FS-20240619.5E1

Forum Standaardisatie

Standaard Samenwerken

Meting Informatieveiligheidstandaarden overheid begin 2024

Inclusief IPv6

Datum document: 7 juni 2024

Status document: FS

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 buiten RPKI (voor betrouwbare internetroutering) al verstreken, waardoor verwacht mag worden dat alle webapplicaties en e-mailsystemen deze standaarden correct toepassen. Daarnaast is een tweetal standaarden daarvan sinds 1 juli 2023 wettelijk verplicht. In dit document wordt gerapporteerd over de stand van zaken per 1 februari 2024. In de eerste maanden van 2024 is de analyse uitgevoerd en zijn eventuele correcties doorgevoerd. Bij de totstandkoming van dit rapport lag de focus op het toevoegen van de nieuwe domeinnamen uit het Register Internetdomeinen Overheid (RIO). De meting is teruggelegd bij de gemeten organisaties, maar nog niet alle reacties hieruit zijn verwerkt. Terugleggingen bij eerdere metingen waren vooral waardevol ter stimulering van de adoptie en zorgden in een zeer klein aantal gevallen tot correcties, maar hebben toen niet geleid tot grote wijzigingen van de geaggregeerde resultaten. Eventuele correcties en ontvangen motivaties voor afwijking zal Forum Standaardisatie in de uiteindelijke te publiceren versie van het rapport opnemen.

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. Een ander voorbeeld is een zeer serieus incident in 2020 waarbij e-mail van de Tsjechische overheid werd afgeluisterd via een man-in-the-middle-aanval (in aanloop naar het voorzitterschap van de Raad van de Europese Unie). Merk op dat dit soort incidenten ook niet altijd aan het (publieke) licht komt. Hoe dan ook: des te meer domeinnamen voldoen aan de standaarden, des te kleiner de kans is dat dergelijke incidenten zich voordoen.

De nieuwe meting laat zien dat bij 64% van de internetdomeinen die ook in de vorige meting werden gemeten, alle verplichte website internetveiligheidstandaarden correct zijn toegepast (excl. IPv6 en RPKI). Dit is een stijging van 2 procentpunt ten opzichte van de vorige meting van juli 2023 (d.w.z. van 62% naar 64%). Het gaat om belangrijke beveiligingsstandaarden voor vertrouwelijk webverkeer. Inclusief IPv6 voor duurzame bereikbaarheid van online diensten voldoet 56%; hier is de toename 3 procentpunt (van 53% naar 56%). Het percentage websites met volledige adoptie van de webstandaarden (incl. RPKI en incl. IPv6) groeide van 49% naar 54% (d.w.z. een stijging van 5 procentpunt).

Bij 44% van de ook in de vorige meting gemeten internetdomeinen zijn alle verplichte e-mailstandaarden correct toegepast (excl. IPv6 en excl. RPKI). Dit is een afname van 1 procentpunt ten opzichte van de vorige meting (van 45% naar 44%). Hier gaat het om belangrijke beveiligingsstandaarden die e-mailvervalsing uit naam van de overheid kunnen voorkomen en het e-mailverkeer vertrouwelijk kunnne houden. Inclusief IPv6 voor duurzame bereikbaarheid van online diensten voldoet 43%; dit is een afname van 2 procentpunt (van 45% naar 43%).

Er zijn in het algemeen zeer kleine verbeteringen zichtbaar ten opzichte van de vorige meting. 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 laat zien dat het consequent meten en publiceren van de compliance van internetdomeinen helpt om de kwaliteit te verhogen.

In deze meting zijn in totaal 10959 overheidsdomeinen gecontroleerd. In de vorige meting waren dit 5190 overheidsdomeinen. Deze bijna verdubbeling komt voornamelijk door het toevoegen van het Register Internetdomeinen Overheid (RIO). In het register kan worden nagegaan of een website of e-mailadres van een overheidsorganisatie is. Het RIO heeft ten doel om alle domeinnamen die door overheidsorganisaties zijn geregistreerd bij te houden en te publiceren. Daarnaast is er een stijging van nieuw geregistreerde domeinnamen en oudere domeinnamen die pas later aan de domeinnaamportfolio's zijn toegevoegd. Het RIO is momenteel alleen gevuld met domeinen en domeinregistraties van de Rijksoverheid. Dit zijn nog niet alle overheidsdomeinnamen, het totaalportfolio heeft vele duizenden meer domeinen. Het ontbreekt vooral aan een register van de domeinnamen van decentrale overheden. Zo hebben gemeenten meer dan 10.000 websites, maar hiervan staat slechts een fractie in de officiële registers. De overheid zelf maar zeker ook de burger hebben daardoor 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 van de standaarden 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. Ondanks het toevoegen van vele domeinnamen, is er geen zicht op het totaalportfolio aan domeinnamen van de overheid, vooral de decentrale overheden zijn ondervertegenwoordigd in de meting.

Advies 1 (aan BZK, KOOP/Logius en decentrale overheidsorganisaties): Maak een afspraak over wanneer alle decentrale overheden moeten zijn aangesloten op het centrale Register Internetdomeinen Overheid (RIO). Het RIO heeft ten doel om alle domeinnamen die door overheidsorganisaties zijn geregistreerd bij te houden en te publiceren. Burgers kunnen in het register nagaan of een website of e-mailadres van een overheidsorganisatie is. Daarnaast geeft het register de overheid zelf zicht op het totaalportfolio waardoor beter op kwaliteit van de digitale dienstverlening kan worden gestuurd. Daarom is het van belang dat ook domeinnamen van decentrale overheden worden toegevoegd aan het RIO.

Advies 2 (aan alle overheidsorganisaties): Organiseer regie op internetdomeinen binnen individuele overheidsorganisaties. Zet in op een groeistop van het domeinnaamportfolio en stuur idealiter op een inkrimping.

Om de adoptieopgave behapbaar te maken en te houden, is actief bejeer van het domeinnaamportfolio met als doel het beperkten van het domeinnaamportfolio noodzakelijk. Stel een maximum aan nieuwe domeinnamen per jaar vast. De samenvoeging van verschillende websites en het vaker inzetten van subdomeinen in plaats van nieuwe domeinnamen, verkleinen het digitale oppervlak waar de standaarden geïmplementeerd moeten worden.

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 2024 nog steeds actueel en kan helpen bij deze opgave.

Advies 3 (aan Forum Standaardisatie en aan overheidsorganisaties): Inventariseer waar gebruik wordt gemaakt van Microsoft Office 365 Exchange Online en combineer vanaf juni 2024 de configuratie van zowel DANE als IPv6.

Overheden besteden hun e-mailvoorzieningen steeds vaker uit aan clouddienstverleners. Een aantal van dit soort dienstverleners ondersteunen niet alle verplichte standaarden. Zo voldoet Microsoft Office 365 Exchange Online voor e-maildiensten op dit moment niet door de onvolledige implementatie van DANE. Daarnaast is de standaard configuratie van Microsoft Office 365 Exchange Online zonder IPv6; deze moet actief worden geconfigureerd. Vanaf juni 2024 komt DANE volledig beschikbaar. Gebruik dit moment om zowel de veilige e-mailtransport standaard DANE als duurzame ontsluiting via IPv6 op Exchange Online te implementeren.

Advies 4 (aan alle overheidsorganisaties): 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. Vraag in ieder geval achterblijvende leveranciers naar wanneer de implementatie van RPKI op de roadmap staat. Stuur op implementatie van RPKI voor het einde van 2024 om aan de adoptieafspraak te voldoen.

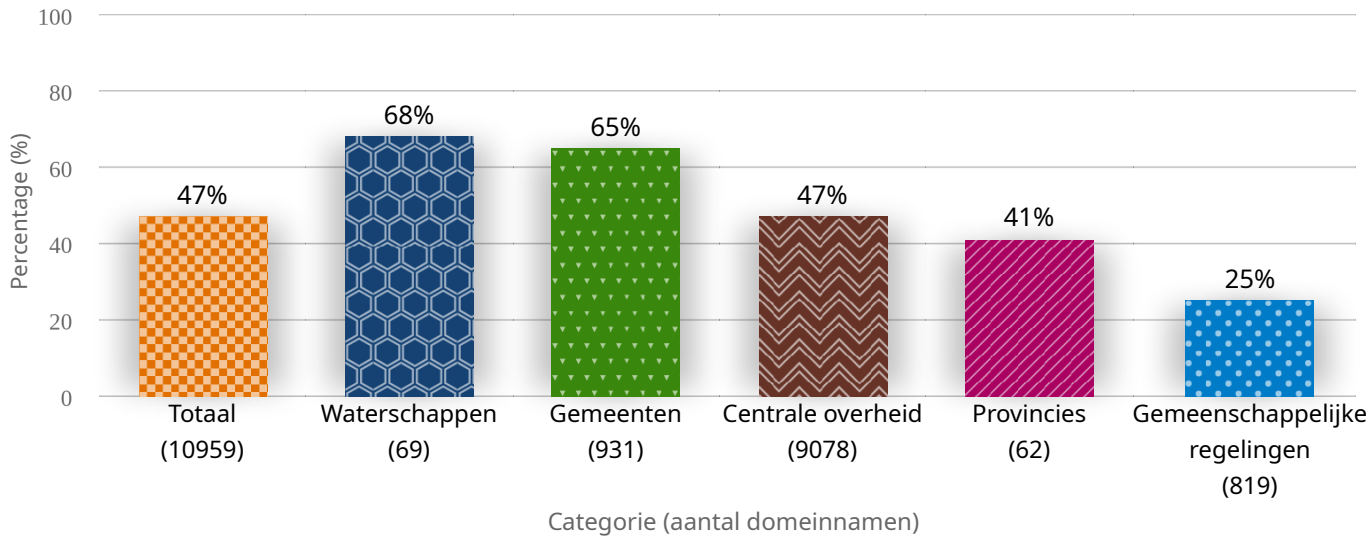
1.2. Websitestandaarden

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.

Grafiek 1: Volledige adoptie van alle webstandaarden per overheidscategorie



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

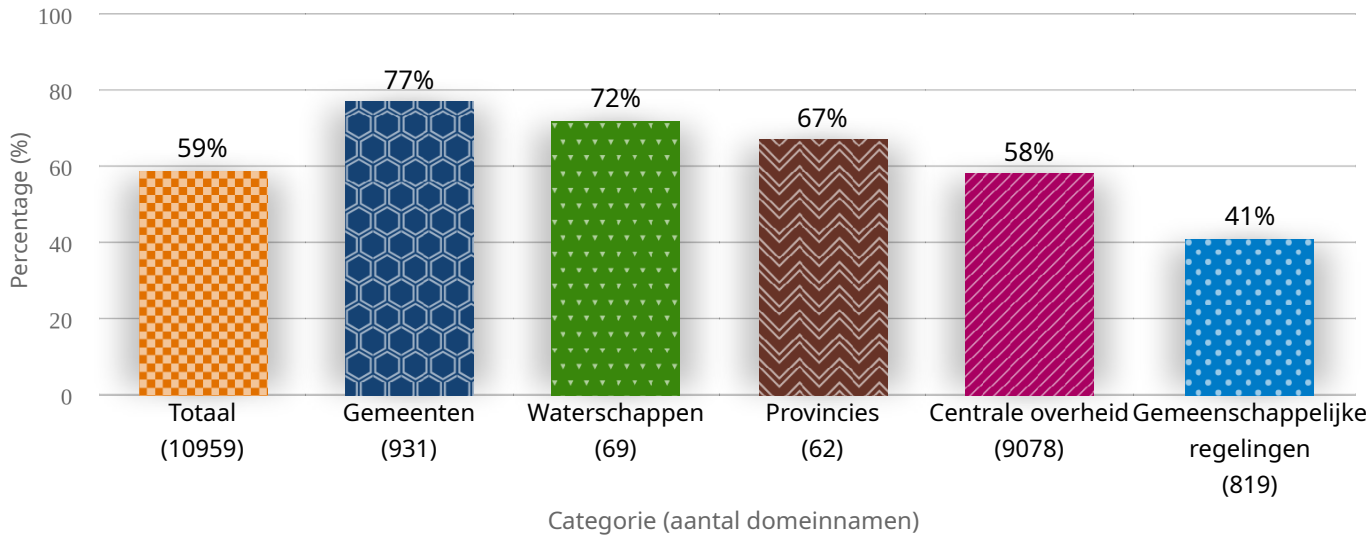
Door toepassing van websitebeveiligingsstandaarden wordt de verbinding met overheidswebsites beter beveiligd, zodat criminelen niet zomaar uitgewisselde gegevens kunnen onderscheppen of manipuleren.

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 gemeenschappelijke regelingen en centrale overheid. 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 er grotere gemeenten wel honderden websites in beheer kunnen hebben.

Grafiek 2: Volledige adoptie van alle webbeveiligingsstandaard per overheidscategorie

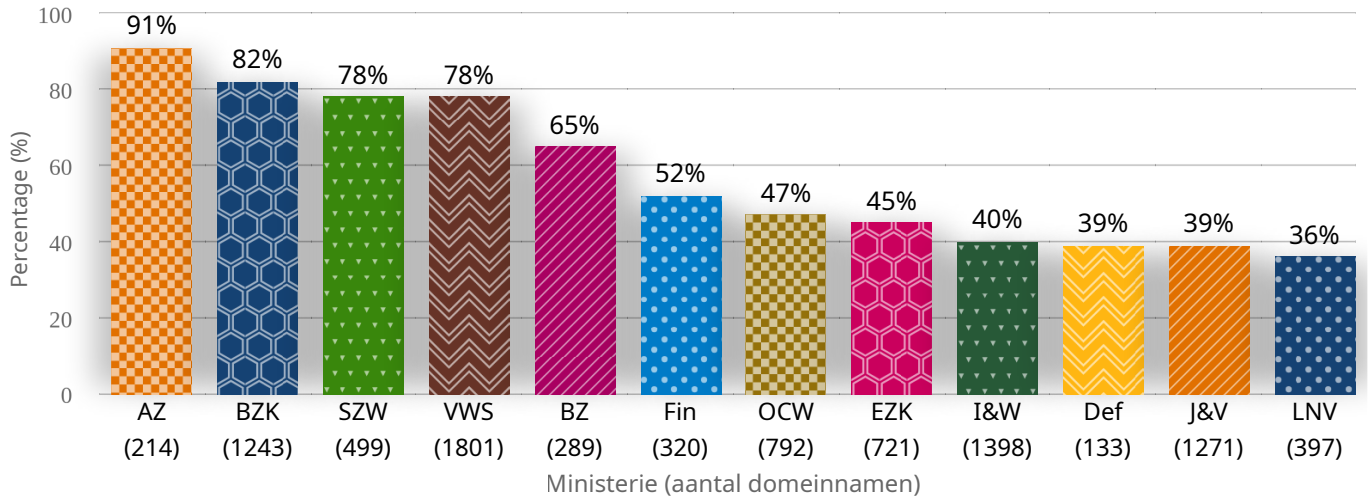


Voor meer details per overheidscategorie zie hoofdstuk 6.

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 (91%), Binnenlandse Zaken en Koninkrijksrelaties (82%), Sociale Zaken en Werkgelegenheid (78%) en Volksgezondheid, Welzijn en Sport (78%) in positieve zin op. De achterblijvers zijn de ministeries van Landbouw, Natuur en Voedselkwaliteit (36%), Justitie en Veiligheid (39%), Defensie (39%) en Infrastructuur en Waterstaat (40%).

