FS-20230412.5B1

Forum Standaardisatie
Standaard Samenwerken

Meting Informatieveiligheidstandaarden overheid begin 2023

Inclusief IPv6

Datum document: 30-03-2023

Status document: versie voor Forum Standaardisatie

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 geeft een achtergrondanalyse in leveranciersafhankelijkheid met betrekking tot de adoptie van standaarden.

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 bijlagen geven 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 januari 2023. In de eerste maanden van 2023 is de analyse uitgevoerd en zijn eventuele correcties doorgevoerd.

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 56% van de internetdomeinen alle verplichte websitestandaarden correct zijn toegepast. Dit is een stijging van 3 procentpunt ten opzichte van de vorige meting. Het gaat om belangrijke beveiligingsstandaarden voor vertrouwelijk webverkeer, en IPv6 voor duurzame bereikbaarheid van online diensten.

Bij 50% van de internetdomeinen zijn alle verplichte e-mailstandaarden correct toegepast. Dit is een toename van 6 procentpunt ten opzichte van mei 2022. Hier gaat het om belangrijke beveiligingsstandaarden om e-mailvervalsing uit naam van de overheid te voorkomen en het e-mailverkeer vertrouwelijk te houden, en ook IPv6 voor duurzame bereikbaarheid van online diensten.

Er zijn dus verbeteringen zichtbaar, maar het tempo moet omhoog. Op de huidige snelheid zouden de streefbeeldafspraken op zijn snelst over 7,5 jaar gehaald worden. Dit terwijl er mogelijk ook nieuwe afspraken over standaarden gemaakt zullen worden. Er zal dus meer vaart achter de adoptie gezet moeten worden.

In deze meting zijn in totaal 2654 overheidsdomeinen gecontroleerd. In de vorige meting waren dit 2584 overheidsdomeinen. De stijging komt voort uit nieuwe domeinnamen die zijn geregistreerd of 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. Wel is zichtbaar dat er verbeteringen plaatsvinden op het gebied van adoptie, zij het op een (te) langzaam tempo. De Wet Digitale Overheid wordt van kracht op 1 juni 2023. Middels deze wet kunnen standaarden wettelijk worden verplicht, zoals reeds is voorgenomen voor HTTPS en HSTS (veilige websiteverbindingen). Ook hier speelt de vraag hoe deze verdergaande verplichtingen de operationele werkvloer bereiken, en hoe vervolgens gestuurd wordt op naleving van de verplichtingen.

Ten opzichte van de vorige meting laten de ministeries van Binnenlandse Zaken en Economische Zaken en Klimaat een grote stijging in adoptie zien. De toegepaste methodiek van deze ministeries kan gebruikt worden als voorbeeld van een effectieve aanpak.

Bij lokale overheden is een zeer volledige adoptie te zien bij de gemeenten Aalten, Bergen (L), Bergen op Zoom, Bronckhorst, Doesburg, Doetinchem, Staphorst en Zuidplas.

Advies 1: maak per individuele overheidsorganisatie een plan van aanpak om de streefbeeldafspraken effectief te laten landen in de uitvoering zodat de verplichte standaarden worden geïmplementeerd. Een voorbeeld kan genomen worden aan de aanpak van de ministeries van BZK en EZK.

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.

Advies 2: organiseer regie op internetdomeinen binnen individuele overheidsorganisaties. Zet in op een groeistop van het domeinnaamportfolio en stuur idealiter op een inkrimping.

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.

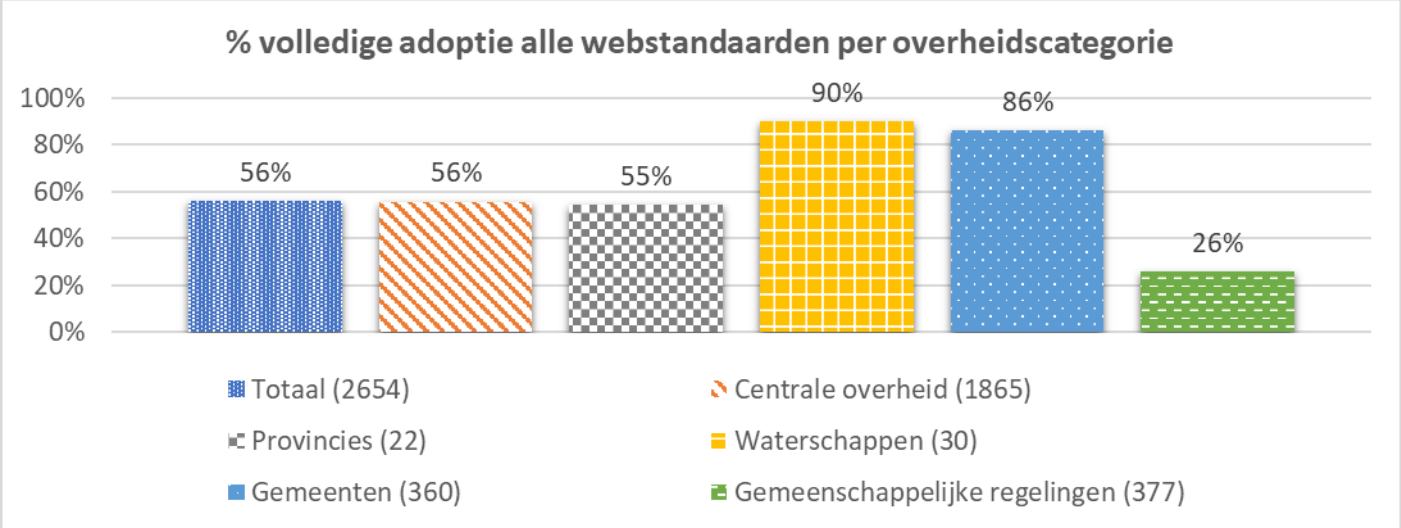
Advies 3: zorg ervoor dat de ondersteuning van verplichte open standaarden onderdeel zijn van het leveranciersmanagement van individuele overheidsorganisaties. Vraag leveranciers periodiek naar de planning voor ondersteuning van standaarden. Overweeg om over te stappen als een leverancier onvoldoende meebeweegt.

Advies 4: 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)

Onderstaande cijfers laten zien in welke mate de domeinnamen van verschillende overheidscategorieën *alle* afgesproken websitestandaarden voor veilig en modern webverkeer toepassen (inclusief IPv6). 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.

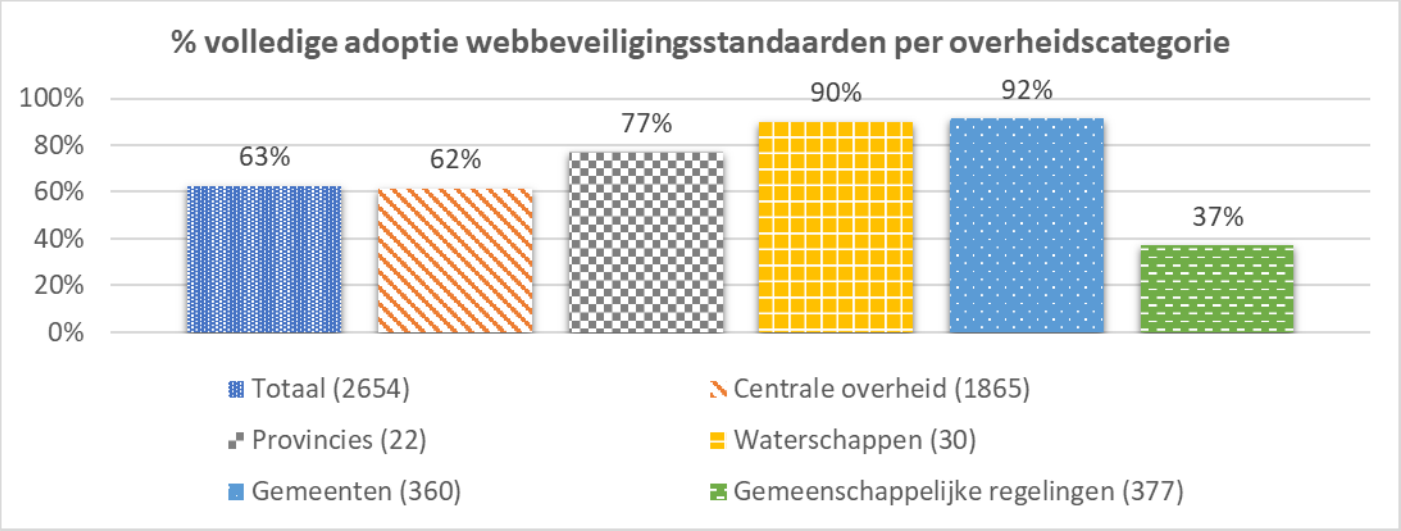
1.2.2. Websitebeveiligingsstandaarden (excl. IPv6)

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).

1.2.2.1. Adoptie per overheidscategorie

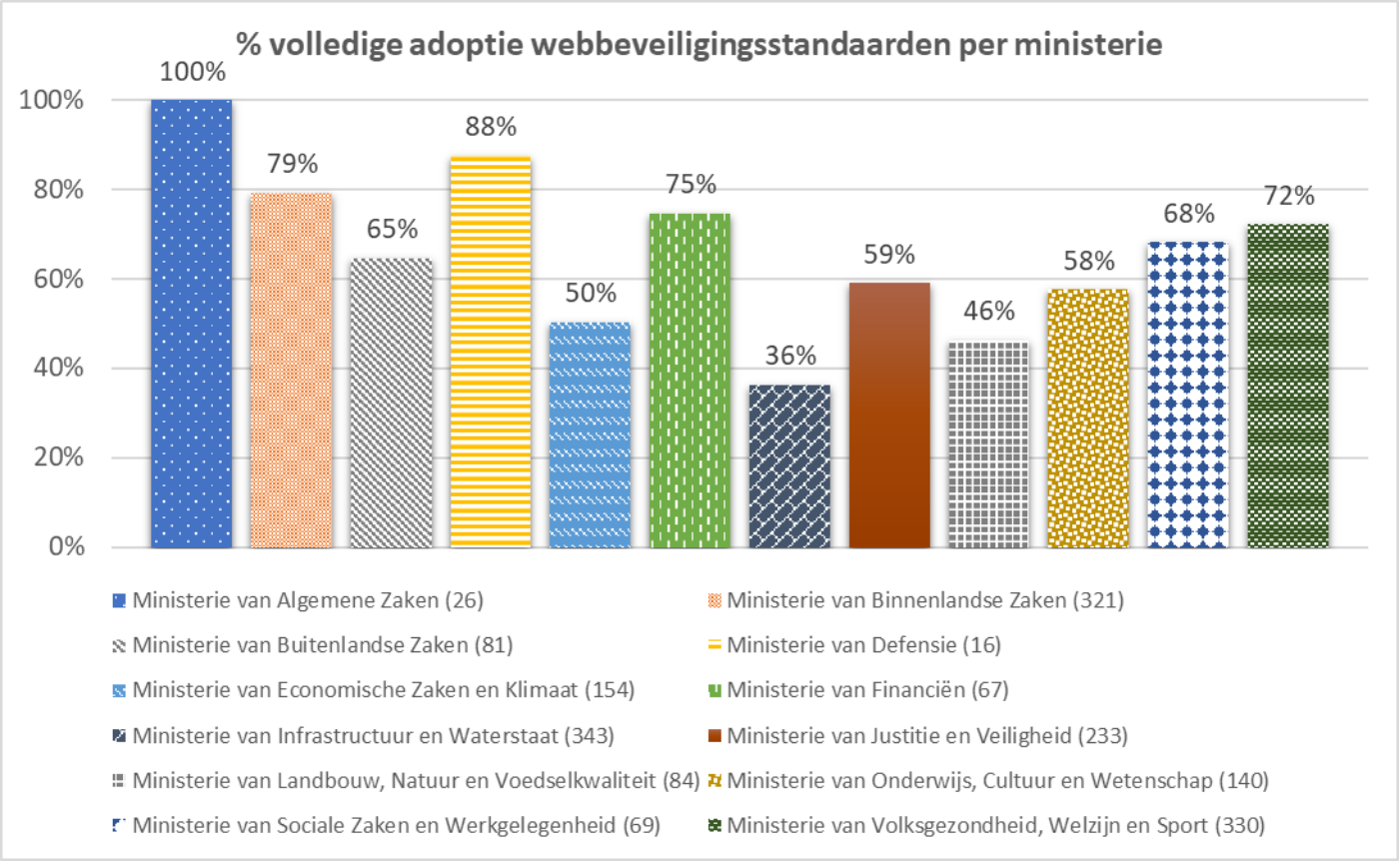
De achterblijvers zijn met name te vinden bij de centrale overheid en de gemeenschappelijke regelingen. De centrale overheid is getalsmatig oververtegenwoordigd in de meting doordat er veel secundaire internetdomeinen (campagnesites, projectsites, etc.) zijn meegenomen. Er is geen goed beeld van secundaire 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 (100%), Defensie (88%) en Binnenlandse Zaken (79%) in positieve zin op. De achterblijvers zijn de ministeries van Infrastructuur en Waterstaat (36%), Landbouw, Natuur en Voedselkwaliteit (46%), en Economische Zaken en Klimaat (50%).

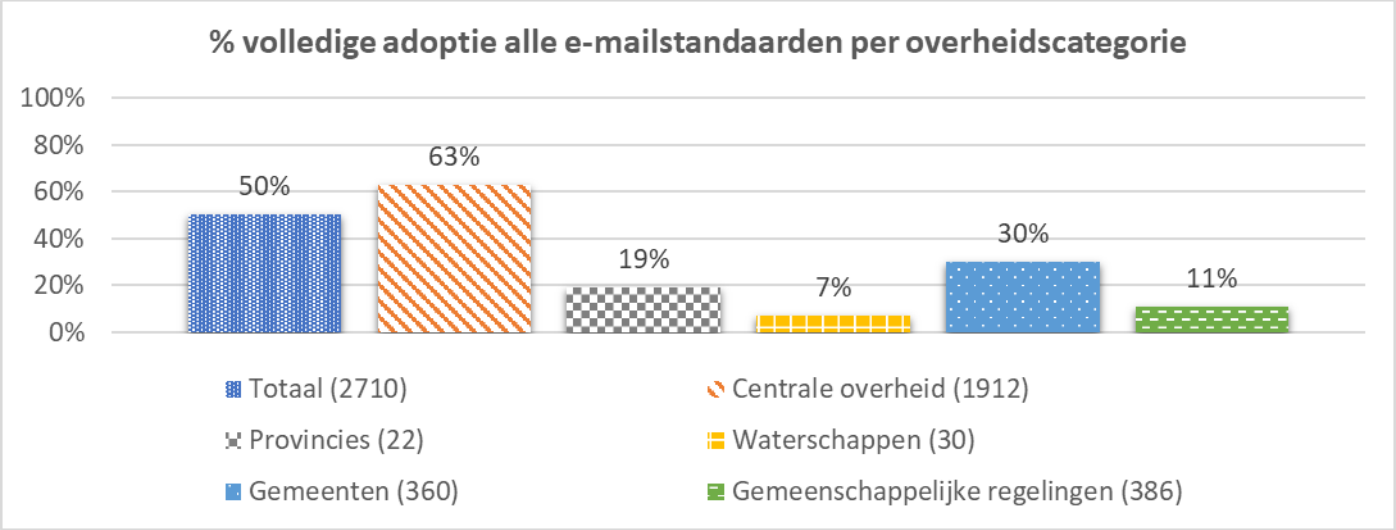


Voor meer details per ministerie zie hoofdstuk 7.

1.3. E-mailstandaarden

1.3.1. Totaalbeeld e-mail per overheidscategorie (incl. IPv6)

Onderstaande cijfers laten zien in welke mate de verschillende overheidscategorieën *alle* afgesproken websitestandaarden voor veilig en modern e-mailverkeer (inclusief IPv6) toepassen. De centrale overheid (63%) 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 (7%). 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.

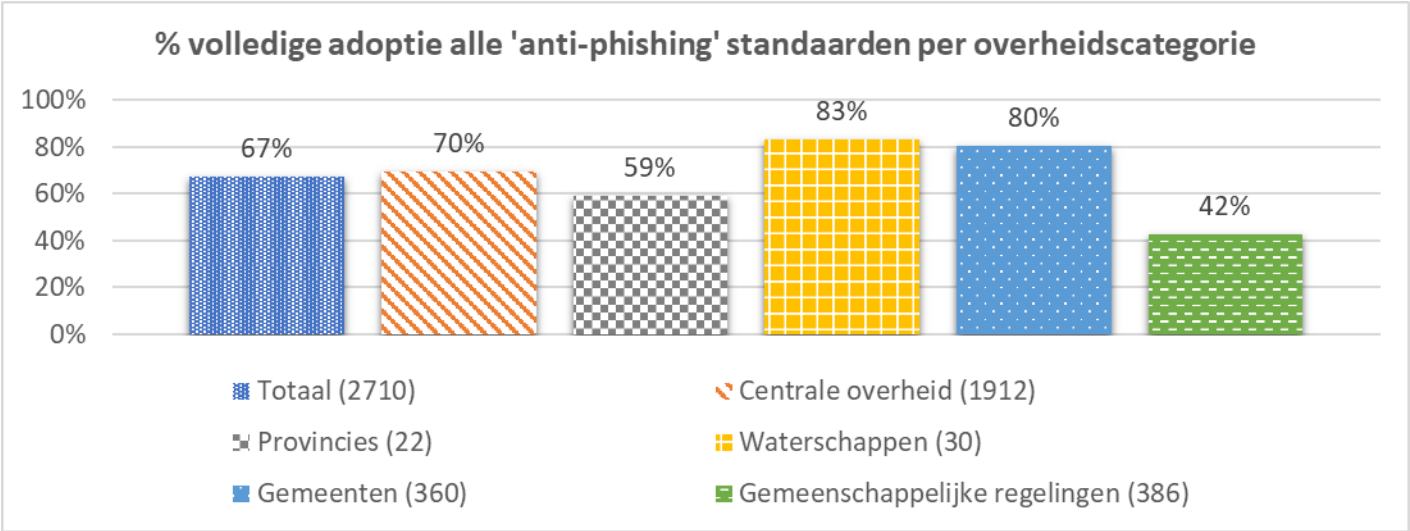
1.3.2. E-mailstandaarden voor bestrijding van phishing (excl. IPv6)

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).

1.3.2.1. Adoptie per overheidscategorie

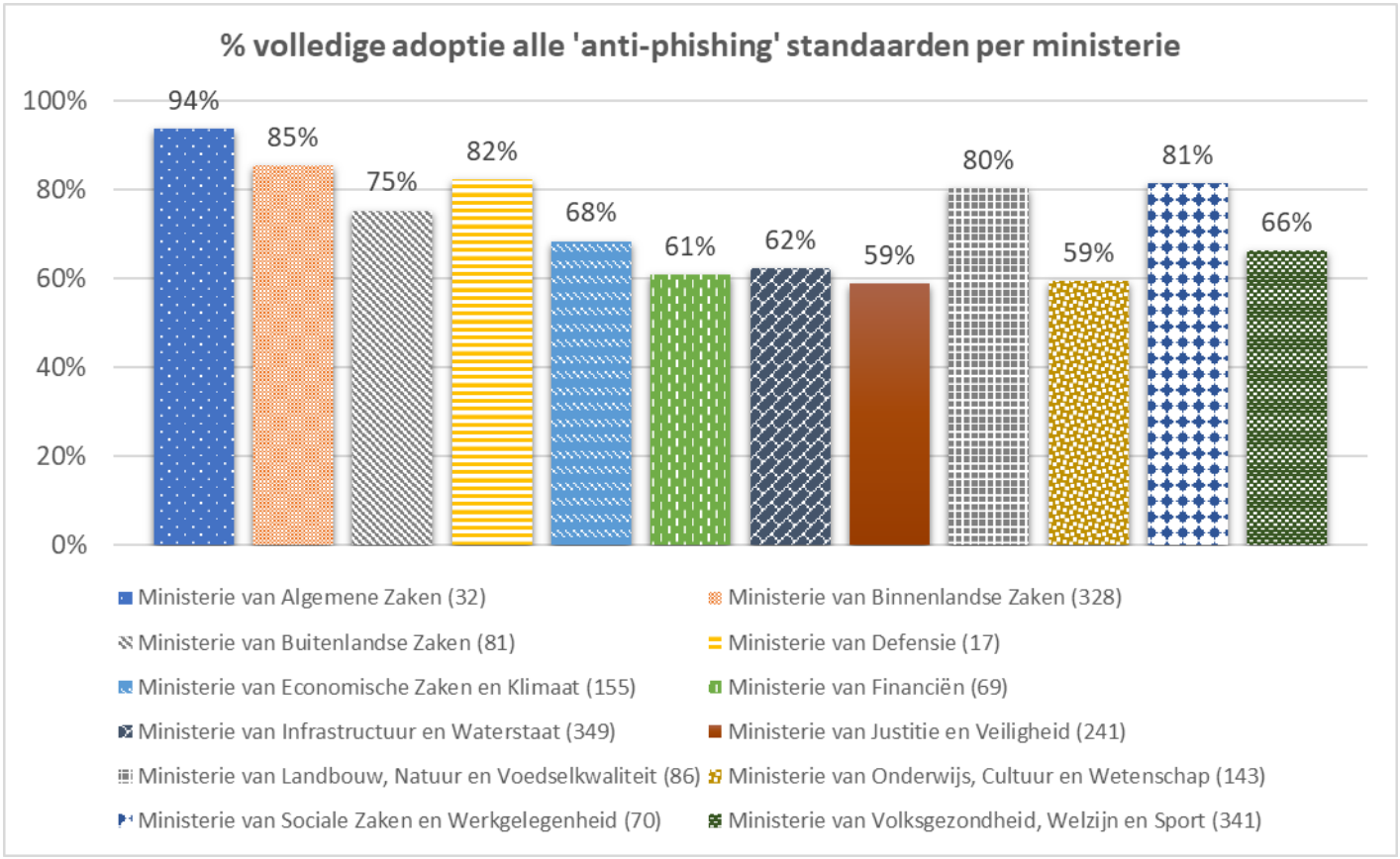
De waterschappen en gemeenten zijn positieve uitschieters in deze categorie. Wel gaat het bij deze categorieën voornamelijk om primaire domeinnamen. Er is geen inzicht in secundaire domeinnamen die in gebruik zijn, die waarschijnlijk gezamenlijk in de duizenden lopen. De gemeenschappelijke regelingen, waar lokale overheden vaak in participeren, scoren slecht met 42% goed geconfigureerde e-maildomeinen.



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 (94%) en Binnenlandse Zaken (85%) positief op. De ministeries van Justitie en Veiligheid (59%) en Onderwijs, Cultuur en Wetenschap (59%) 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)

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.

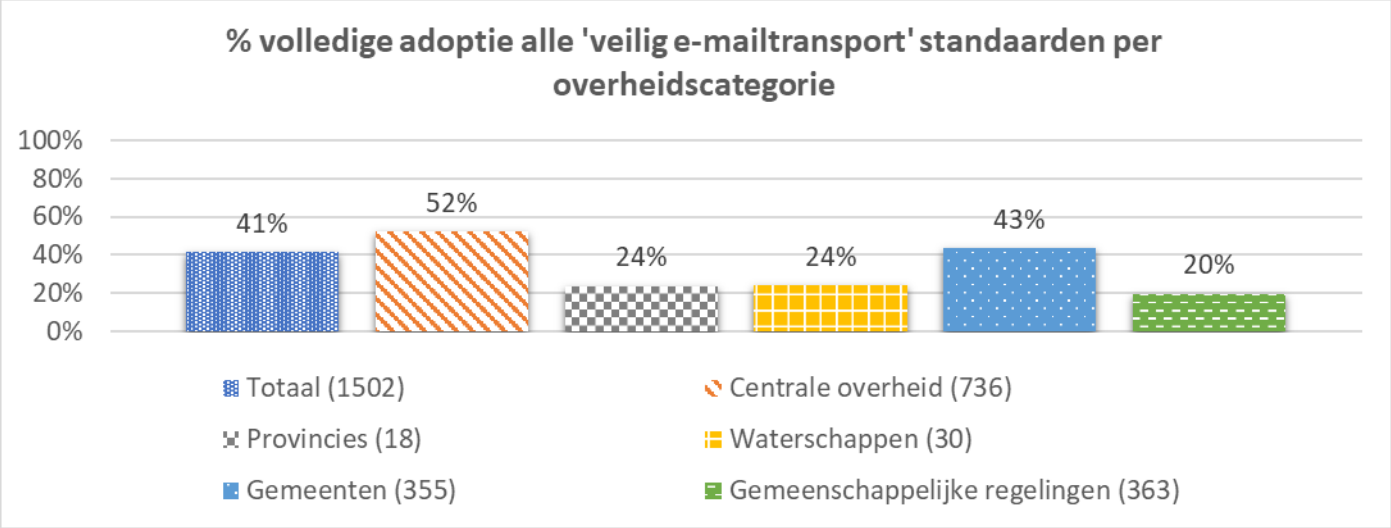
Omdat de test zich beperkt tot een controle of de e-mailontvangst van de betreffende overheden voldoende veilig e-mailverkeer mogelijk maakt, zijn alleen de internetdomeinen met een ontvangende mailserver (MX) meegenomen in de statistieken. Hierdoor is het aantal

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).

