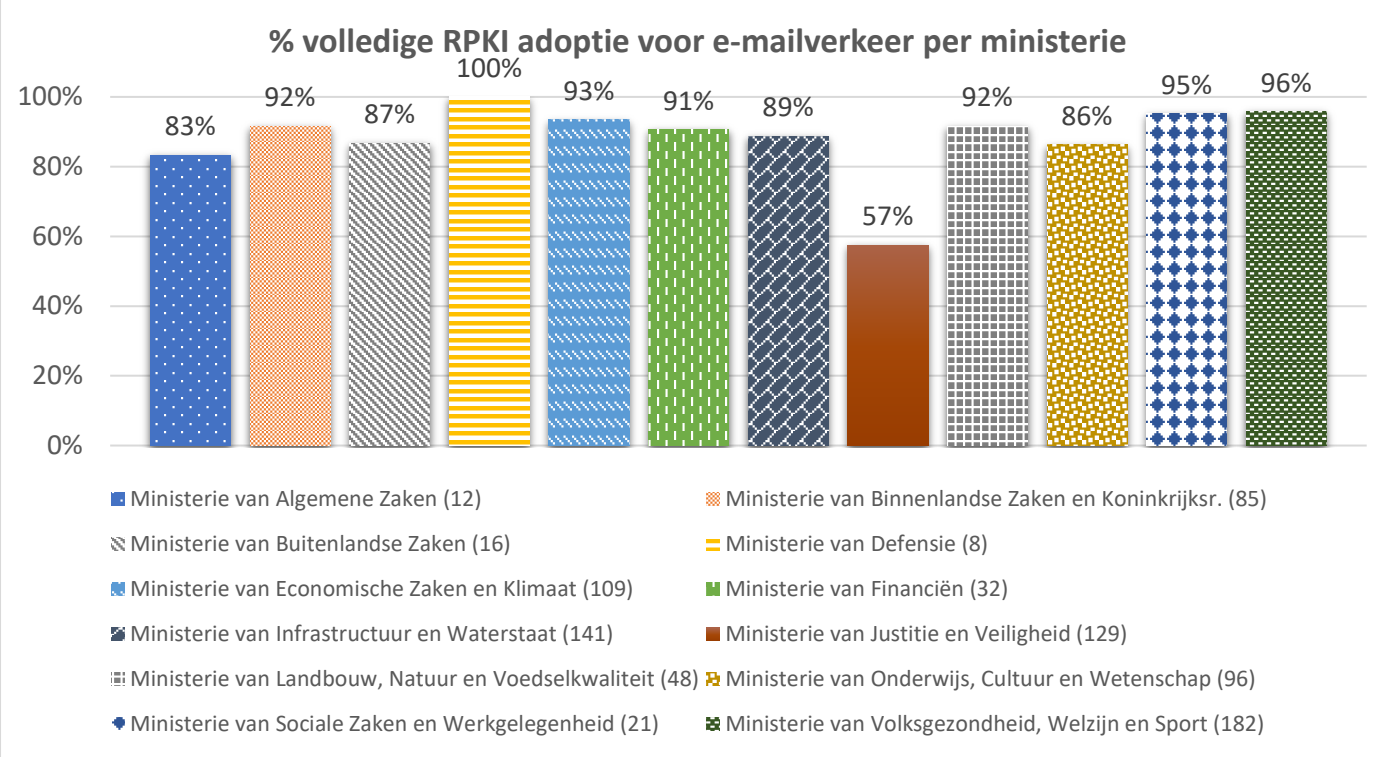
5.3. RPKI voor e-mailverkeer per overheidscategorie

Het gebruik van RPKI voor e-mailverkeer is voor alle overheidscategorieën al op behoorlijk niveau. De verschillen in adoptie tussen de overheidscategorieën zijn klein, al blijven ook hier de provincies licht achter.



5.4. RPKI voor e-mailverkeer per ministerie

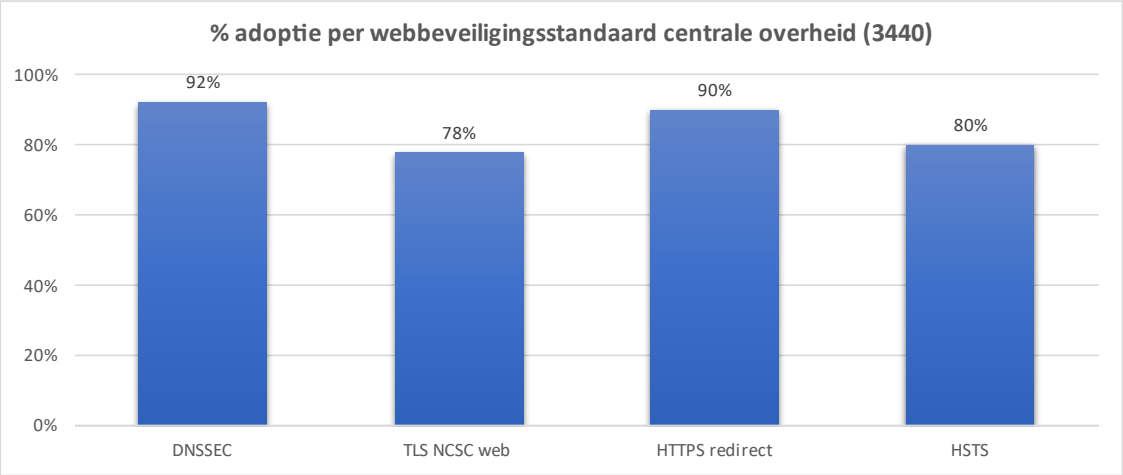
De ministeries hebben bijna allemaal een zeer hoge adoptie van rond de 90%. Enige achterblijver is wederom Justitie en Veiligheid (57%) waar een paar niet ondertekende routes zorgt voor een lagere scores dan de overige ministeries. Het ministerie van Defensie (100%) heeft mede dankzij een klein portfolio aan ontvangen e-maildomeinen de afspraak behaald voor RPKI op de IP-adressen gebruikt in het emailverkeer.

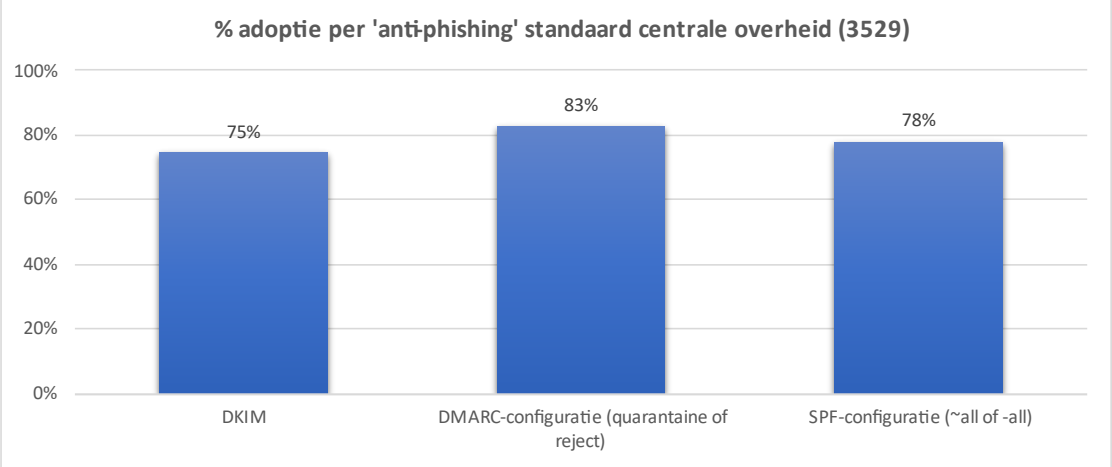


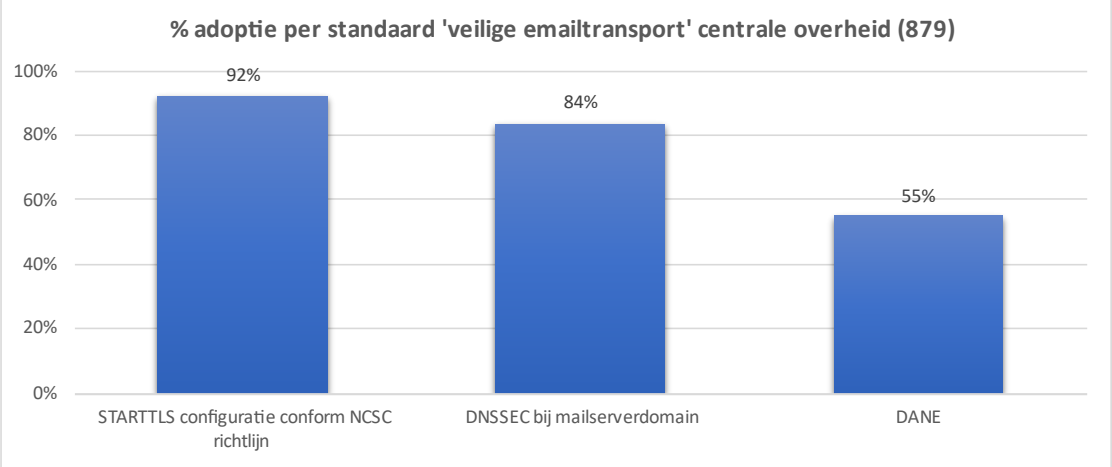
6. Adoptie per overheidscategorie

De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per overheidscategorie.