Grafiek 3: Volledige adoptie van alle webbeveiligingsstandaard per ministerie



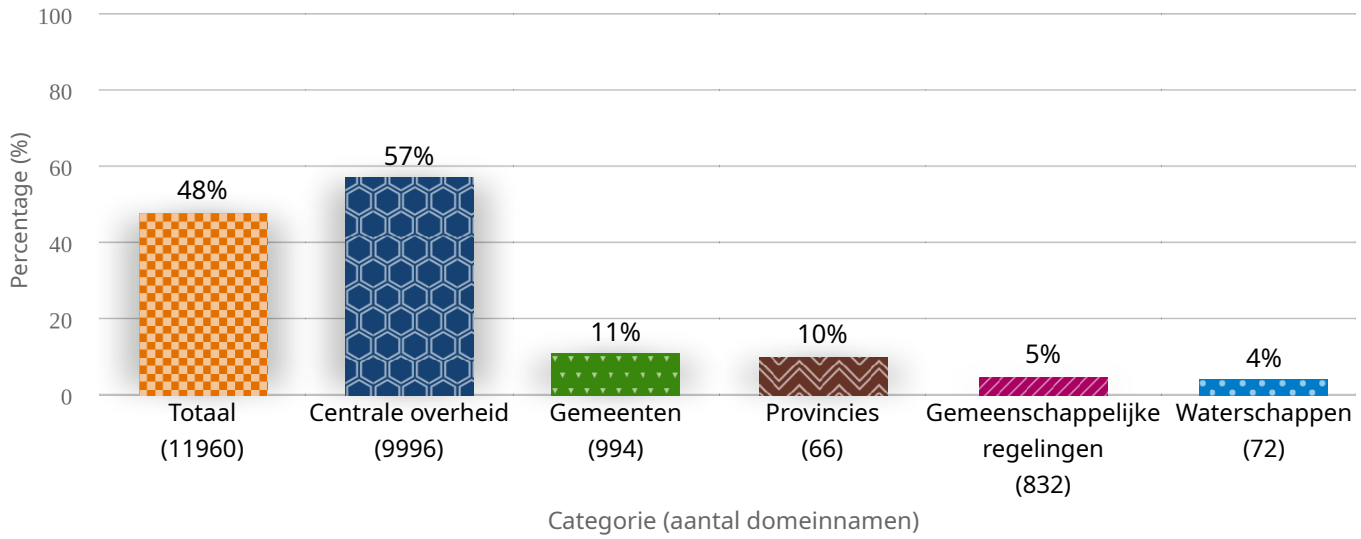
Voor meer details per ministerie zie hoofdstuk 7.

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 (57%) 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 (4%) en gemeenschappelijke regelingen (5%). 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.

Grafiek 4: Volledige adoptie van alle e-mailstandaarden per overheidscategorie



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)

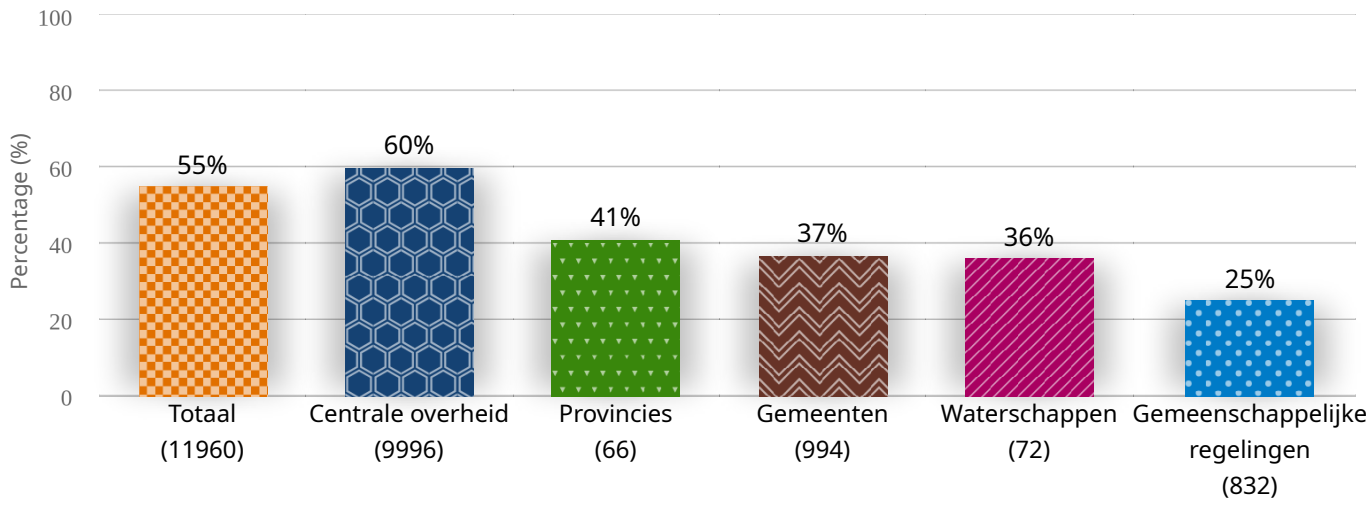
Door toepassing van e-mailstandaarden voor het bestrijden van phishing wordt e-mailverkeer met de overheid beter beveiligd, zodat criminelen niet zomaar overheidsdomeinen kunnen misbruiken als afzenddomein voor bijvoorbeeld phishing-aanvallen. Deze standaarden zijn relevant voor alle domeinnamen, ook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

Grafiek 5: Volledige adoptie 'anti-phishing' standaarden per overheidscategorie

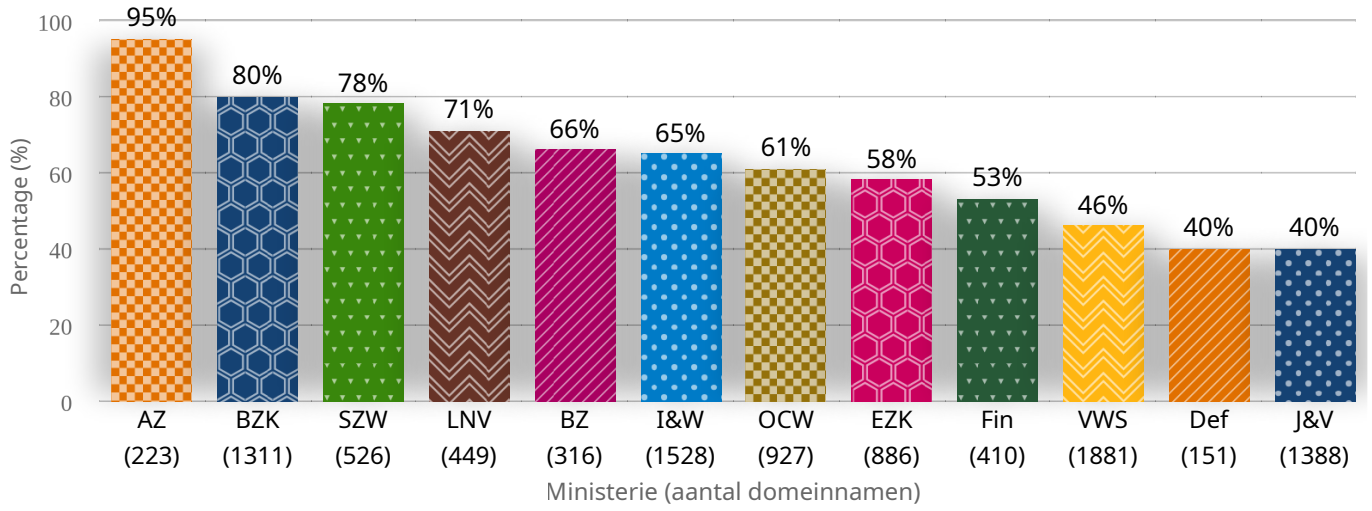


Voor meer details per overheidscategorie zie hoofdstuk 6.

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 (95%), Binnenlandse Zaken en Koninkrijksrelaties (80%) en Sociale Zaken en Werkgelegenheid (78%) positief op. De ministeries van Justitie en Veiligheid (40%) en Defensie (40%) hebben nog veel werk te verzetten om e-mailvervalsing namens haar domeinnamen te voorkomen.

Grafiek 6: Volledige adoptie 'anti-phishing' standaarden per ministerie



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.

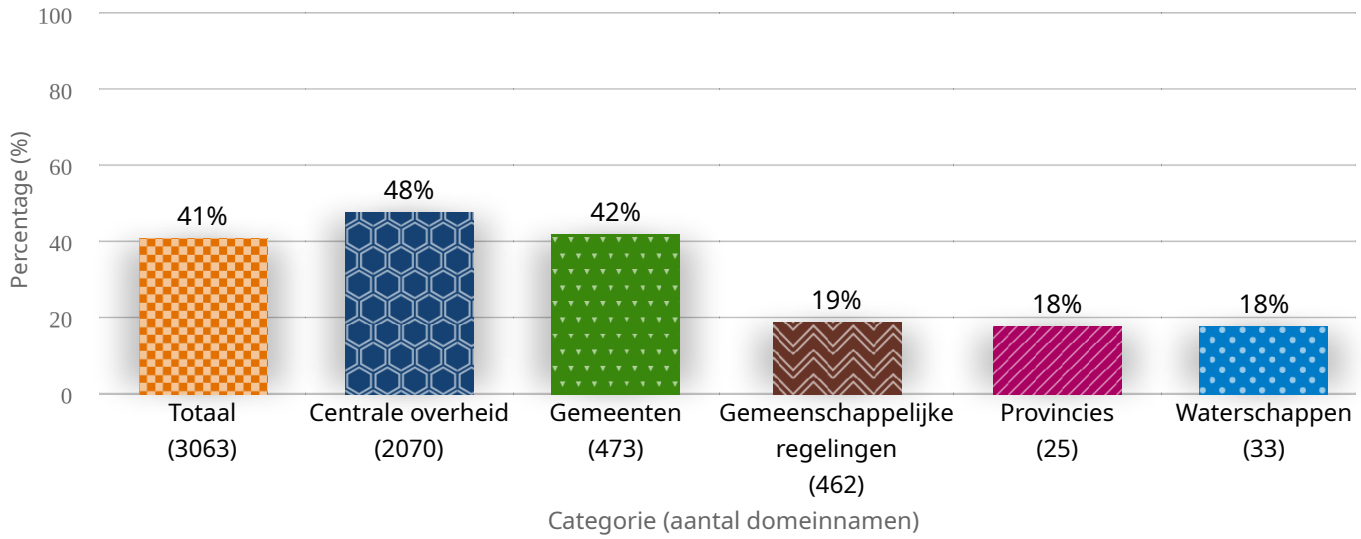
Omdat de test zich beperkt tot een controle of de e-mailontvangst van de betreffende overheden voldoende veilig e-mailverkeer mogelijk maakt, zijn alleen de internetdomeinen met een ontvangende mailserver (MX) meegenomen in de statistieken. Hierdoor is het aantal gecontroleerde domeinen significant lager 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 (48%) en gemeenten (42%) 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.

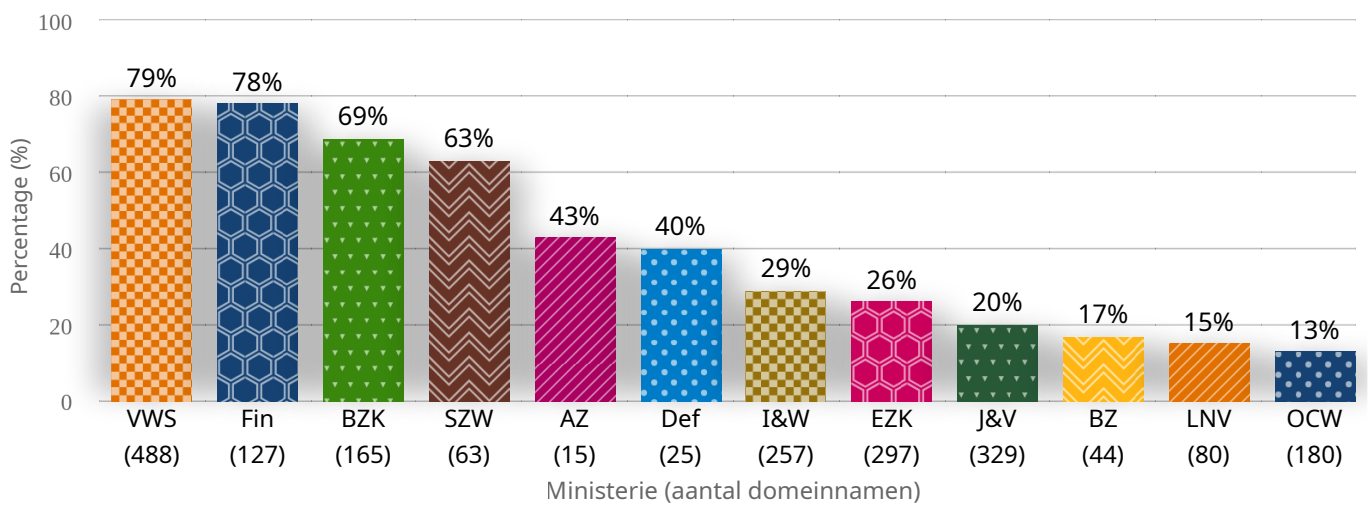
Grafiek 7: Volledige adoptie 'veilige e-mailtransport' standaarden per overheidscategorie



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, Financiën, Binnenlandse Zaken en Koninkrijksrelaties en Sociale Zaken en Werkgelegenheid. Het ministerie van Onderwijs, Cultuur en Wetenschap is een negatieve opvaller met slechts 13% volledige adoptie van standaarden voor veilig e-mailtransport.

Grafiek 8: Volledige adoptie 'veilige e-mailtransport' standaarden per ministerie



Voor meer details per ministerie zie hoofdstuk 7.