1.3.3.1. Adoptie per overheidscategorie

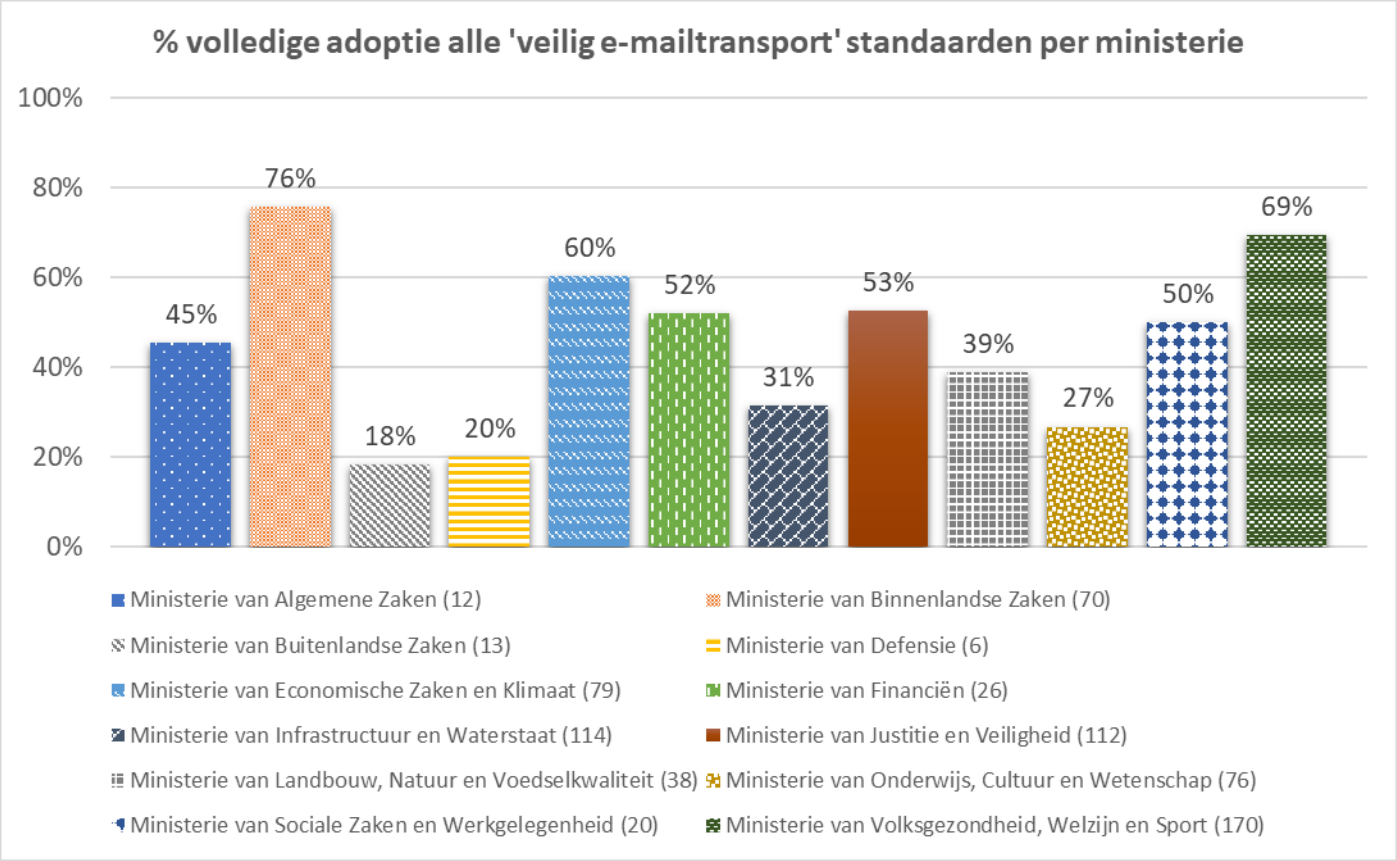
De standaarden op het gebied van veilige e-mailtransport blijken over het algemeen het minst goed geïmplementeerd. De centrale overheid (52%) en gemeenten (43%) scoren relatief het beste op deze standaarden. Het gebruik van gemeenschappelijke e-maildienstverleners geeft daarbij een hefboomeffect. Decentrale 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 Buitenlandse Zaken is een negatieve opvaller met slechts 8% volledige adoptie van standaarden voor veilig e-mailtransport.



Voor meer details per ministerie zie hoofdstuk 7.

1.4. Leveranciersafhankelijkheid

Nieuw in deze meting is dat er ook gekeken is naar de leveranciersafhankelijkheid in relatie tot het achterblijven op adoptie. Het doel van de analyse is om individuele leveranciers in kaart te brengen, die veroorzaken dat een (groot) deel van de overheid niet aan een specifieke standaard voldoet. Op deze manier kan achterhaald worden welke leveranciers aangespoord dienen te worden deze standaarden te implementeren, om een grote stijging in adoptie te behalen.

Hieronder volgt een samenvatting van de resultaten. Een uitgebreidere analyse over adoptie is uitgezet in hoofdstuk 5.

1.4.1. Leveranciers en IPv6

IPv6 moet worden toegepast op webservers, mailservers en nameservers die verbonden zijn aan de domeinnaam.

Allereerst is gekeken naar de IPv6 adoptie bij nameservers. Als naar de achterliggende leveranciers voor de domeinnamen gekeken wordt, valt de hoge adoptie van IPv6 onder nameservers op, slechts 2% van de domeinnamen voldoet niet. Het bleek hier om meerdere kleine leveranciers te gaan die hun implementatie nog niet op orde hebben.

Een ander beeld is te zien wanneer gekeken wordt naar de nameservers van de gebruikte mailservers. Hiervan maakt 34% gebruik van een nameserver van Microsoft Office 365, welke nog geen IPv6 ondersteunt.

1.4.2. Leveranciers en DNSSEC/DANE

Van de websites is 10% niet beveiligd met DNSSEC. Voor 6.5% is te stellen dat de nameserverleveranciers van het domein geen technische limitatie hebben om DNSSEC in te stellen. Meer onderzoek is nodig naar de onderliggende reden, zoals configuratie bij de domeinregistratie of verwijzingen naar een niet-DNSSEC ondertekend domein.

Slechts 56% van de mailservers is ondertekend met DNSSEC. De grootste 2 mailleveranciers zonder DNSSEC hebben een aandeel van 36%, het betreft hier Microsoft Office 365 en Google Mail.

Als mailservers niet met DNSSEC zijn ondertekend, kan DANE niet worden ondersteund. Daarom is dit percentage lager dan DNSSEC, slechts 46% heeft een geldig DANE-record. De DANE-adoptie blijft dus 10 procentpunt achter bij DNSSEC. Hier kan relatief eenvoudig verbetering geboekt worden door DANE-records te publiceren.

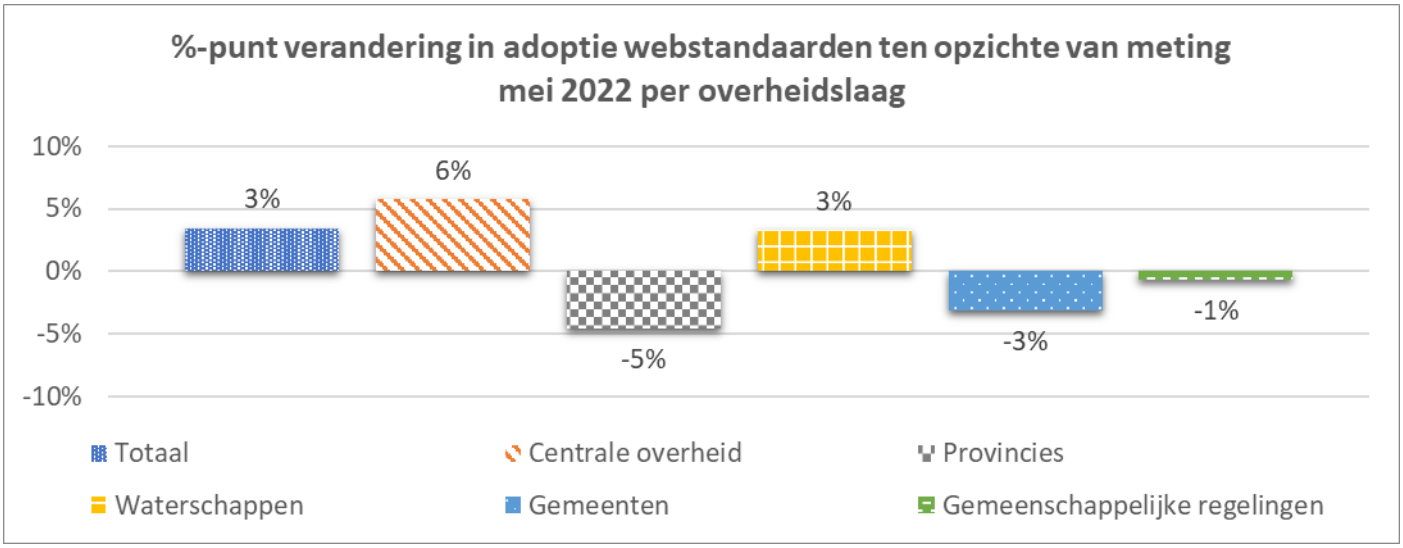
1.5. Vergelijking vorige meting

In de vorige meting van mei 2022 werd voor het eerst gewerkt met een grotere set aan domeinnamen. Het gevolg hiervan was dat de meetresultaten niet goed te vergelijken waren met de metingen van eerdere jaren. In deze meting is een vergelijkbare set aan domeinnamen getest, wat een vergelijking met voorgaande meting mogelijk maakt.

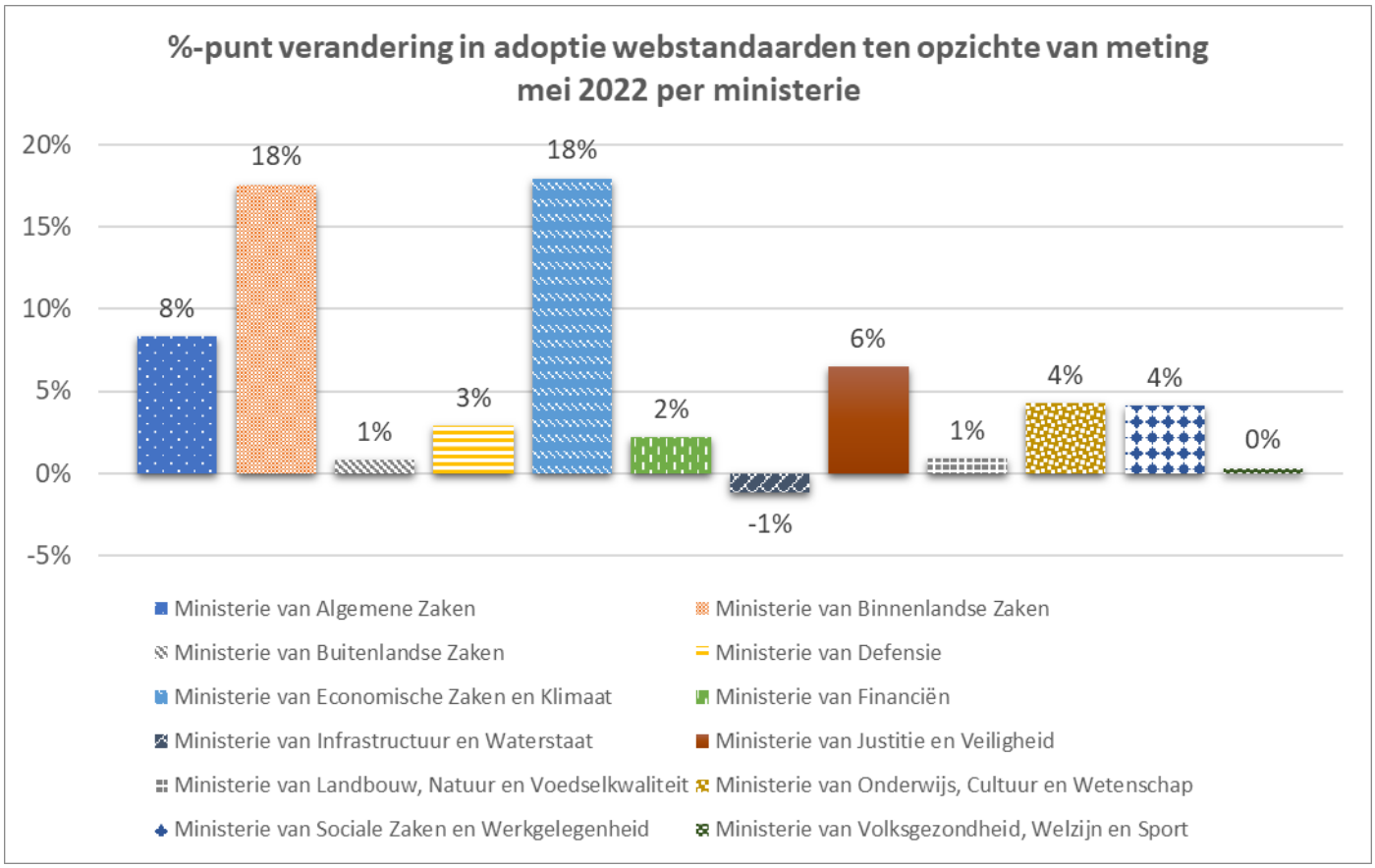
De voorgaande secties laten zien dat adoptie nog steeds verre van volledig is binnen de overheid. Echter is het ook van belang om bewegingen in kaart te brengen. In deze vergelijking worden de verbeteringen en verslechteringen zichtbaar gemaakt door het verschil in procentpunten uit te drukken.

1.5.1. Vergelijking webstandaarden

Kijkende naar de veranderingen in adoptie van webstandaarden per overheidslaag, 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, gemeenten en gemeenschappelijke regelingen. Bij provincies en gemeenten lijkt de voornaamste oorzaak een terugloop in het gebruik van IPv6.



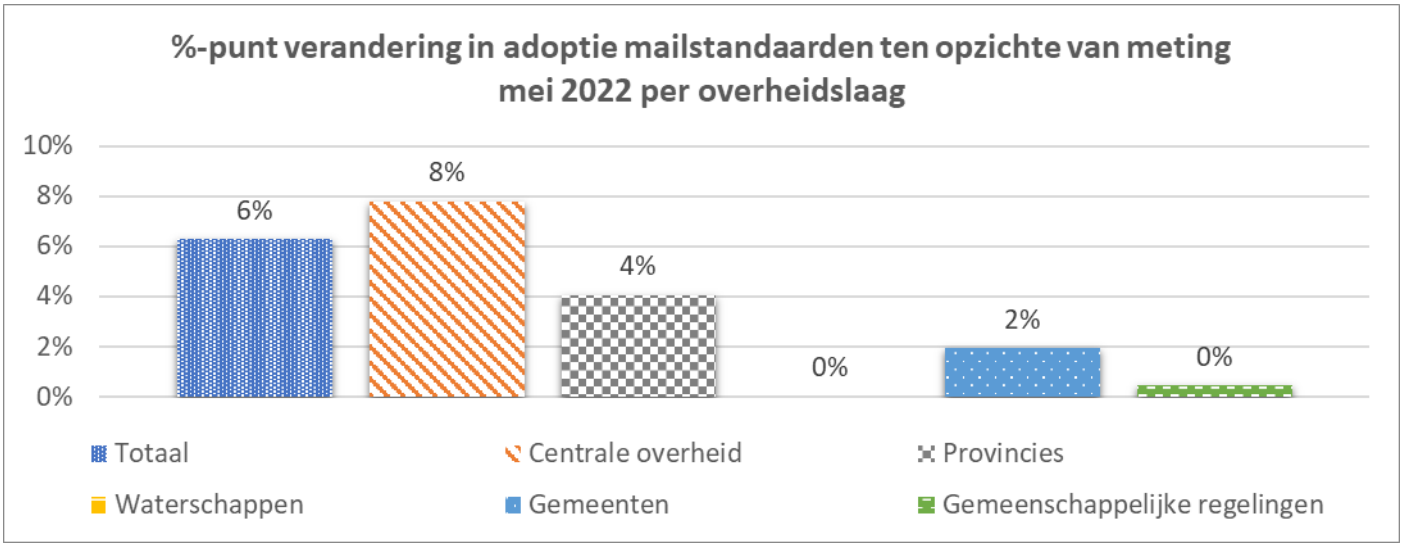
Kijkende naar de centrale overheid, zien we een mooie verbetering in de adoptie van webstandaarden. In het bijzonder de ministeries van Binnenlandse Zaken en Economische Zaken en Klimaat hebben het been bijgetrokken met een enorme verbetering (beide 18 procentpunt). Buitenlandse Zaken, Infrastructuur en Waterstaat en Volksgezondheid, Welzijn en Sport laten daarentegen weinig verbeteringen zien sinds mei 2022.



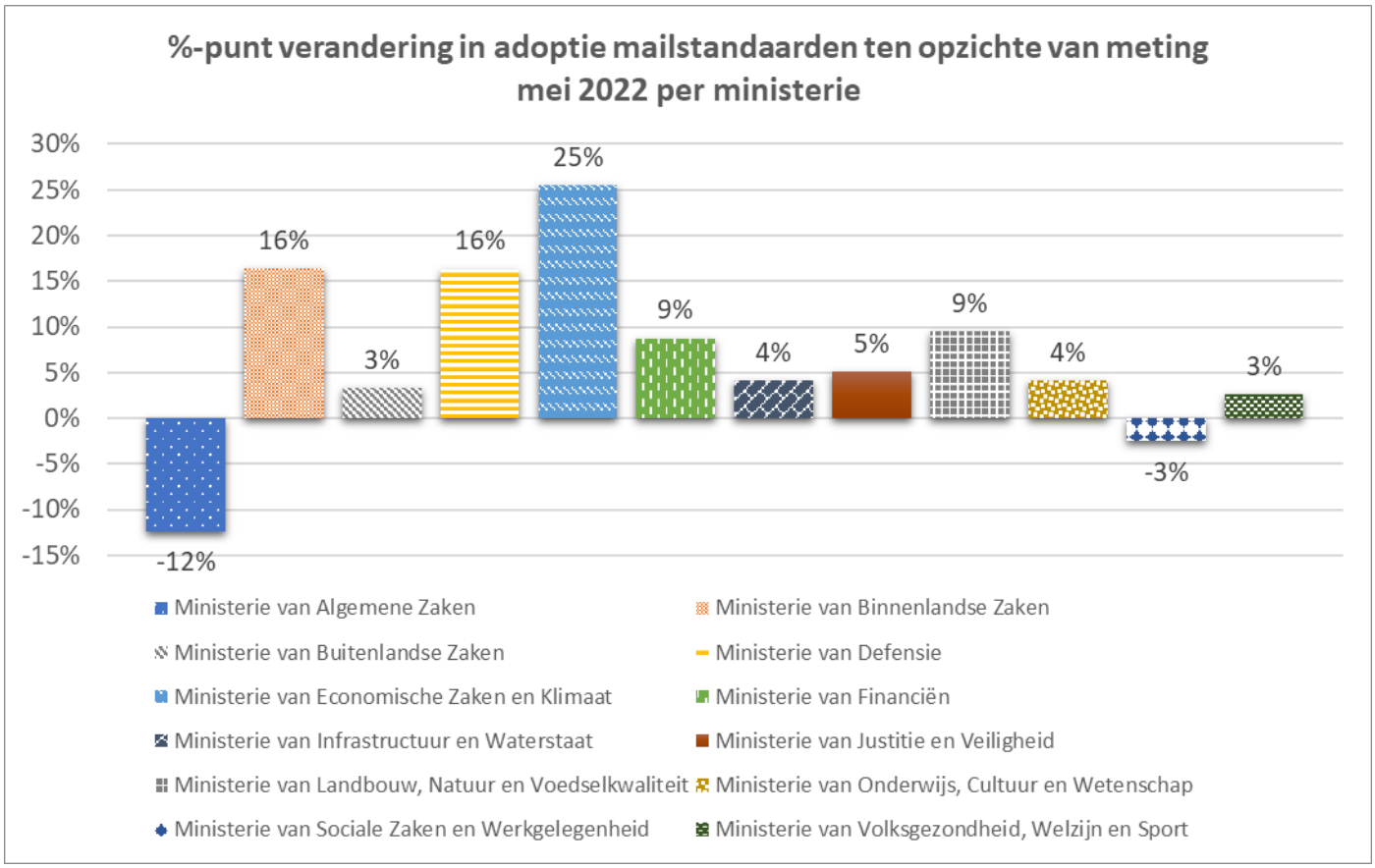
Achterliggend blijkt dat het ministerie van Binnenlandse Zaken op alle webstandaarden een flinke vooruitgang heeft geboekt. Tegelijkertijd blijkt dat Economische Zaken en Klimaat vooral gegroeid is op IPv6 (24 procentpunt), wat kennelijk voor veel domeinnamen de laatste stap naar 100% adoptie is geweest.

1.5.2. Vergelijking mailstandaarden

Bij de mailstandaarden is een nog grotere verbetering te zien ten opzichte van mei 2022. Over de gehele breedte van de domeinnamenset is een stijging van 6 procentpunt waar te nemen. Voornamelijk de centrale overheid laat een grote verbetering zien.



Verder kijkende naar de veranderingen per ministerie, is wederom een enorme stijging te zien bij de ministeries van Economische Zaken en Klimaat en Binnenlandse Zaken, maar ook bij Defensie. Een grote afname bij het ministerie van Algemene Zaken is voornamelijk te wijten aan een groei in het aantal geteste domeinnamen, waar het ministerie nog steeds het kleinste domeinnaamportfolio heeft. Hierdoor hebben de nieuw toegevoegde domeinnamen, die nog niet volledige voldoen aan de verplichte standaarden, een grote impact op het gemiddelde.



1.5.3. Conclusie

De vergelijking laat zien dat er sinds de vorige meting verbeteringen zijn doorgevoerd in de adoptie van standaarden. Wel is er nog een grote weg te gaan naar volledige adoptie. In het bijzonder zijn stijgingen waar te nemen bij de ministeries van Binnenlandse Zaken en Economische Zaken en Klimaat. Een sturende aanpak bij deze ministeries lijkt te helpen om de adoptie te verbeteren.

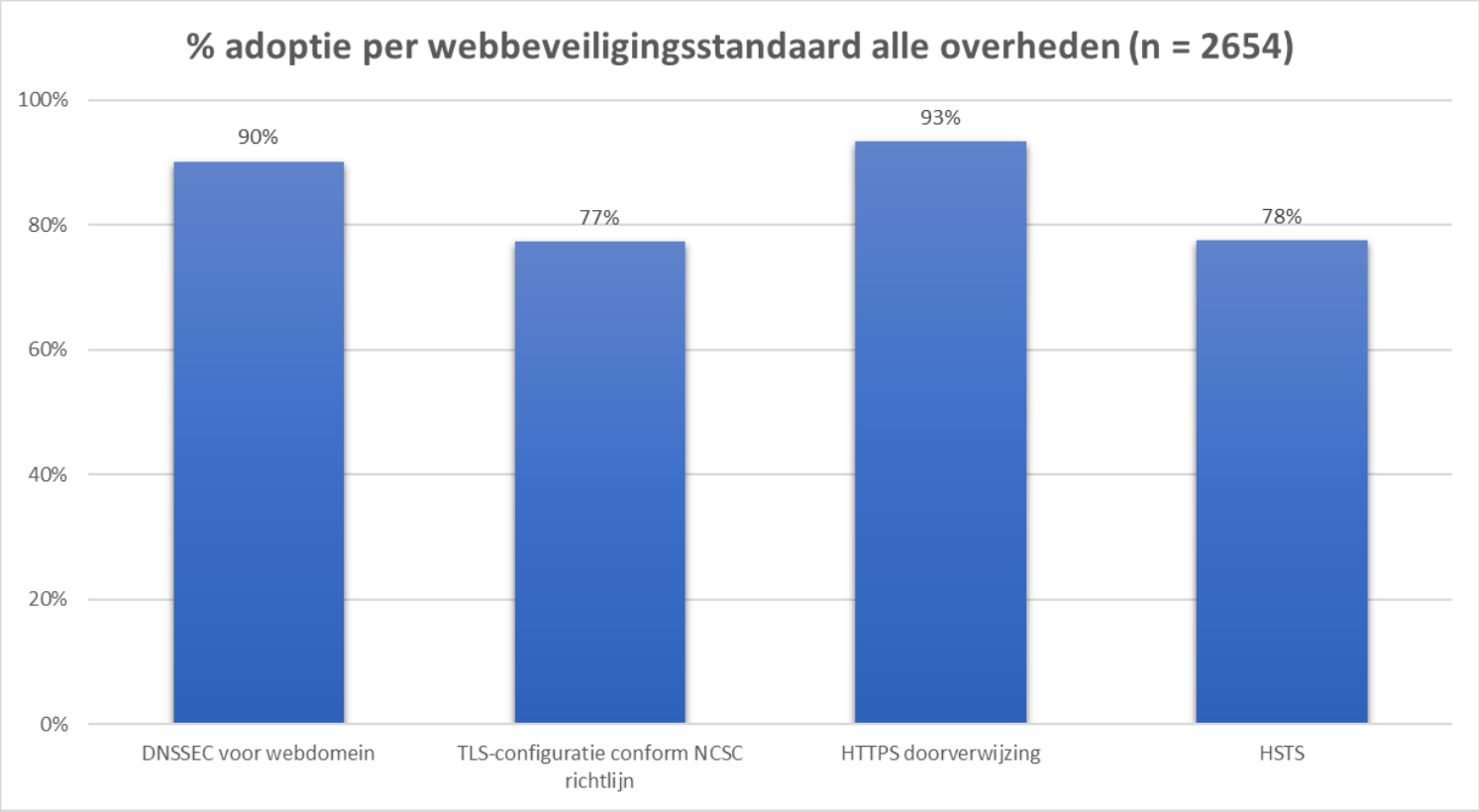
Het is de hoop dat andere overheidsorganisaties dit voorbeeld volgen en inzetten op verbetering van de adoptiecijfers. De voorbeelden laten zien dat verbeteringen mogelijk en uitvoerbaar zijn.

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.