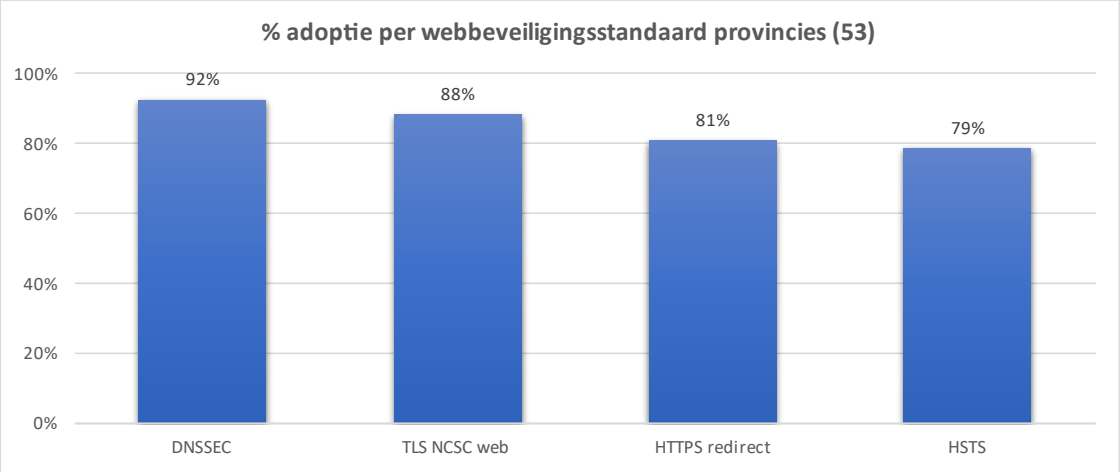
6.1. Centrale overheid

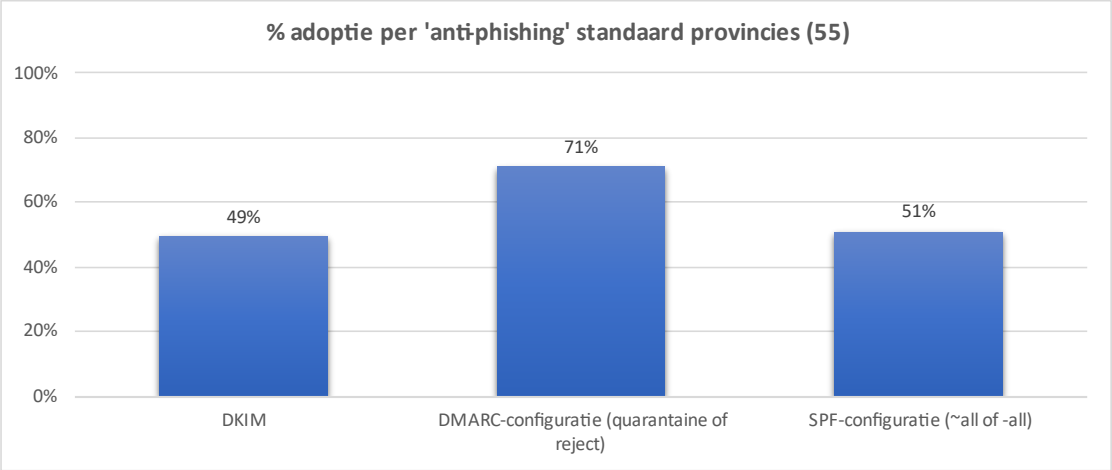


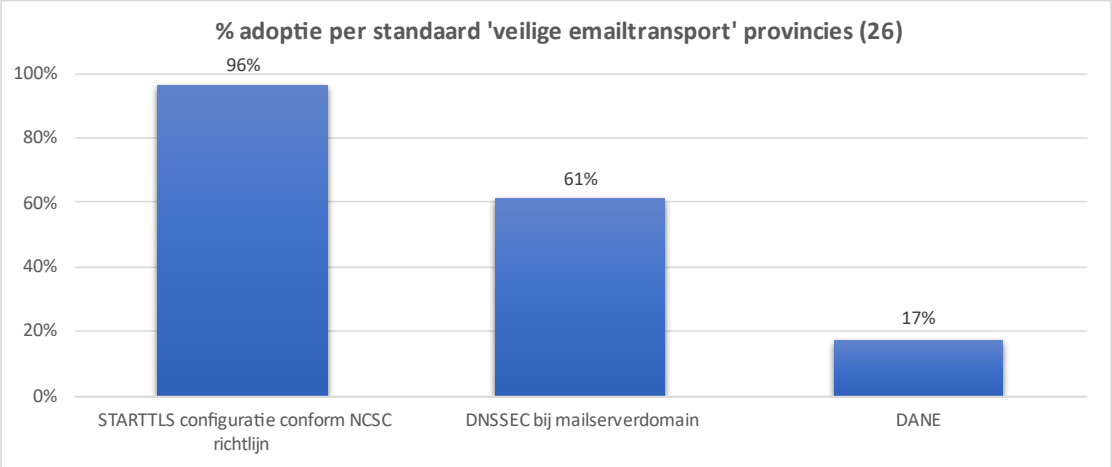




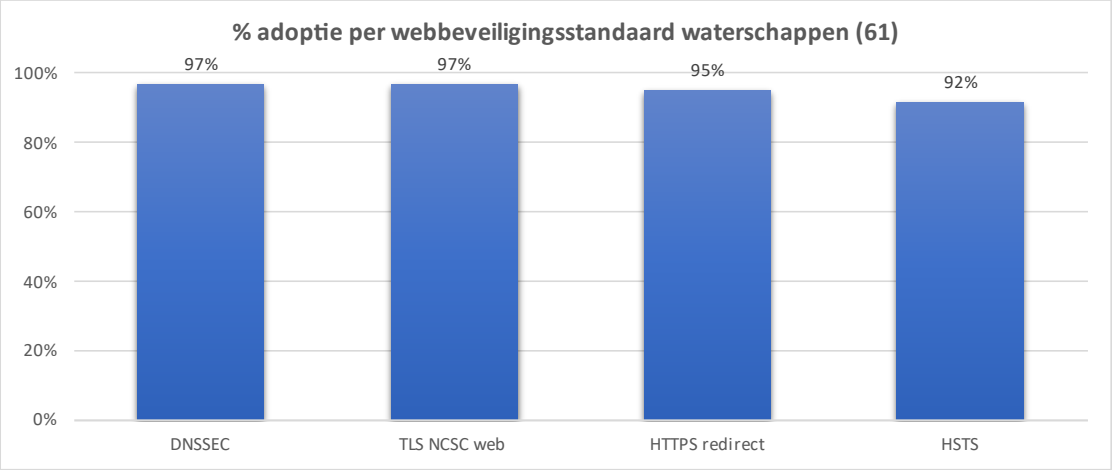
6.2. Provincies

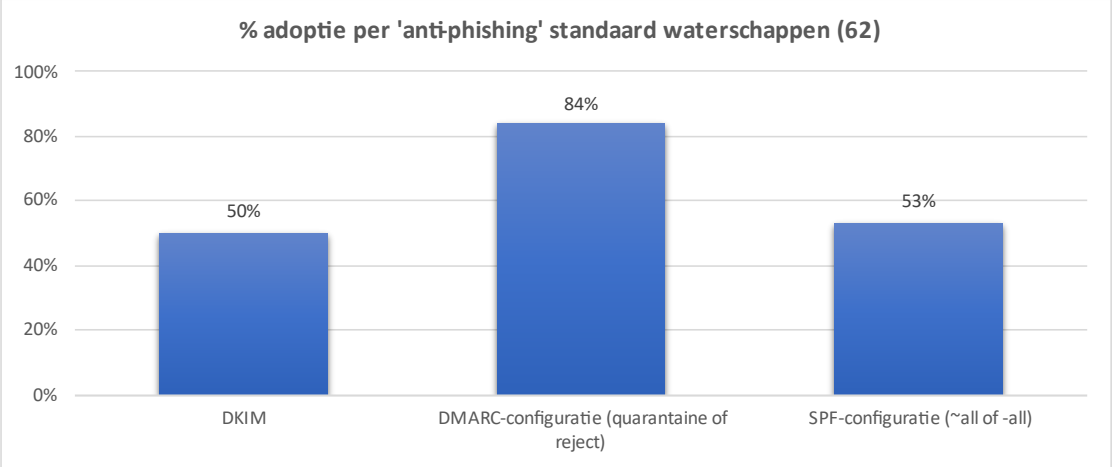


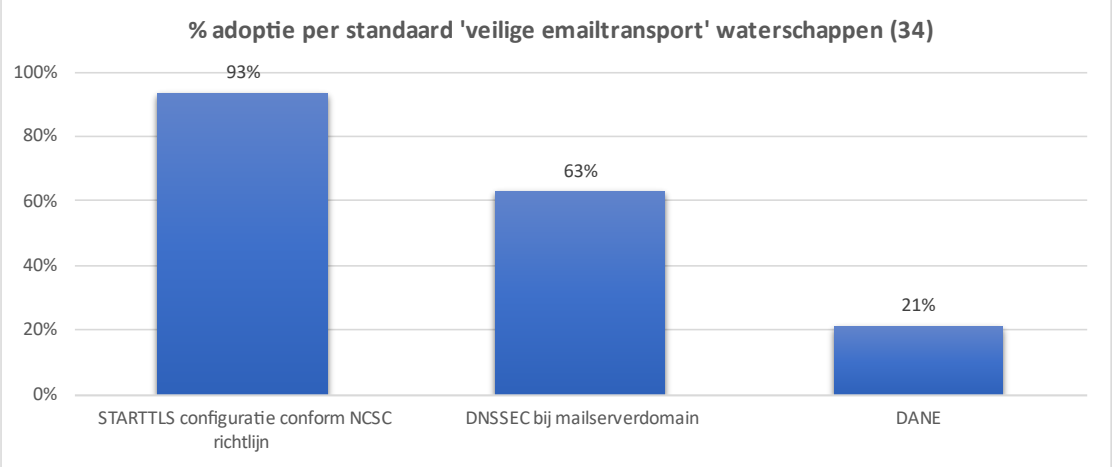




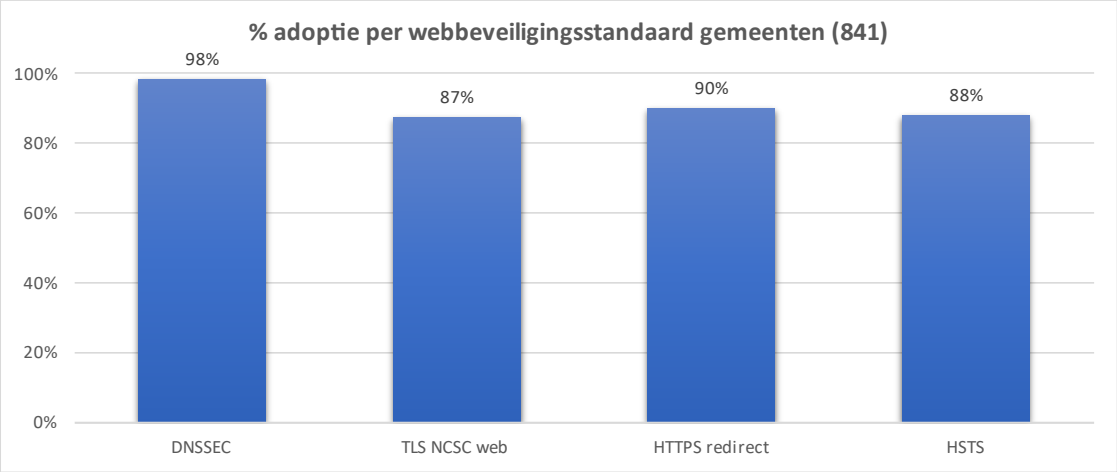
6.3. Waterschappen

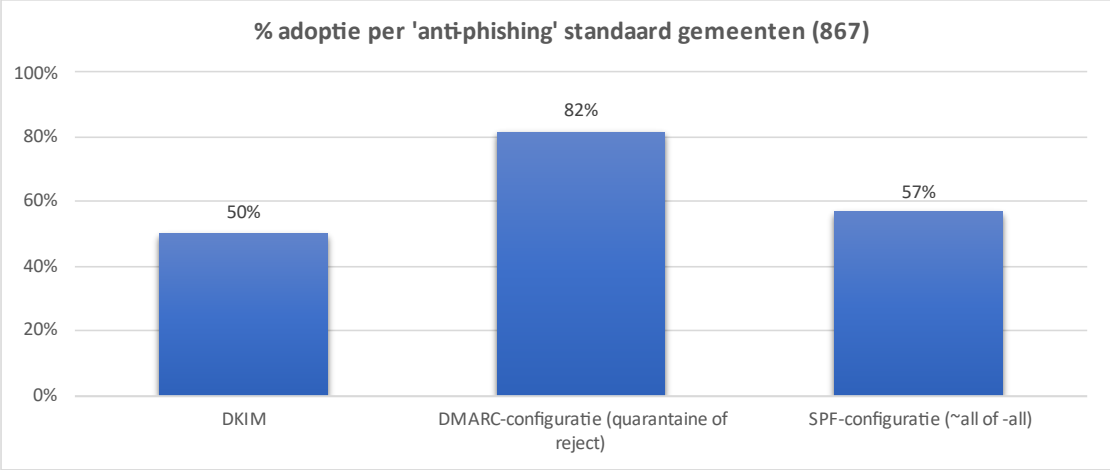


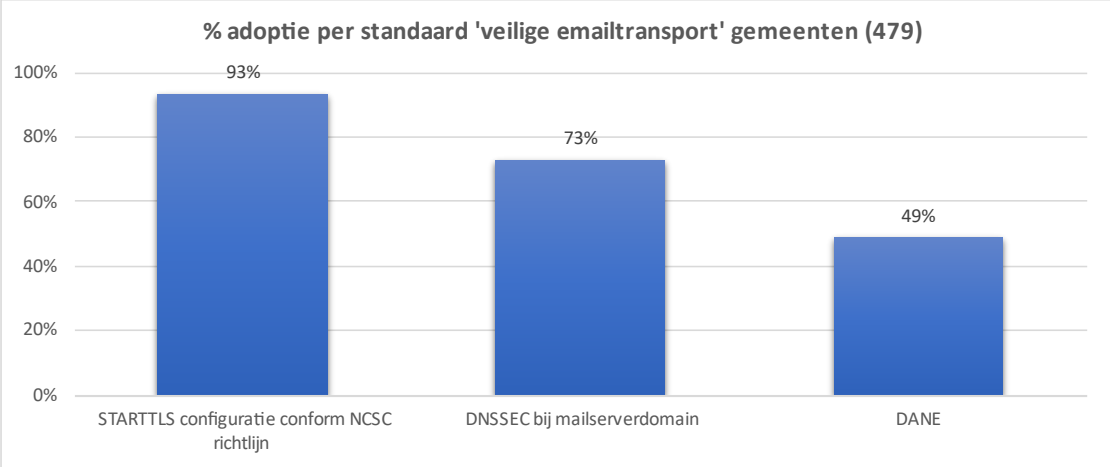




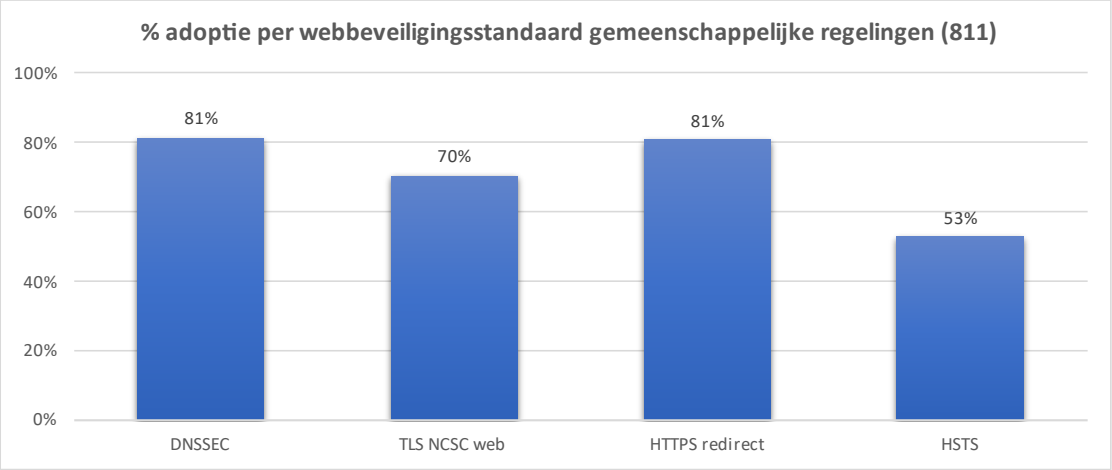
6.4. Gemeenten

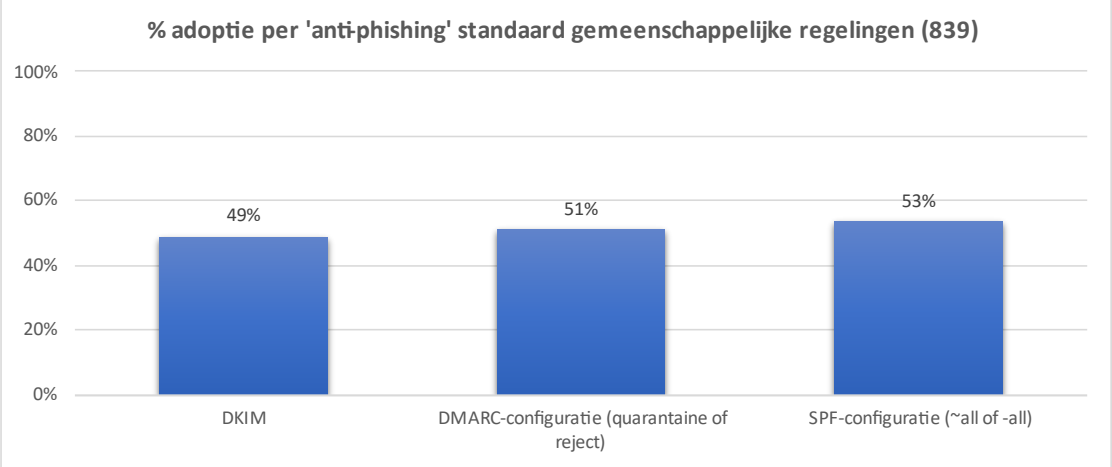


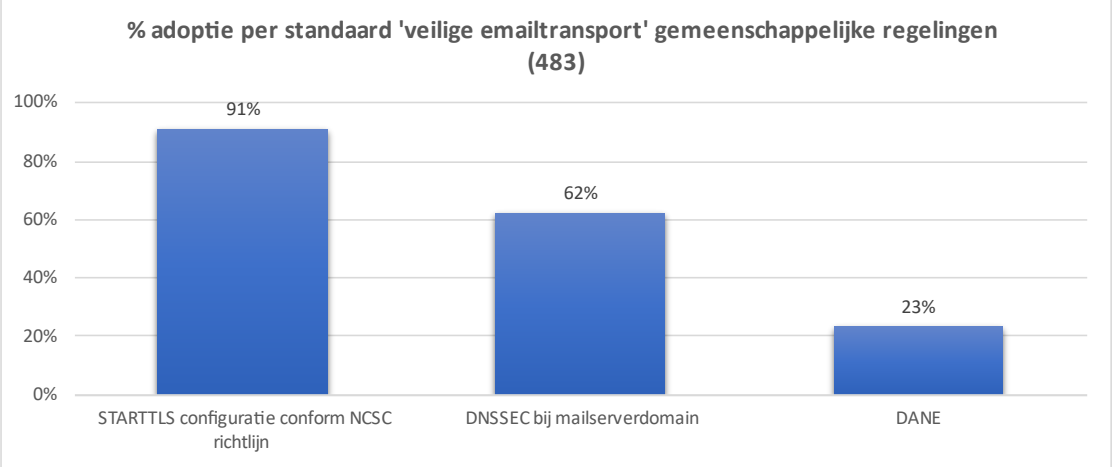




6.5. Gemeenschappelijke regelingen



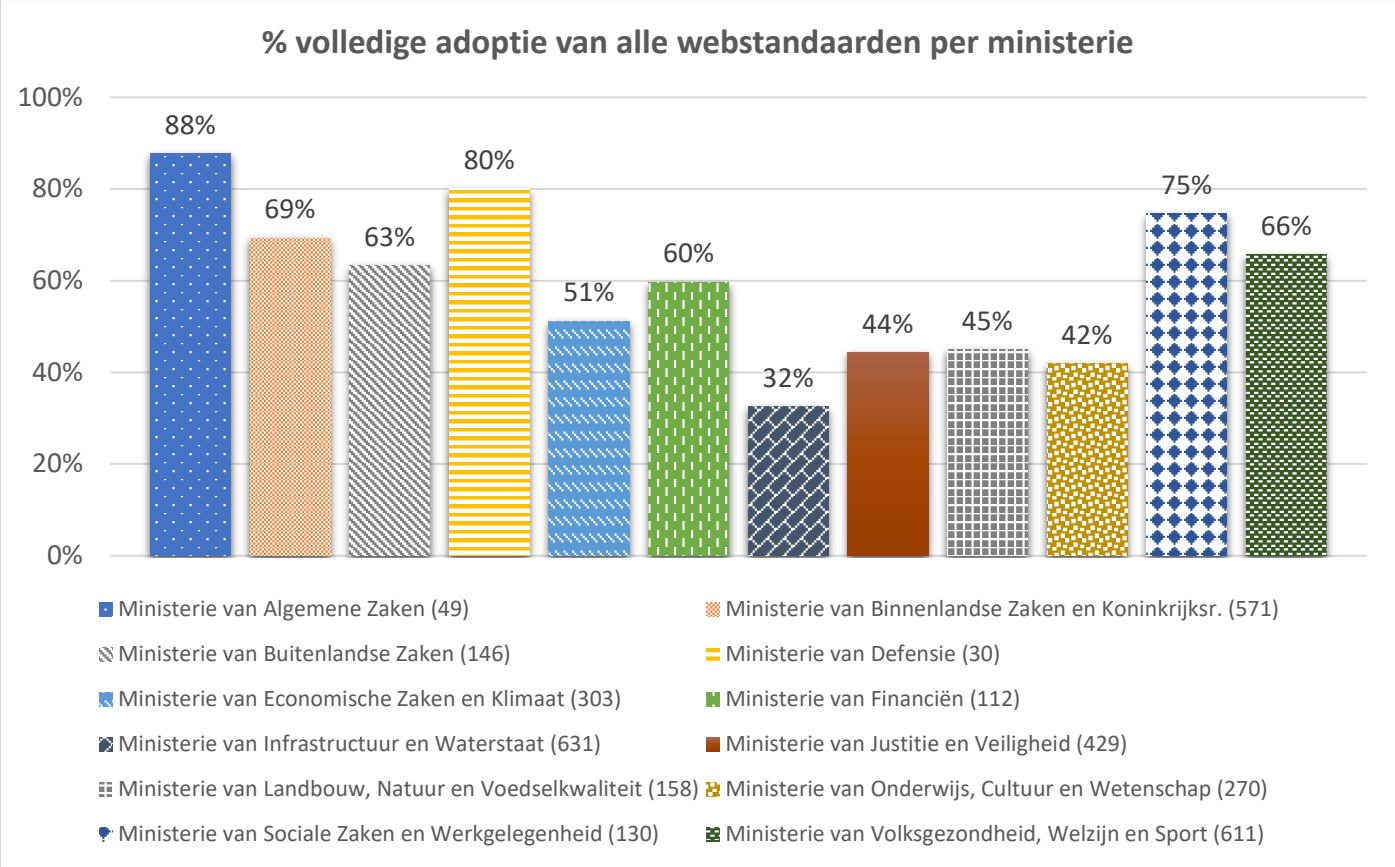




7. Adoptie per ministerie

7.1. Totaalbeeld websitestandaarden (incl. IPv6 en incl. RPKI)

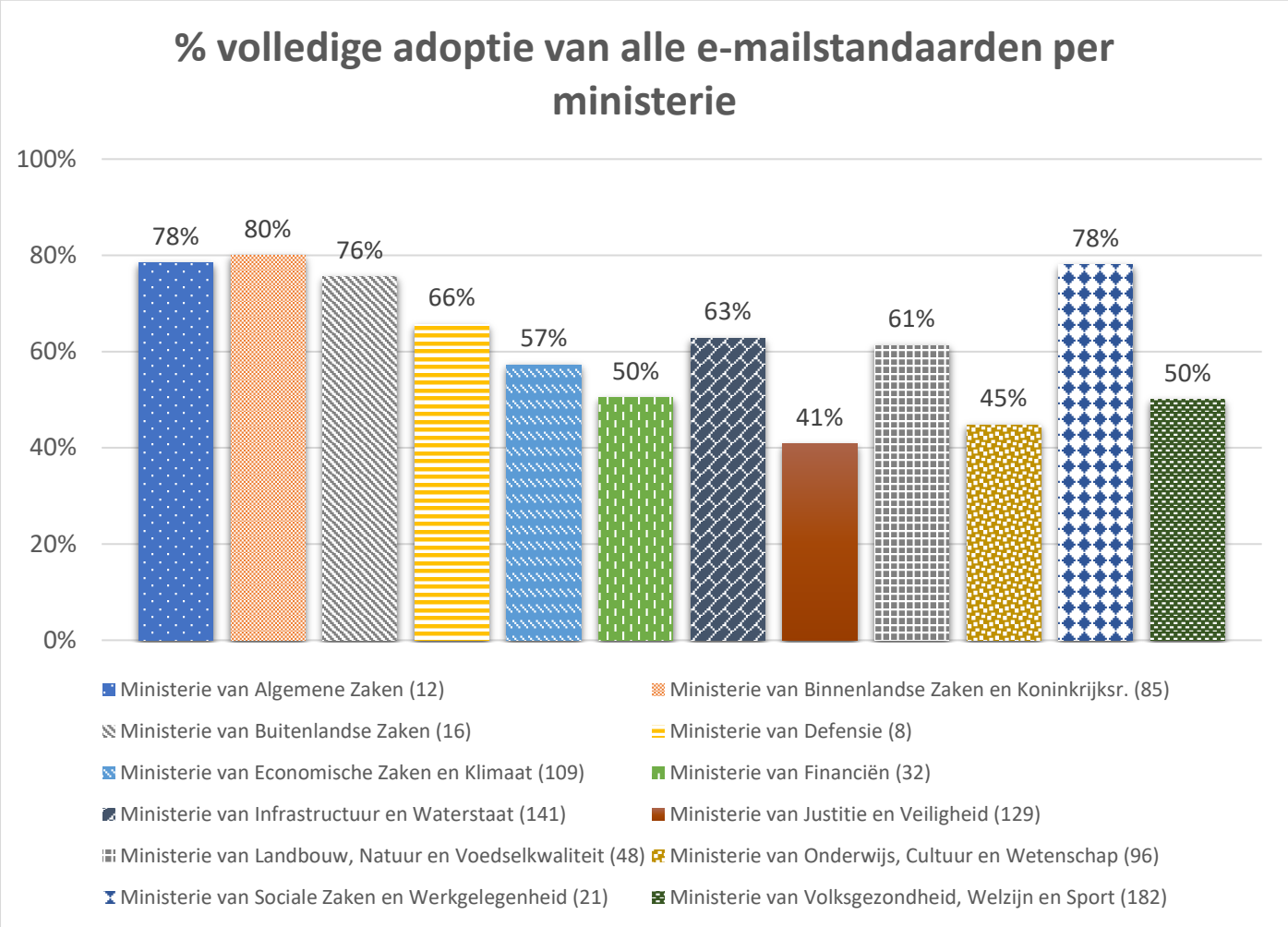