1.4. Vergelijking vorige meting

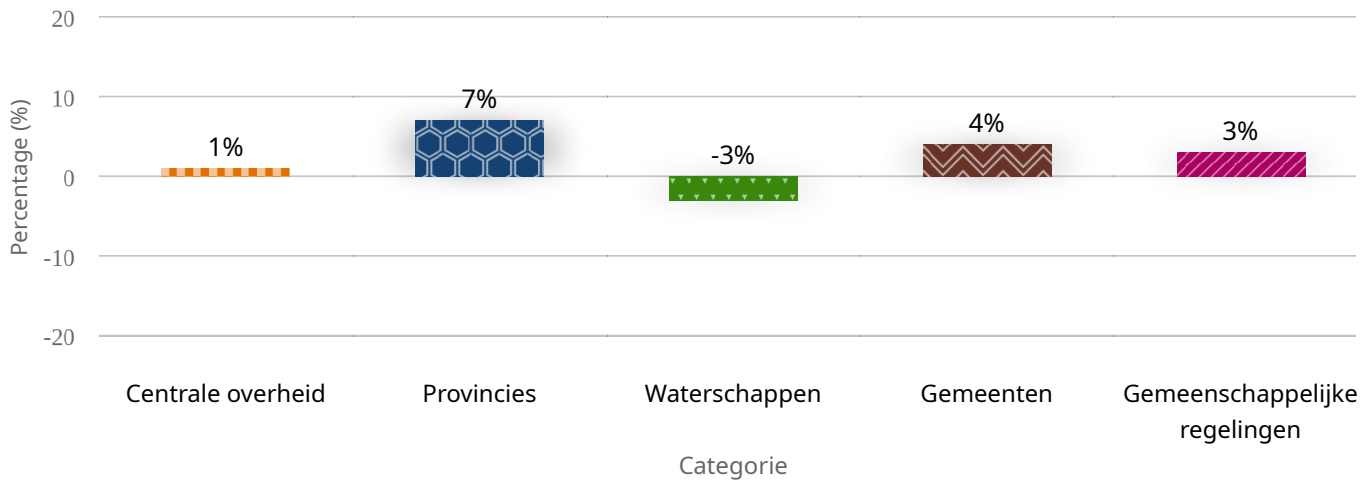
In de vorige meting van juli 2023 werd gewerkt met een kleinere set aan domeinnamen. Het gevolg hiervan was dat de meetresultaten niet goed te vergelijken zijn met deze metingen. Hierom is hier apart gekeken naar enkel de domeinnamen die in beide metingen voorkomen, wat een vergelijking met voorgaande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

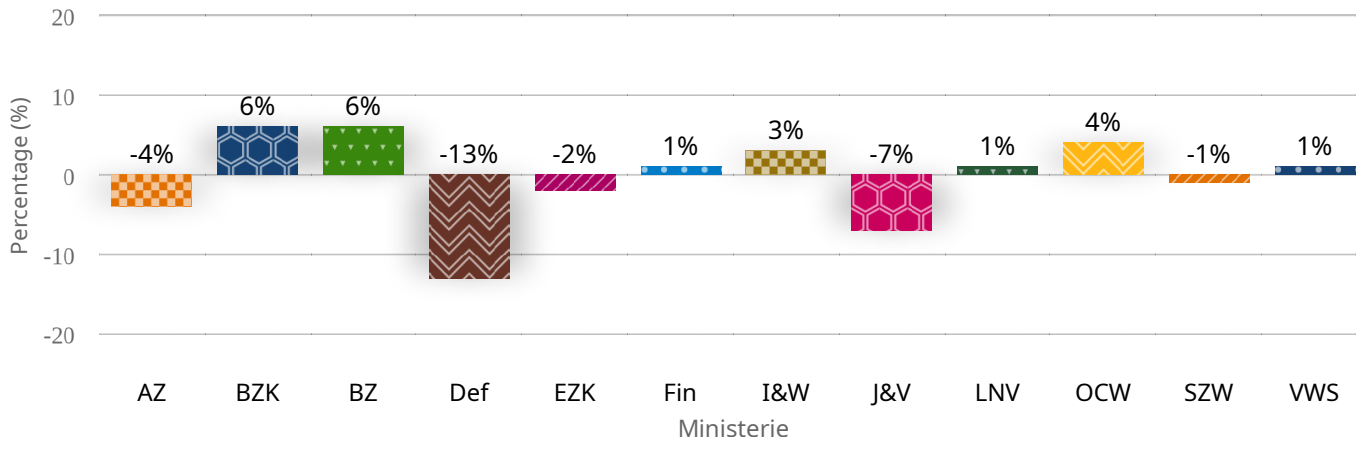
Kijkende naar de veranderingen in adoptie van webbeveiligingsstandaarden per overheidslaag (excl. IPv6 en excl. RPKI), zien we over de gehele breedte van de domeinnamenset een lichte stijging in het aantal domeinen dat aan alle afspraken voldoet. Helaas is er tegelijkertijd een lichte afname te zien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

Grafiek 9: Verschil webbeveiligingsstandaarden t.o.v. de juli 2023 meting per overheidscategorie



De ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Onderwijs, Cultuur en Wetenschap en Infrastructuur en Waterstaat laten een verbetering zien. Het ministerie van Defensie gaat voornamelijk achteruit vanwege een terugval op DNSSEC, ministerie van Justitie en Veiligheid valt terug vanwege verslechterde TLS configuraties.

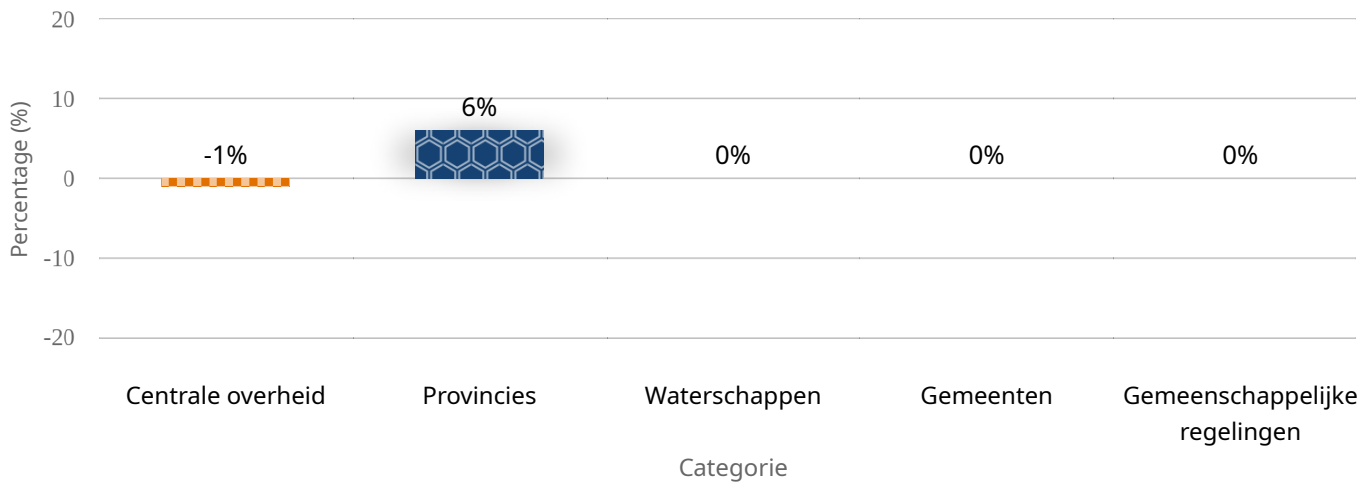
Grafiek 10: Verschil e-mailbeveiligingsstandaarden t.o.v. de juli 2023 meting per ministerie



1.4.2. Vergelijking e-mailstandaarden

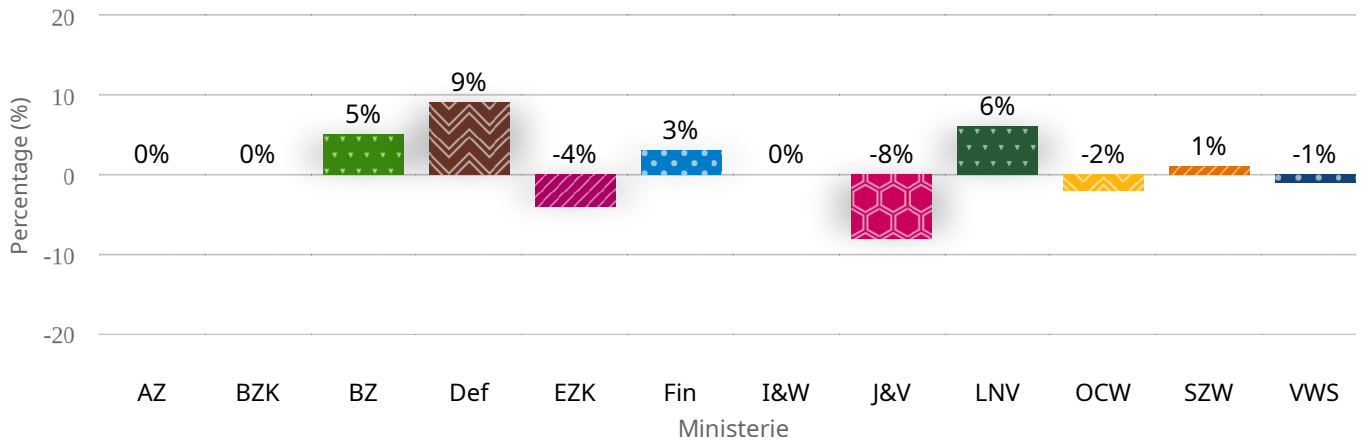
Bij de e-mailbeveiligingsstandaarden is er buiten de provincies geen verbetering te zien ten opzichte van juli 2023.

Grafiek 11: Verschil e-mailbeveiligingsstandaarden t.o.v. de juli 2023 meting per overheidscategorie



Verder kijkende naar de veranderingen per ministerie, dan stijgt wederom het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Het ministerie van Defensie stijgt, al bestaat deze stijging uit een grote verbetering van STARTTLS, maar tegelijkertijd een achteruitgang op DNSSEC.

Grafiek 12: Verschil webbeveiligingsstandaarden t.o.v. de juli 2023 meting per ministerie



1.4.3. Conclusie

De vergelijking laat zien dat er sinds de vorige meting verbeteringen zijn doorgevoerd in de adoptie van de webstandaarden. De adoptie bij e-mailbeveiligingsstandaarden is echter licht achteruit gegaan. Bij de kleine domeinnaamportfolio van de provincies is een significante stijging waar te nemen, zowel bij de web- als e-mailbeveiligingsstandaarden.

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.

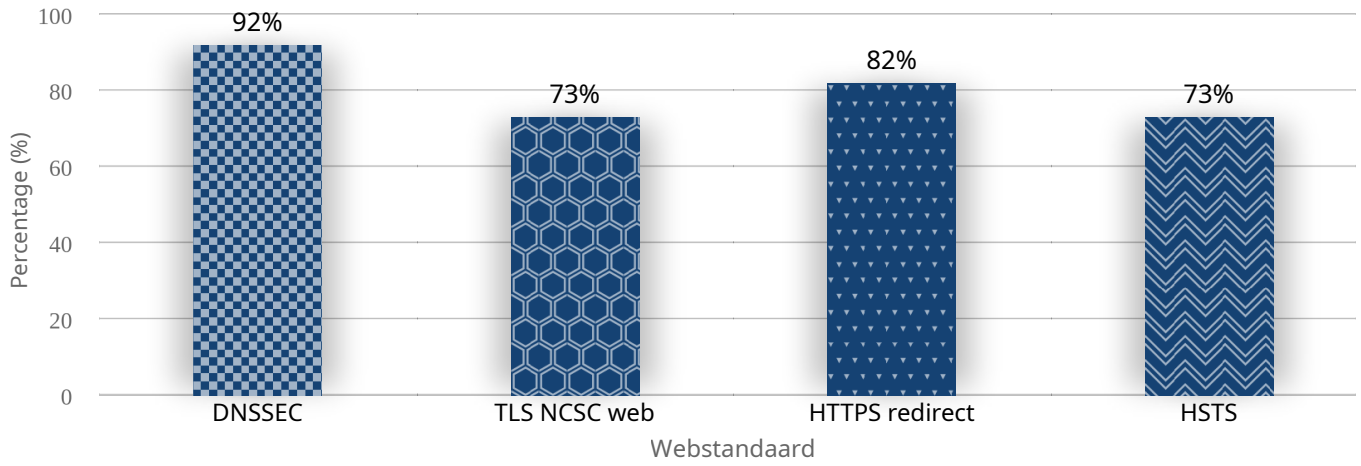
2. Adoptie per websitebeveiligingsstandaard

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.

Grafiek 13: Adoptie per webbeveiligingsstandaard alle overheden (n=10959)



3. Adoptie per e-mailbeveiligingsstandaard

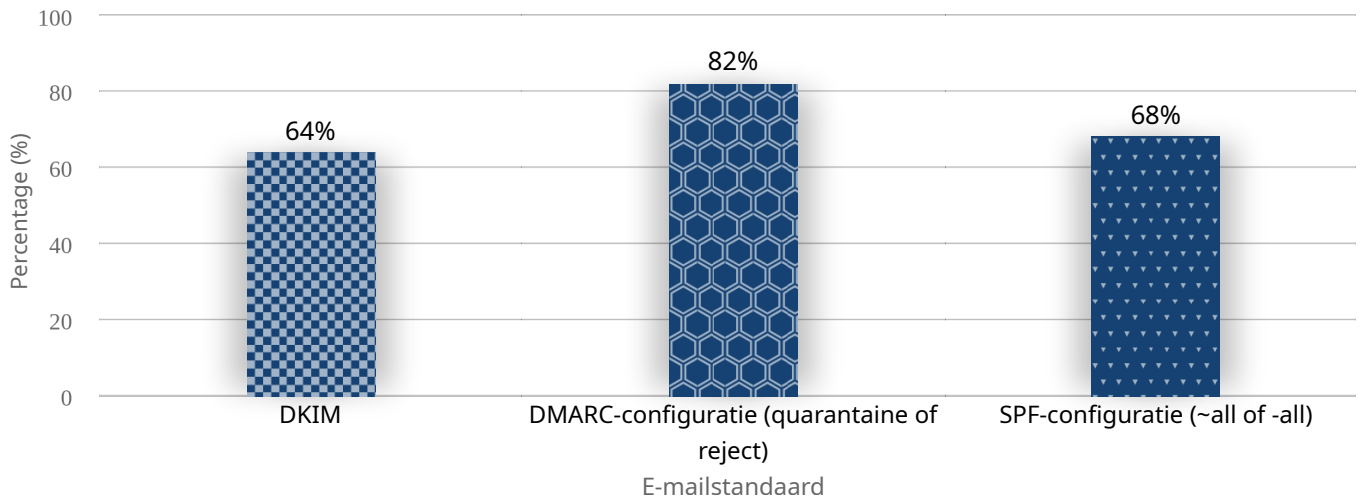
Dit hoofdstuk toont de algehele adoptiegraad per e-mailbeveiligingsstandaard.

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 18% van de internetdomeinen nog een strikt DMARC-beleid worden ingesteld en 32% 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 streefbeeld was om dit eind 2019 voor elkaar te hebben.

Grafiek 14: Adoptie per 'anti-phishing' standaard alle overheden (n=11960)



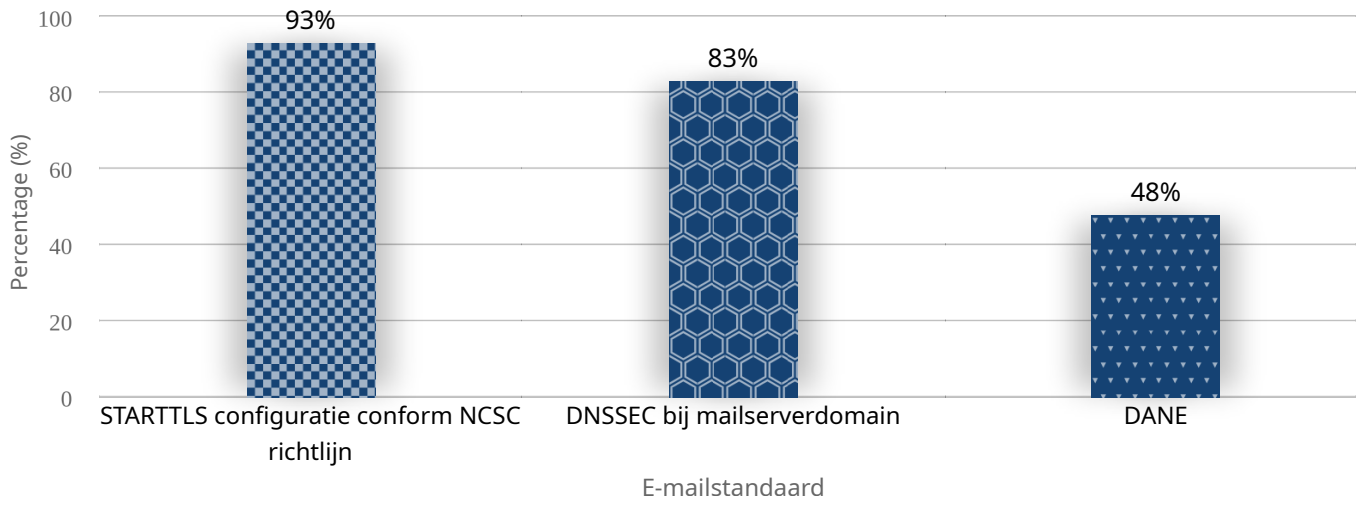
3.2. E-mailstandaarden voor vertrouwelijk e-mailverkeer

Bij nog 7% 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 48%. 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.