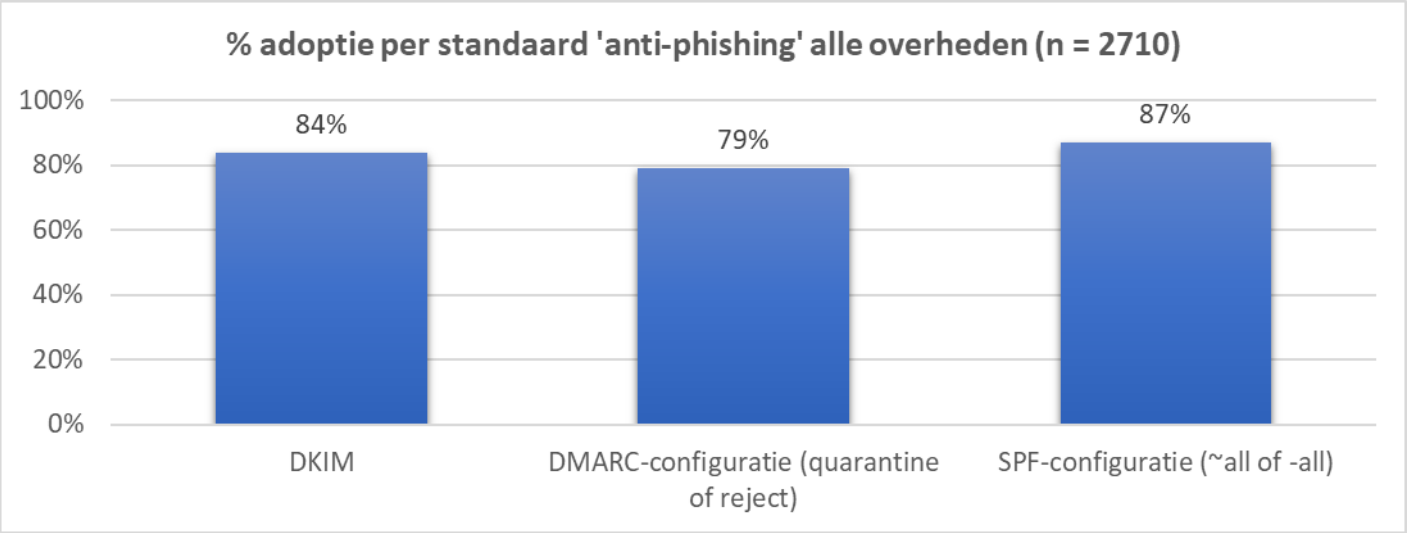
3. Adoptie per e-mailbeveiligingsstandaard

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 21% van de internetdomeinen nog een strikt DMARC-beleid worden ingesteld. Het streefbeeld was om dit eind 2019 voor elkaar te hebben.

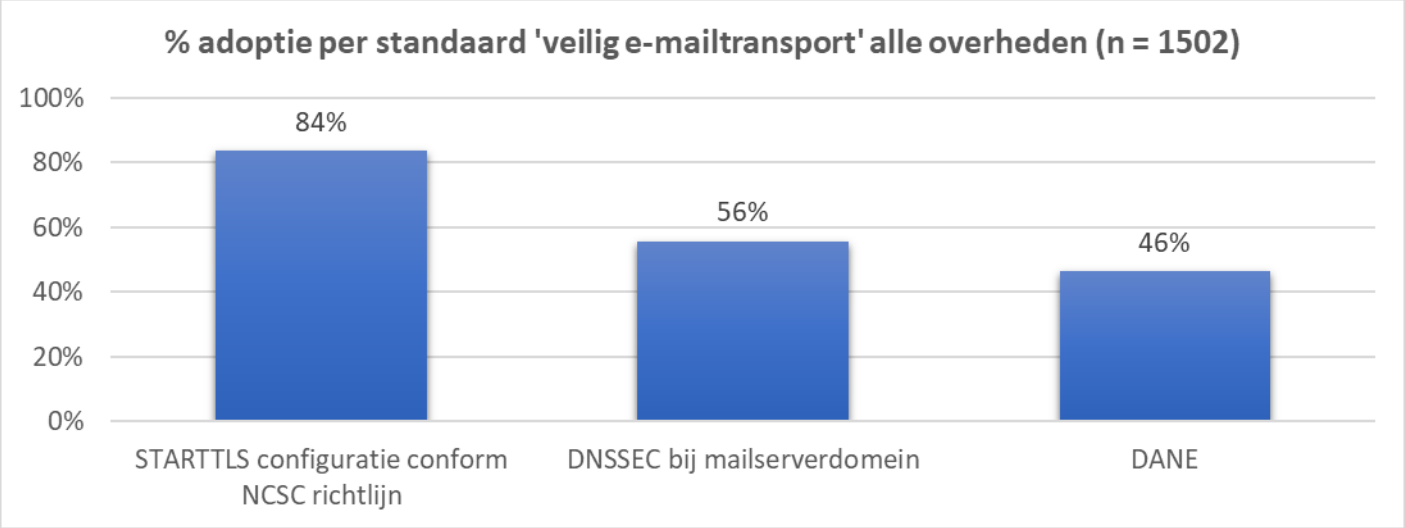


3.2. E-mailstandaarden voor vertrouwelijk e-mailverkeer

Bij nog 16% 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 46%. 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.



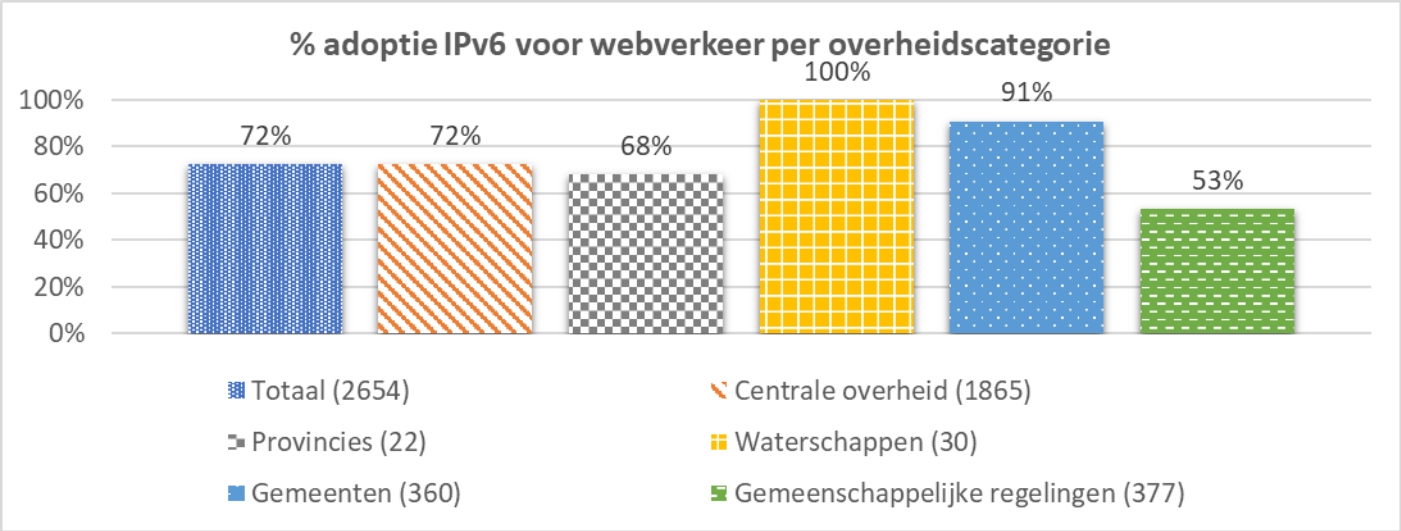
4. Adoptie IPv6 voor websites en e-mail

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.

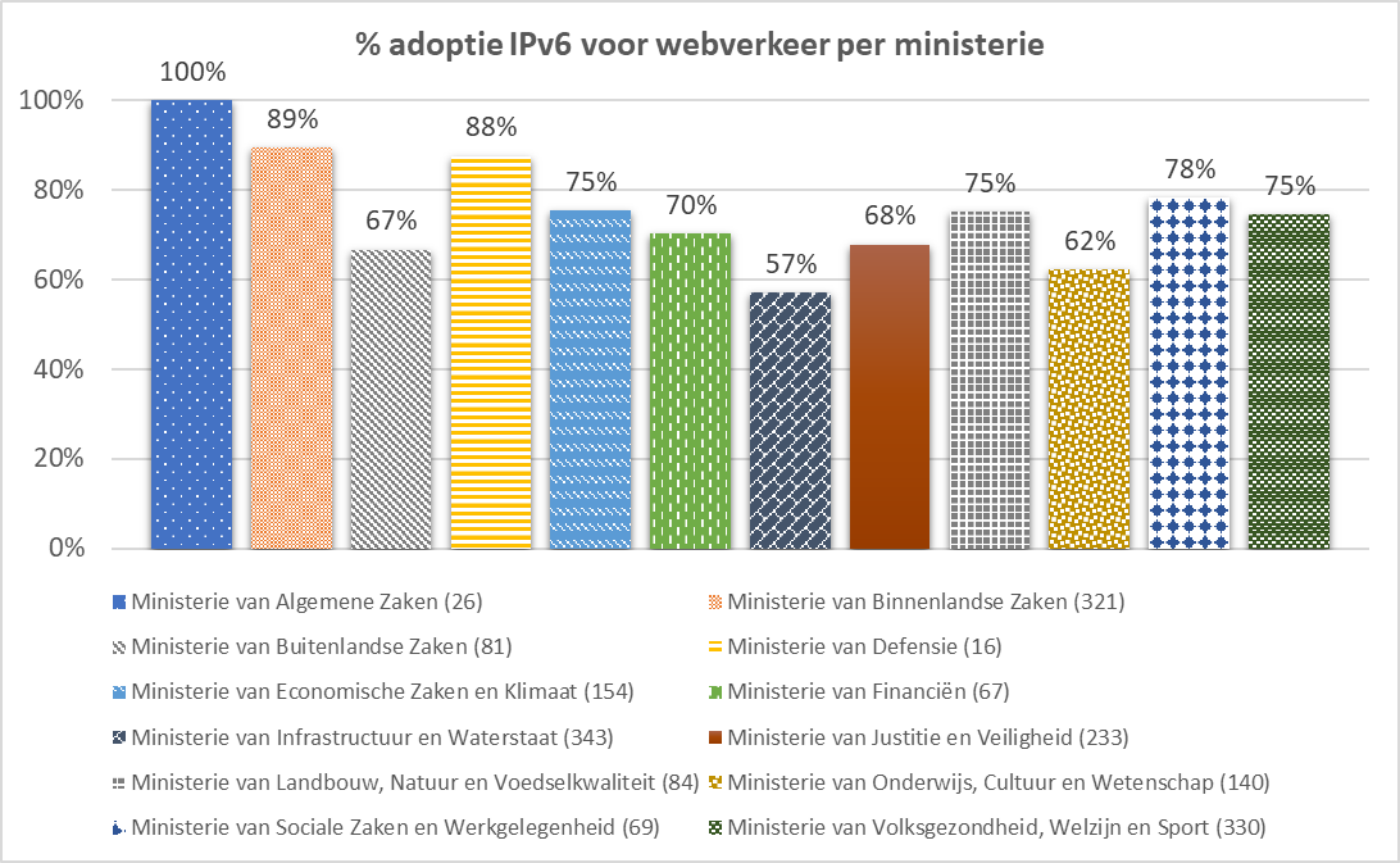
4.1. IPv6 voor webverkeer per overheidscategorie

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.



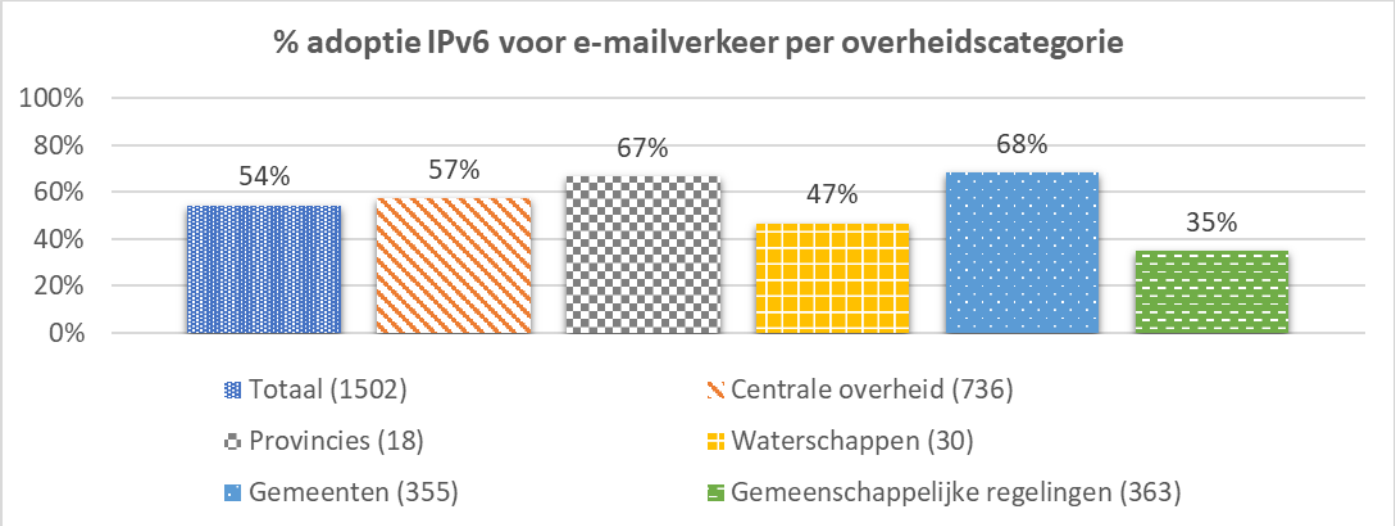
4.2. IPv6 voor webverkeer per ministerie

Positieve uitschieters – met een klein webportfolio – zijn de ministeries van Algemene Zaken (100%), Binnenlandse Zaken (89%) en Defensie (88%). Negatieve opvaller is het ministerie van Infrastructuur en Waterstaat (57%), waarvan de websites het minst bereikbaar waren via IPv6.



4.3. IPv6 voor e-mailverkeer per overheidscategorie

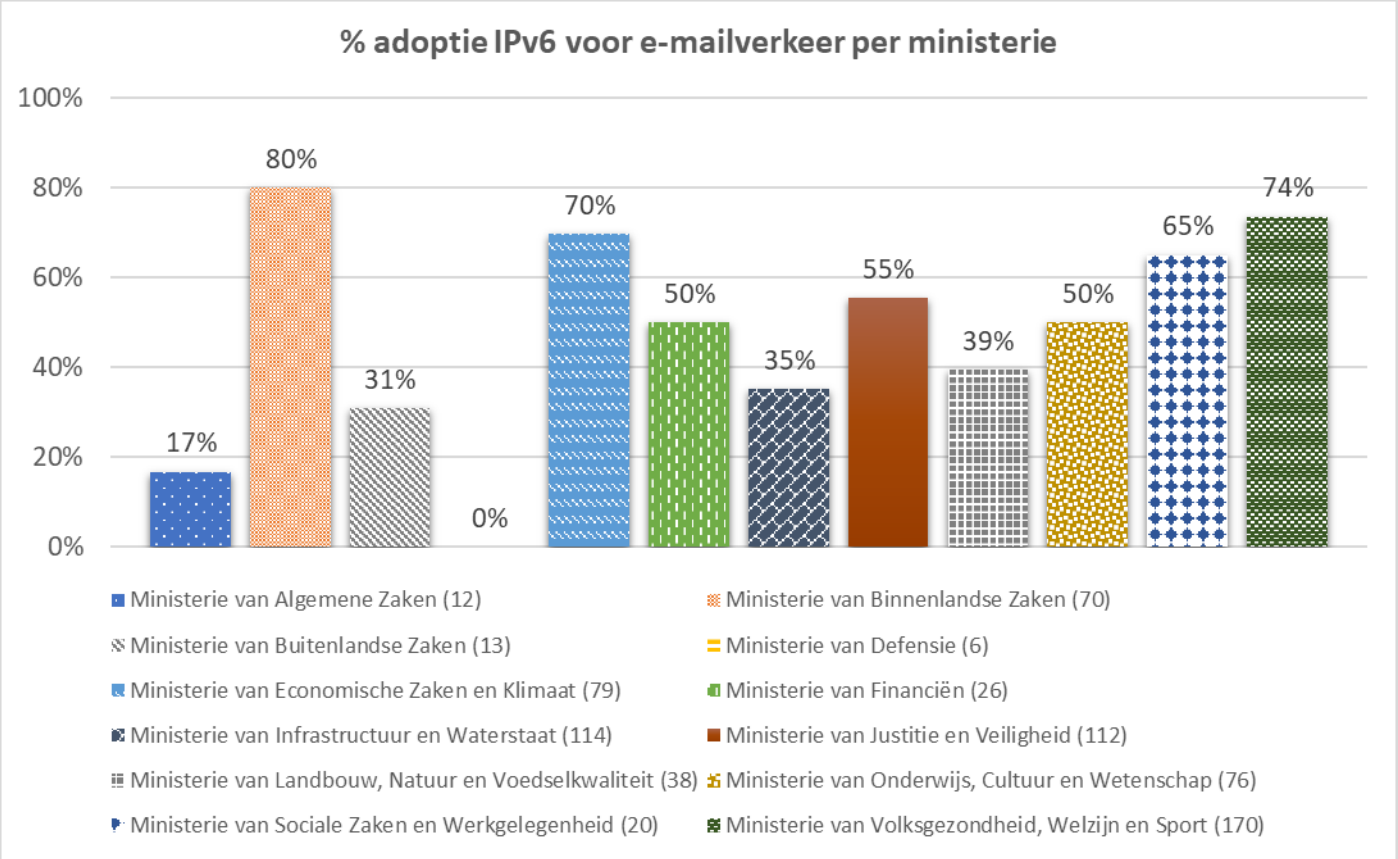
Ook bij het gebruik van IPv6 voor e-mailverkeer scoren de gemeenschappelijke regelingen ver onder de maat met een adoptiegraad van slechts 35%. Ook de waterschappen blijven achter met 47%.



4.4. IPv6 voor e-mailverkeer per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan valt in eerste instantie het ministerie van Defensie negatief op, die helemaal geen IPv6 e-mailverkeer mogelijk maakt. Ook het ministerie Algemene Zaken (17%) heeft ondanks een klein portfolio aan ontvangen e-maildomeinen een erg lage adoptiegraad.

Positieve opvallers zijn de ministeries Binnenlandse Zaken (80%), Volksgezondheid, Welzijn en Sport (74%), en Economische Zaken en Klimaat (70%).



5. Leveranciersafhankelijkheid

Het doel van de analyse is ontdekken of er individuele leveranciers zijn die ervoor zorgen dat een groot deel van de overheid niet aan een specifieke standaard voldoen. Op deze manier kan achterhaald worden welke leveranciers direct aangespoord dienen te worden deze standaarden te implementeren, om een grote stijging in adoptie te behalen.

In dit hoofdstuk volgt een uitgebreide analyse op de leveranciers van overheden in combinatie met het achterblijven op specifieke standaarden.

5.1. Adoptie IPv6 voor websites

Het blijkt dat 28% van de websiteservers IPv6 niet heeft ingesteld. Het was echter lastig om uit deze groep achterblijvers significante leveranciers te destilleren. Hiervoor gaat nader onderzoek uitgevoerd worden, waarvan de resultaten hopelijk in een later rapport gepresenteerd kunnen worden.

Als naar de onderliggende nameserverleveranciers voor websites gekeken wordt, valt de hoge adoptie van IPv6 onder nameservers op, slechts 2% (56 van 2653) van de domeinnamen voldoet niet aan de eis van twee nameservers met een IPv6 adres.

Door deze achterblijvende domeinnamen werden 46 verschillende nameservers gebruikt. Hieruit zijn geen significant grote leveranciers te destilleren, het gaat dus om een grote groep kleine leveranciers die niet aan de eisen voldoen.

5.2. Adoptie IPv6 voor e-mail

Bij mailservers heeft 41% IPv6 nog niet in orde. Het was echter lastig om uit deze groep achterblijvers significante leveranciers te destilleren. Hiervoor gaat nader onderzoek uitgevoerd worden, waarvan de resultaten hopelijk in een later rapport gepresenteerd kunnen worden.

Voor de nameservers kijken we alleen naar de nameservers van de mailservers (MX). Hier voldoet 35% (529 van 1502) niet aan IPv6.

Het bleek dat van de binnenkomende mailservers heeft 34% (510 van 1502) een nameserver van Microsoft Office 365 gebruikt zonder IPv6-ondersteuning. Buiten deze leverancier zijn er geen andere leveranciers van nameservers bij binnenkomende email (MX) met enig significant aandeel.

5.3. DNSSEC voor websites

Van de websites is 10% niet beveiligd met DNSSEC. Het kan zijn dat een nameserverleverancier het domein wel ondertekend, maar de DNSSEC-test geen positief resultaat geeft doordat er een niet-ondertekend domein wordt gebruikt in een CNAME-verwijzing. Daarom is gekeken welke nameserverleveranciers geen enkel DNSSEC-ondertekend domein hebben.

Van deze 10% heeft een derde (94 van 2654) een nameserverleveranciers (totaal 69 leveranciers) die geen enkel domein met DNSSEC ondertekend hadden. Hiervan hebben 14 leveranciers meer dan één domein, gezamenlijk verantwoordelijk voor 42 domeinnamen. Van deze 14 geven de 4 in de tabel genoemde leveranciers aan op hun website geen technische ondersteuning voor DNSSEC te hebben.

Nameserverleverancier zonder DNSSEC	**Aantal domeinnamen**
Microsoft Azure DNS	9
SiteGround	4
DigitalOcean	2
WIX	2

Bij de overgebleven twee derde, is te stellen dat de nameserverleveranciers van het domein geen technische limitatie hebben om DNSSEC in te stellen. Meer onderzoek is nodig naar de onderliggende reden, zoals configuratie bij de domeinregistratie of CNAME-verwijzingen naar een niet-DNSSEC-ondertekend domein. Dit zal worden meegenomen in een latere meting.

5.4. DNSSEC/DANE voor e-mail

Slechts 56% van de mailservers is ondertekend met DNSSEC. De grootste 4 mailleveranciers zonder DNSSEC hebben een aandeel van 36% (544 van 1502).

Mailleverancier zonder DNSSEC	**Aantal domeinnamen**
Microsoft Office 365	510
Google Mail*	24
MimeCast	5
SiteGround (MailSpamProtection)	5

* Google biedt alternatieve mailservers met DNSSEC-ondertekening. Dit aantal bevat alleen de domeinnamen die de niet-ondertekende mailservers gebruiken.

Wanneer deze vier leveranciers DNSSEC zouden ondersteunen zou het percentage boven de 90% komen. Google Mail heeft ook mailservers welke wél zijn ondertekend met DNSSEC, echter is dit niet in officiële documentatie opgenomen.

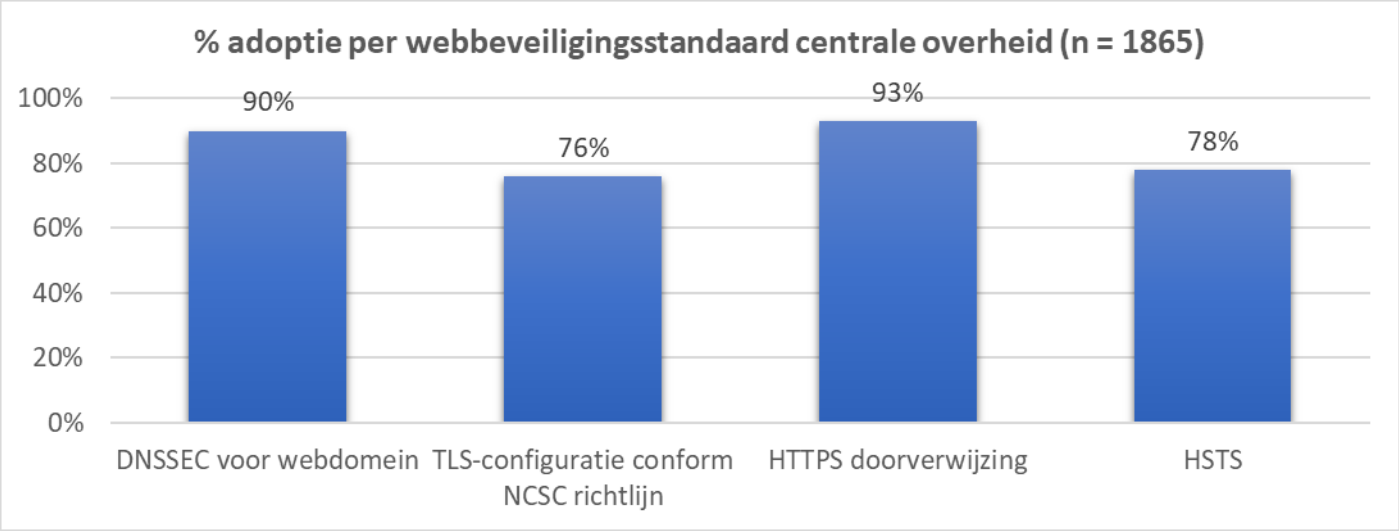
Als mailservers niet met DNSSEC zijn ondertekend, kan DANE niet worden ondersteund. Daarom is dit percentage lager dan DNSSEC, slechts 46% heeft een geldig DANE-record. De DANE-adoptie blijft 10 procentpunt achter bij DNSSEC.