Onderstaande cijfers laten zien in welke mate de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – *alle* afgesproken websitestandaarden voor veilig en modern webverkeer toepassen (inclusief IPv6 en RPKI).



Over het algemeen hebben ministeries met een klein webportfolio, zoals de ministeries van Algemene Zaken en Defensie, een hoge mate van adoptie. Het ministerie van Sociale Zaken en Werkgelegenheid, met een relatief beperkt portfolio, scoort hoger dan gemiddeld.

7.2. Totaalbeeld e-mailstandaarden (incl. IPv6 en incl. RPKI)

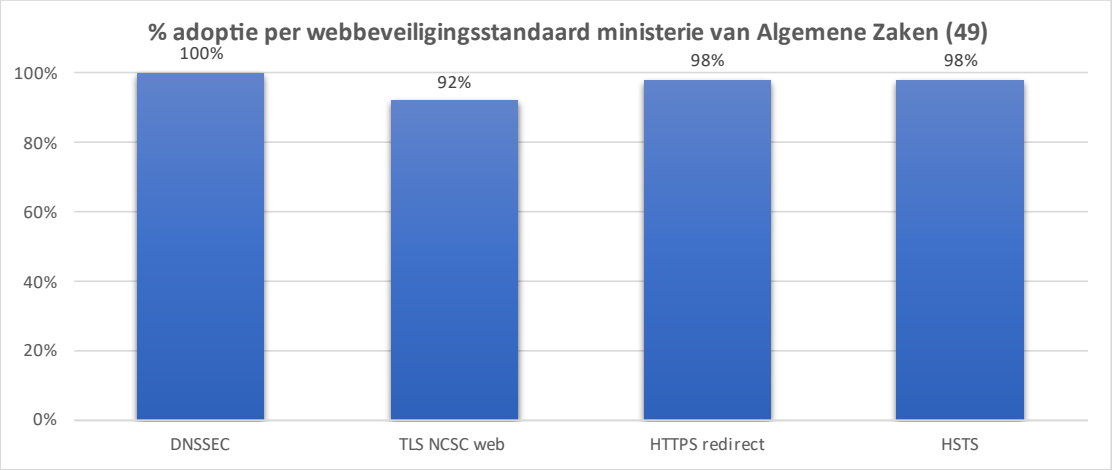
Onderstaande cijfers laten zien in welke mate de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – *alle* afgesproken e-mailstandaarden voor veilig en modern e-mailverkeer toepassen (inclusief IPv6 en RPKI).