Grafiek 15: Adoptie per 'veilige e-mailtransport' standaard alle overheden (n=3063)



4. Adoptie IPv6 voor websites en e-mail

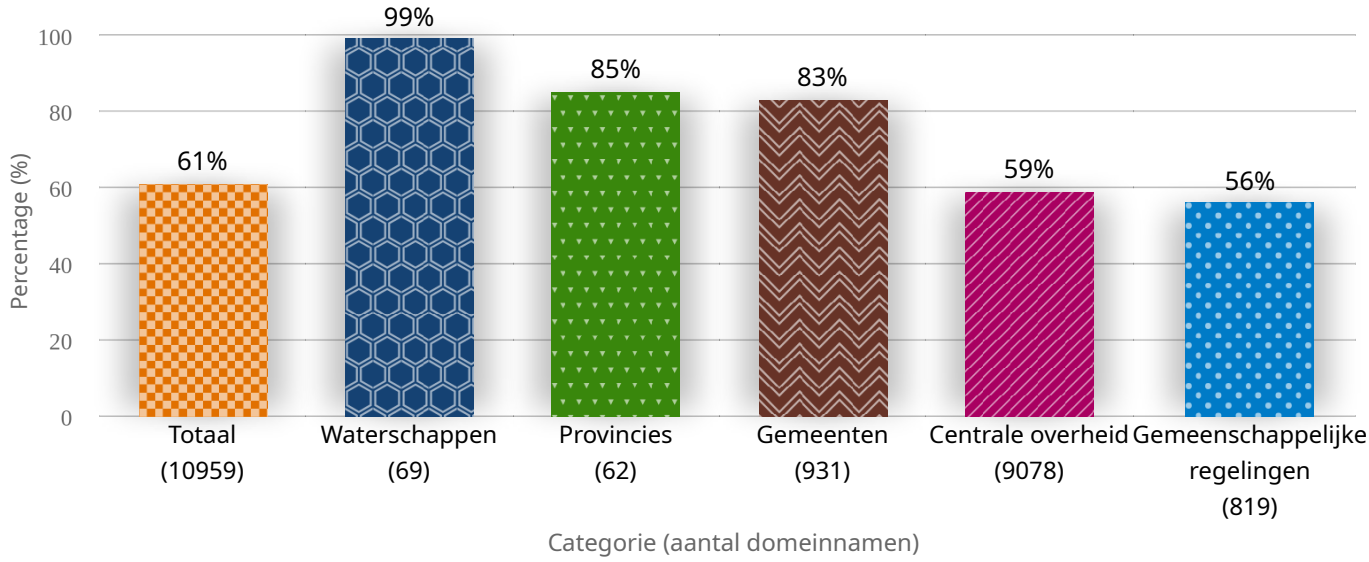
IPv6 is de open internetstandaard die iedere internetgebruiker nodig heeft om ook in de toekomst onbelemmerd gebruik te kunnen maken van internet. Er zijn verschillende goede redenen om voor IPv6 te kiezen, juist ook als overheid: groei en innovatie van internet, directere en snellere dienstverlening,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

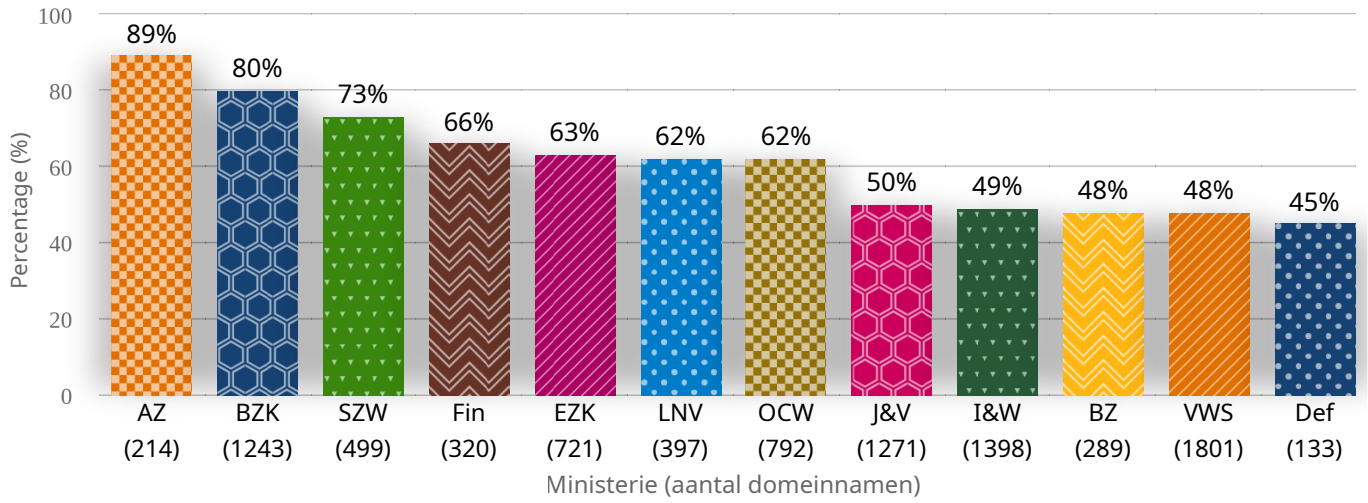
Grafiek 16: Volledige IPv6 adoptie voor webverkeer per overheidscategorie



4.2. IPv6 voor webverkeer per ministerie

De toevoeging van het Register Internetdomeinen Overheid heeft voor ministeries waar veel domeinnamen (redirects en een groot aantal misconfiguraties) geleidt tot een achteruitgang van IPv6 voor enkele ministeries zoals Volksgezondheid, Welzijn en Sport. Positieve uitschieters zijn de ministeries van Algemene Zaken (89%), Binnenlandse Zaken en Koninkrijksrelaties (80%) en Sociale Zaken en Werkgelegenheid (73%). Negatieve opvaller is het ministerie van Defensie (45%), waarvan de websites het minst bereikbaar zijn via IPv6.

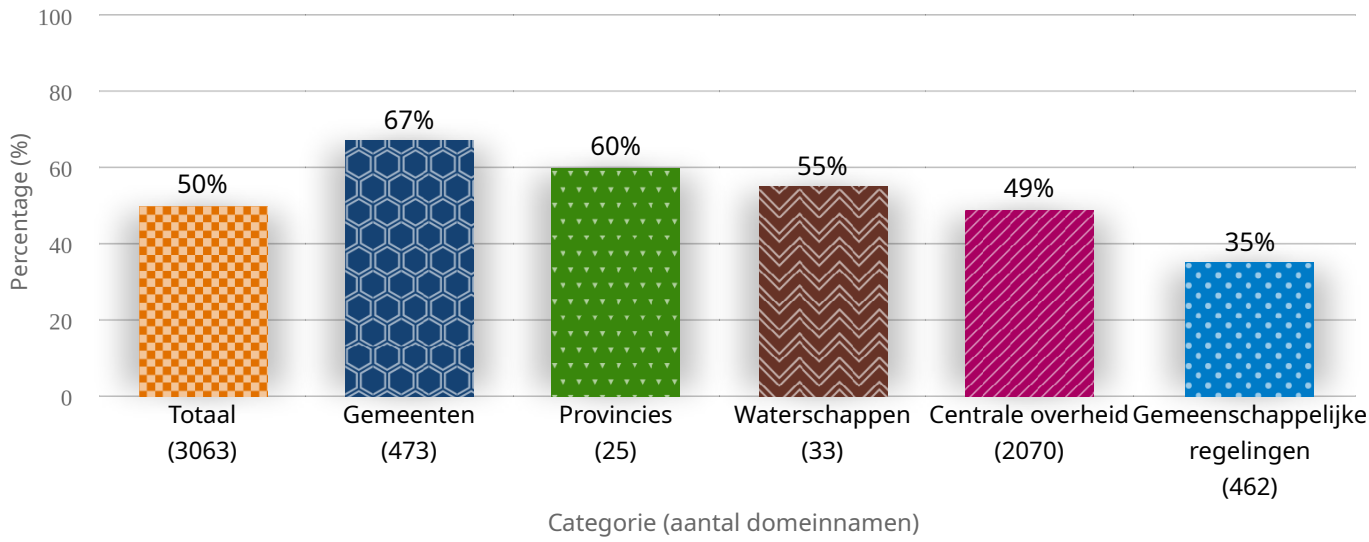
Grafiek 17: Volledige IPv6 adoptie voor webverkeer per ministerie



4.3. IPv6 voor e-mailverkeer per overheidscategorie

Ook bij het gebruik van IPv6 voor e-mailverkeer zijn de gemeenschappelijke regelingen de hekkensluiter.

Grafiek 18: Volledige IPv6 adoptie voor e-mailverkeer per overheidscategorie

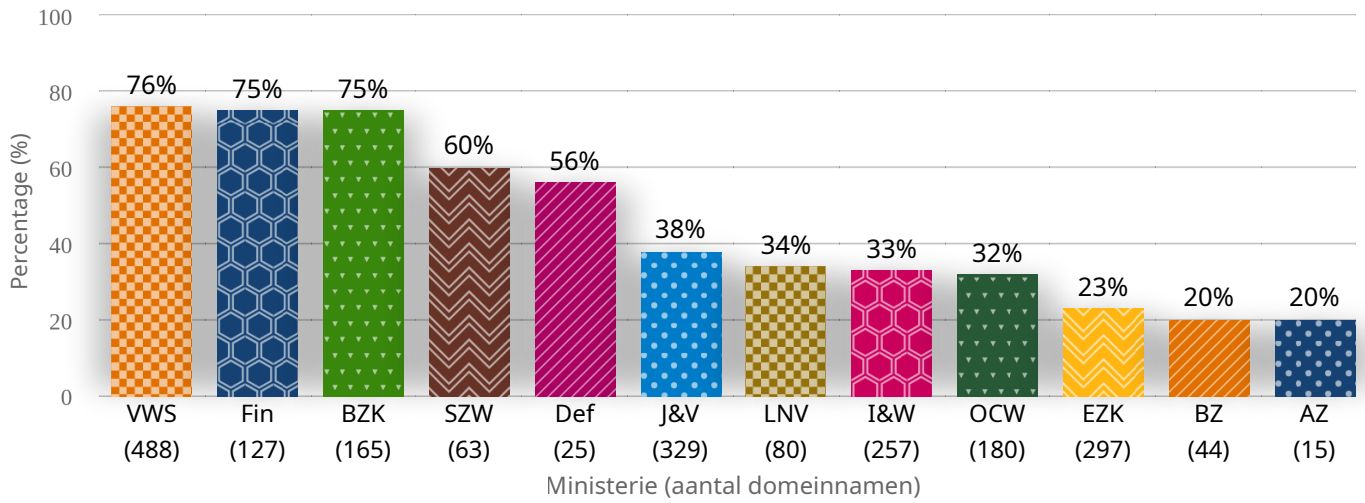


4.4. IPv6 voor e-mailverkeer per ministerie

De ministeries van Algemene Zaken (20%) en Buitenlandse Zaken (20%) hebben ondanks een klein portfolio van domeinnamen waarop e-mailverkeer mogelijk is een erg lage adoptiegraad.

De hoogste sores zijn voor de ministeries van Volksgezondheid, Welzijn en Sport (76%), Financiën (75%) en Binnenlandse Zaken en Koninkrijksrelaties (75%) .

Grafiek 19: Volledige IPv6 adoptie voor e-mailverkeer per ministerie



5. Adoptie RPKI voor websites en e-mail

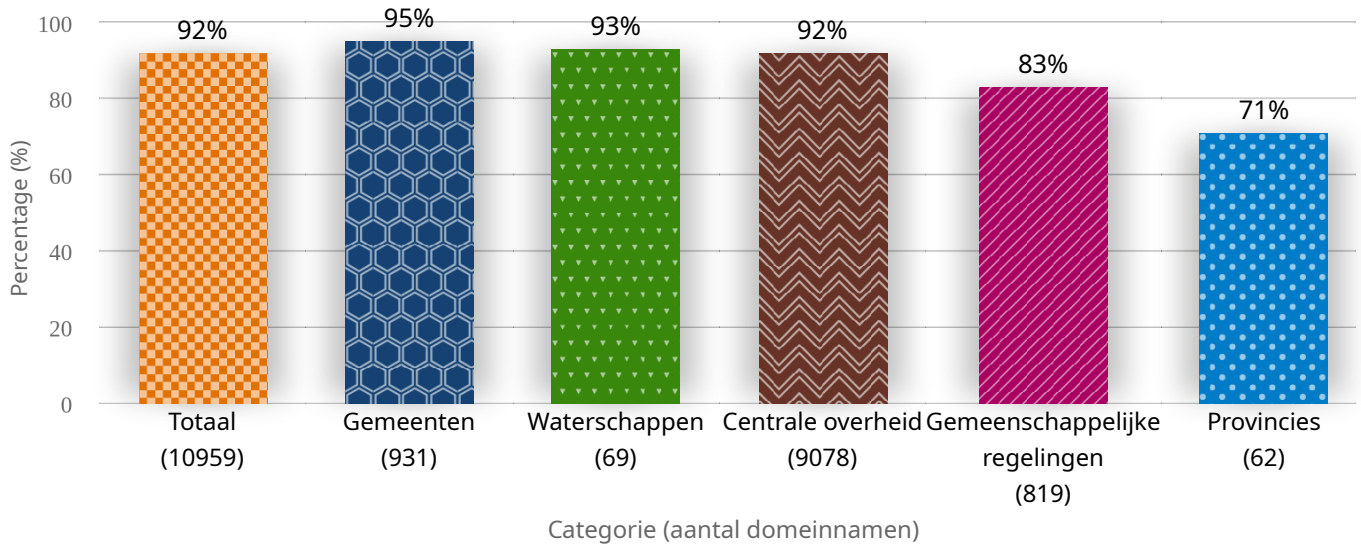
Resource Public Key Infrastructure (RPKI) is een standaard met als doel om zogenaamde route hijacks te voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet geautoriseerd netwerk. Een hijack kan het gevolg zijn van een simpele typefout van een netwerkbeheerder die 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

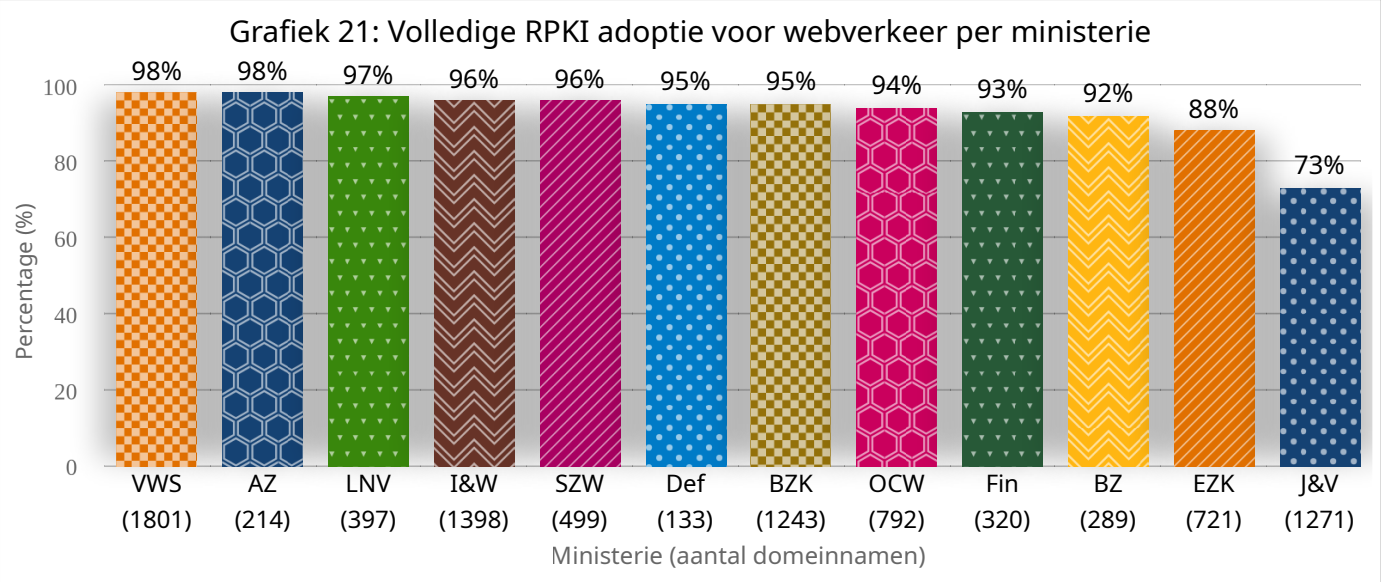
De gemeenten, waterschappen en centrale overheid gaan richting het behalen van de streefbeeldafspraak. De provincies en gemeenschappelijke regelingen hebben extra inzet nodig om de afspraak te behalen.