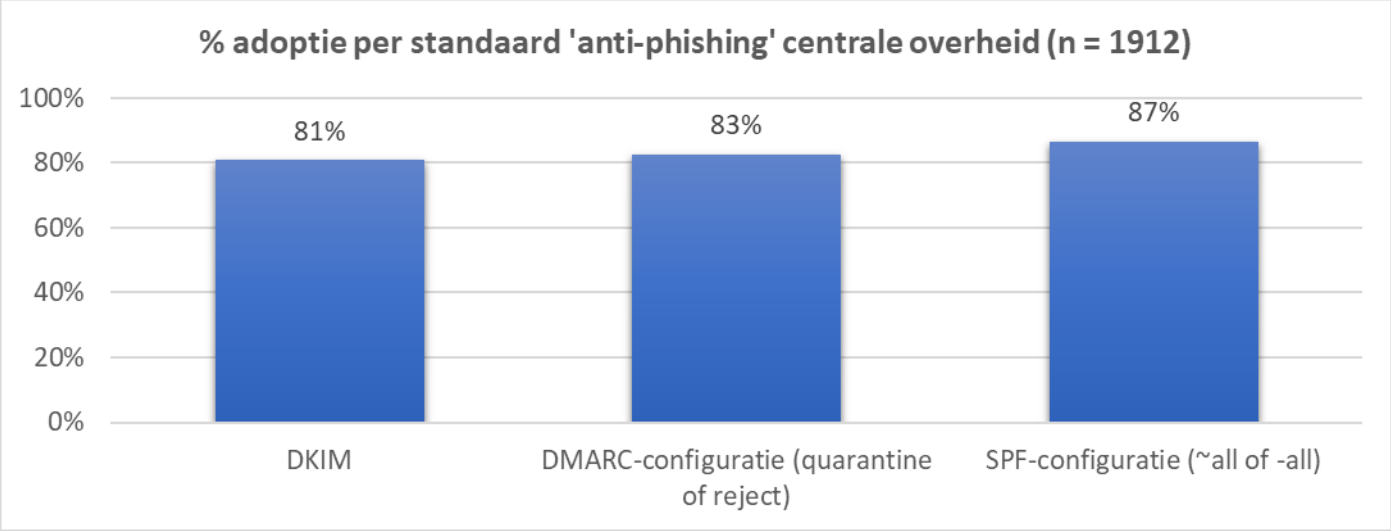
Voor deze mailservers vergt succesvolle DANE-implementatie alleen nog het publiceren van een DANE-record in de DNS. Hier liggen dus kansen tot eenvoudige verbeteringen. De grootste mailleverancier bij wie deze configuratie mist is Google Mail bij de ondertekende mailservers, die door 8 domeinnamen gebruikt worden.

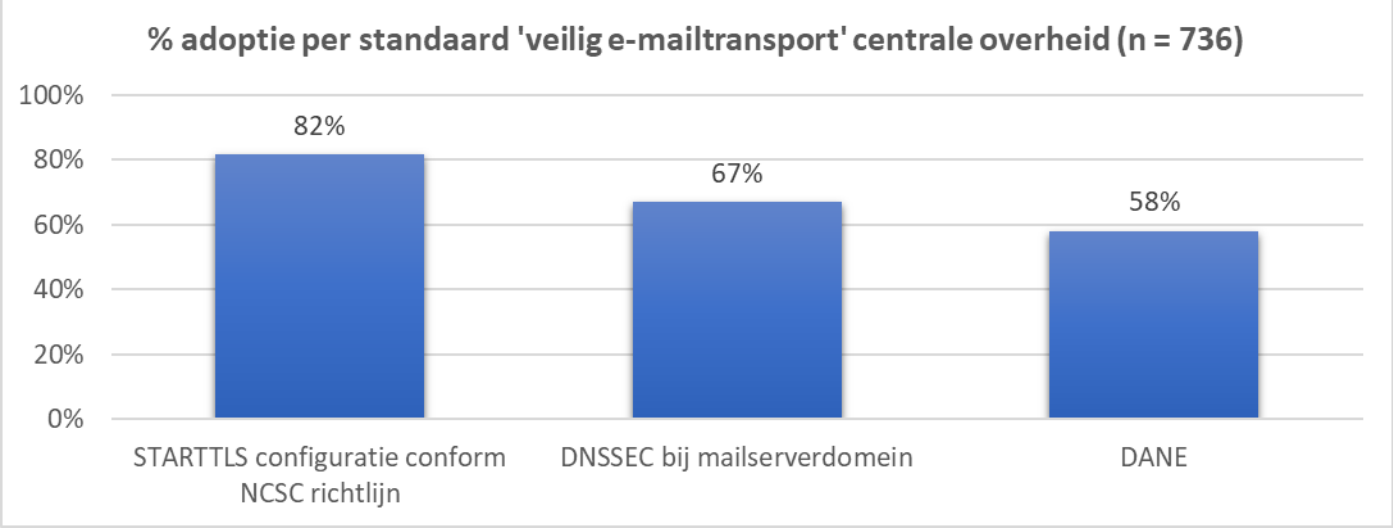
6. Adoptie per overheidscategorie

De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per overheidscategorie.