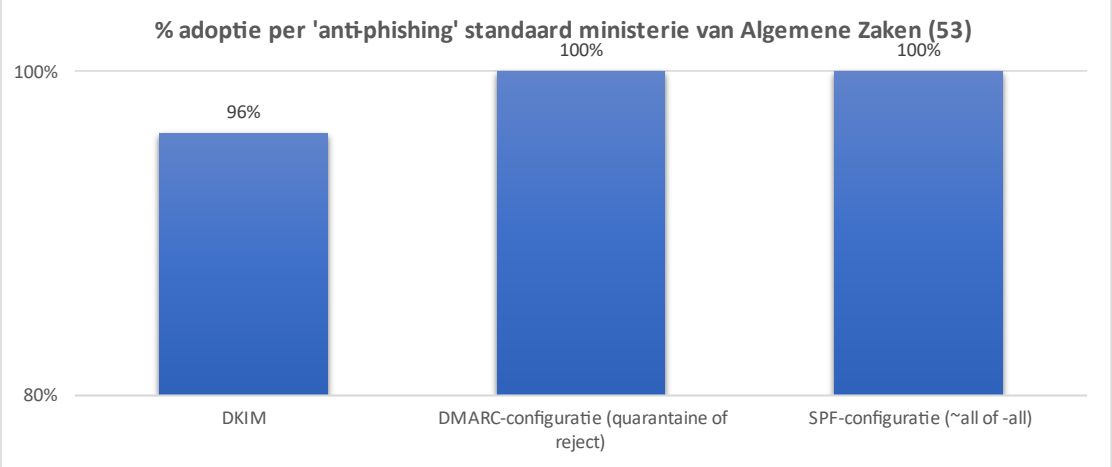


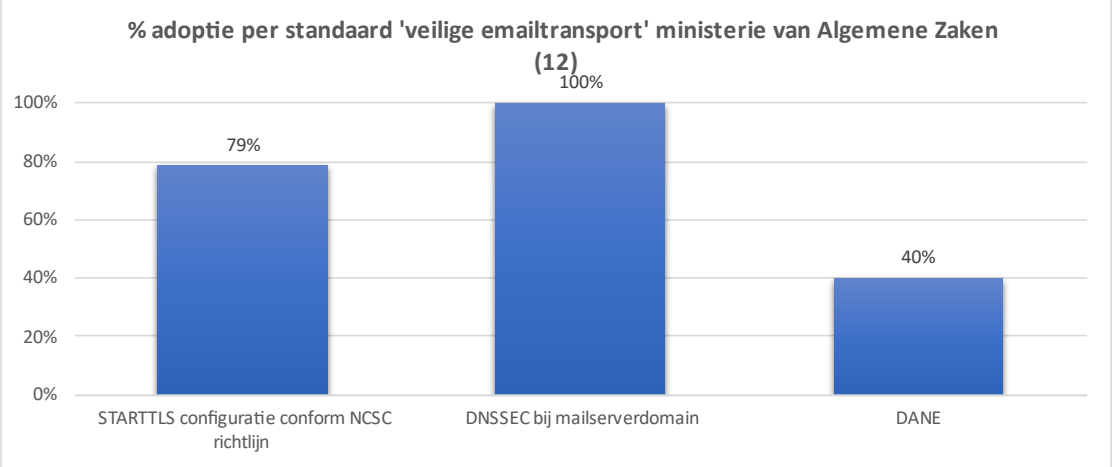
Vergelijkbaar met de adoptie van websitestandaarden, zien we dat ministeries met een beperkt portfolio, of actieve sturing op toepassing van standaarden, over het algemeen een hogere adoptiegraad bereiken.

De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per ministerie.

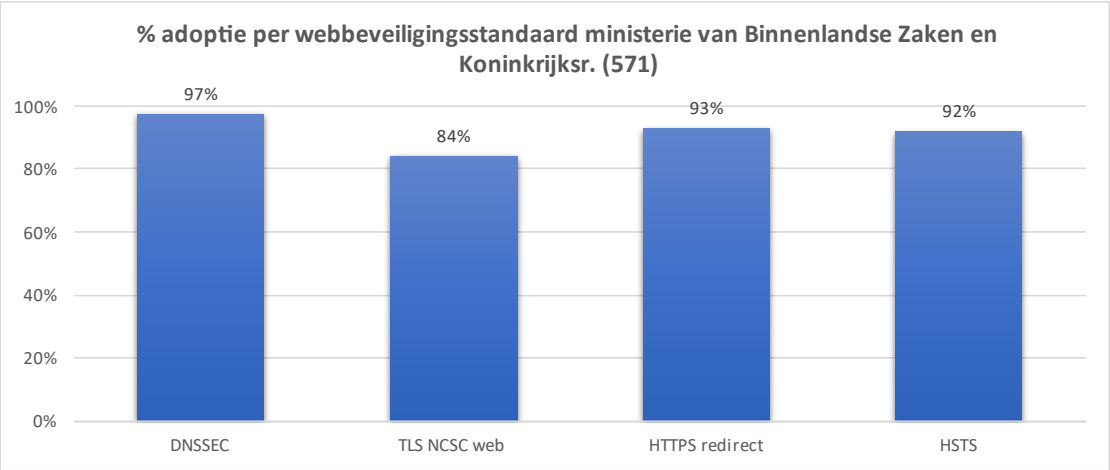
7.3. Ministerie van Algemene Zaken

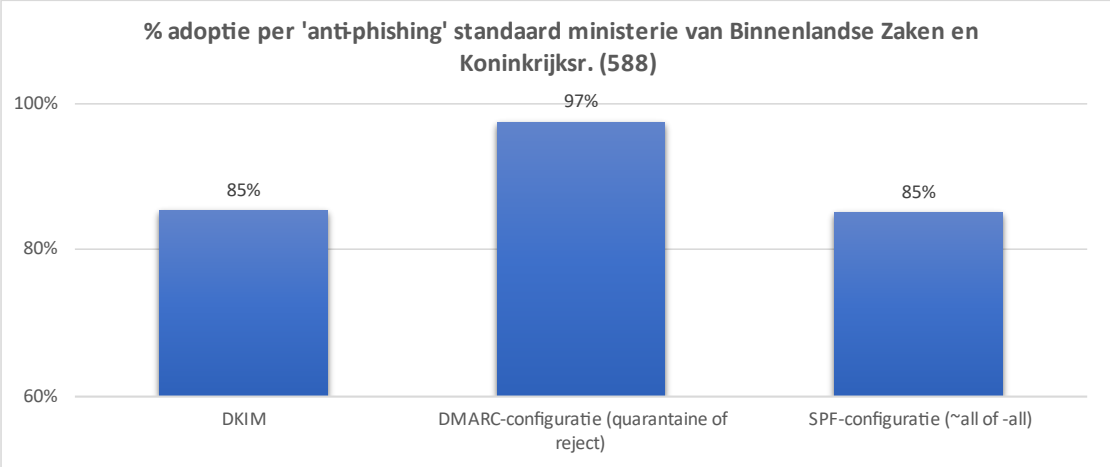


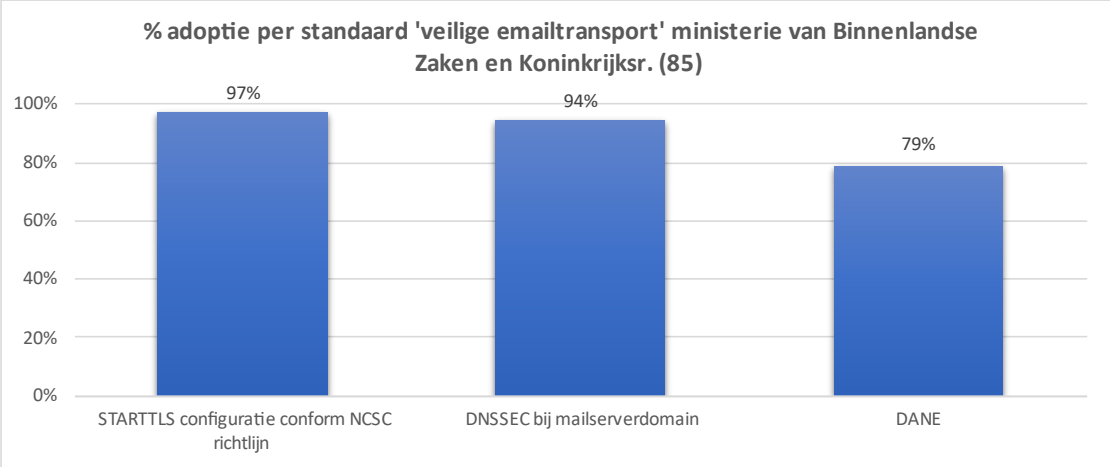




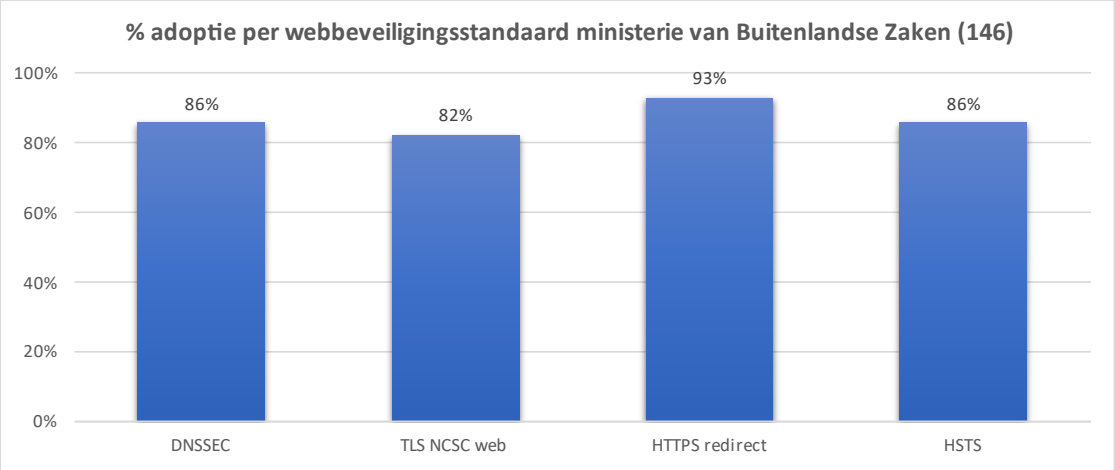
7.4. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