Grafiek 20: Volledige RPKI adoptie voor webverkeer per overheidscategorie



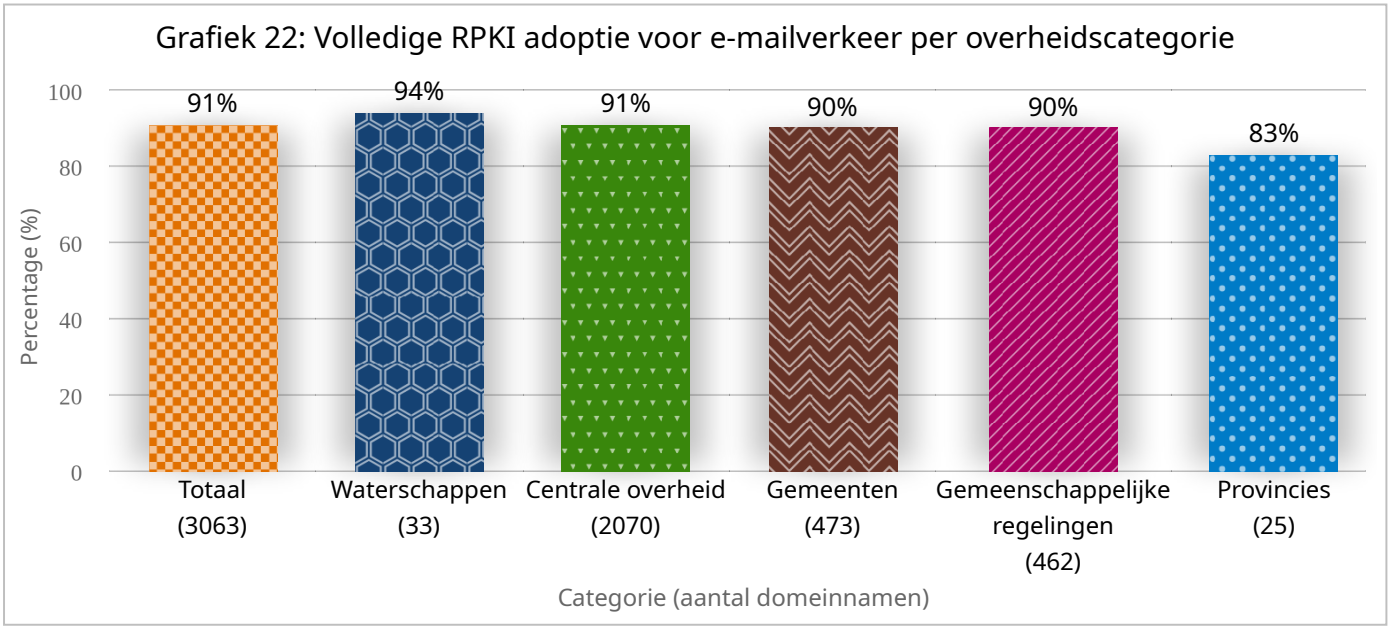
5.2. RPKI voor webverkeer per ministerie

Een aantal ministeries naderen de voltooing van de afspraak om voor het einde van 2024 op de IP-adressen RPKI te gebruiken in het webverkeer. De twee achterblijvers zijn de ministeries van Justitie en Veiligheid (73%) en Economische Zaken en Klimaat (88%). Bij het ministerie van Justitie en Veiligheid betreft het een paar niet ondertekende routes die zorgen voor een lagere score dan de overige ministeries.



5.3. RPKI voor e-mailverkeer per overheidscategorie

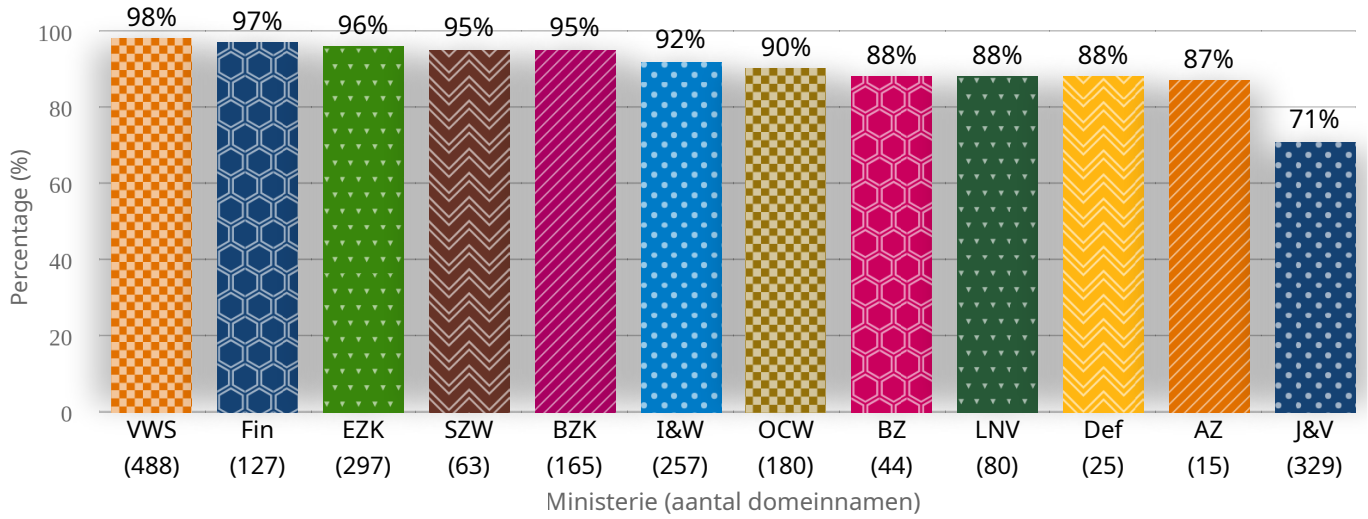
Het gebruik van RPKI voor e-mailverkeer is voor alle overheidscategorieën al op behoorlijk niveau. De verschillen in adoptie tussen de overheidscategorieën zijn klein, al blijven ook hier de provincies licht achter.



5.4. RPKI voor e-mailverkeer per ministerie

De ministeries hebben bijna allemaal een zeer hoge adoptie van gemiddeld 91%. De significante achterblijver is wederom Justitie en Veiligheid (71%) waar een paar niet ondertekende routes zorgt voor een lagere score dan de overige ministeries.

Grafiek 23: Volledige RPKI adoptie voor e-mailverkeer per ministerie

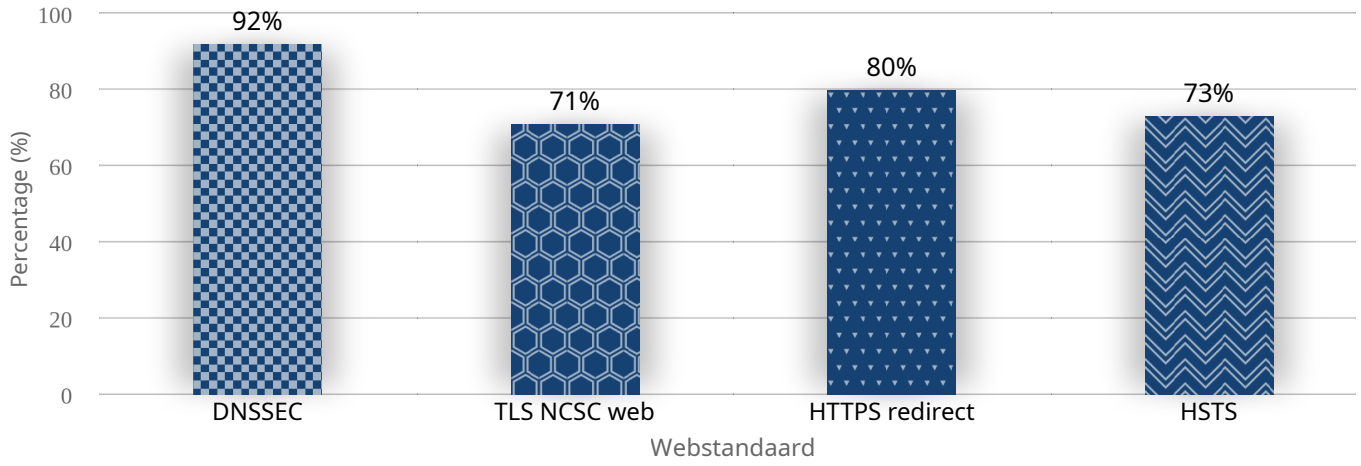


6. Adoptie per overheidscategorie

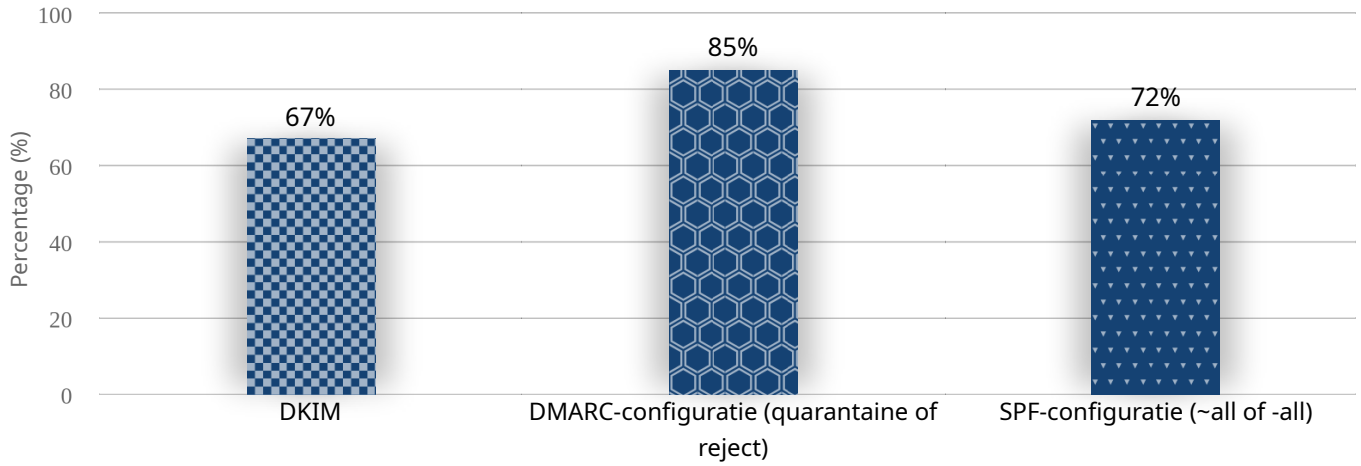
De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per overheidscategorie.

6.1. Centrale overheid

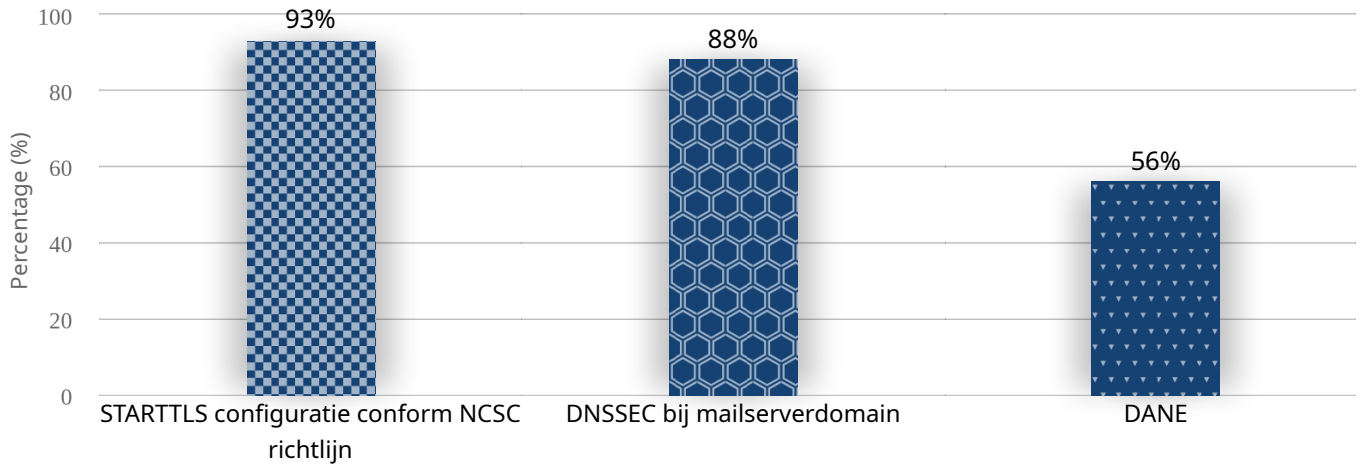
Grafiek 24: Adoptie per webbeveiligingsstandaard centrale overheid (n=9078)