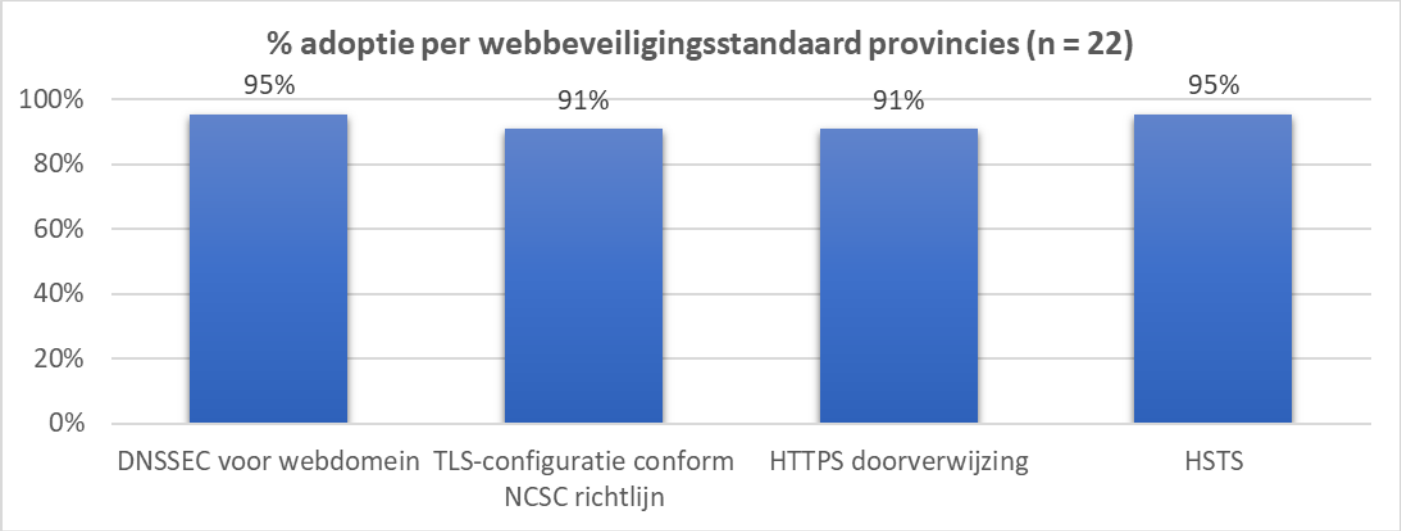
6.1. Centrale overheid

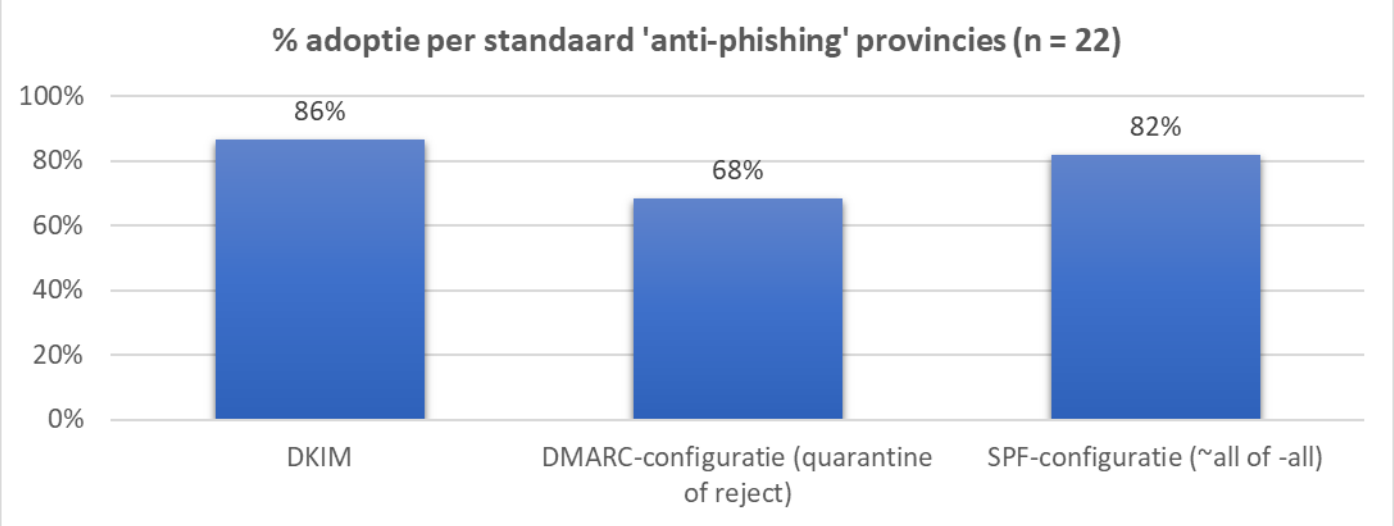


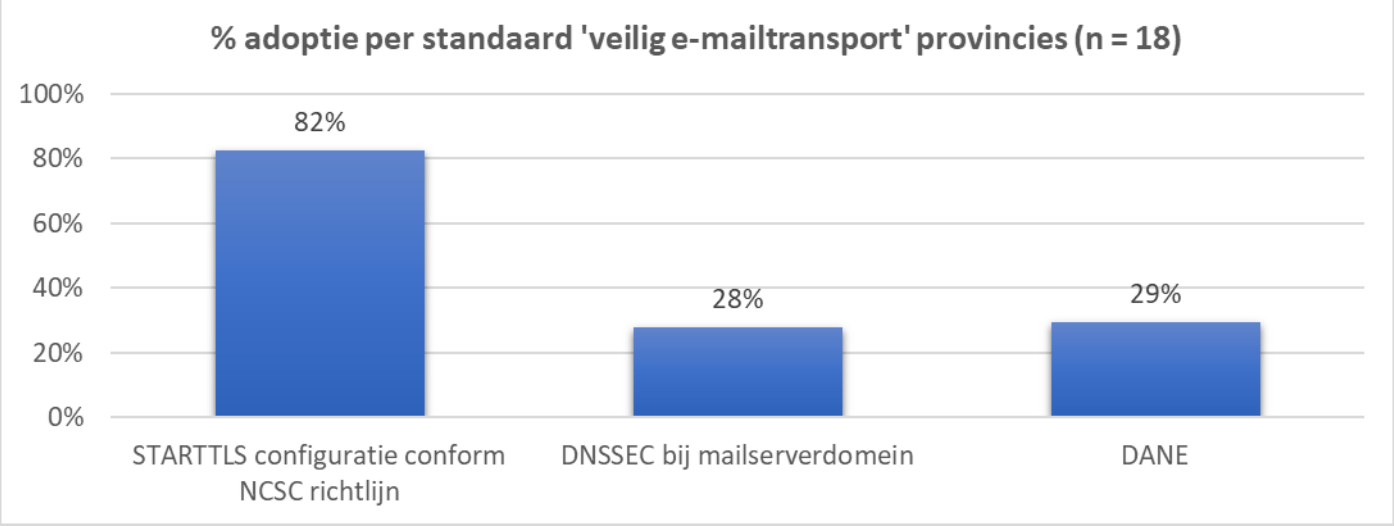




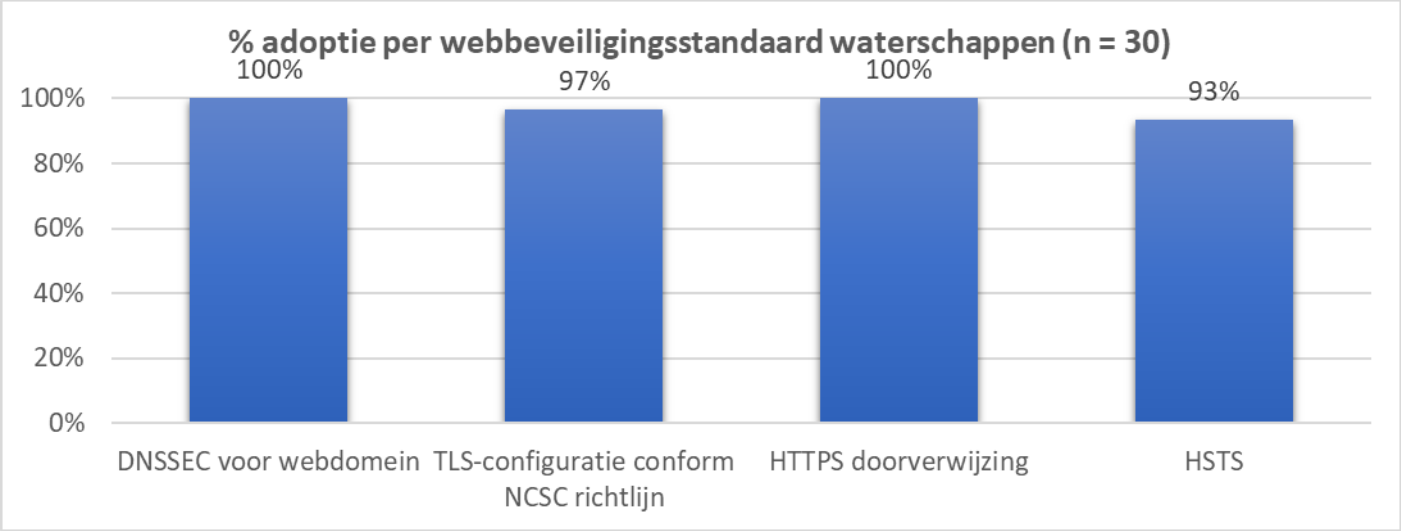
6.2. Provincies

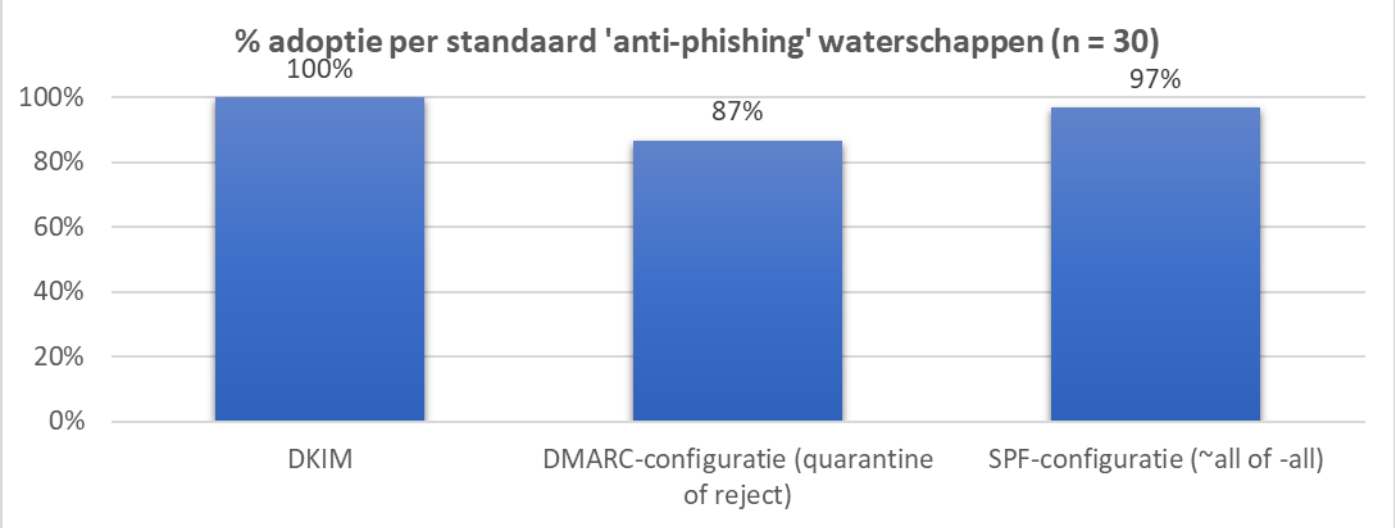


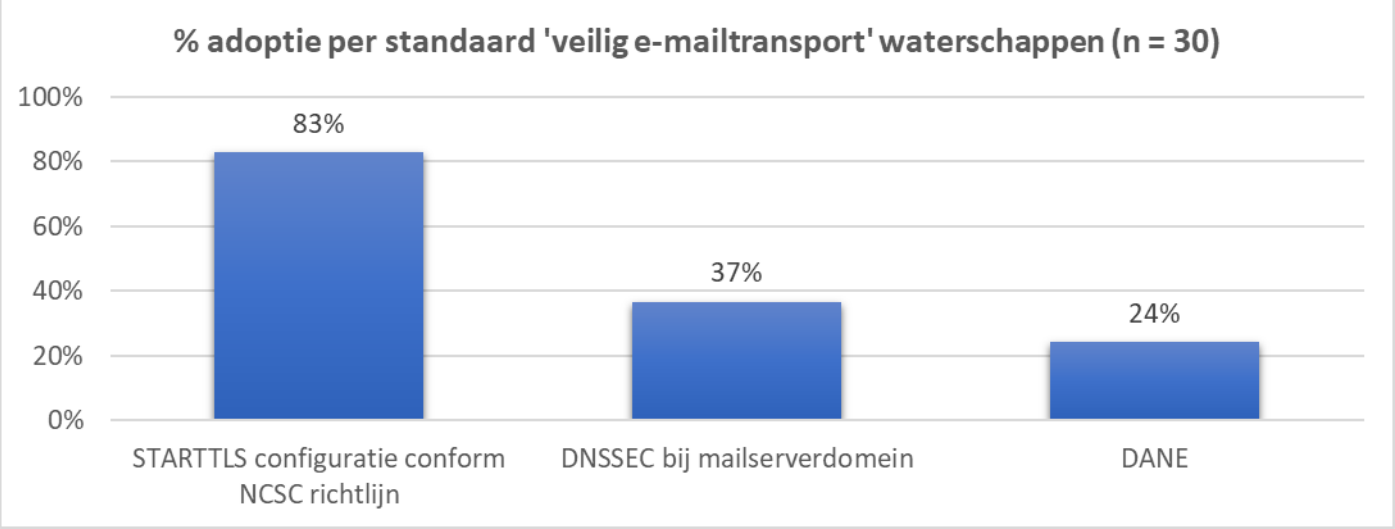




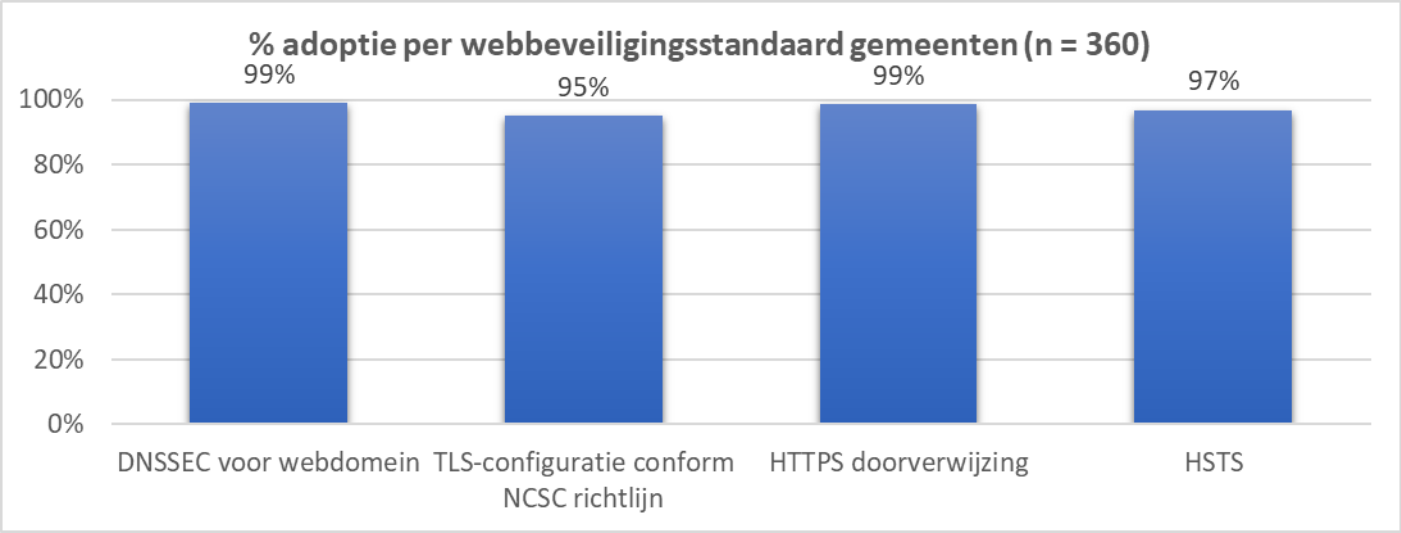
6.3. Waterschappen

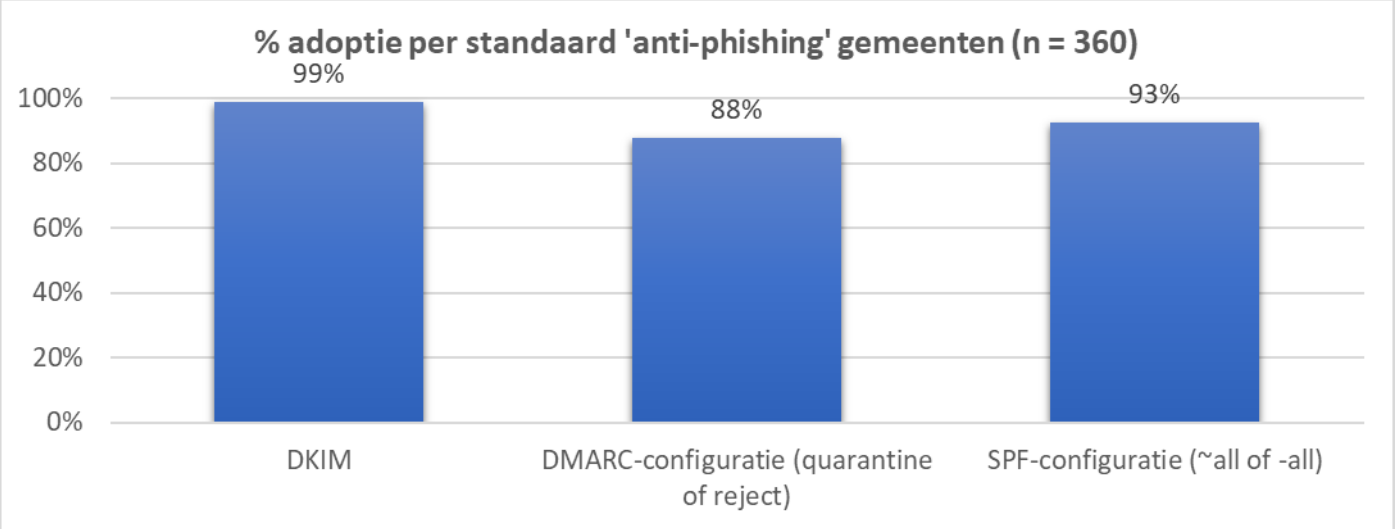


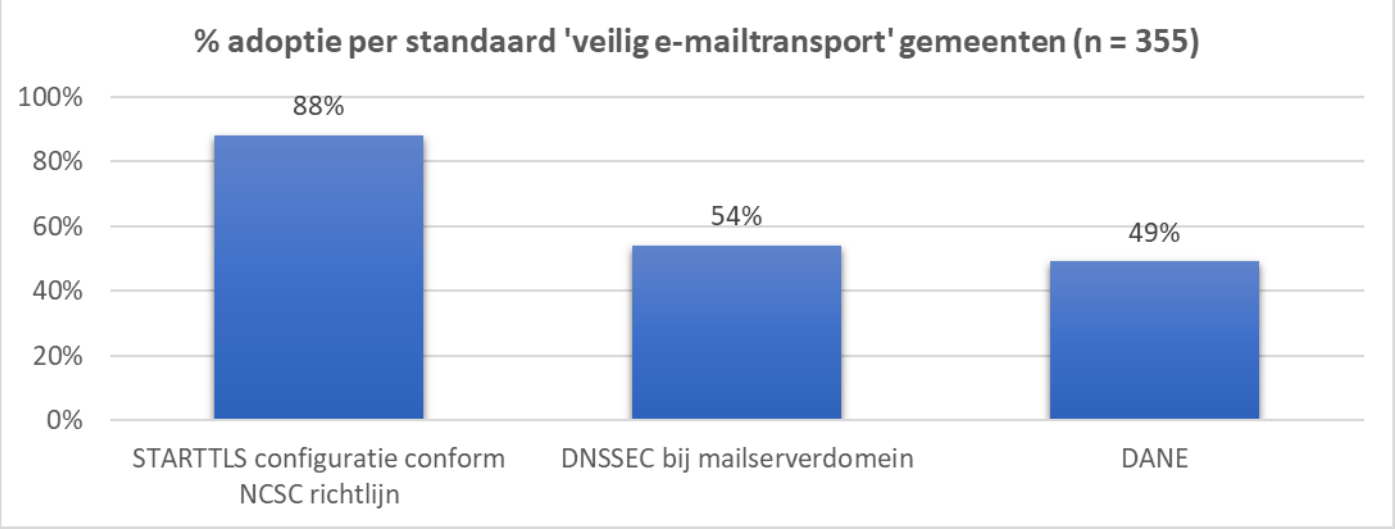




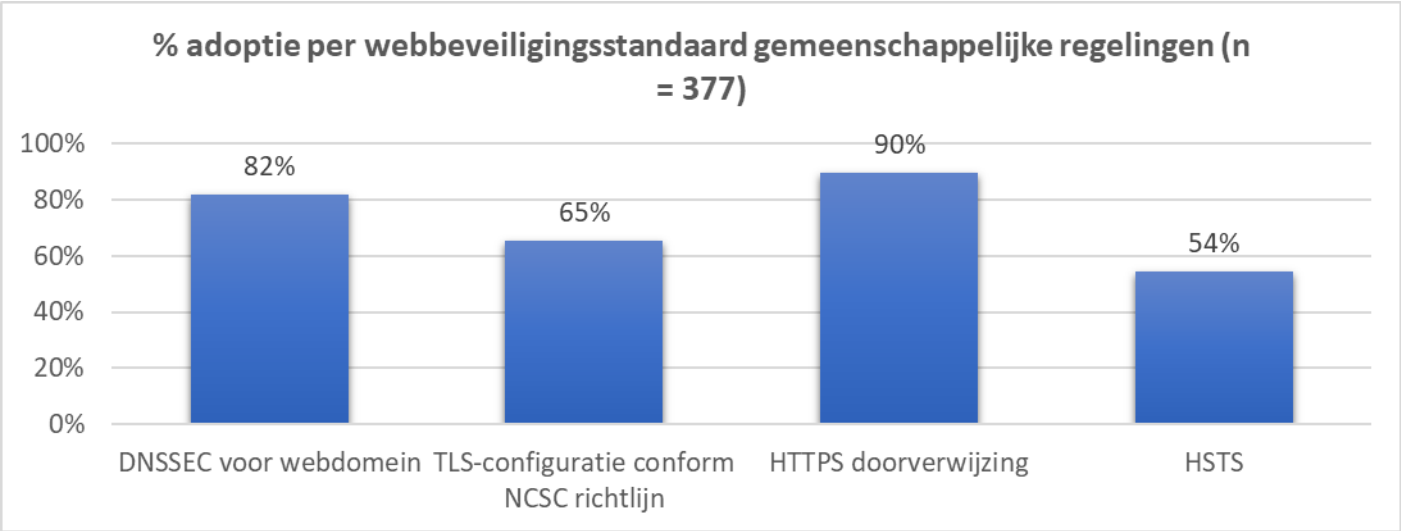
6.4. Gemeenten

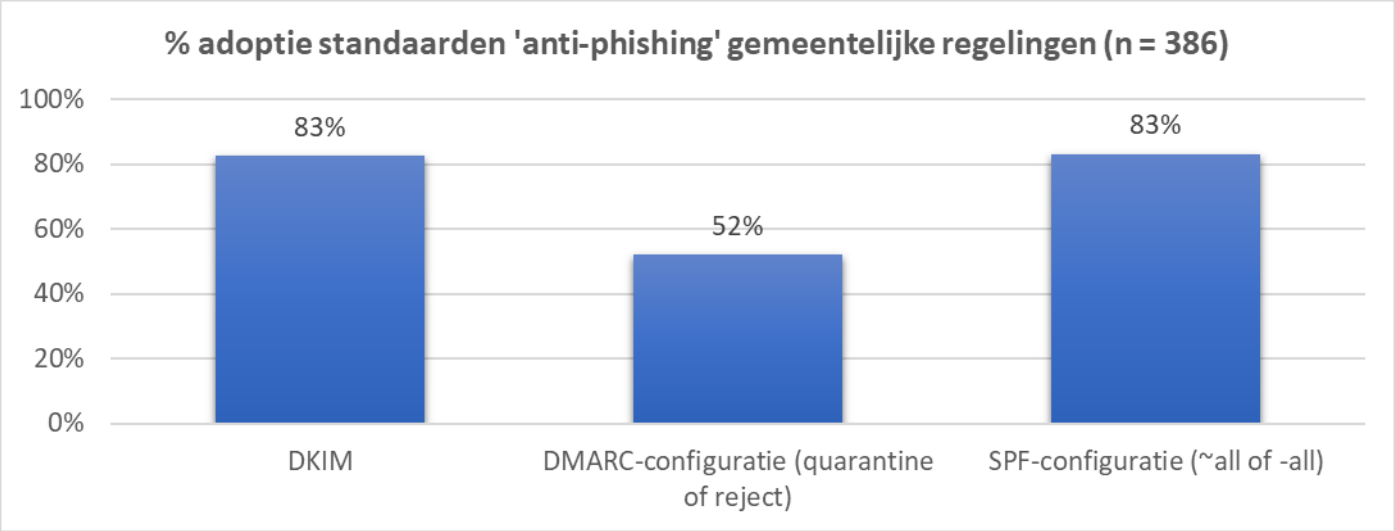


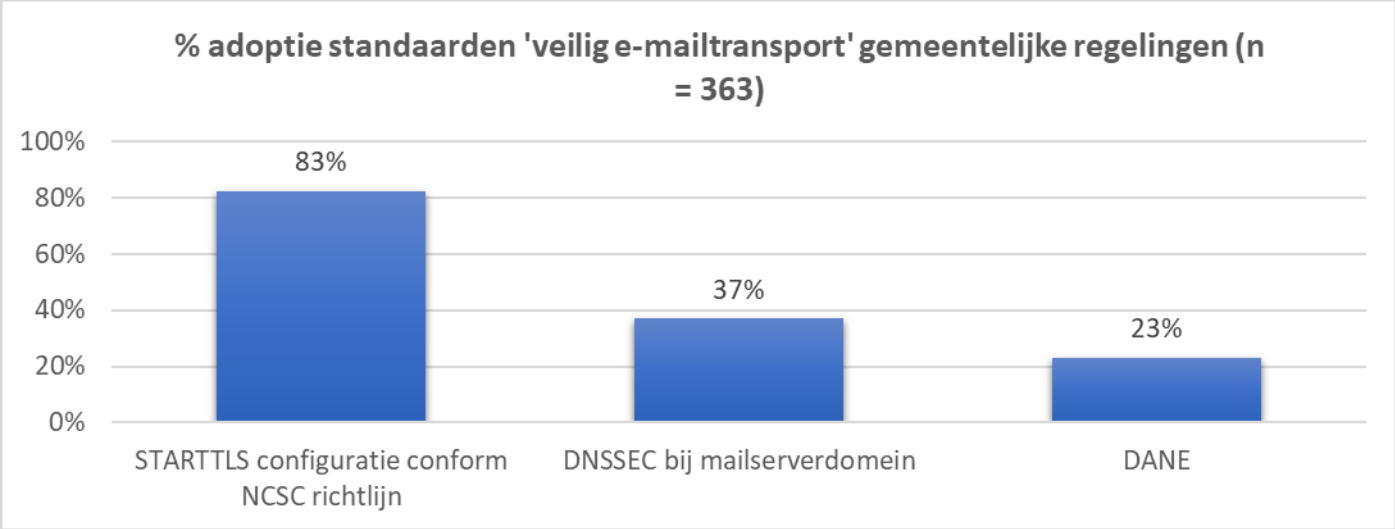




6.5. Gemeenschappelijke regelingen



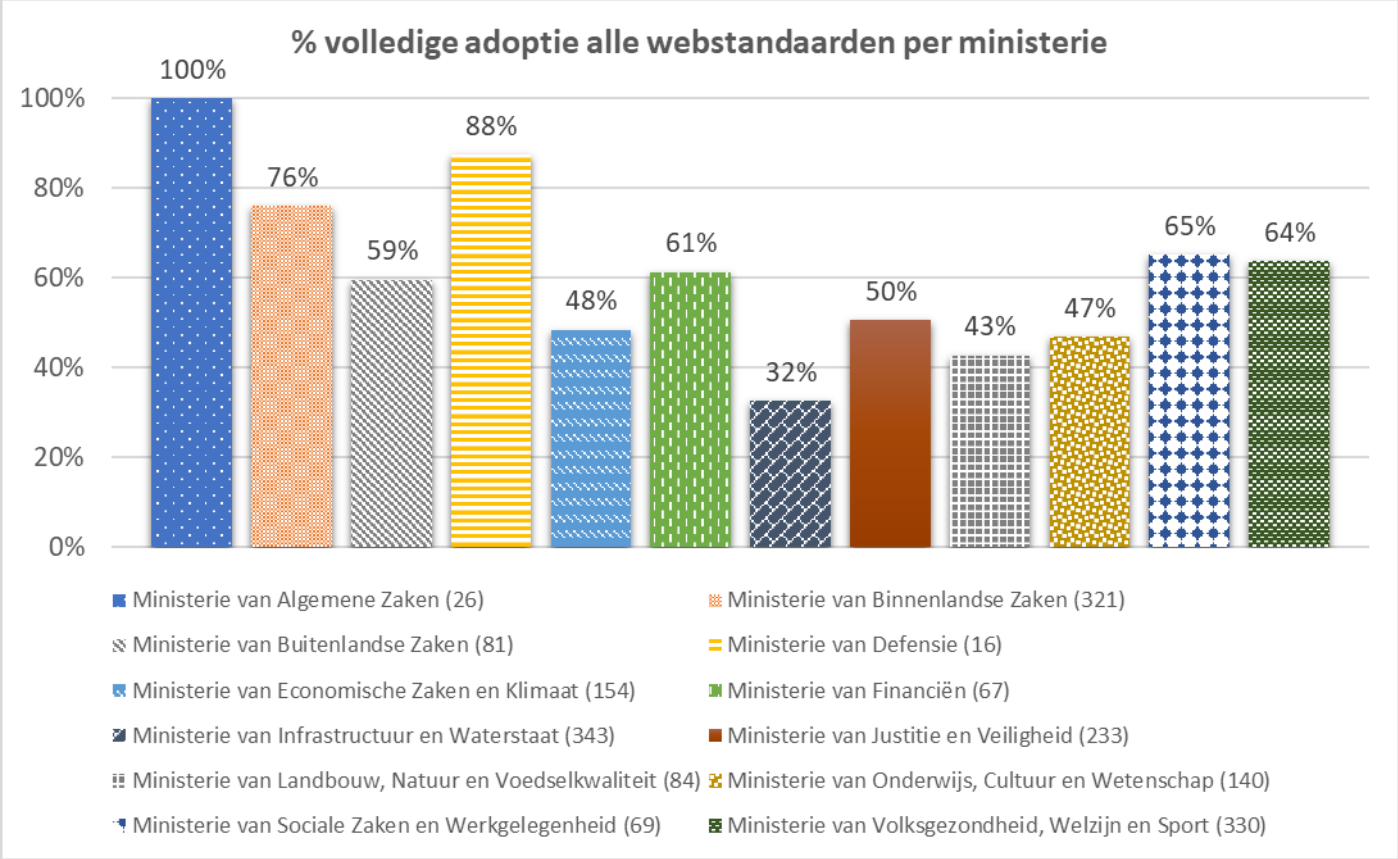




7. Adoptie per ministerie

7.1. Totaalbeeld websitestandaarden (incl. IPv6)

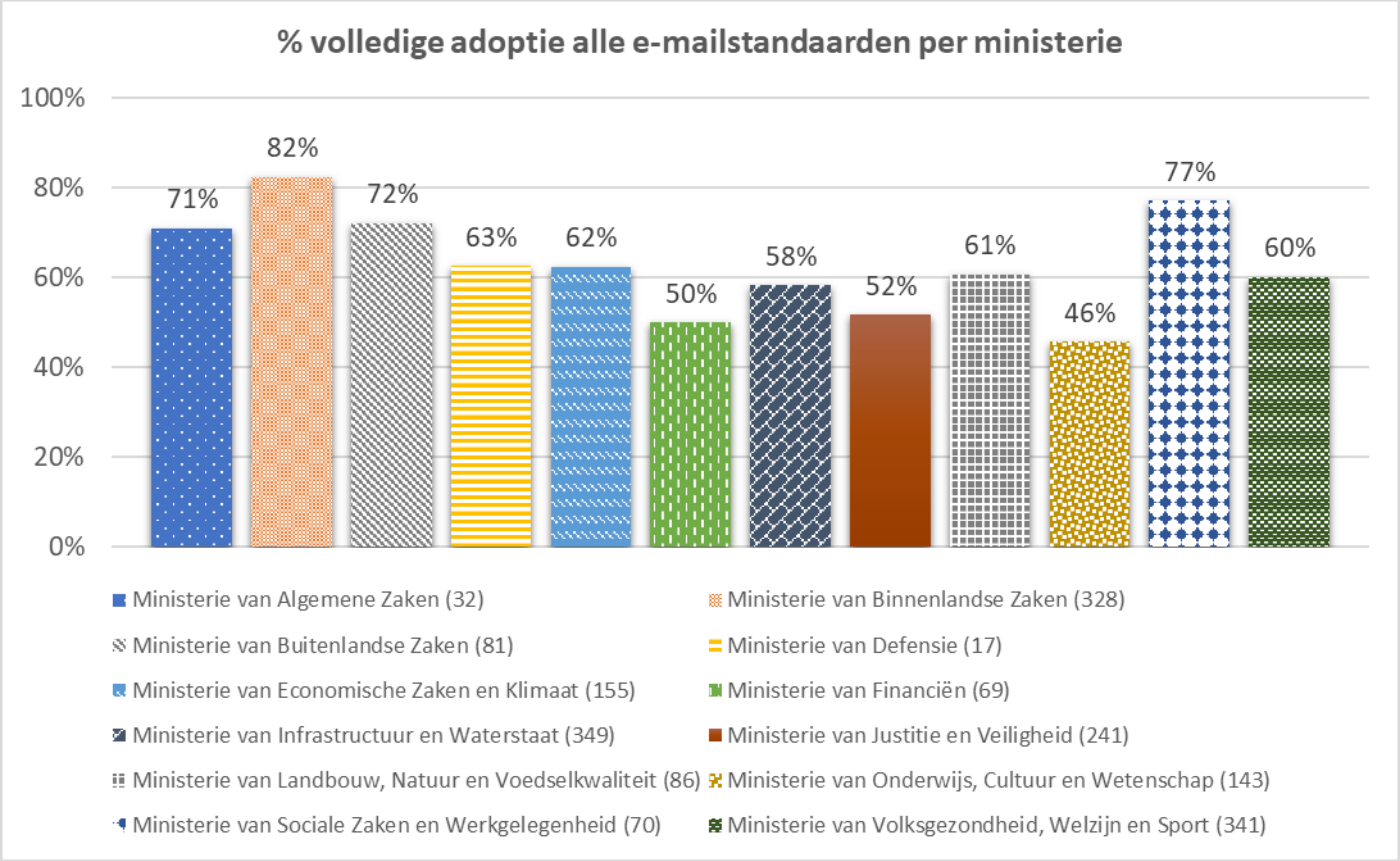
Onderstaande cijfers laten zien in welke mate de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – *alle* afgesproken websitestandaarden voor veilig en modern webverkeer toepassen (inclusief IPv6).



Over het algemeen hebben ministeries met een klein webportfolio, zoals de ministeries van Algemene Zaken en Defensie, een hoge mate van adoptie. Ook ministeries als Buitenlandse Zaken en Financiën, met een relatief beperkt portfolio, scoren hoger dan gemiddeld. Het ministerie van Binnenlandse Zaken heeft een relatief hoge adoptiegraad afgezet tegen de hoge omvang van hun portfolio.

7.2. Totaalbeeld e-mailstandaarden (incl. IPv6)

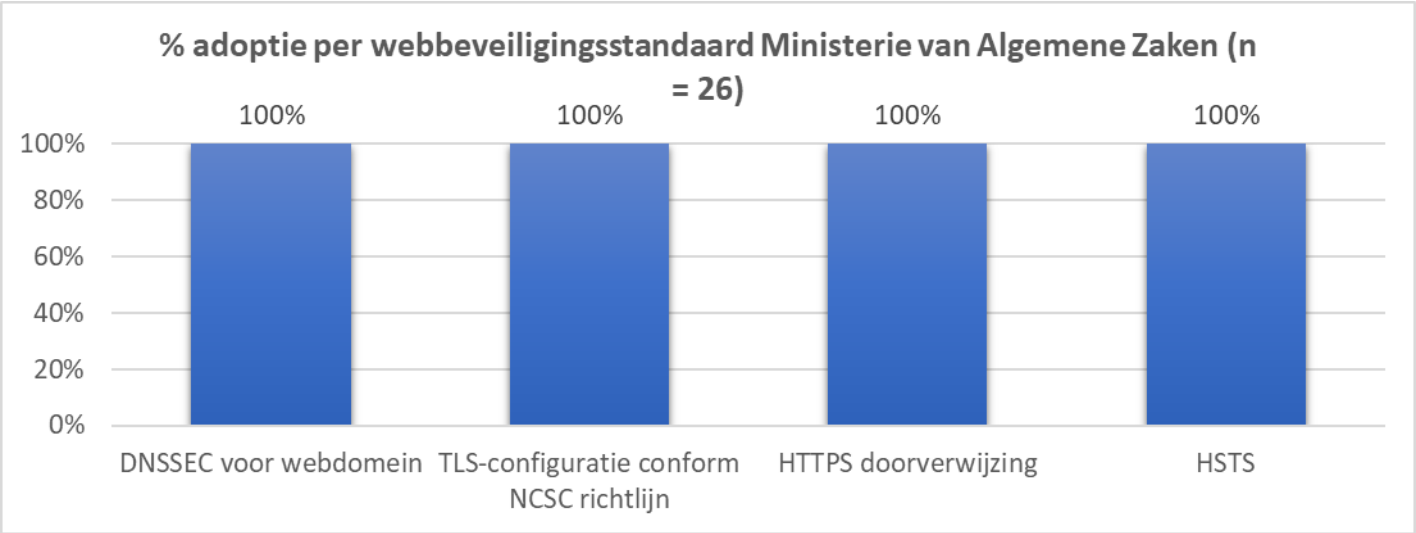
Onderstaande cijfers laten zien in welke mate de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – *alle* afgesproken e-mailstandaarden voor veilig en modern e-mailverkeer toepassen (inclusief IPv6).

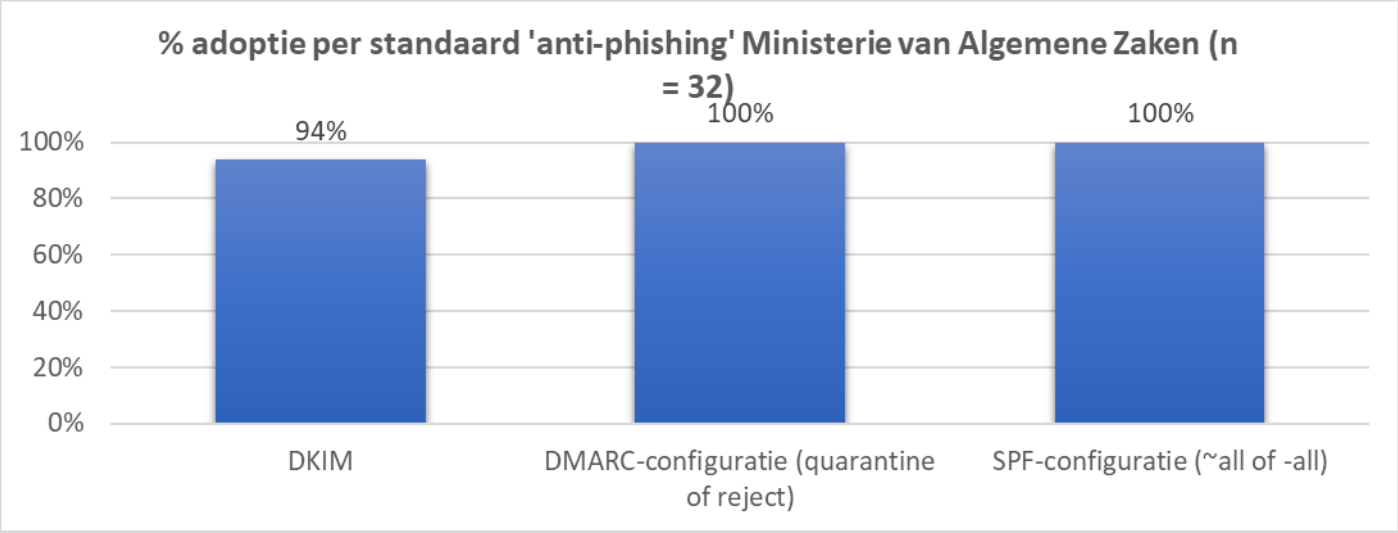


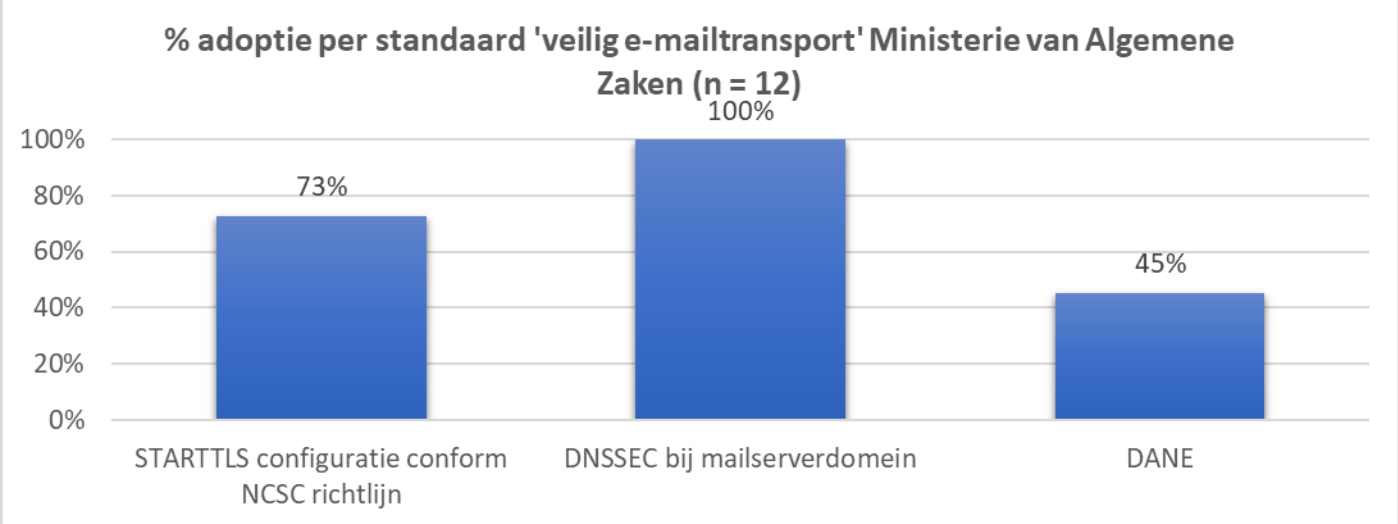
Vergelijkbaar met de adoptie van websitestandaarden, zien we dat ministeries met een beperkt portfolio, of actieve sturing op toepassing van standaarden, over het algemeen een hogere adoptiegraad bereiken.

De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per ministerie.