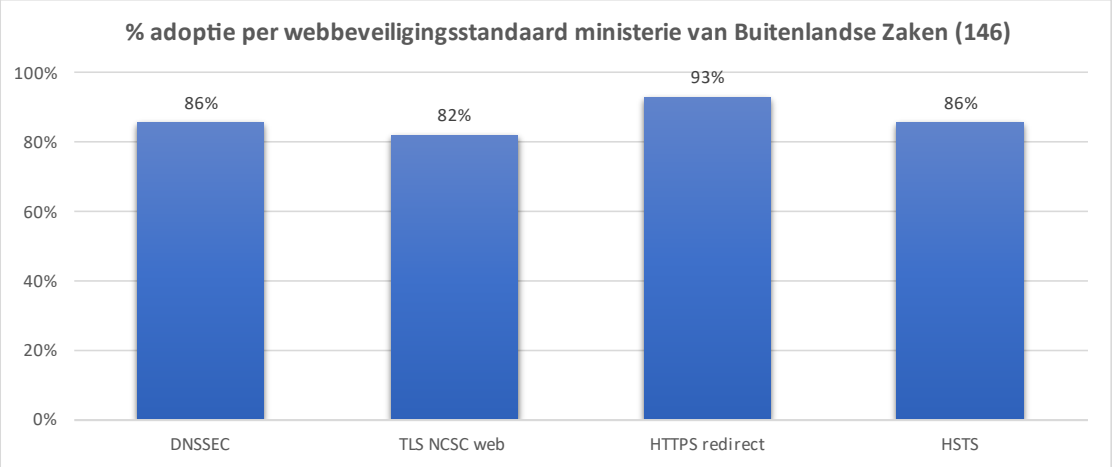


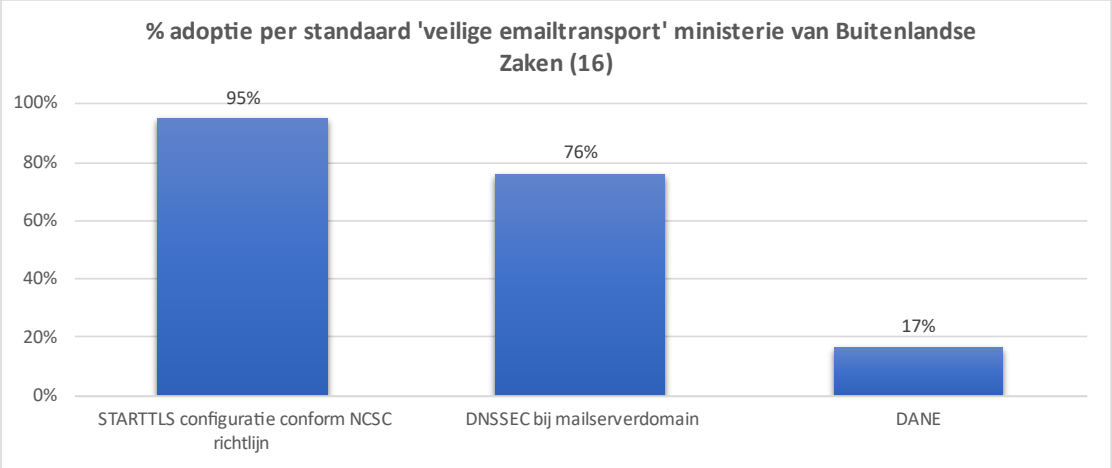




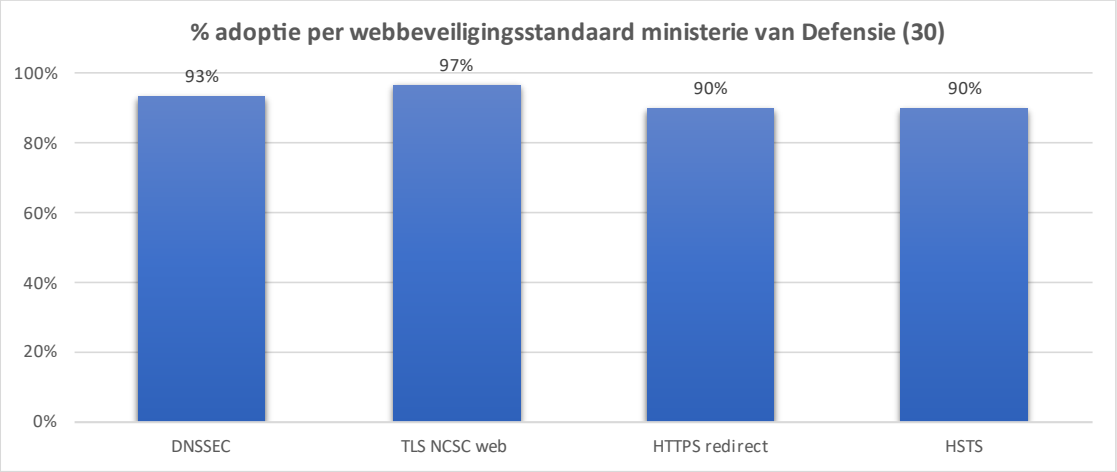
7.5. Ministerie van Buitenlandse Zaken

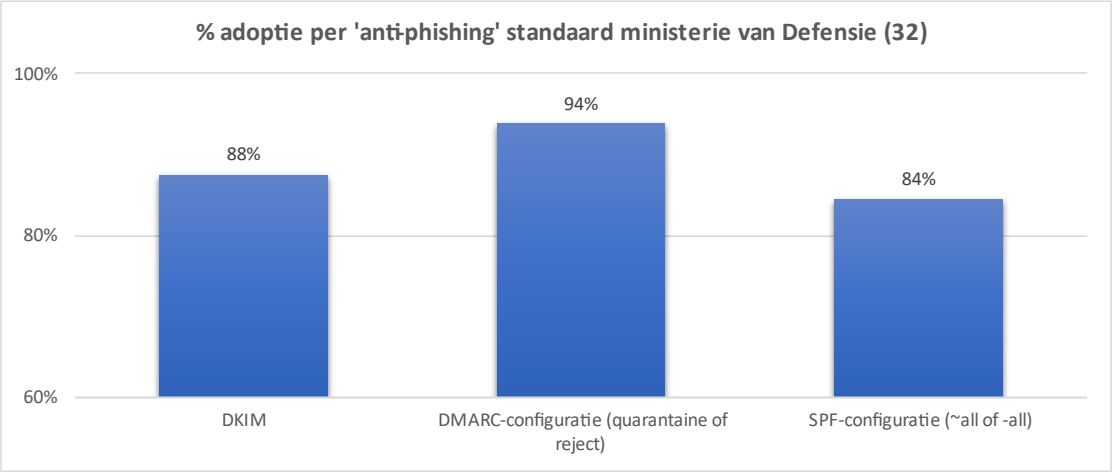


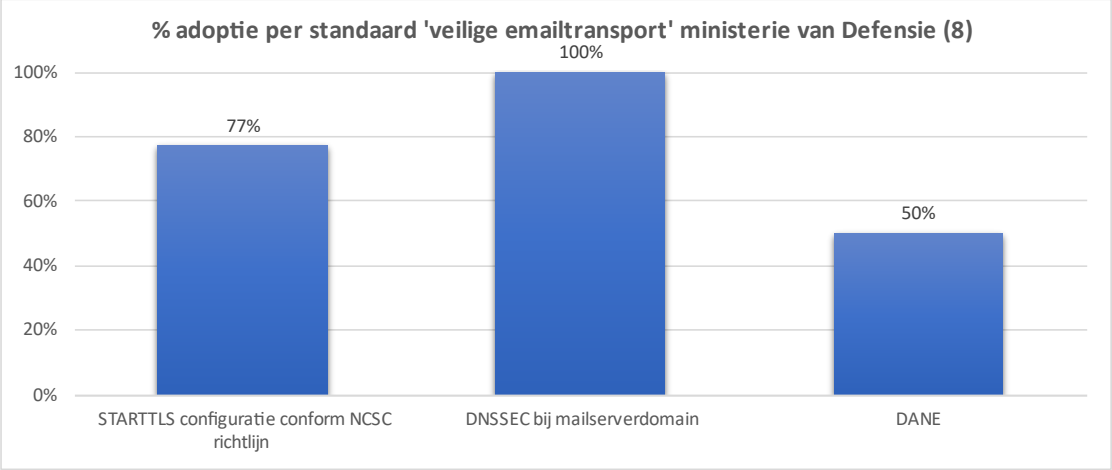




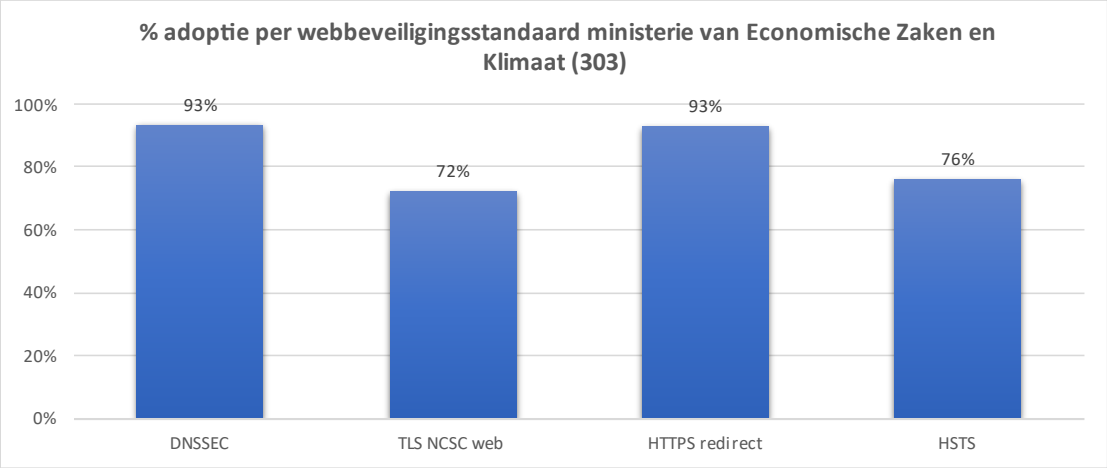
7.6. Ministerie van Defensie

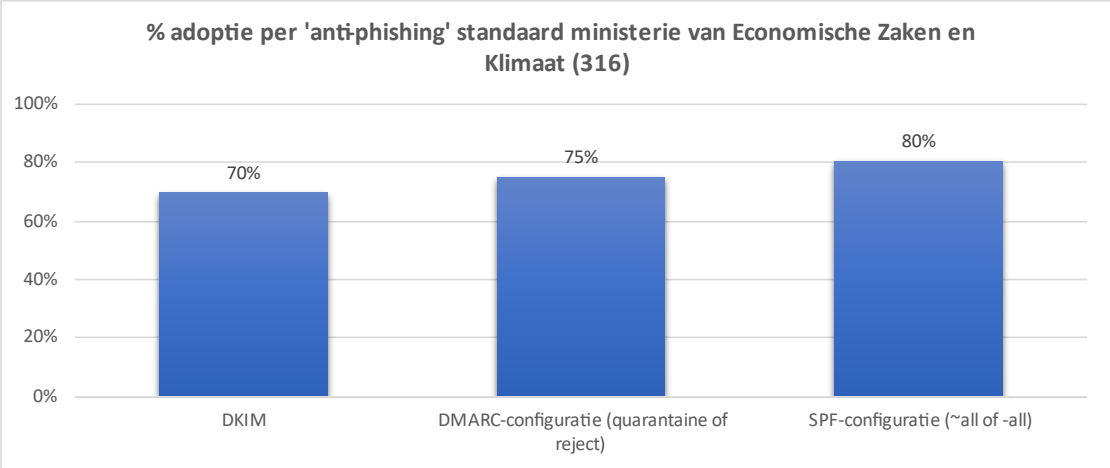


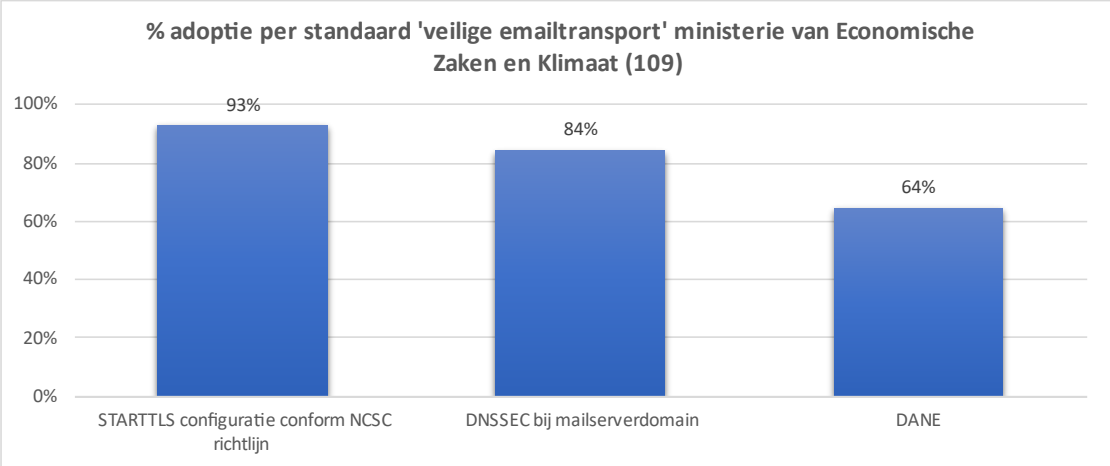




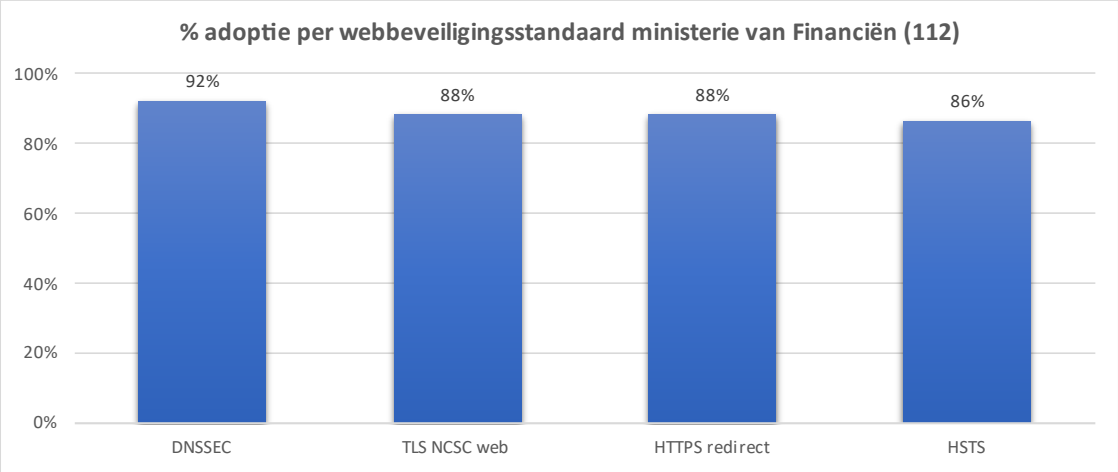
7.7. Ministerie van Economische Zaken en Klimaat