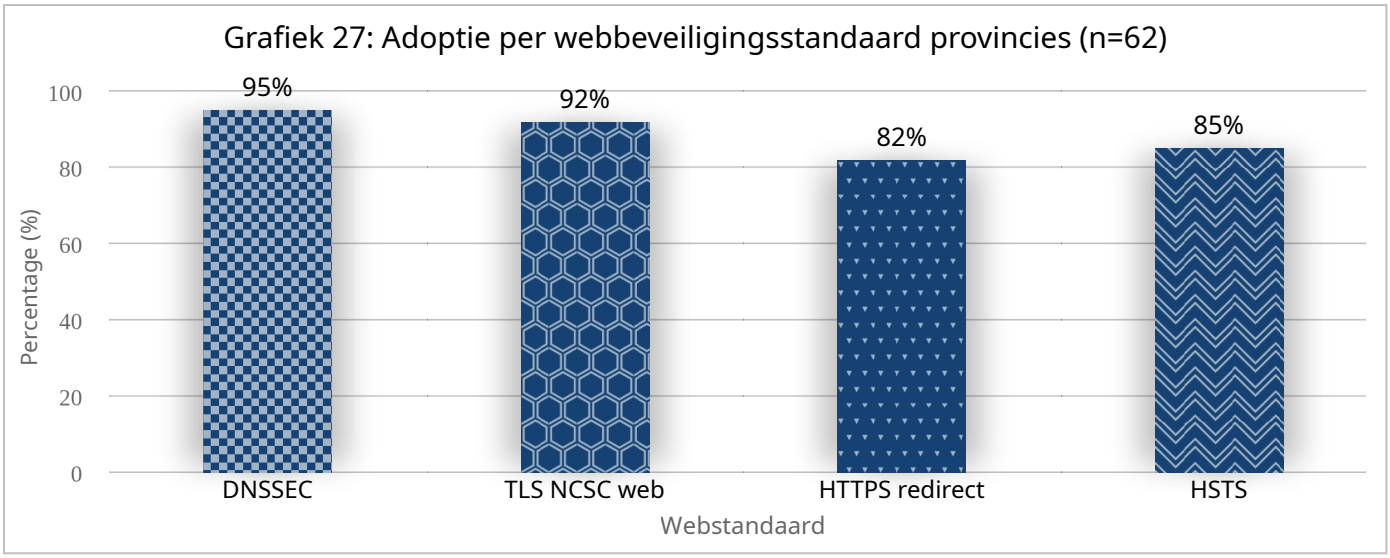
Grafiek 25: Adoptie per 'anti-phishing' standaard centrale overheid (n=9996)

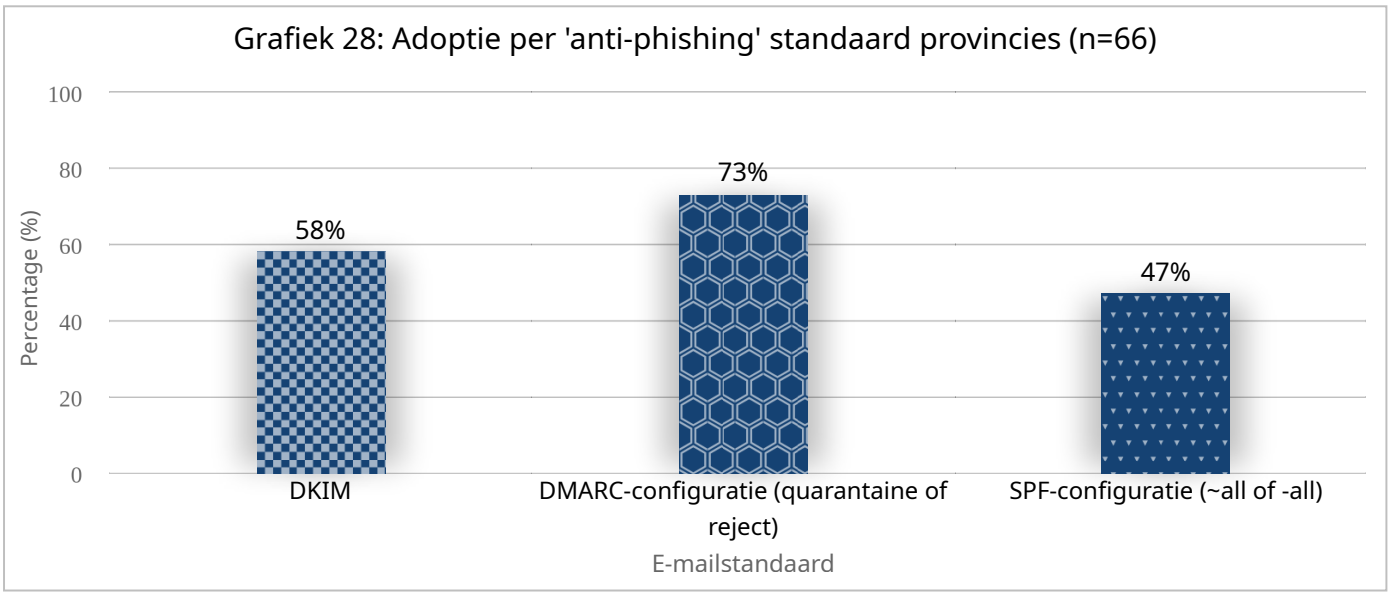


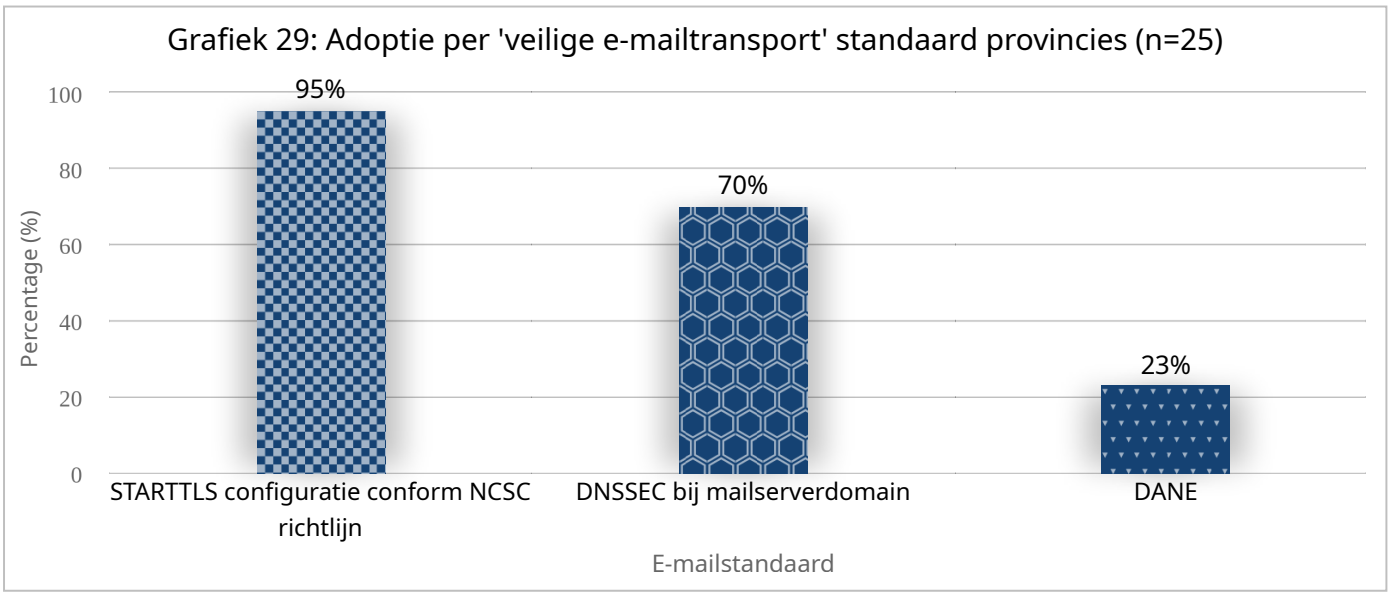
Grafiek 26: Adoptie per 'veilige e-mailtransport' standaard centrale overheid (n=2070)