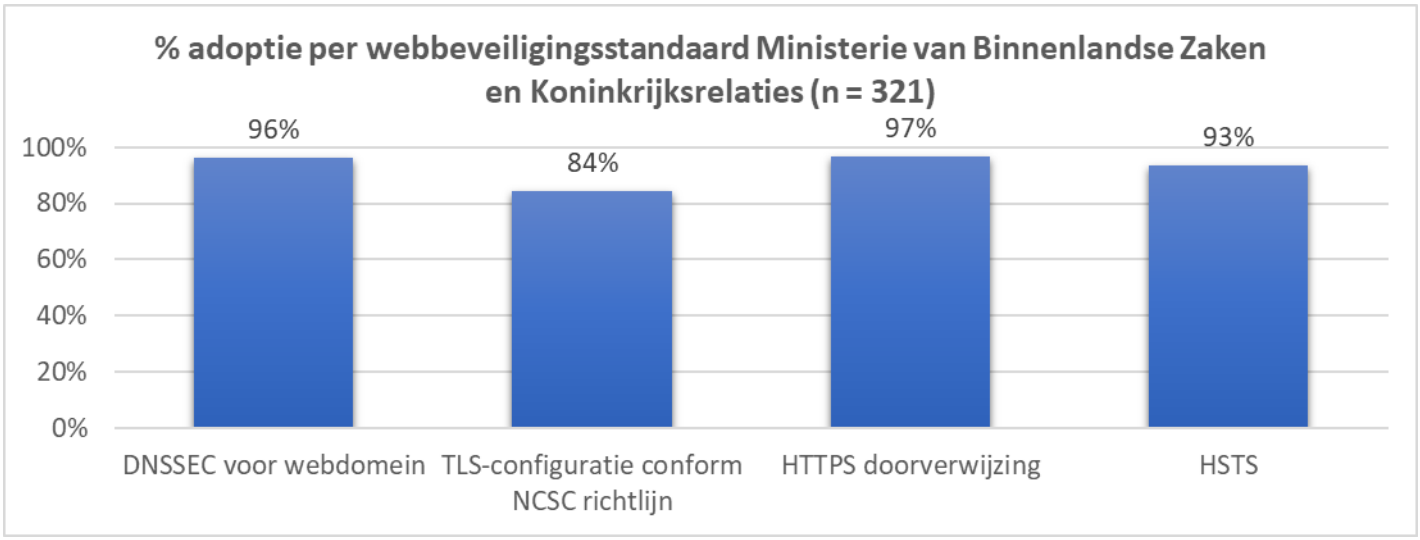
7.3. Ministerie van Algemene Zaken

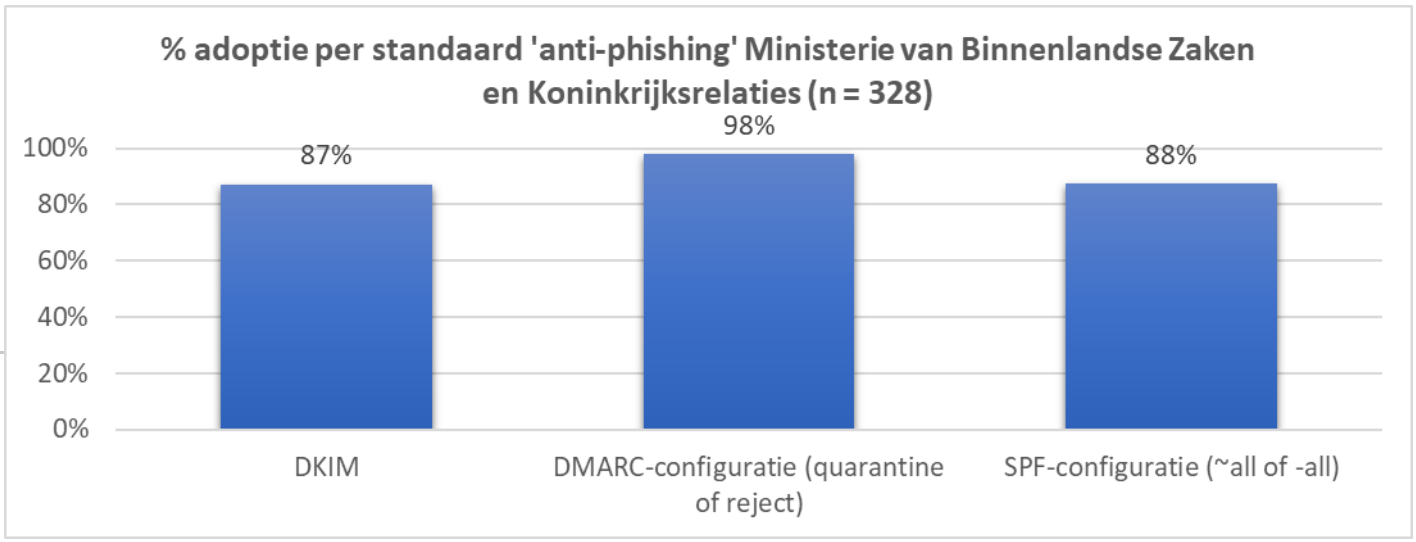


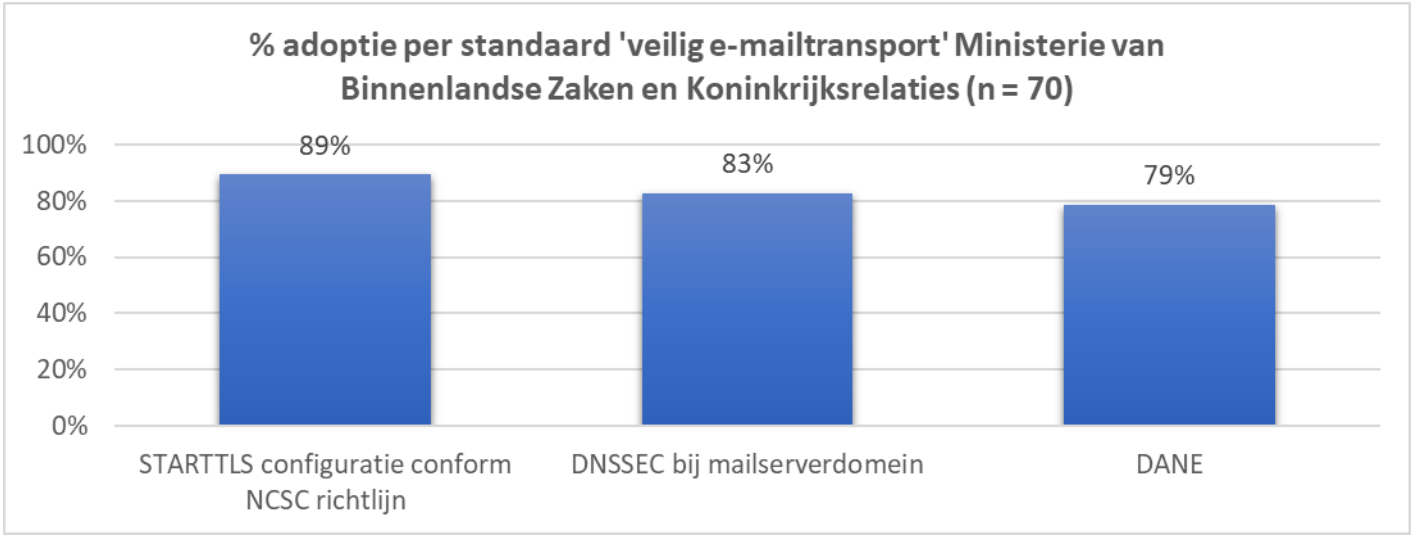




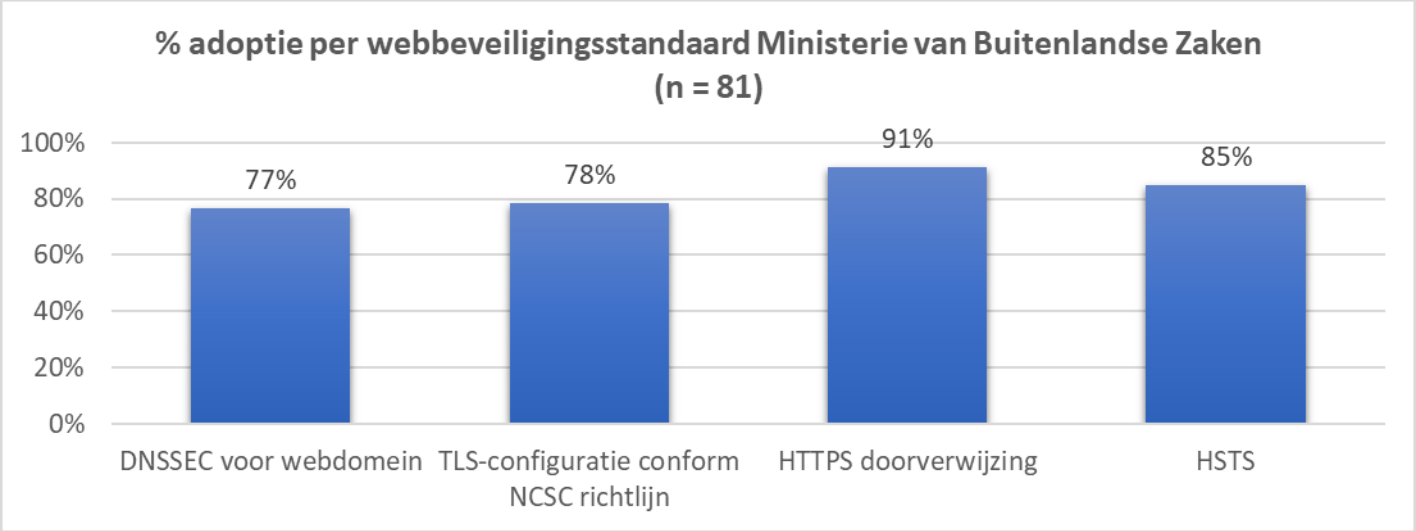
7.4. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

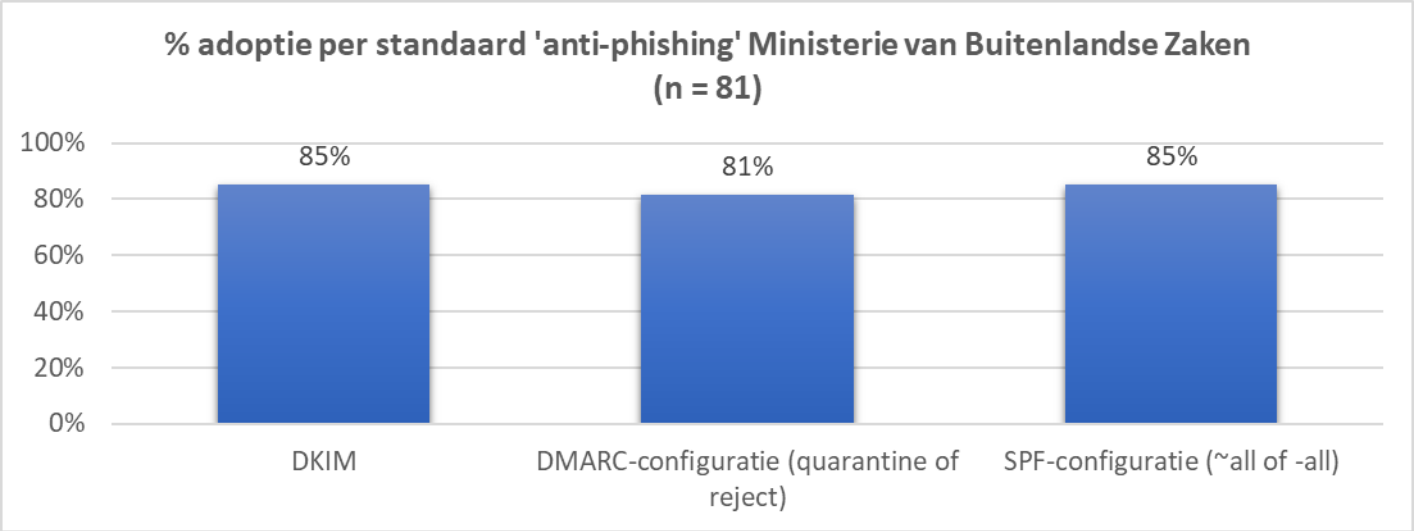


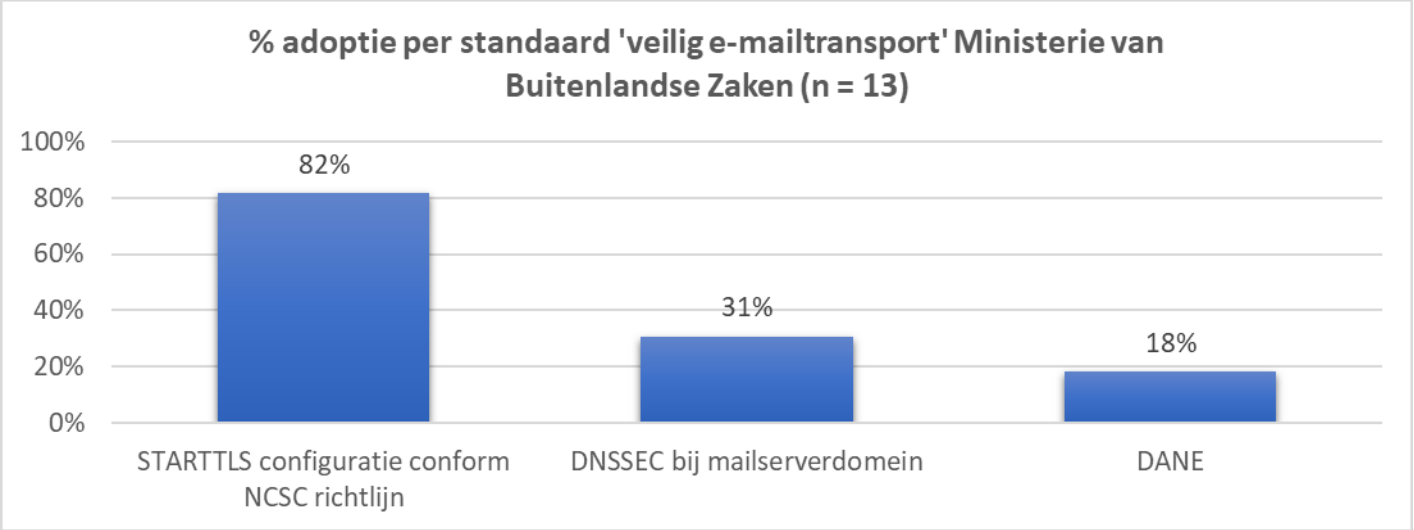




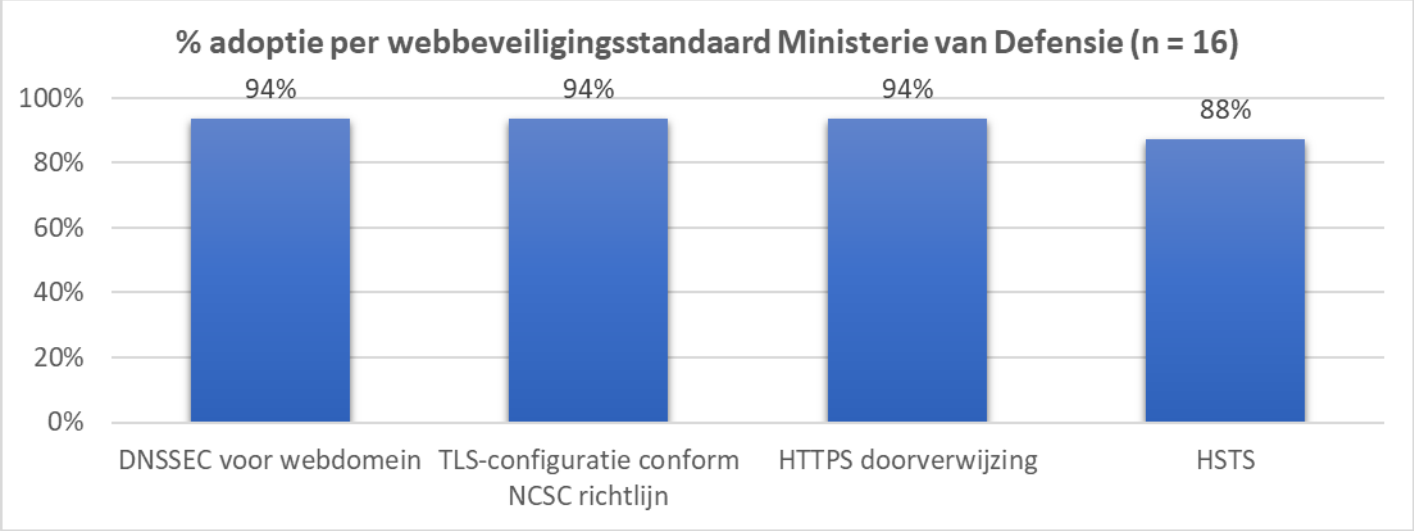
7.5. Ministerie van Buitenlandse Zaken

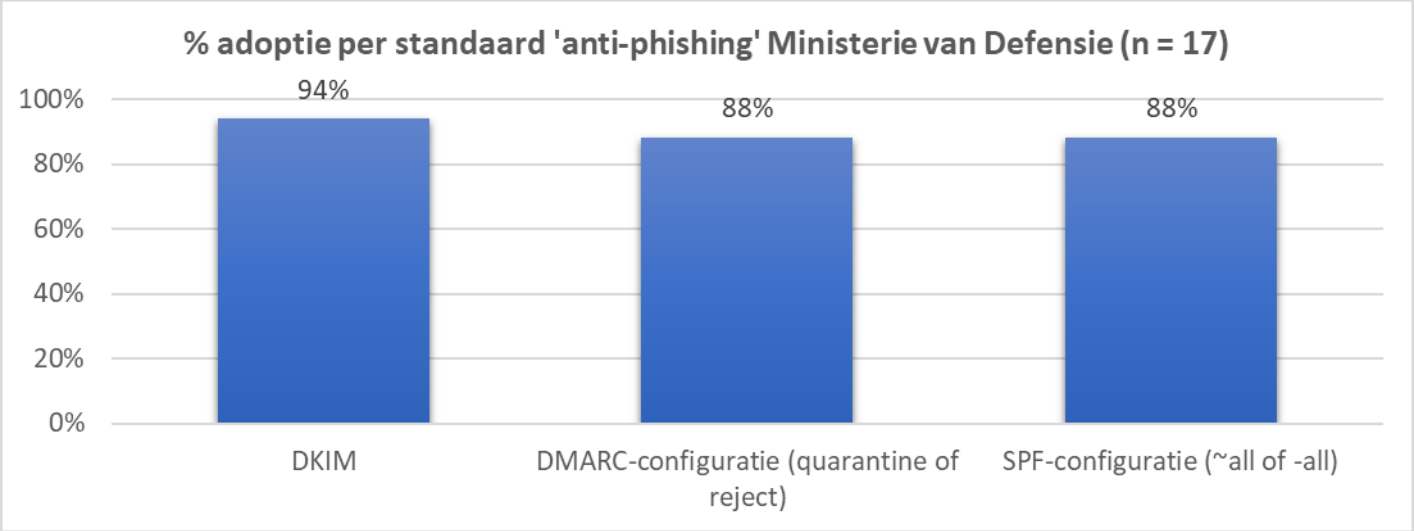


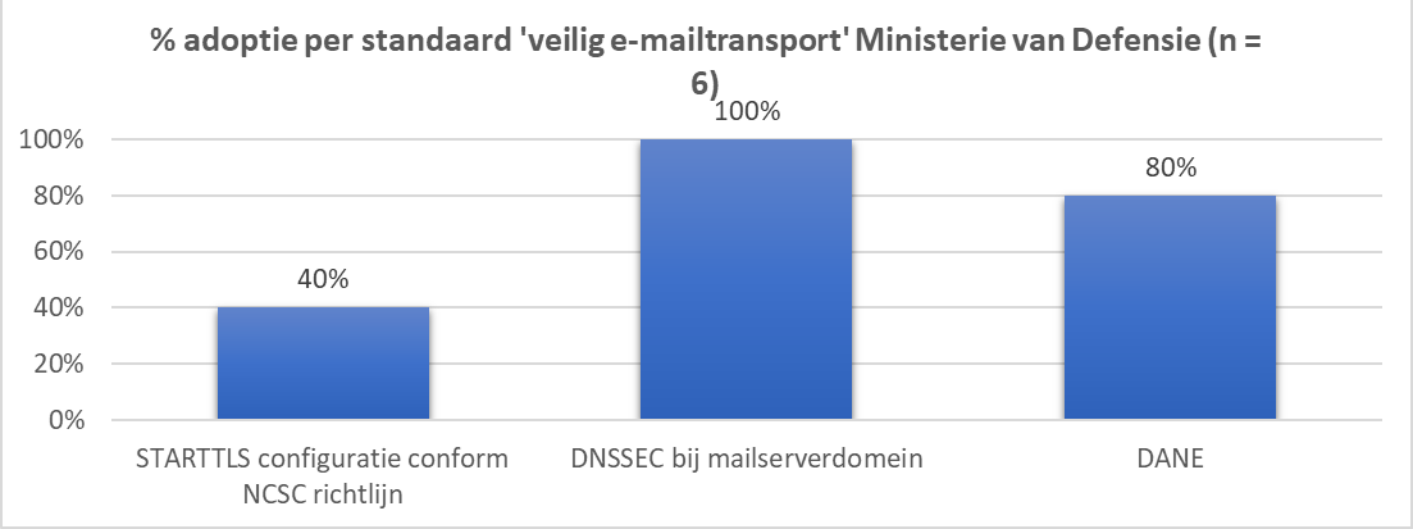




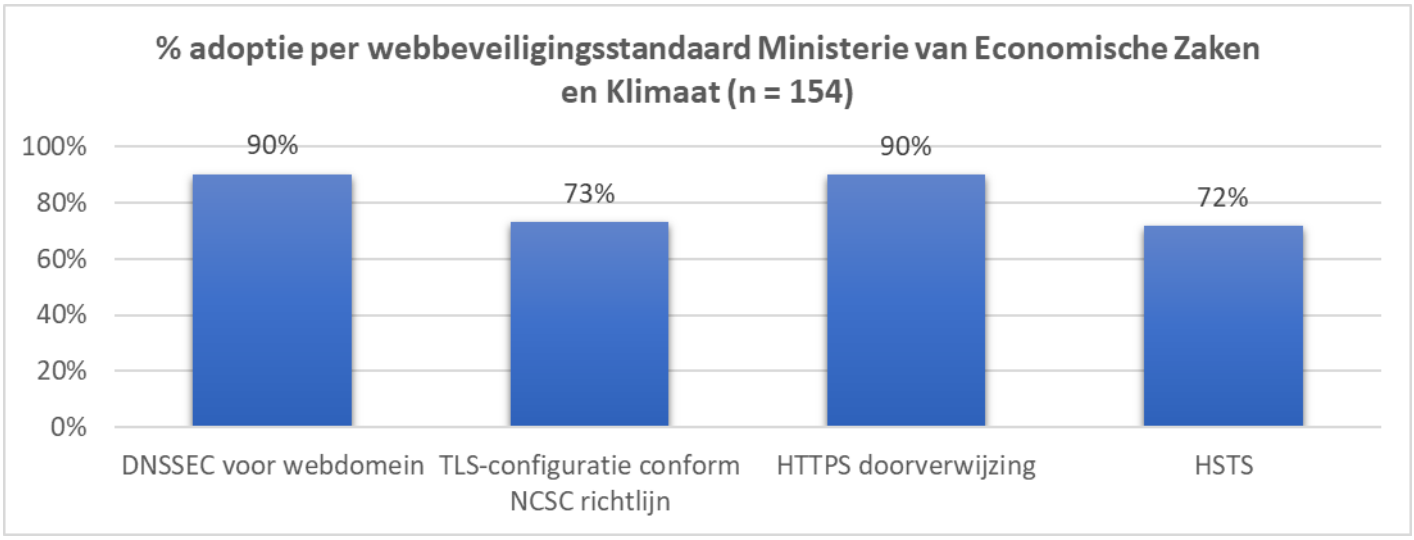
7.6. Ministerie van Defensie

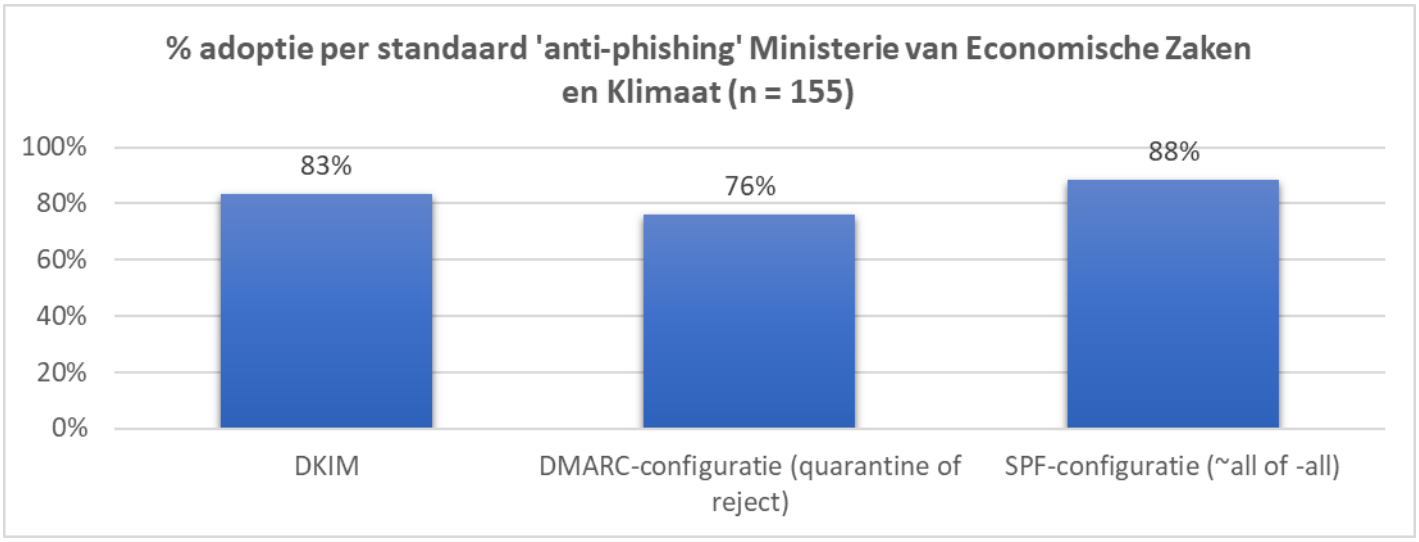


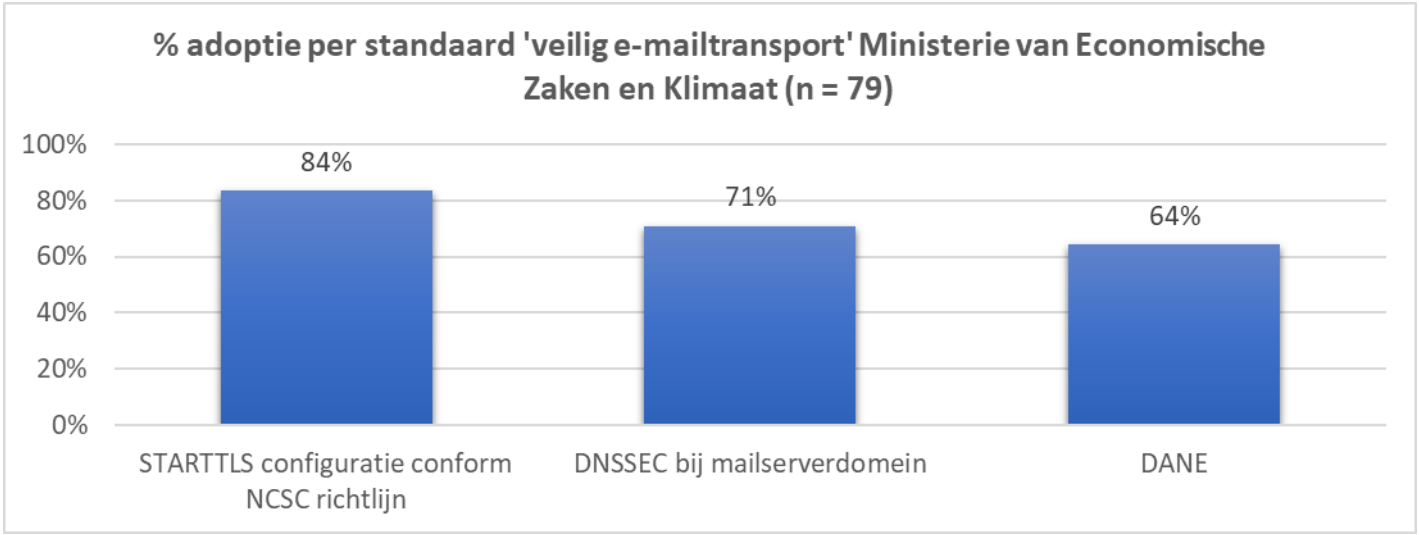




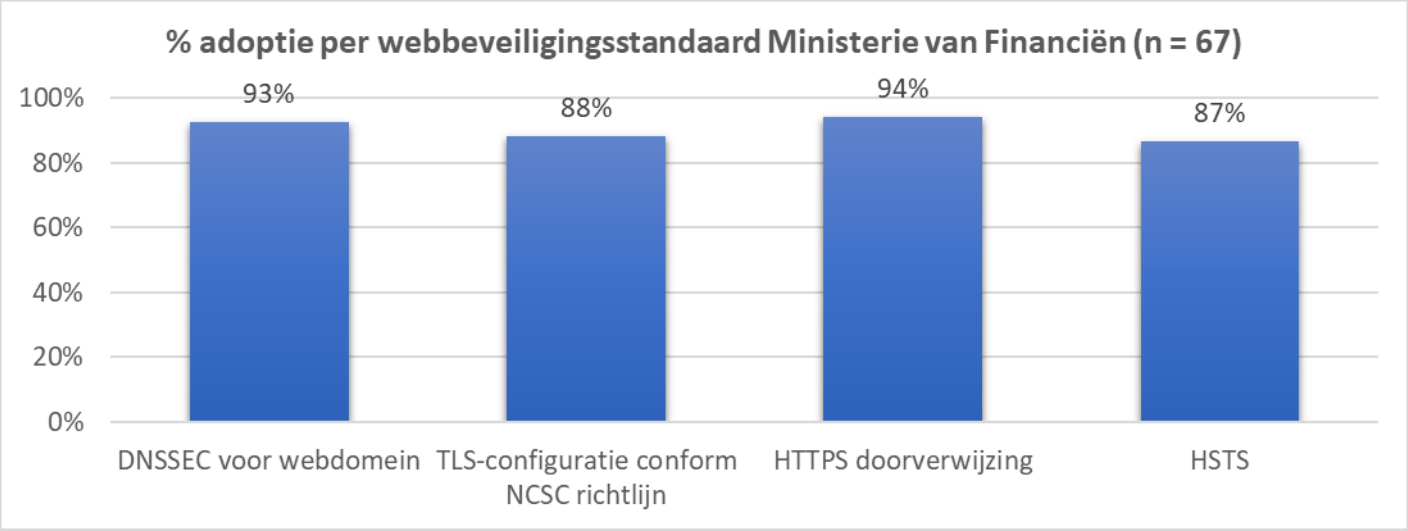
7.7. Ministerie van Economische Zaken en Klimaat