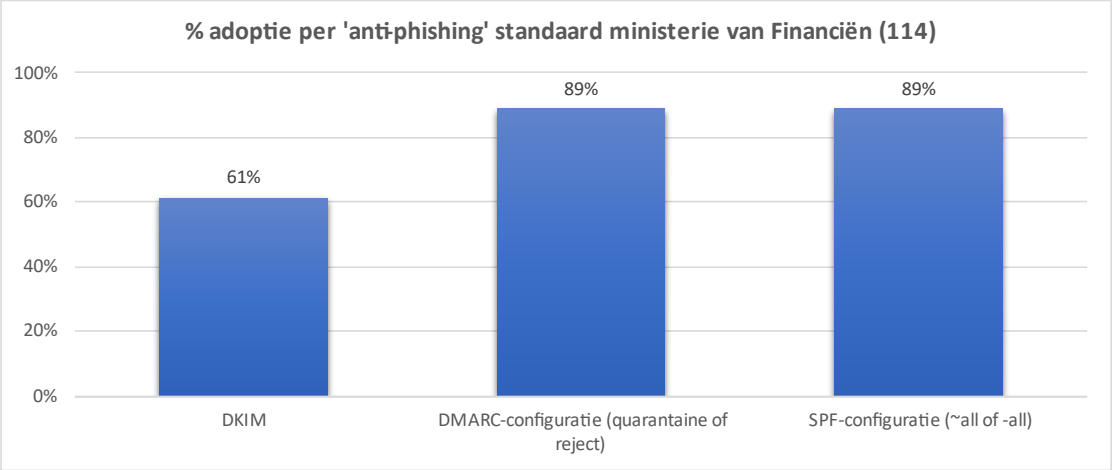


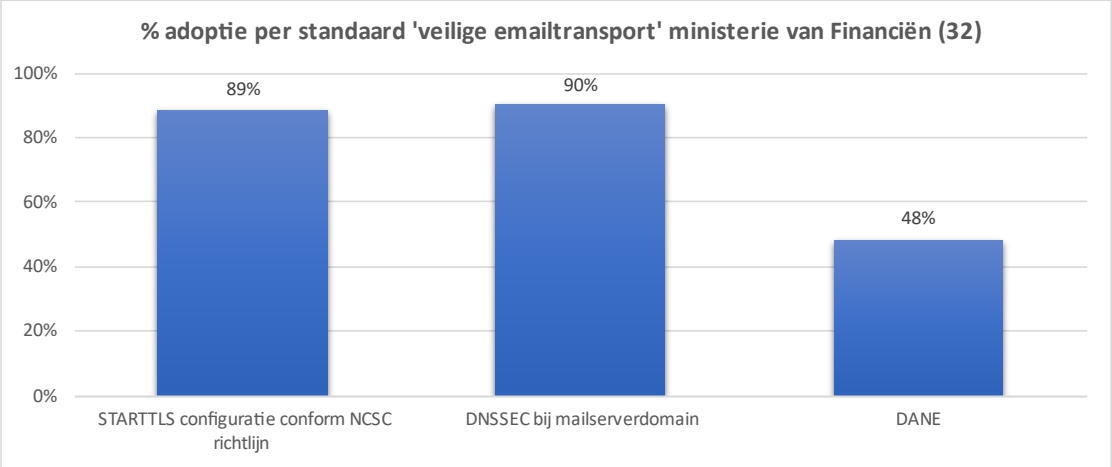




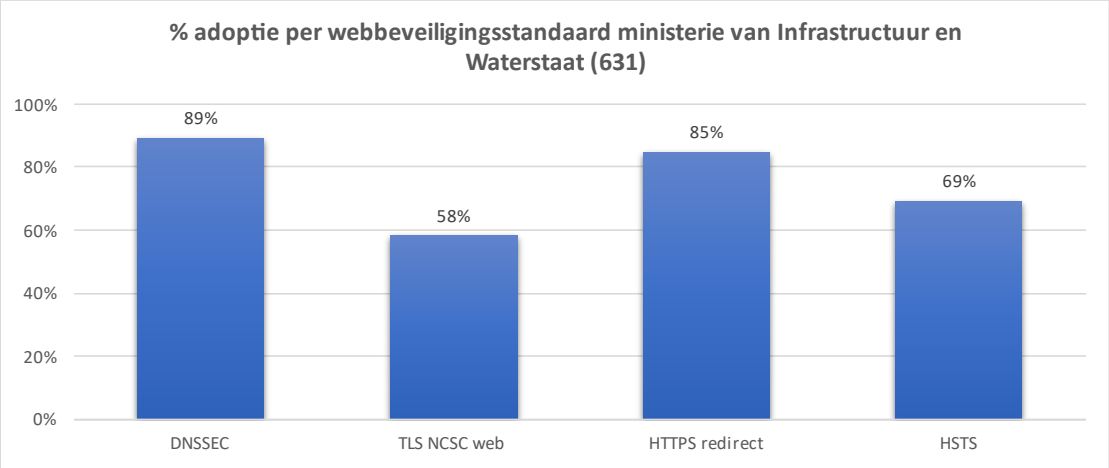
7.8. Ministerie van Financiën

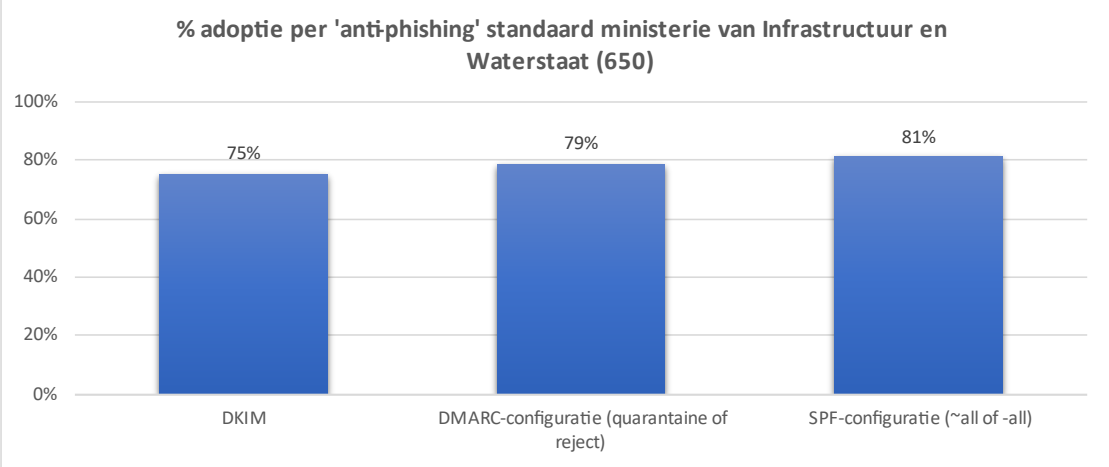


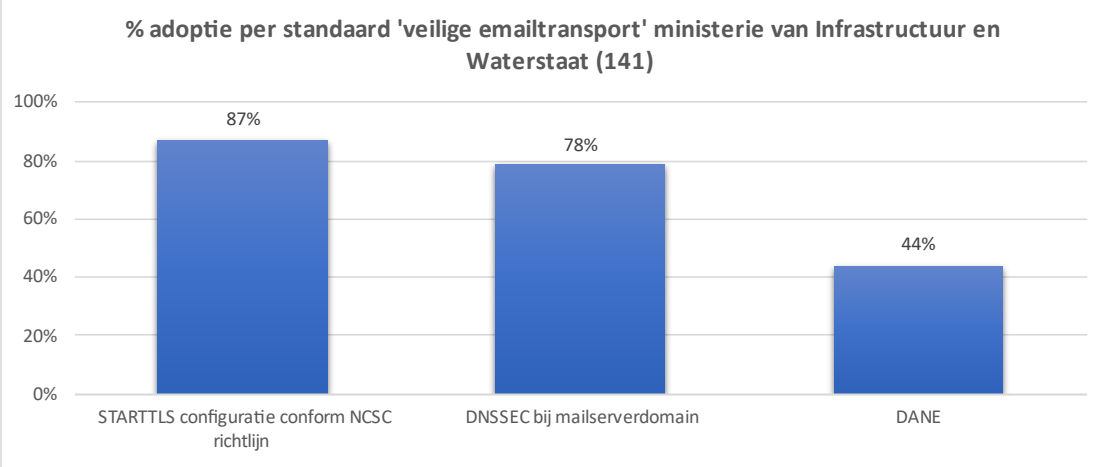




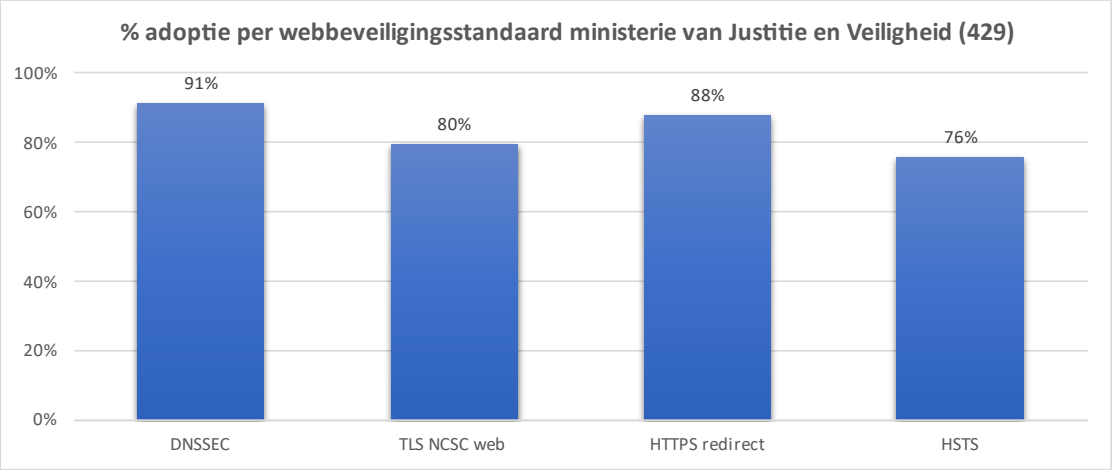
7.9. Ministerie van Infrastructuur en Waterstaat

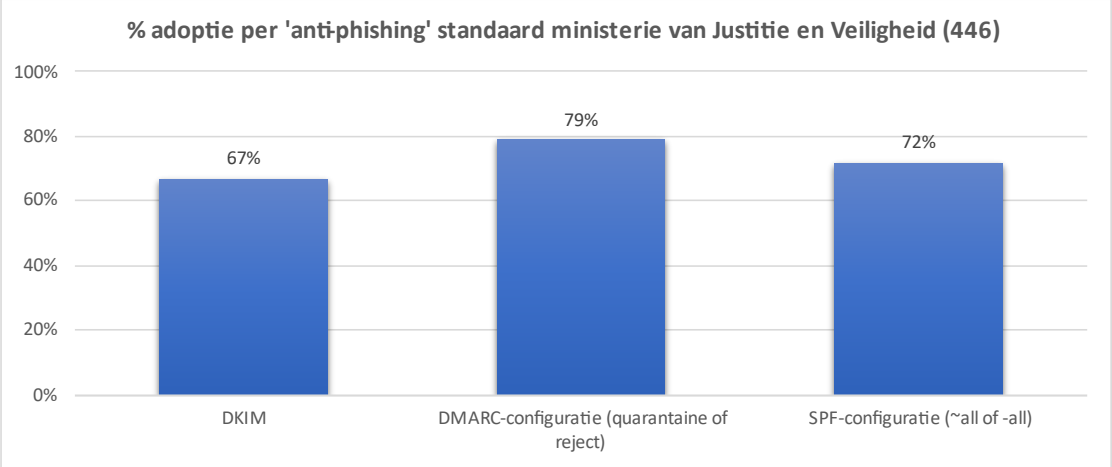


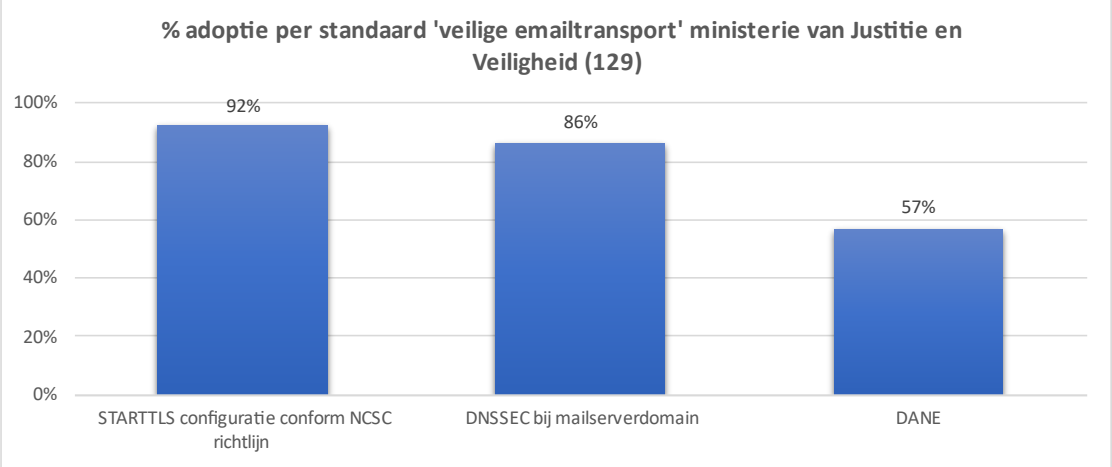




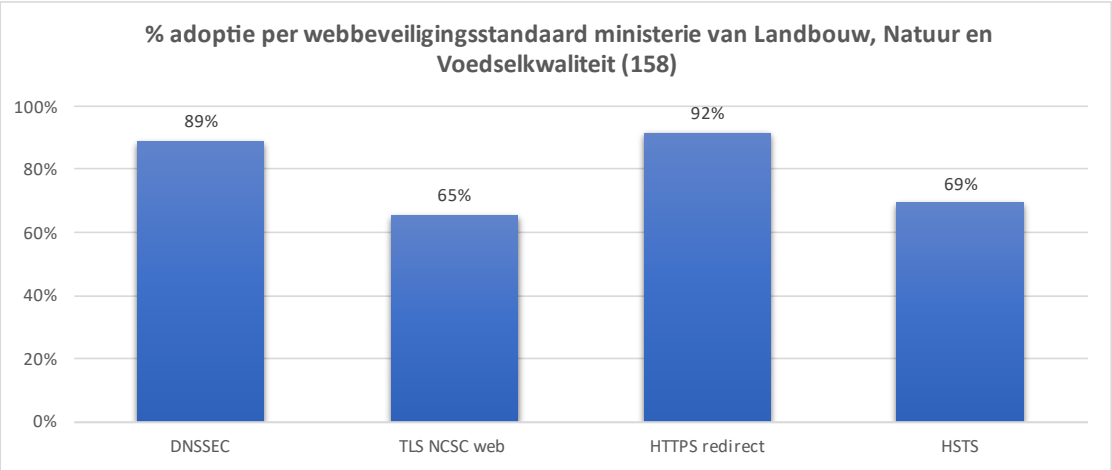
7.10. Ministerie van Justitie en Veiligheid