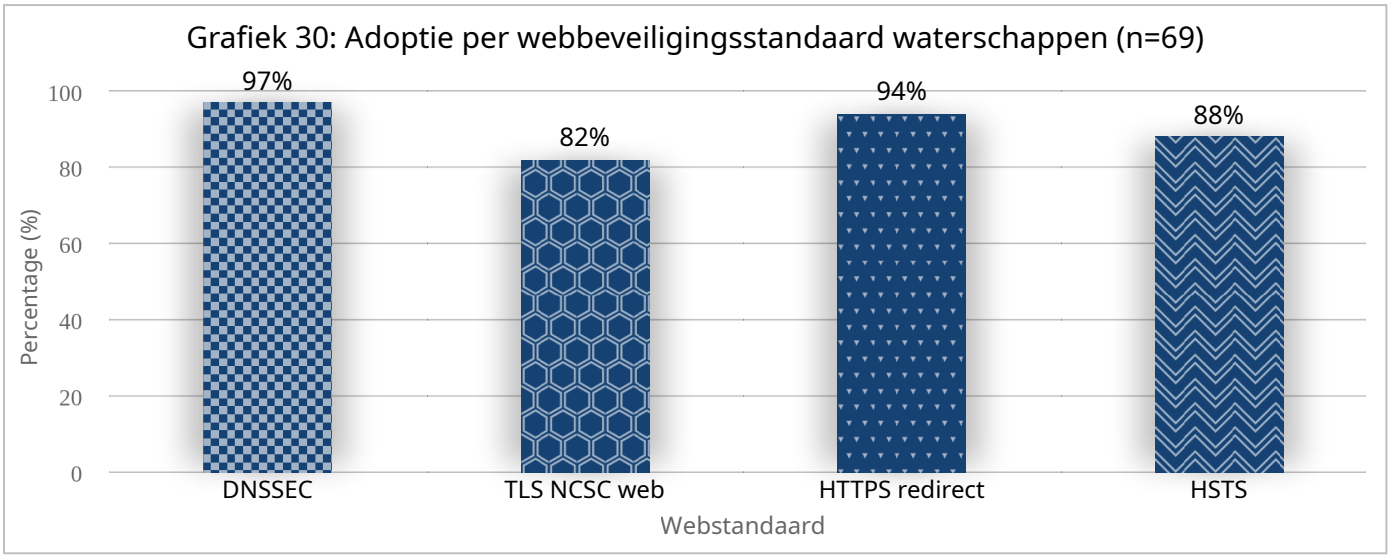
6.2. Provincies

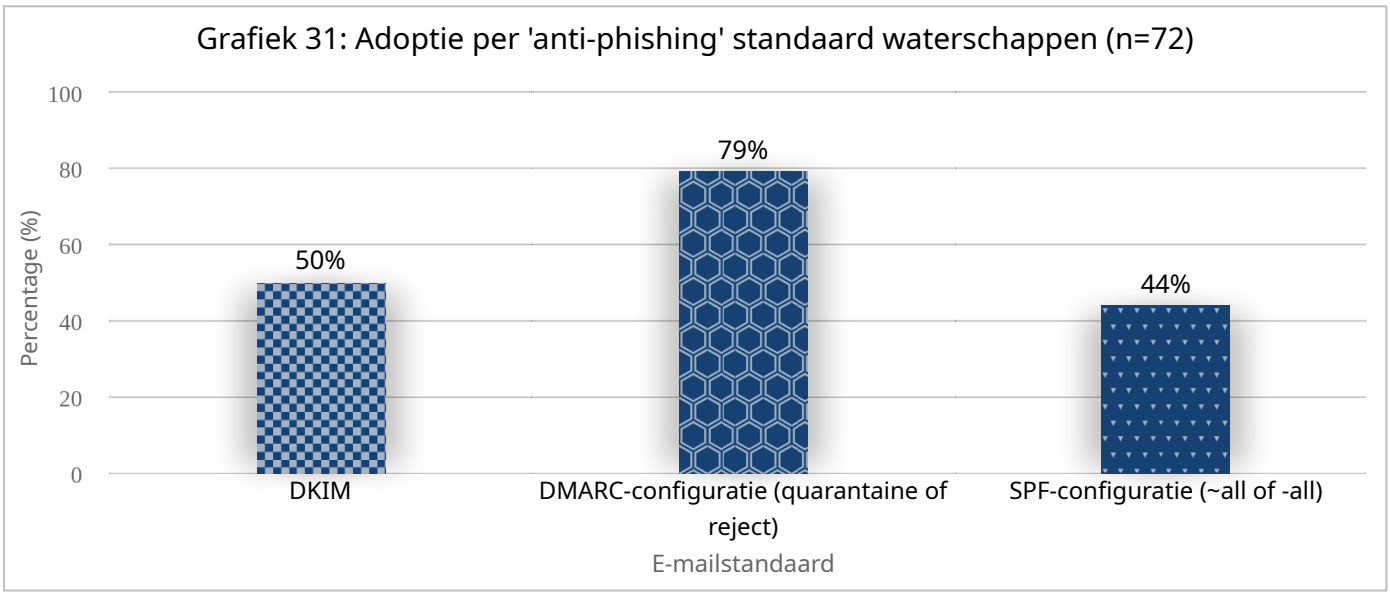


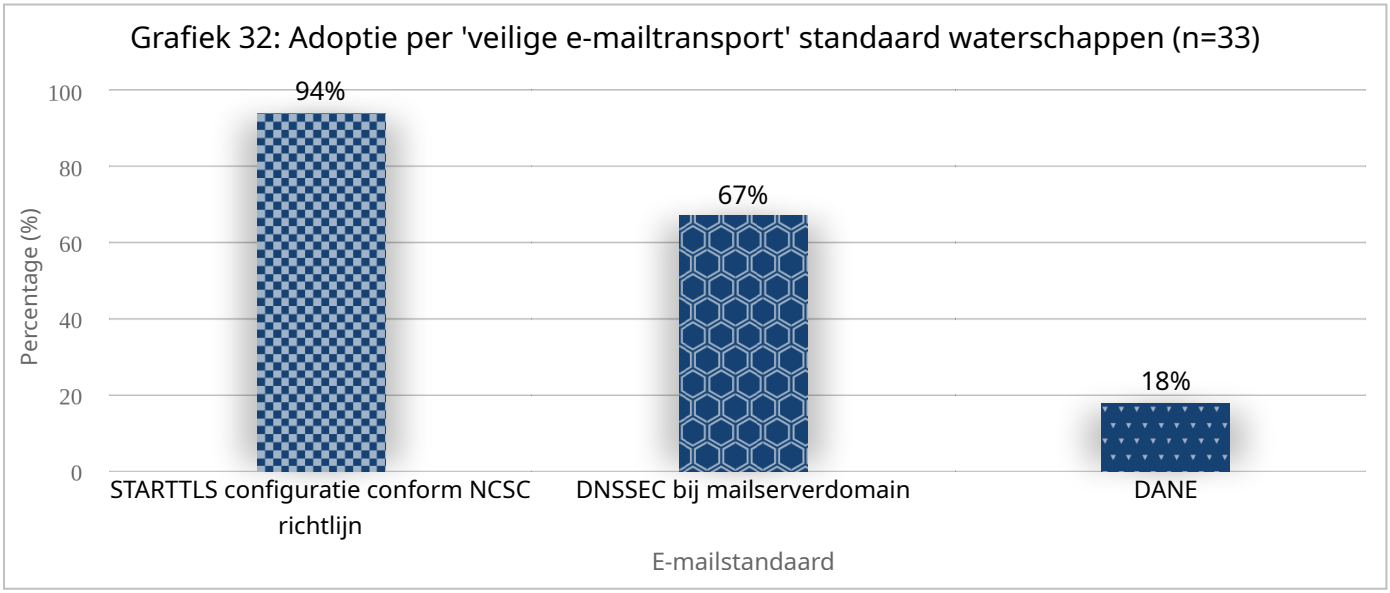




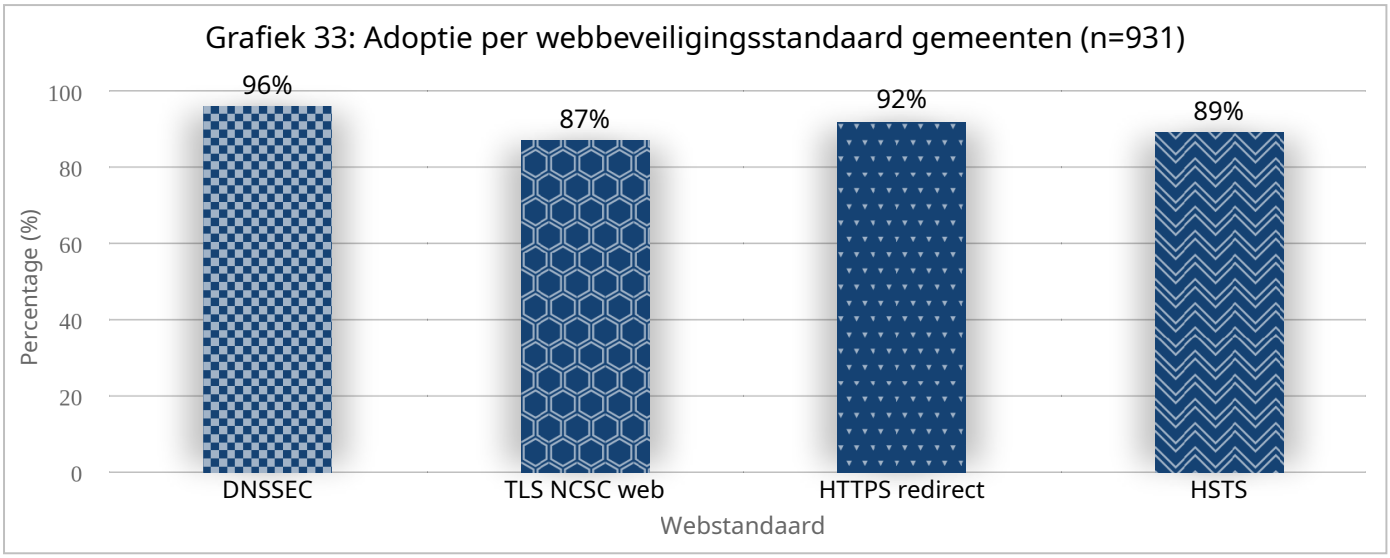
6.3. Waterschappen

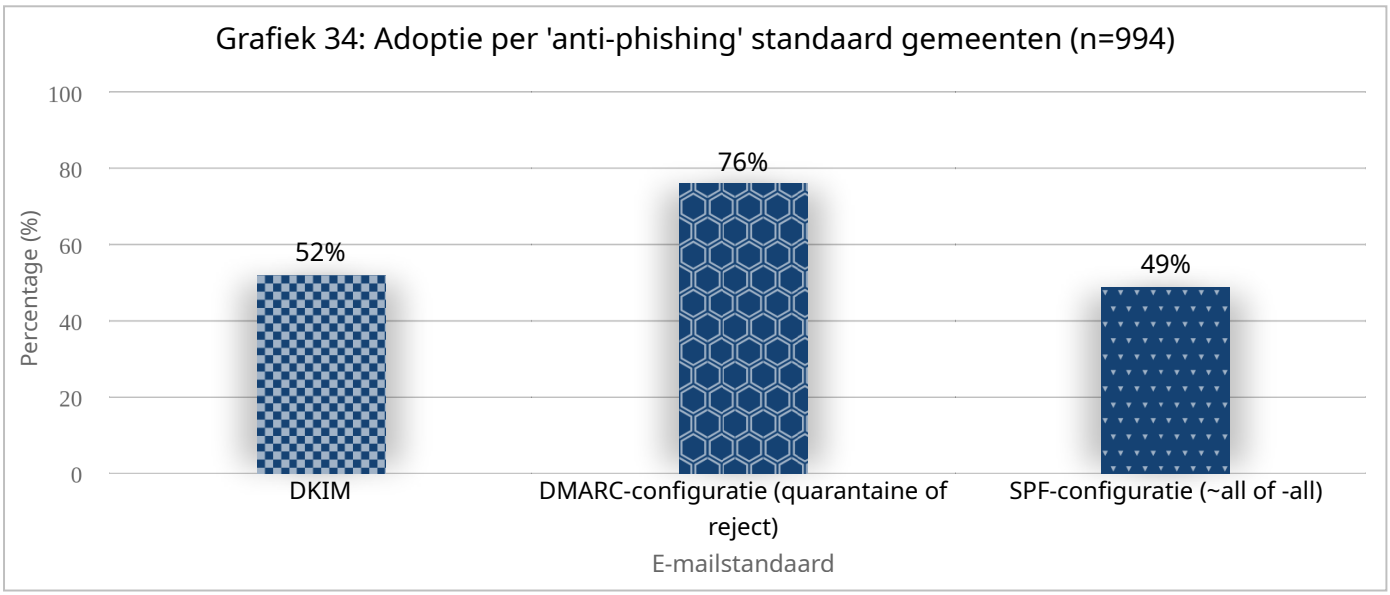


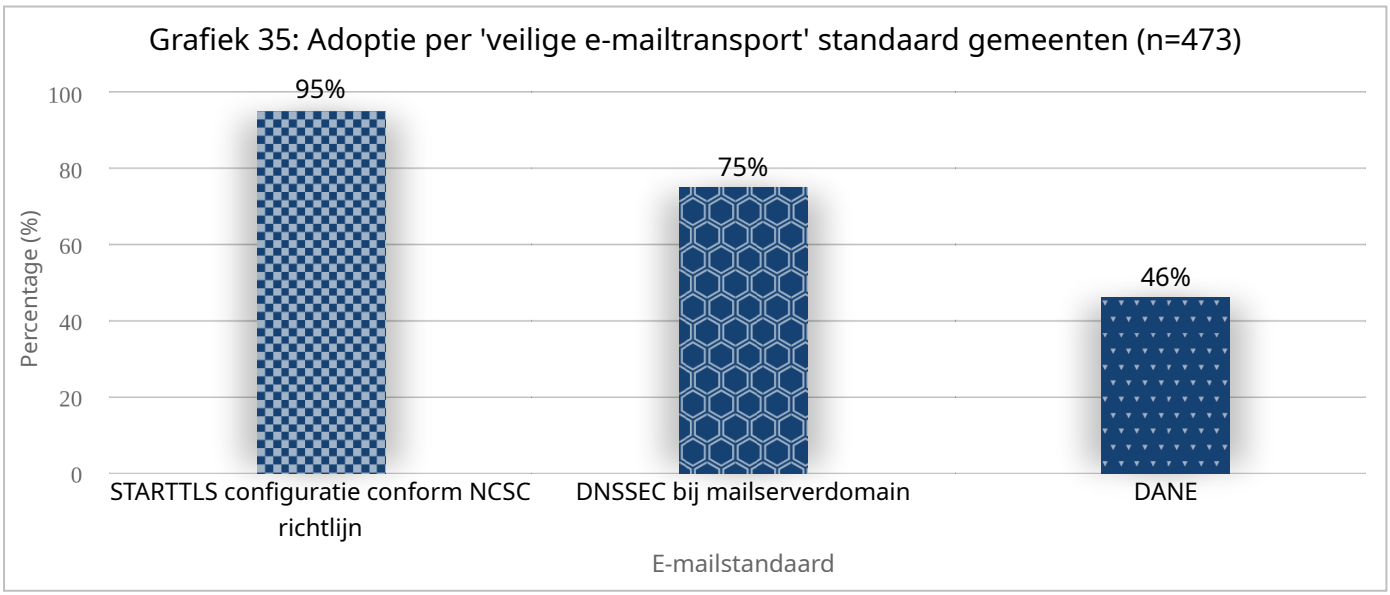




6.4. Gemeenten

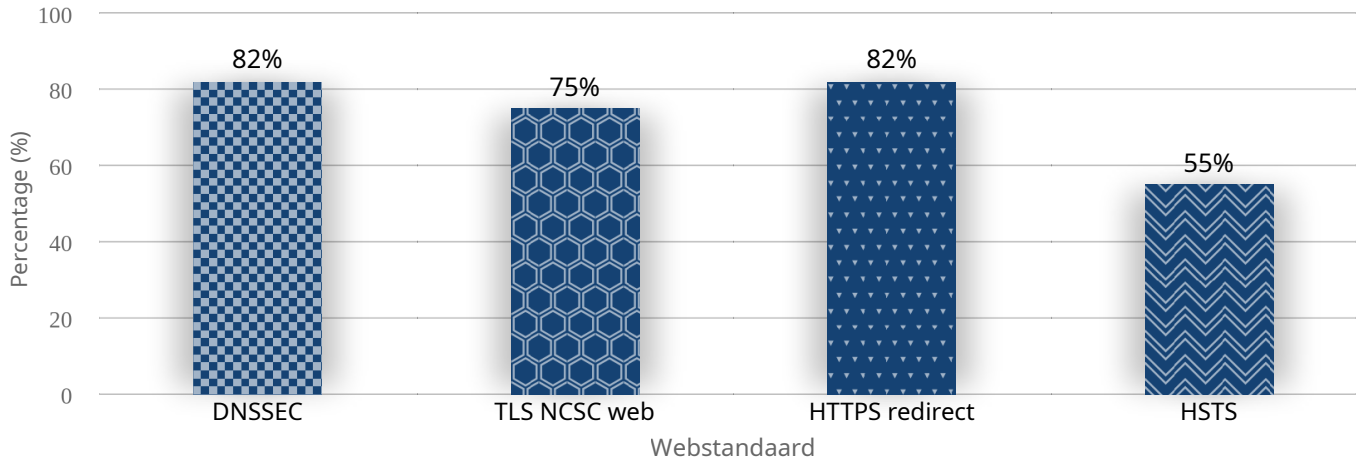




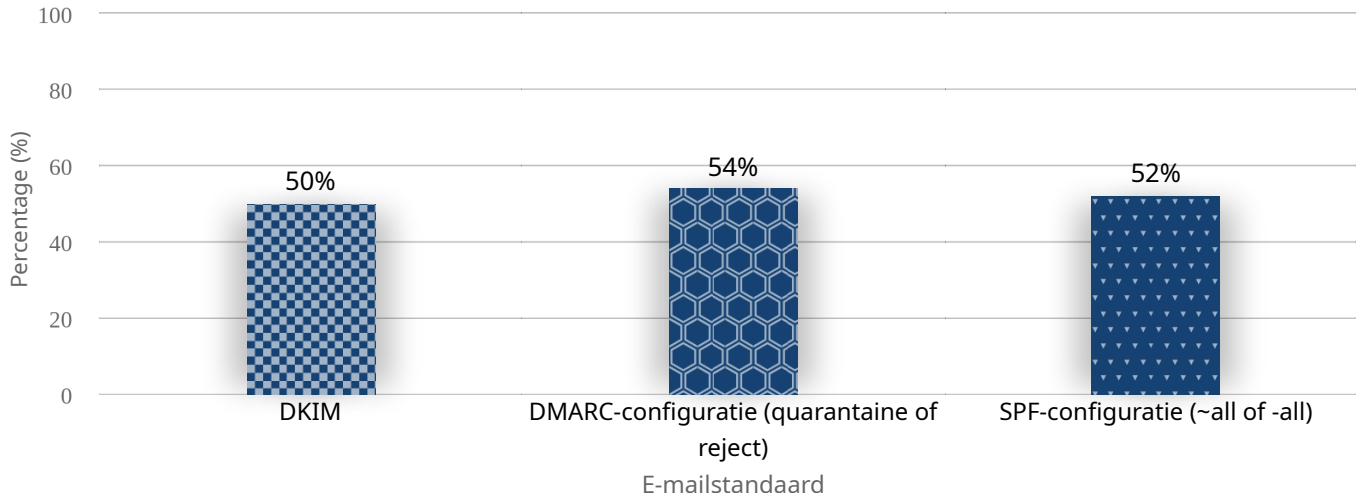


6.5. Gemeenschappelijke regelingen

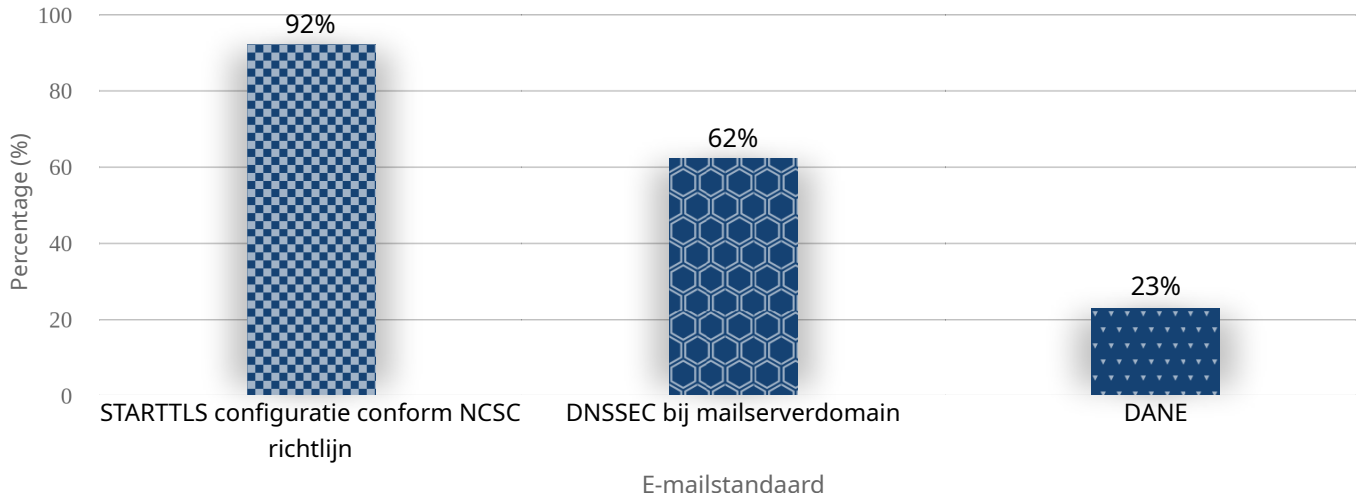
Grafiek 36: Adoptie per webbeveiligingsstandaard gemeenschappelijke regelingen (n=819)



Grafiek 37: Adoptie per 'anti-phishing' standaard gemeenschappelijke regelingen (n=832)



Grafiek 38: Adoptie per 'veilige e-mailtransport' standaard gemeenschappelijke regelingen (n=462)