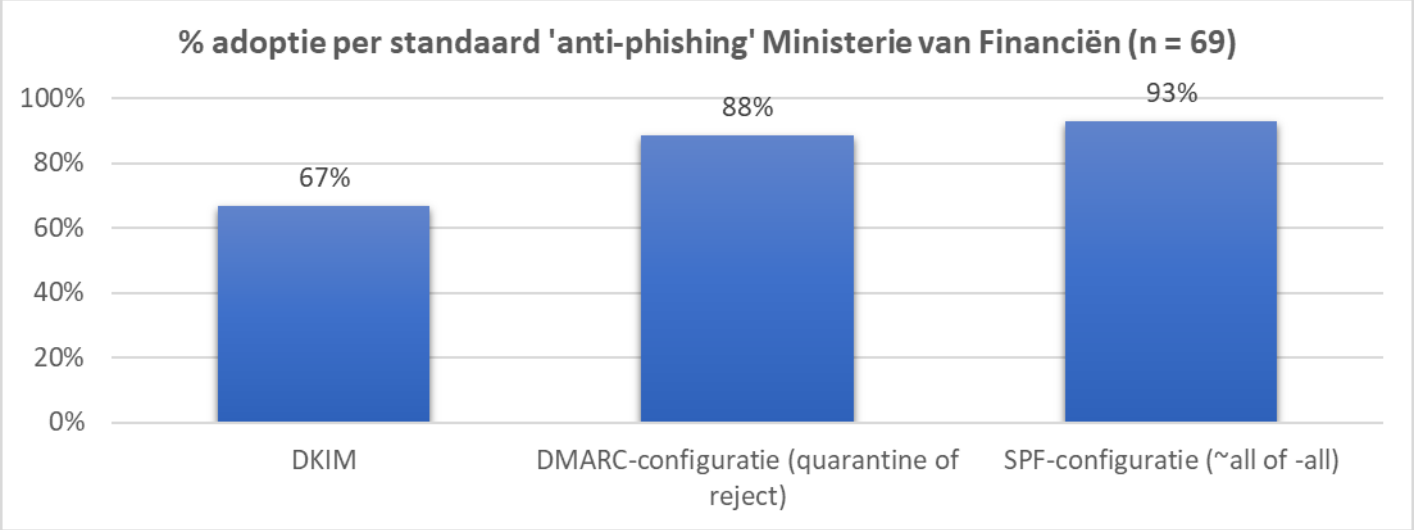


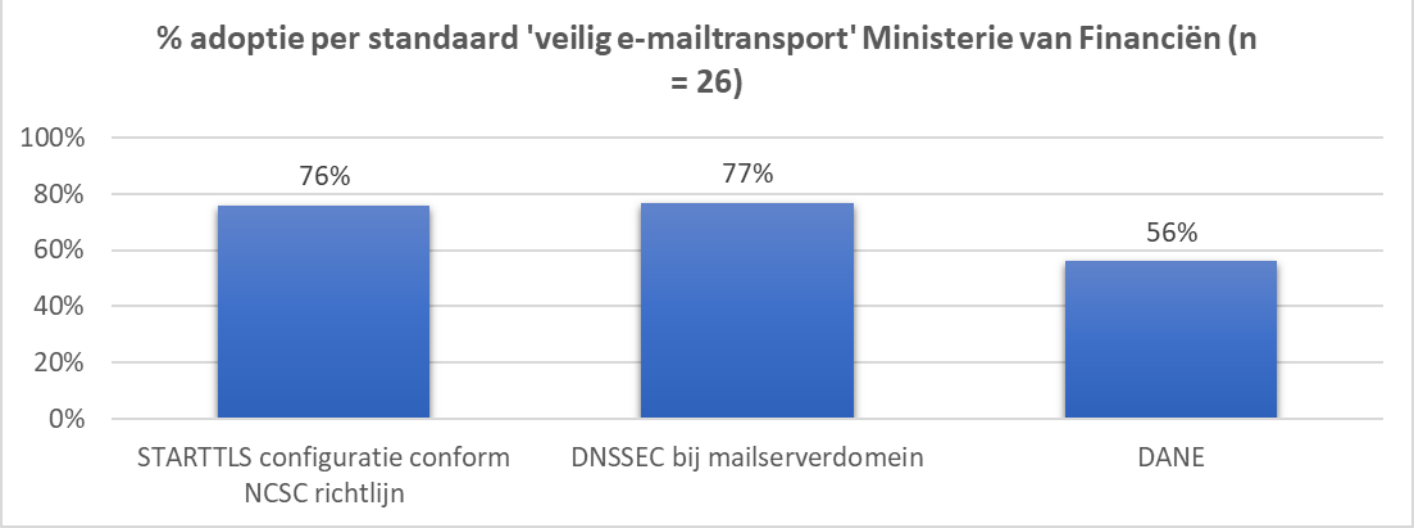




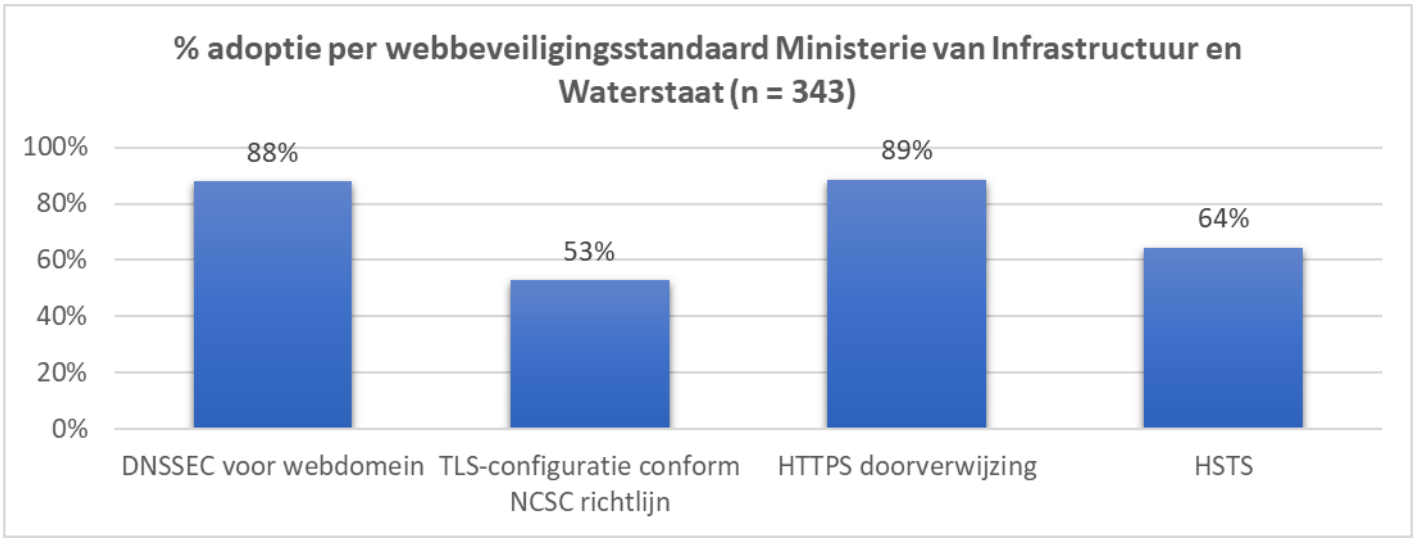
7.8. Ministerie van Financiën

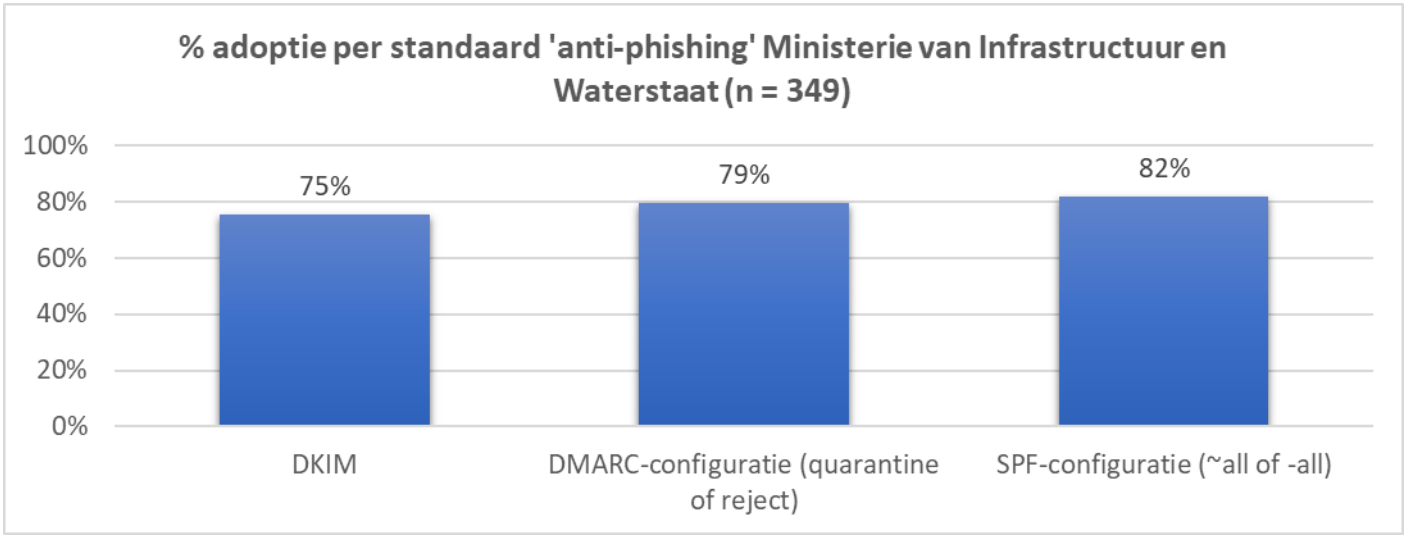


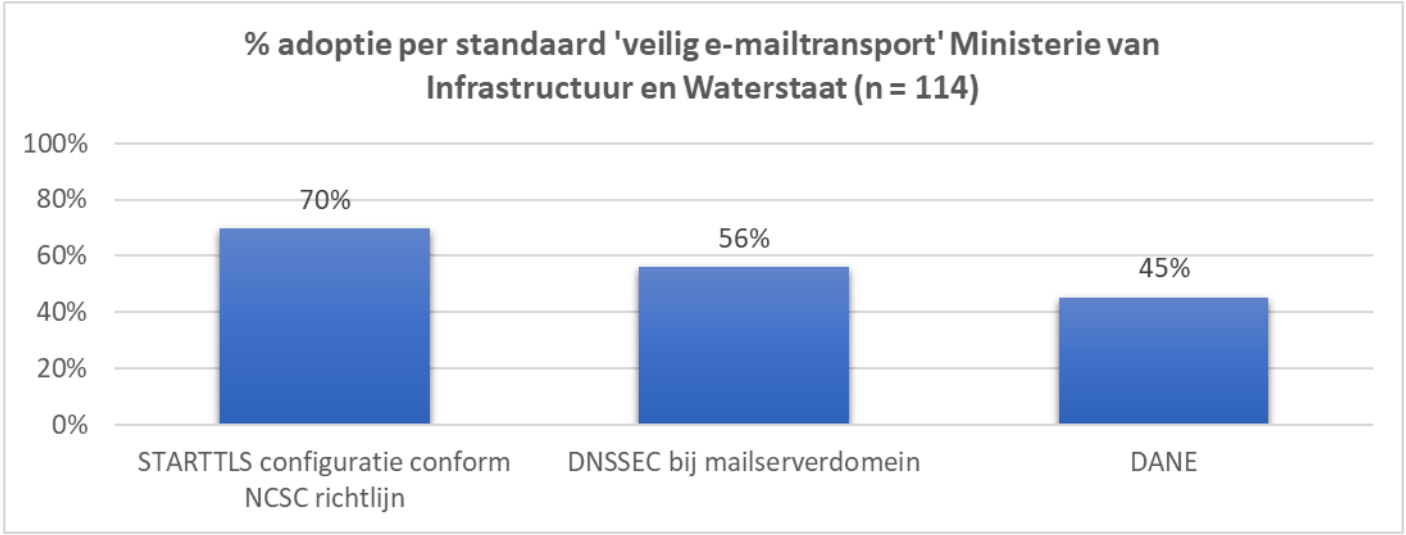




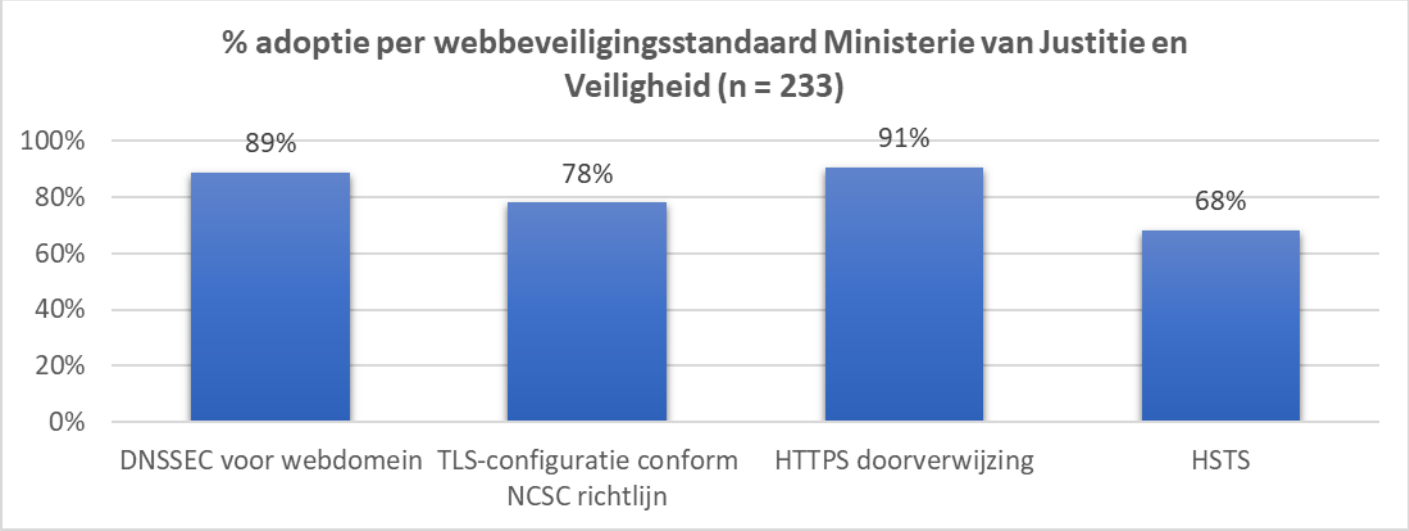
7.9. Ministerie van Infrastructuur en Waterstaat

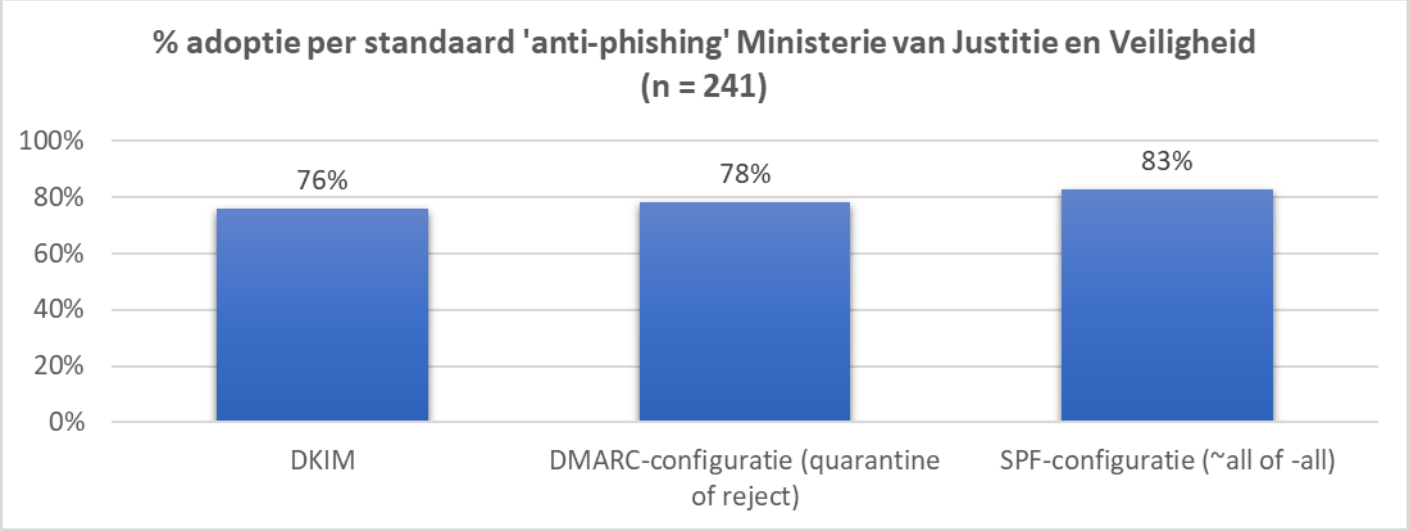


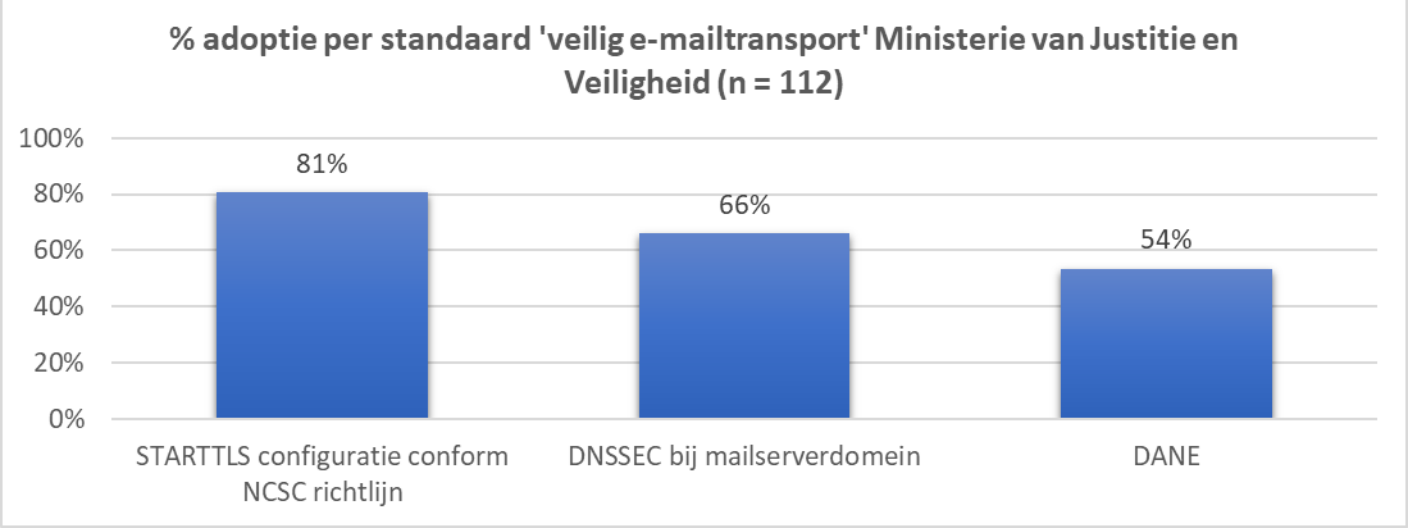




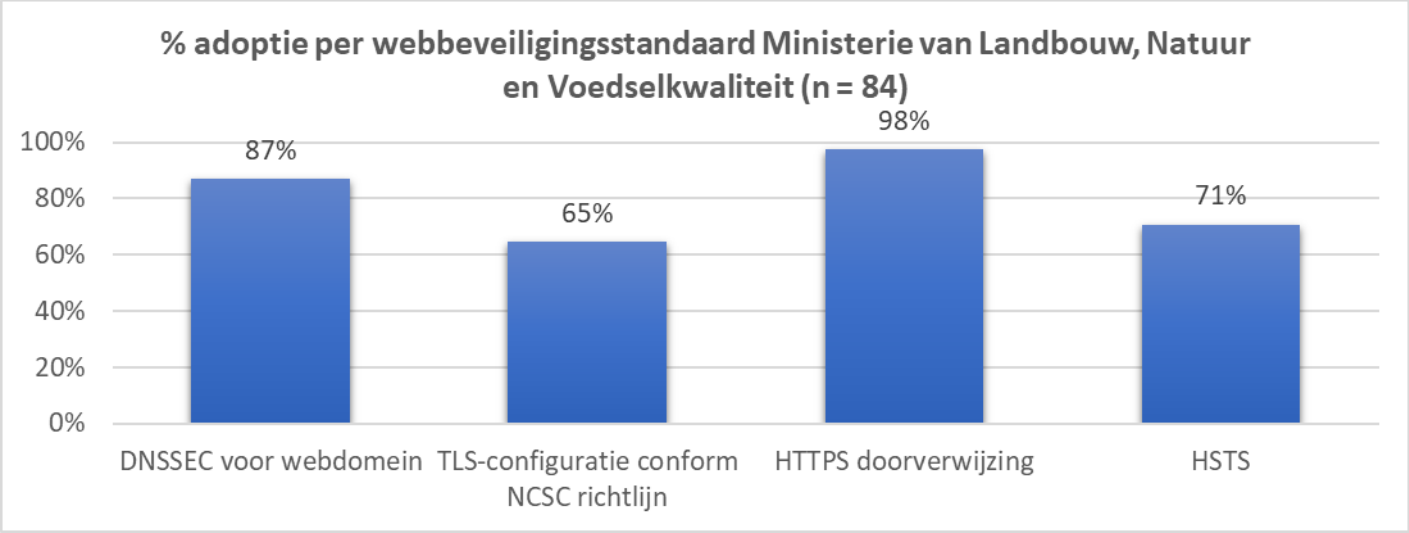
7.10. Ministerie van Justitie en Veiligheid