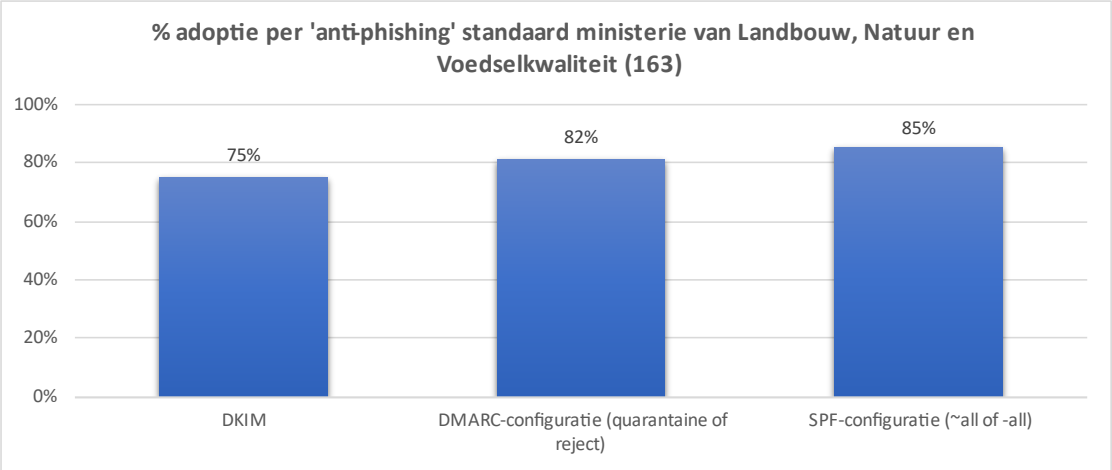


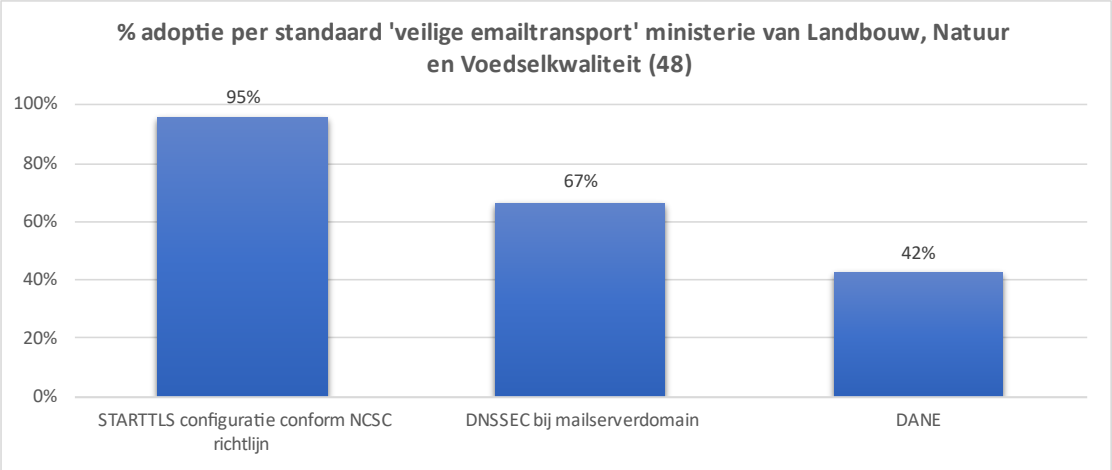




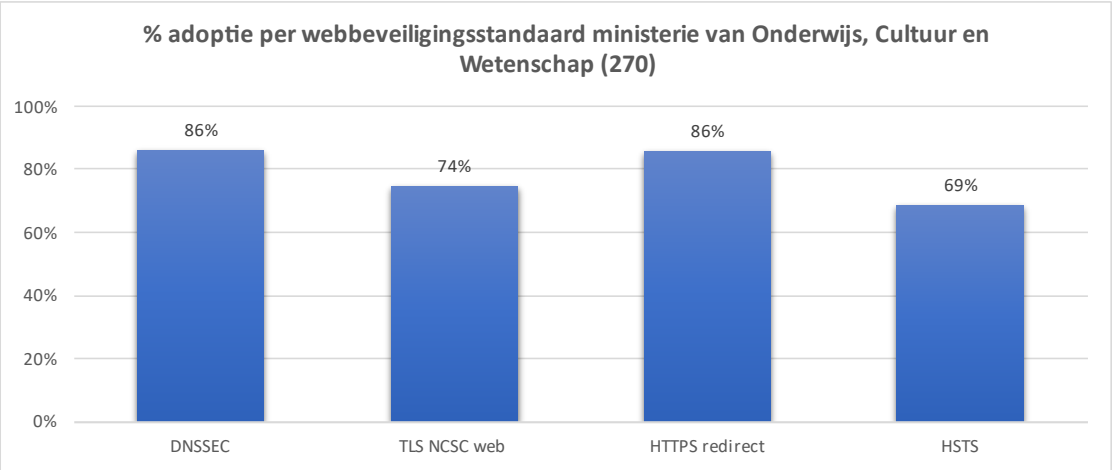
7.11. Ministerie van Landbouw, Natuur en Voedselkwaliteit

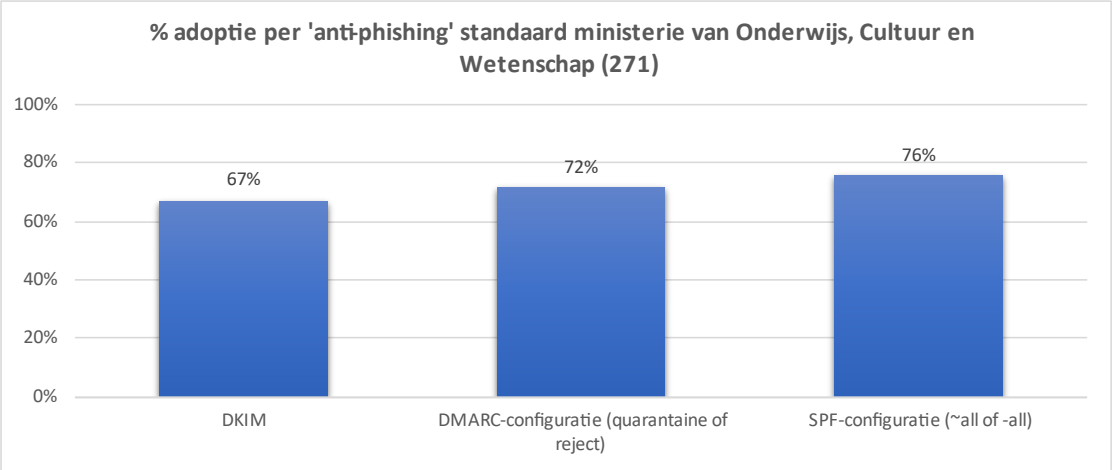


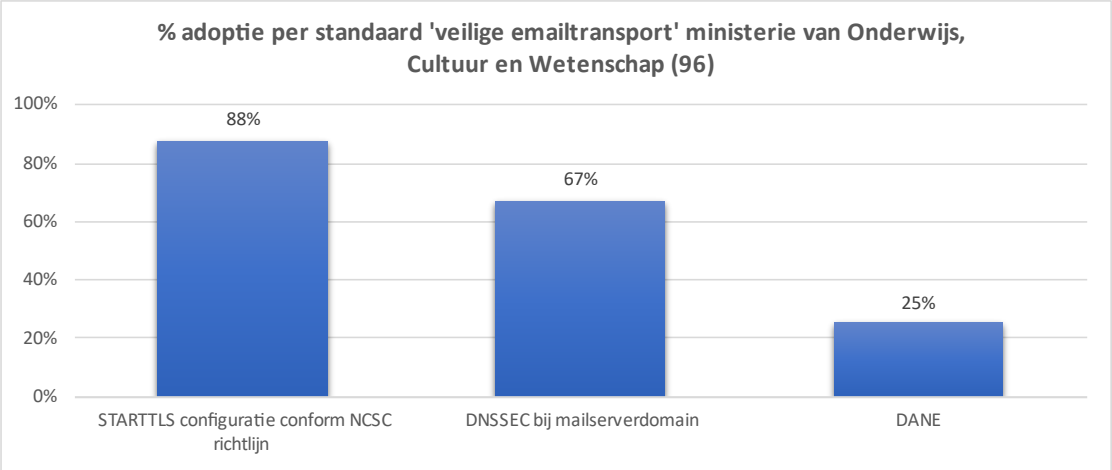




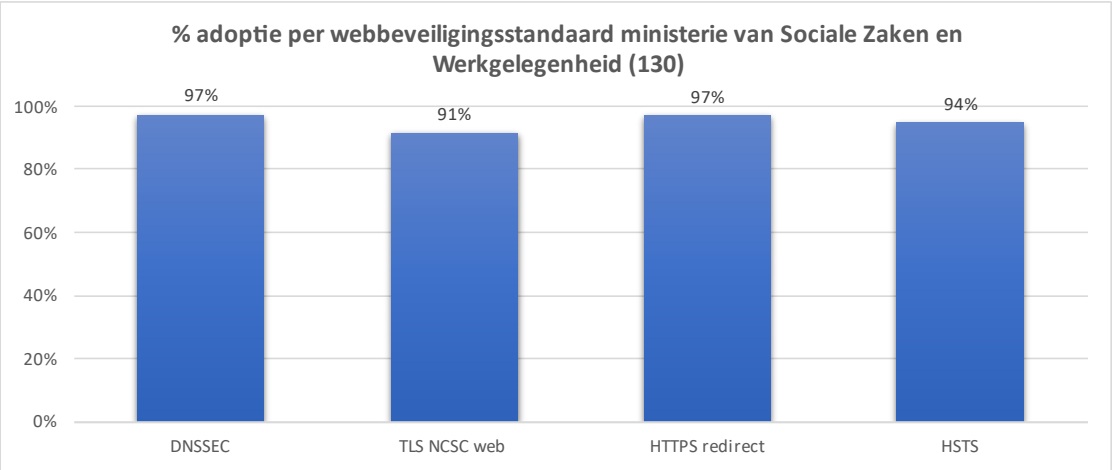
7.12. Ministerie van Onderwijs, Cultuur en Wetenschap