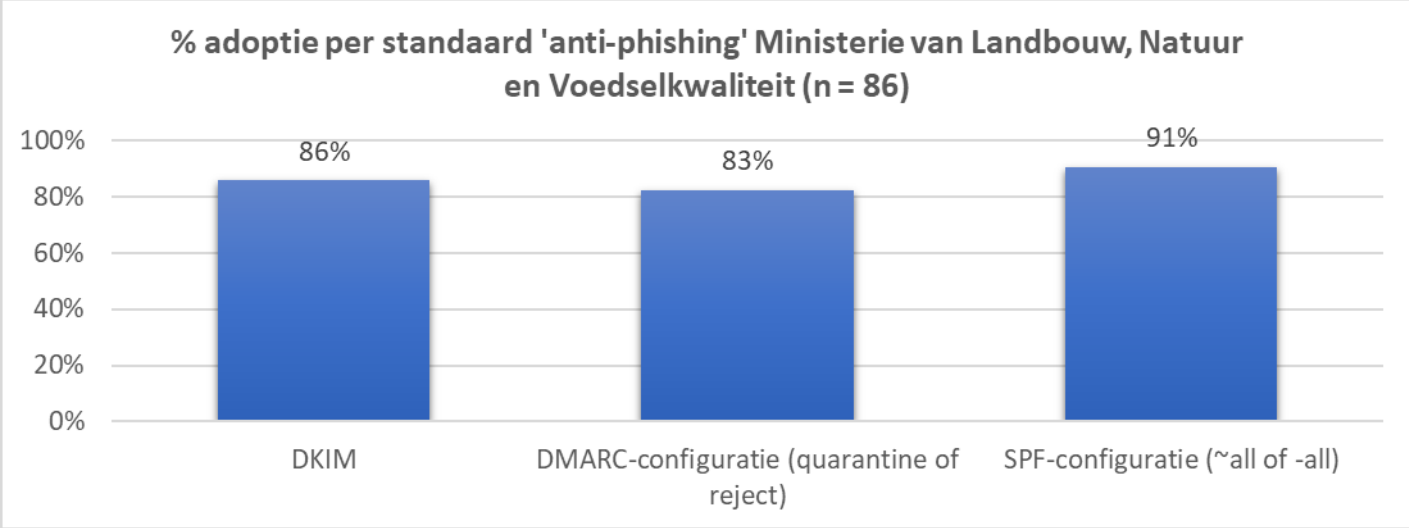


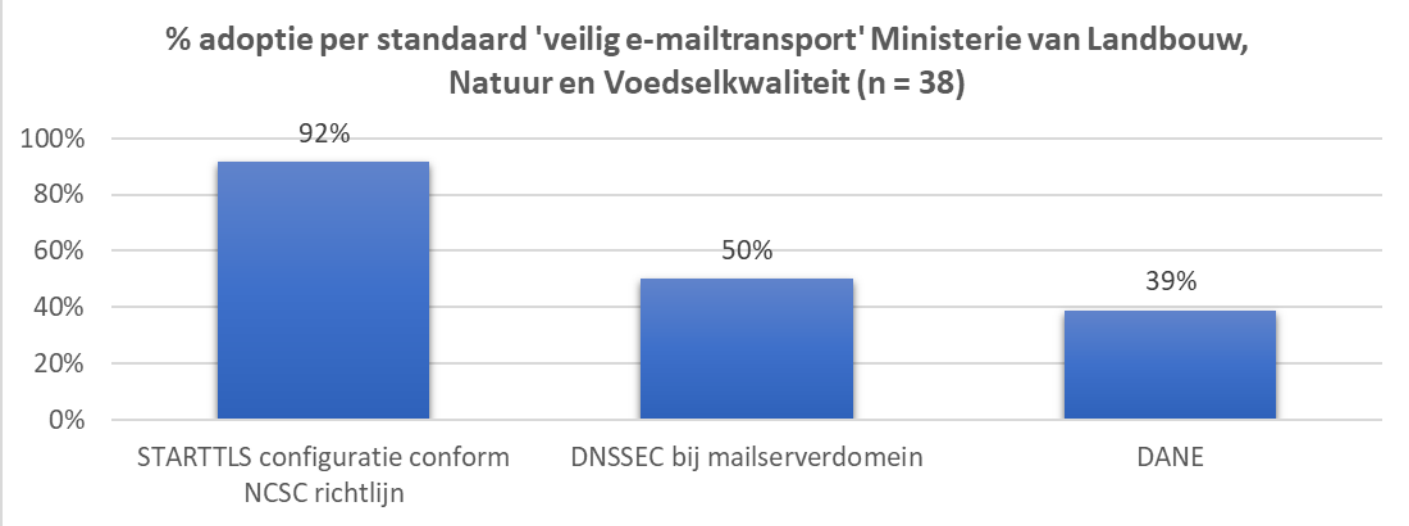




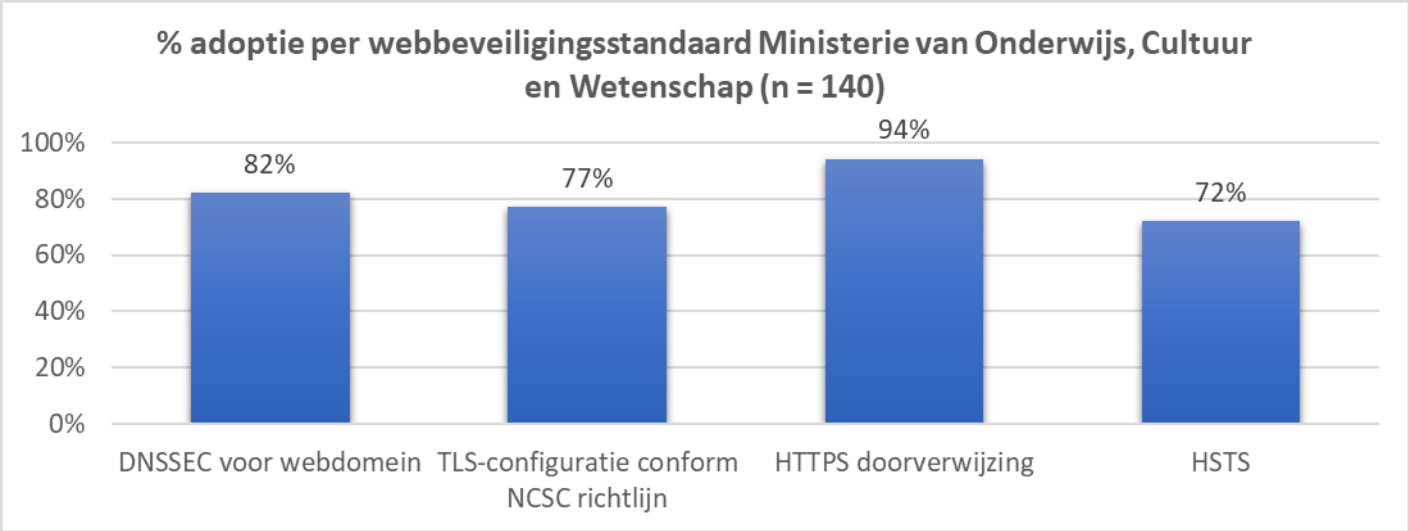
7.11. Ministerie van Landbouw, Natuur en Voedselkwaliteit

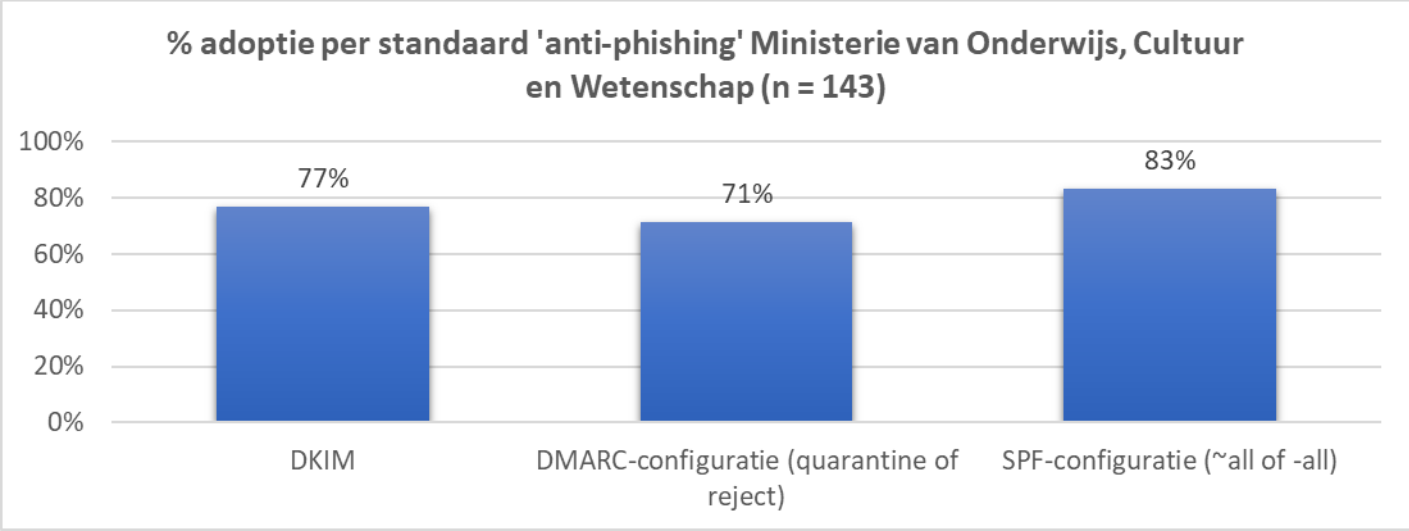


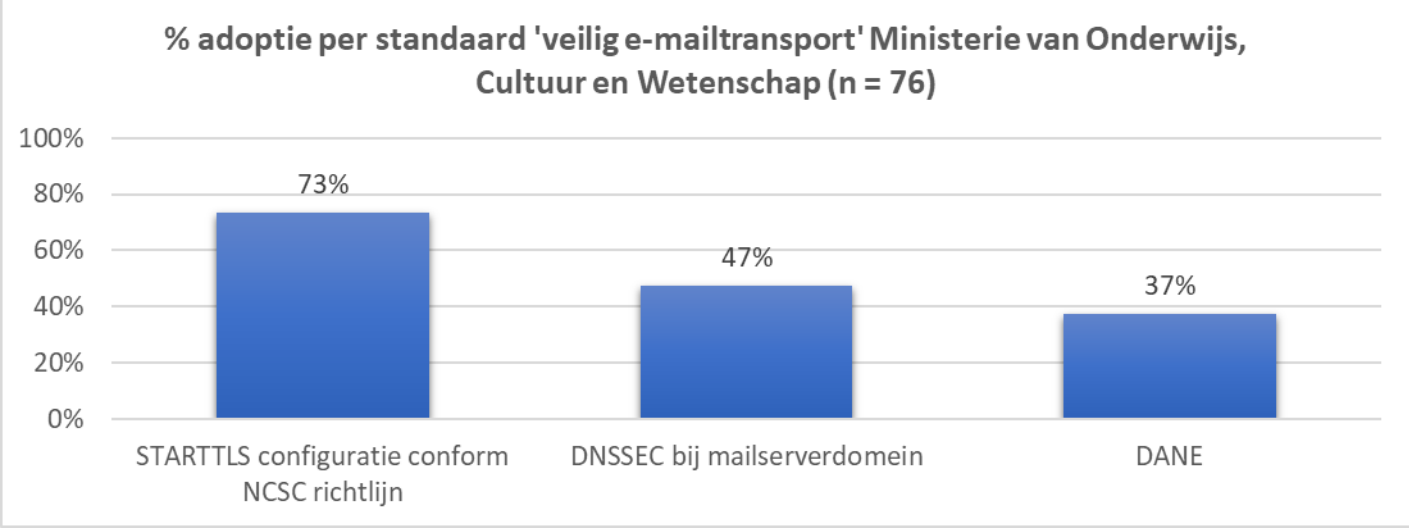




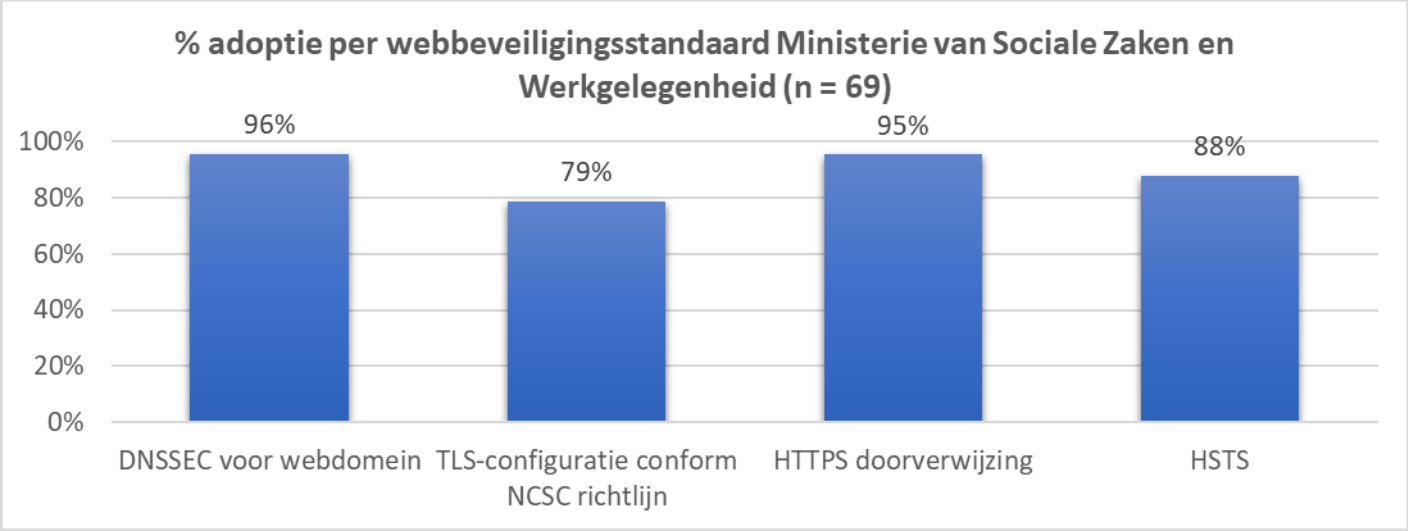
7.12. Ministerie van Onderwijs, Cultuur en Wetenschap

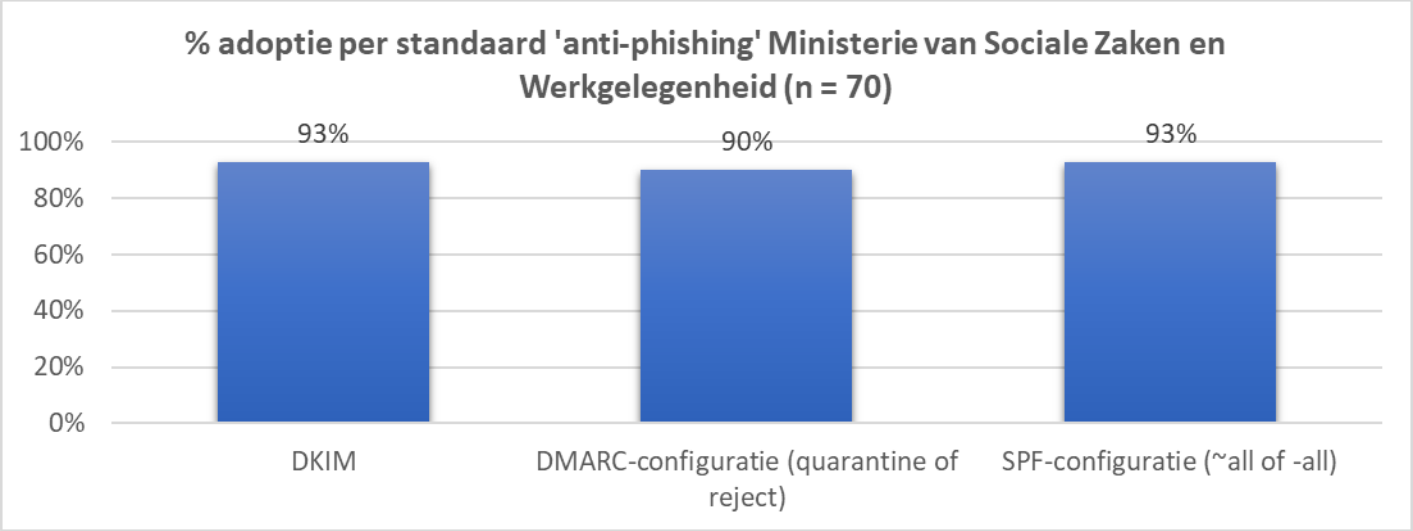


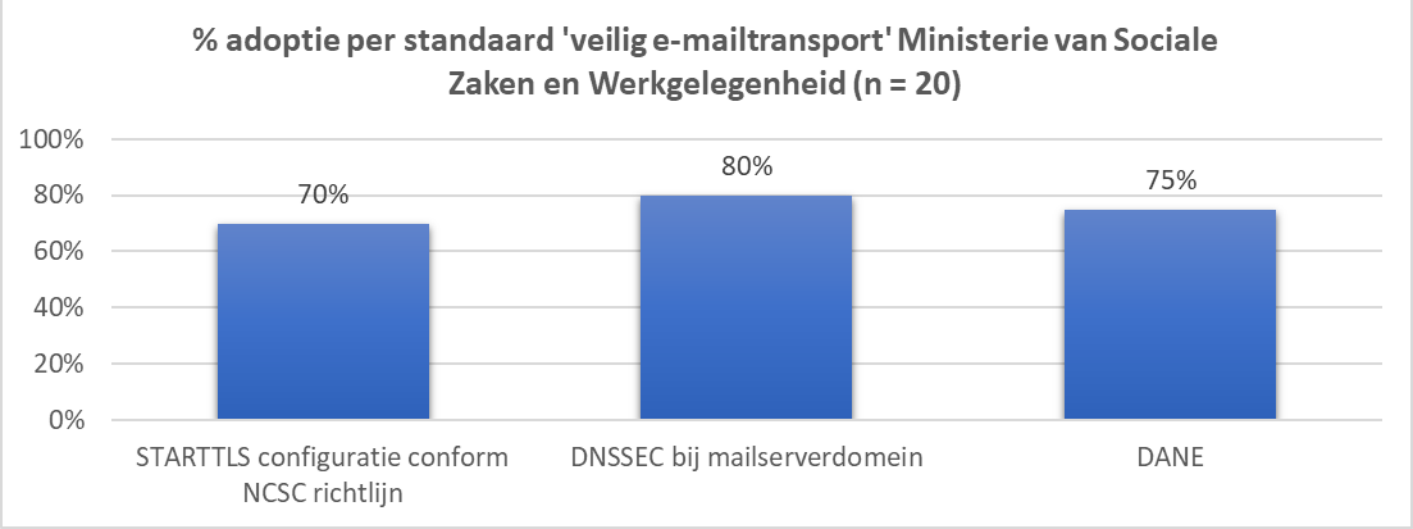




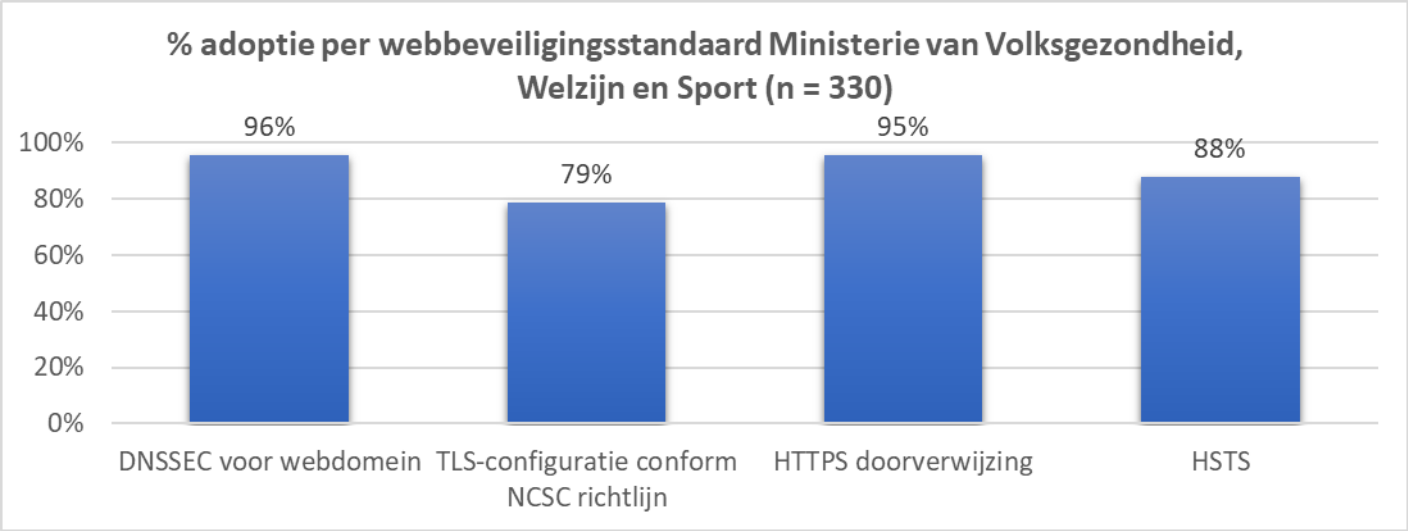
7.13. Ministerie van Sociale Zaken en Werkgelegenheid

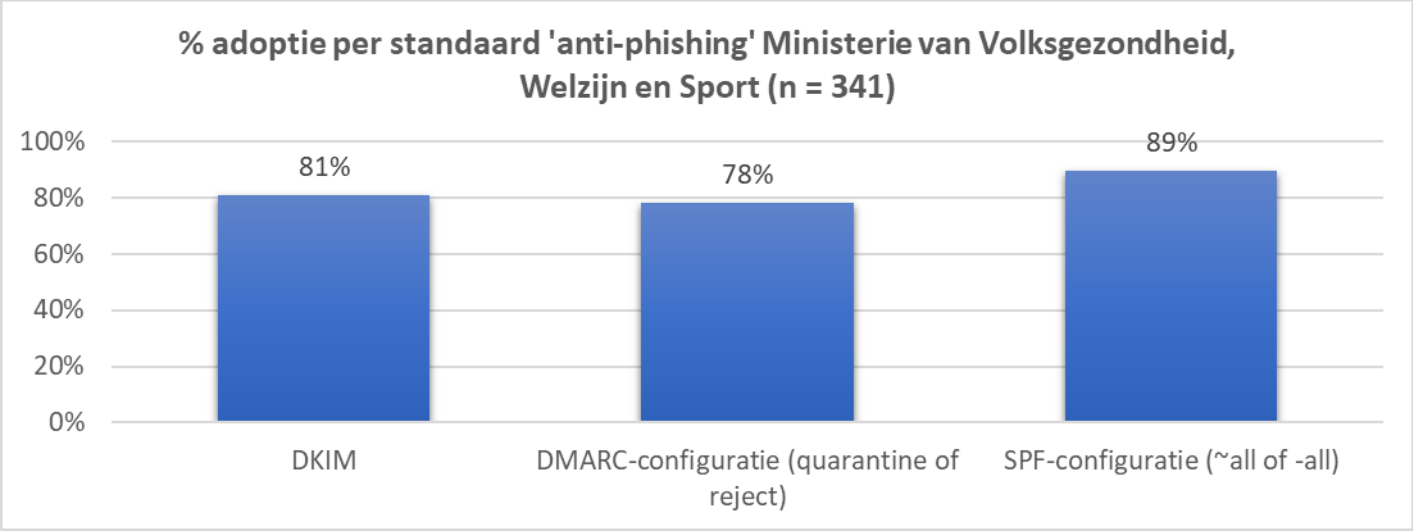


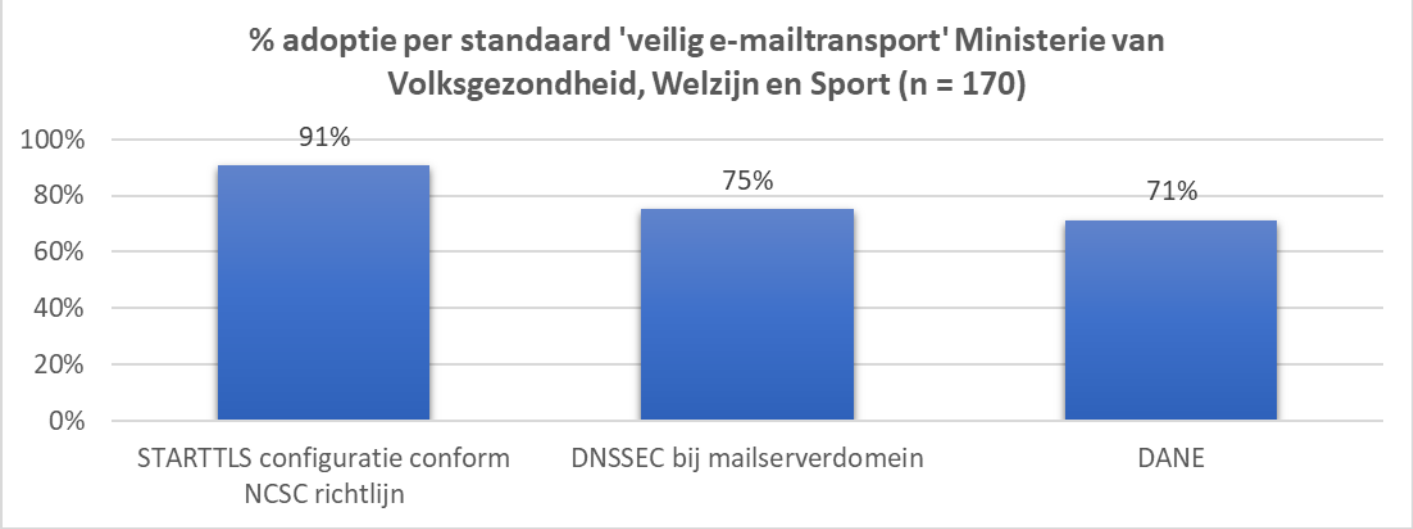




7.14. Ministerie van Volksgezondheid, Welzijn en Sport







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

8.2. Om welke internetdomeinen gaat het

In totaal zijn in deze meting 2710 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 januari 2023. De meting laat zien of op een domeinnaam de standaarden worden toegepast. De resultaten zijn voorgelegd aan een aantal koepelorganisaties en stakeholders en begin maart 2023 geactualiseerd indien nodig.

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.

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.

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.