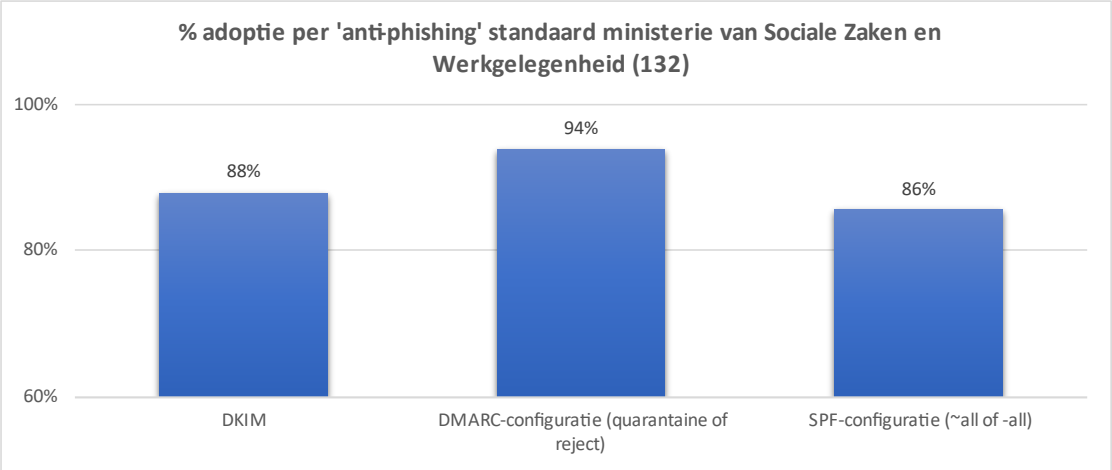


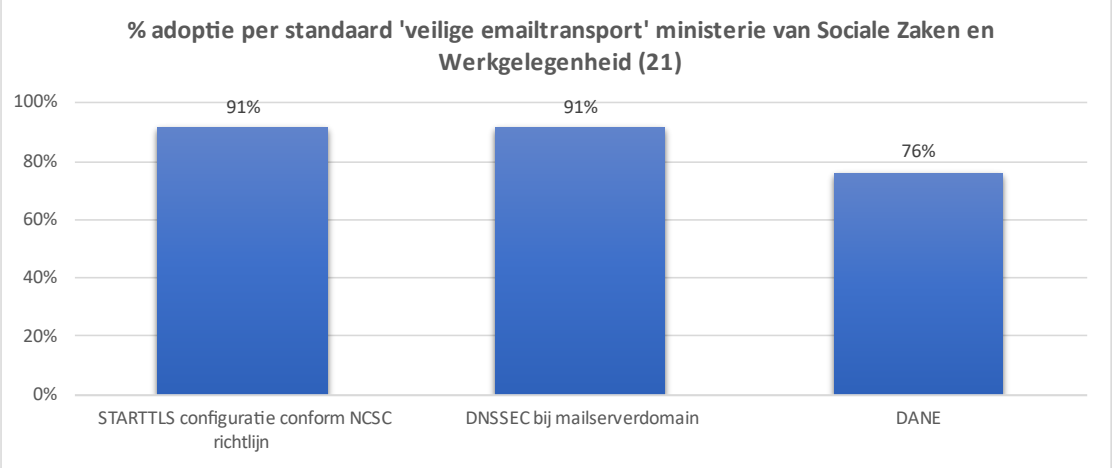




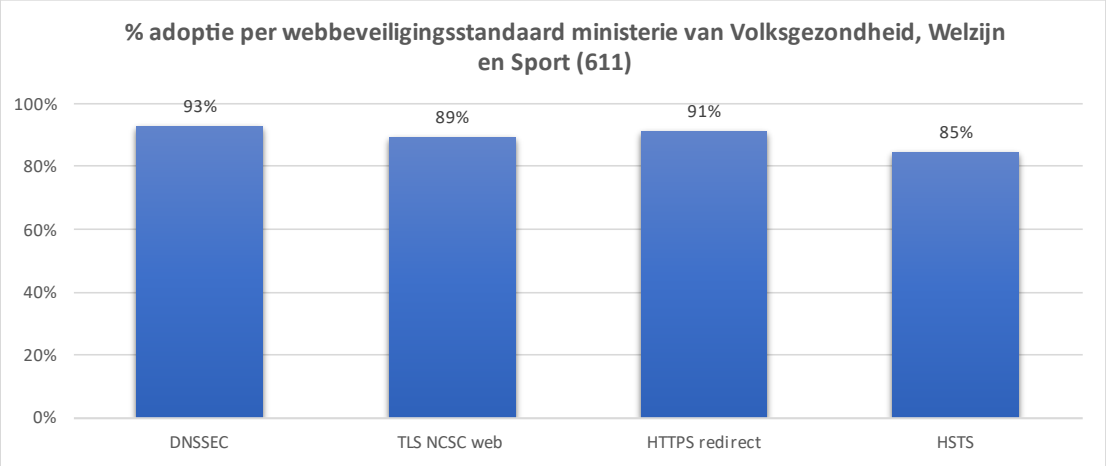
7.13. Ministerie van Sociale Zaken en Werkgelegenheid

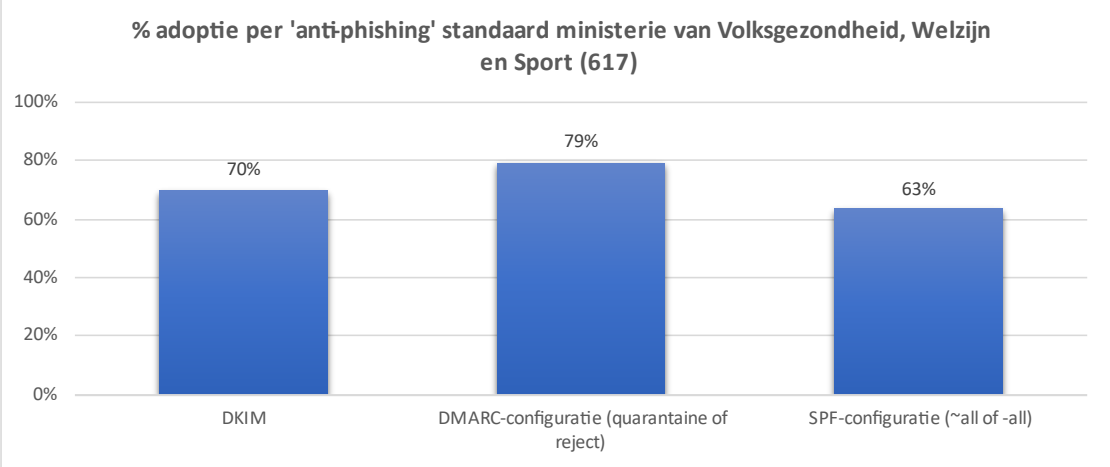


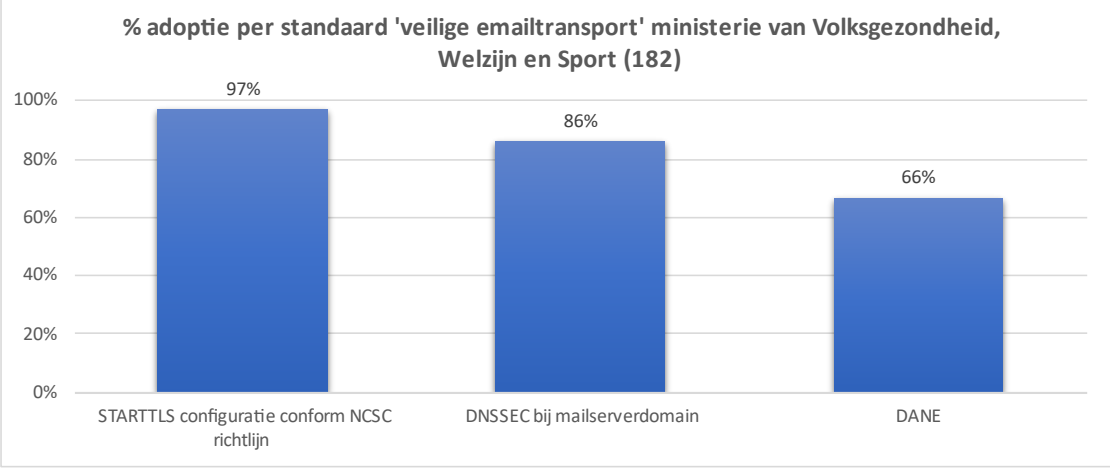




7.14. Ministerie van Volksgezondheid, Welzijn en Sport







8. Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden de mogelijkheid om via de website Internet.nl domeinen te toetsen op het gebruik van verschillende moderne internetstandaarden, waaronder een aantal informatieveiligheidstandaarden en IPv6, 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 bepaalde standaarden versneld te willen adopteren. Dit betekent concreet dat voor deze standaarden niet langer 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.

Na de eerste interbestuurlijke afspraak zijn er door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) aanvullende streefbeeldafspraken met verschillende uiterlijke implementatiedeadlines gemaakt. Van websites en e-mail van de overheid wordt vereist dat deze na het verlopen van de deadlines aan de standaarden en juiste configuratie voldoet.

Onderdeel van de afspraken 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.

8.1. Om welke standaarden gaat het

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

UITERLIJKE IMPLEMENTATIE-DATUM	**STANDAARDEN**
EIND 2017	HTTPS en TLS: beveiligde verbindingen van website 'met gevoelige gegevens' DNSSEC: integriteit domeinnaam-gegevens SPF: echtheidswaarmerk ter preventie mailspoofing DKIM: echtheidswaarmerk ter preventie mailspoofing DMARC: beleid en rapportage ter preventie mailspoofing

EIND 2018	HTTPS, TLS en HSTS conform de TLS-richtlijnen van NCSC: beveiligde verbindingen van alle websites
EIND 2019	STARTTLS en DANE: encryptie van mailverkeer SPF en DMARC: het instellen van strikt beleid voor deze emailstandaarden
EIND 2021	IPv6 (naast IPv4): moderne internetadressering van overheidswebsites en e-maildomeinen van e overheid
EIND 2024	RPKI: beveiliging van internetroutering

8.2. Om welke internetdomeinen gaat het

In totaal zijn in deze meting 5206 internetdomeinen van overheidsorganisaties getoetst, bestaande uit:

- Alle internetdomeinen uit het Websiteregister Rijksoverheid;
- Alle internetdomeinen uit het Register van Overheidsorganisaties;
- Internetdomeinen die als ontbrekend zijn gemeld bij een initiële teruglegging;
- Internetdomeinen uit voorgaande metingen.

De lijst betreft een selectie van alle overheidsdomeinnamen. De lijst is niet volledig en kan dat ook niet zijn omdat er binnen de overheid geen eenduidig overzicht is van domeinnamen. De gemeten internetdomeinen zijn bij lange na niet alle domeinen waar het OBDO direct en indirect voor verantwoordelijk is. Zo heeft het ministerie van Algemene Zaken zicht op meer internetdomeinen van de Rijksoverheid, maar dit overzicht is niet openbaar gepubliceerd. Een 100%-score op de gemeten domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn.

8.3. Hoe wordt gemeten

De meting geeft de stand van zaken weer van 1 juli 2023. De meting laat zien of op een domeinnaam de standaarden worden toegepast. De meting is op dit moment nog niet via de samenwerkingsverbanden en koepels teruggelegd bij de organisaties van wie de domeinnamen zijn gemeten. Terugleggingen bij eerdere metingen waren vooral waardevol ter stimulering van de adoptie en zorgden in een klein aantal gevallen tot correcties, maar hebben toen niet geleid tot grote wijzigingen van de geaggregeerde resultaten. Ook deze meting zal nog worden teruggelegd. Eventuele correcties en ontvangen motivaties voor afwijking zullen in de uiteindelijke te publiceren versie van het rapport worden opgenomen.

De meting wordt uitgevoerd middels een bulktoets via de API van Internet.nl. Voor de webstandaarden wordt het hoofddomein getoetst met het subdomein 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. De score die een domeinnaam op Internet.nl kan halen (namelijk max. 100%) heeft een directe relatie met het resultaat uit deze meting, aangezien deze meting alle standaarden bevat die de Internet.nl score kunnen beïnvloeden.

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.

8.4. 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:

- validatie van DNSSEC door de DNS-resolver van een overheidsorganisatie;
- validatie van de DMARC-, DKIM- en SPF-kenmerken door ontvangende mailservers van een overheidsorganisatie;
- validatie van DANE-kenmerken door verzendende mailservers van een overheidsorganisatie.
- validatie van RPKI door het netwerk van een overheidsorganisatie

Voor optimale bescherming is het van belang dat ook validatie op standaarden wordt toegepast door overheden.

8.5. 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.

8.5.1. Webstandaarden

Wij meten het gebruik van de beveiligingsstandaarden en IPv6 voor het web ook op domeinen die alleen gebruikt worden voor mail, wanneer deze domeinnamen doorverwijzen naar een ander domein. Ook bij deze doorverwijzingen moeten de standaarden juist worden toegepast om burgers te beschermen. Als doorverwijzingen 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).

STANDAARD	BESCHRIJVING
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 vóór 2018 aan te voldoen.
TLS CF. NCSC	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. TLS behoort bovendien zodanig geconfigureerd te zijn dat deze voldoet aan de aanbevelingen van het Nationaal Cyber Security Center (NCSC). 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 REDIRECT	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 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 vóór 2019 aan te voldoen.
IPV6 WEB	Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen op het Internet mogelijk. Er wordt getest of alle nameservers (minimaal twee) en tenminste één webserver een IPv6-adres hebben en bereikbaar zijn. Er wordt ook getest of de IPv6 website gelijk lijkt aan de IPv4 website. De streefbeeldafspraak was om hier vóór 2022 aan te voldoen.
RPKI WEB	Met RPKI kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routering vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routering negeren. Het netwerk valt terug op het 'oude' onbeveiligde routering als RPKI wegvalt. Getest wordt of alle route-aankondigingen naar de IP-adressen van de webservers en nameservers overeenkomen met de gepubliceerde RPKI Route Origin Authorisation (ROA).

8.5.2. E-mailstandaarden

Wij meten het gebruik van anti-phishing standaarden 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 respectievelijk de policies –all en p=reject).

STANDAARD	BESCHRIJVING
DMARC POLICY	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. Zolang er geen beleid is ingesteld weet de ontvanger nog niet wat te doen met verdachte e-mail. De configuratie moet op orde zijn. (NB: 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 niet-mailende domeinen waar dit goed is ingesteld heeft DKIM geen toegevoegde waarde. In de meting wordt dan geen score meegenomen voor DKIM. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF POLICY	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 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 CF. NCSC	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. 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 vóór 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.
IPV6 E-MAIL	Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen op het Internet mogelijk. Er wordt getest of alle nameservers (minimaal twee) van het e-maildomein en alle mailservers (MX) een IPv6-adres hebben en bereikbaar zijn. De streefbeeldafspraak was om hier vóór 2022 aan te voldoen.
RPKI E-MAIL	Met RPKI kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routering vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routering negeren. Het netwerk valt terug op het 'oude' onbeveiligde routering als RPKI wegvalt. Getest wordt of alle route-aankondigingen naar de IP-adressen van de e-mailservers en de nameserver van de e-mailserver overeenkomen met de gepubliceerde RPKI Route Origin Authorisation (ROA).