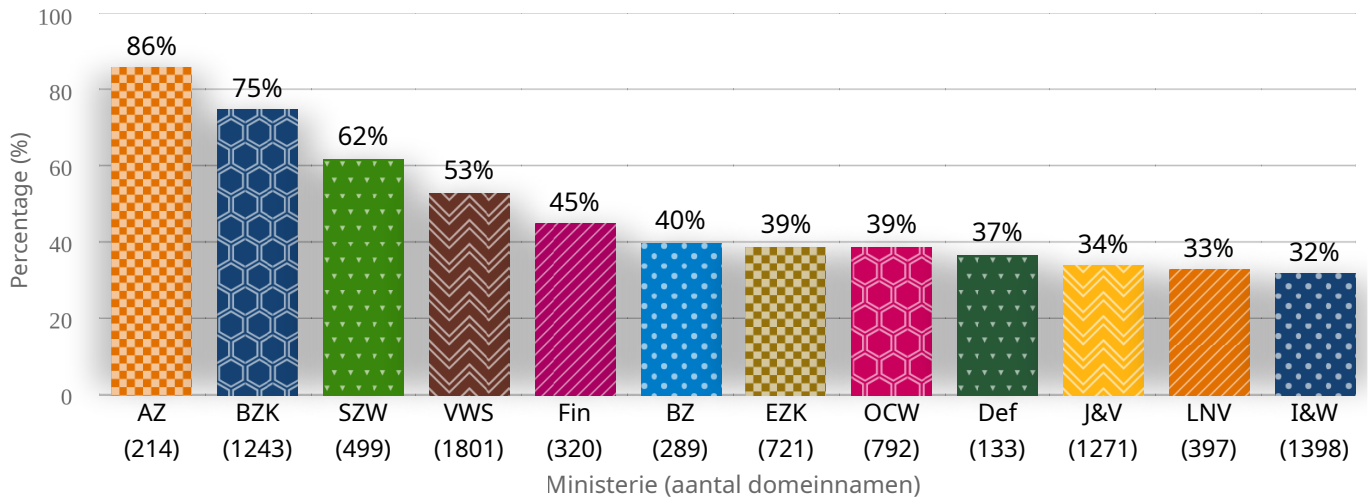


7. Adoptie per ministerie

7.1. Totaalbeeld websites (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).

Grafiek 39: Volledige adoptie van alle webstandaarden per ministerie

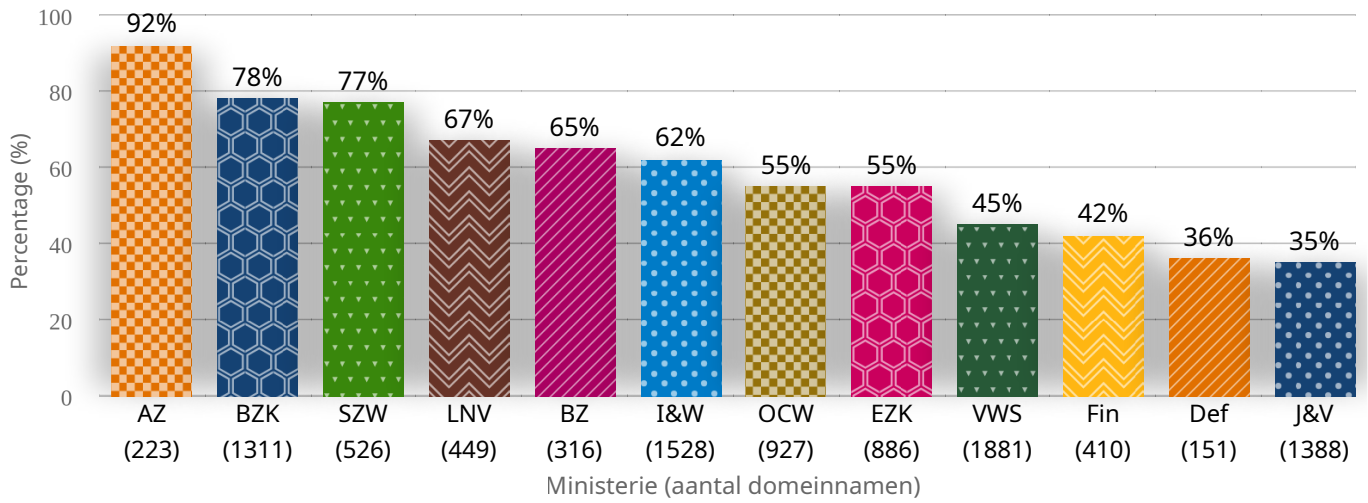


Over het algemeen hebben ministeries met een klein webportfolio, zoals het ministerie van Algemene Zaken, een hoge mate van adoptie. De ministeries van Binnenlandse Zaken en Koninkrijksrelaties en Sociale Zaken en Werkgelegenheid, zowel met een groot als relatief beperkt portfolio, scoren hoger dan gemiddeld.

7.2. Totaalbeeld e-mail (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).

Grafiek 40: Volledige adoptie van alle e-mailstandaarden per ministerie

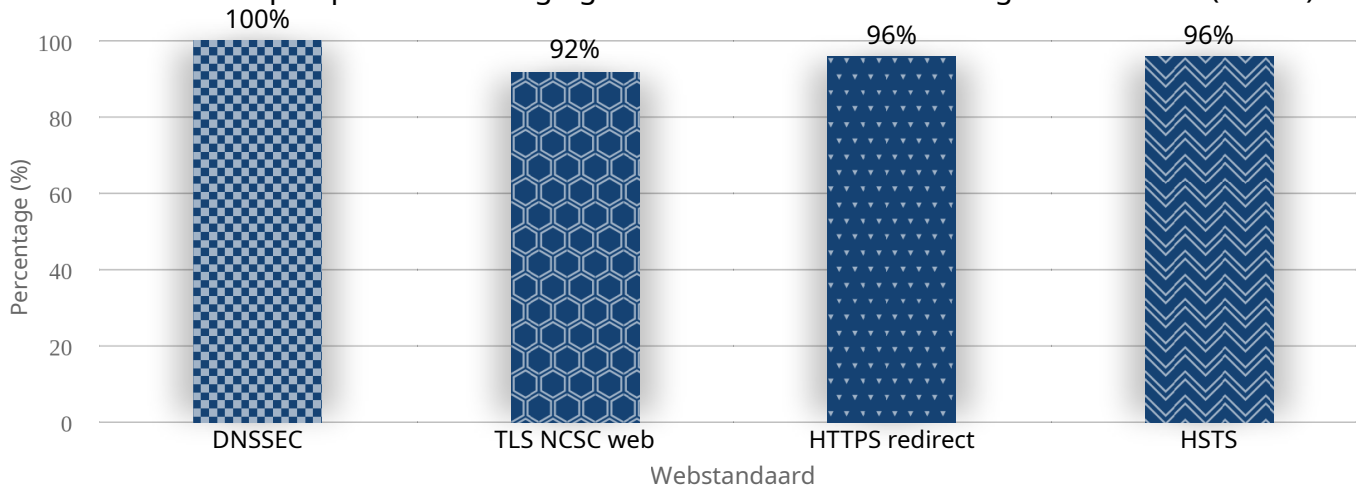


Vergelijkbaar met de adoptie van websitestandaarden, zien we dat ministeries met een beperkt portfolio, of actieve sturing op toepassing van standaarden, over het algemeen een hogere adoptiegraad bereiken.

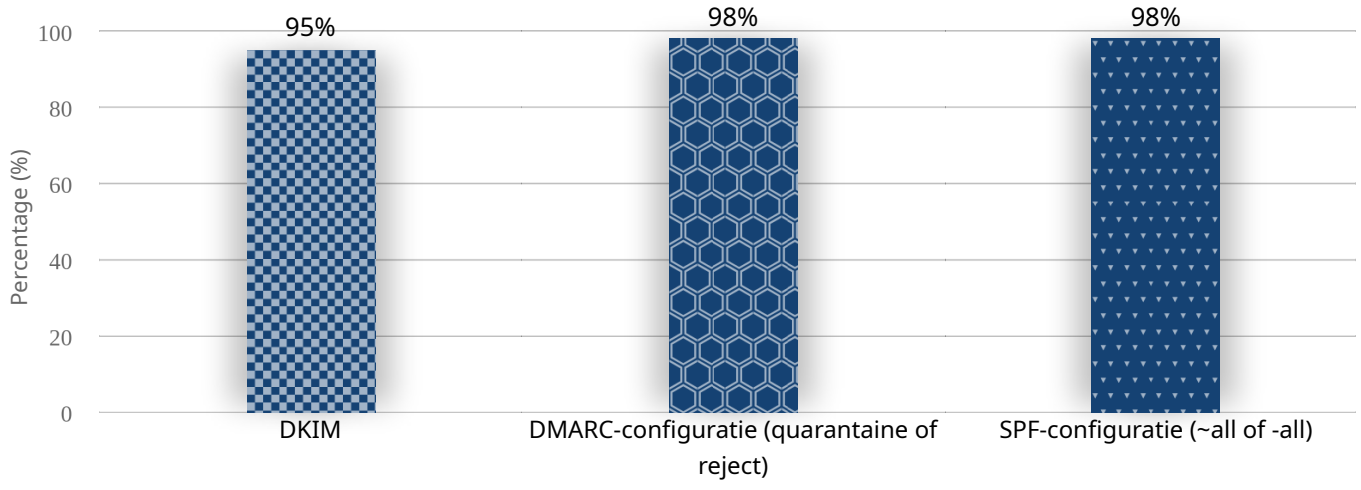
De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per ministerie.

7.3. Ministerie van Algemene Zaken

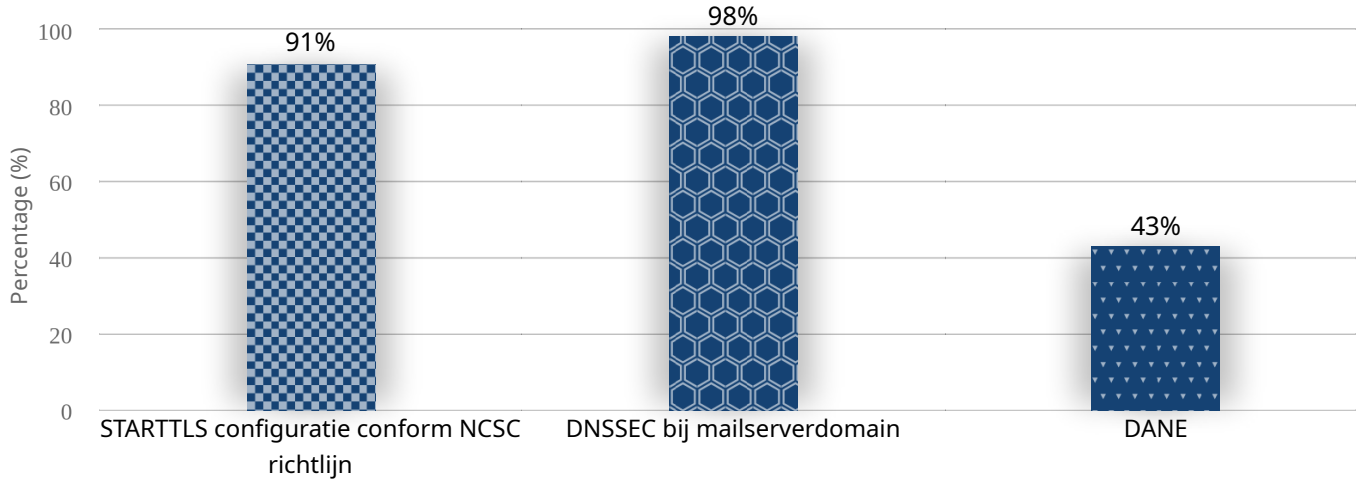
Grafiek 41: Adoptie per webbeveiligingsstandaard ministerie van Algemene Zaken (n=214)



Grafiek 42: Adoptie per 'anti-phishing' standaard ministerie van Algemene Zaken (n=223)

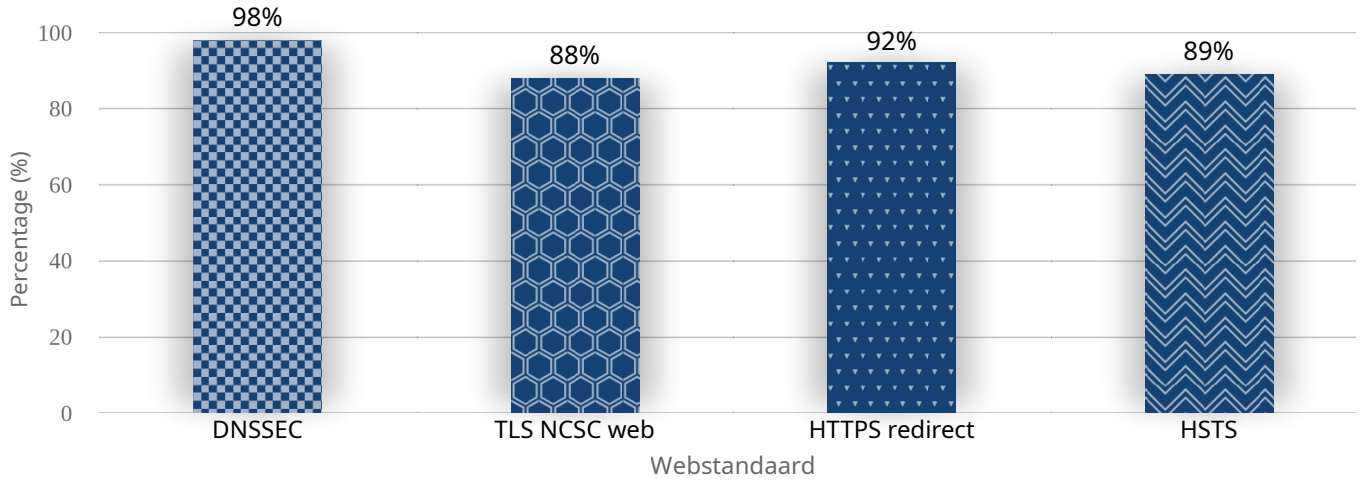


Grafiek 43: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Algemene Zaken (n=15)

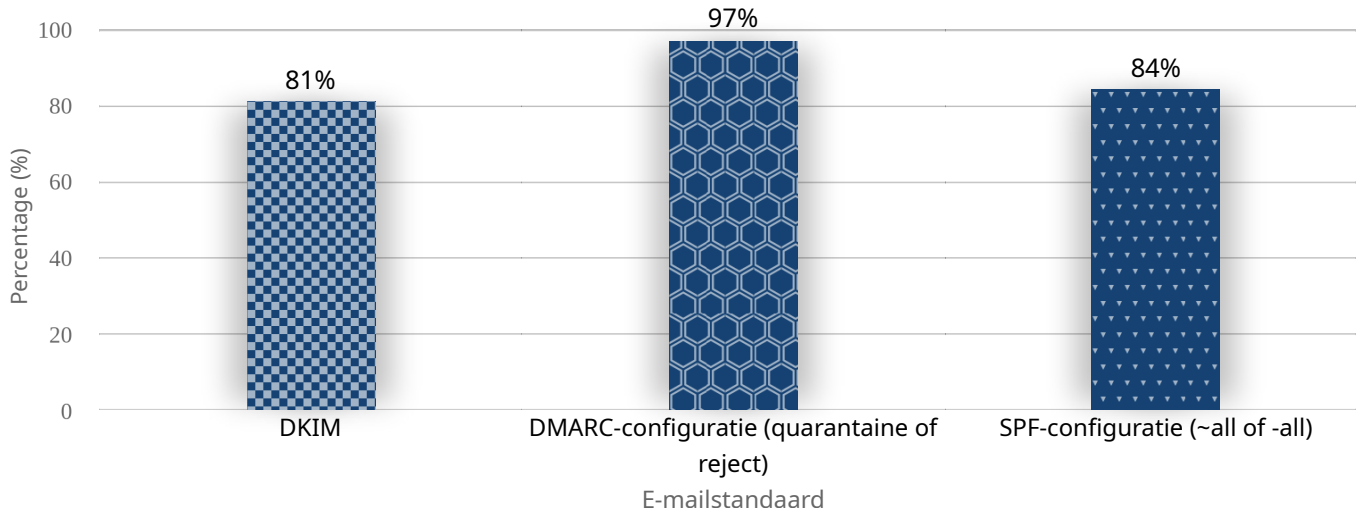


7.4. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

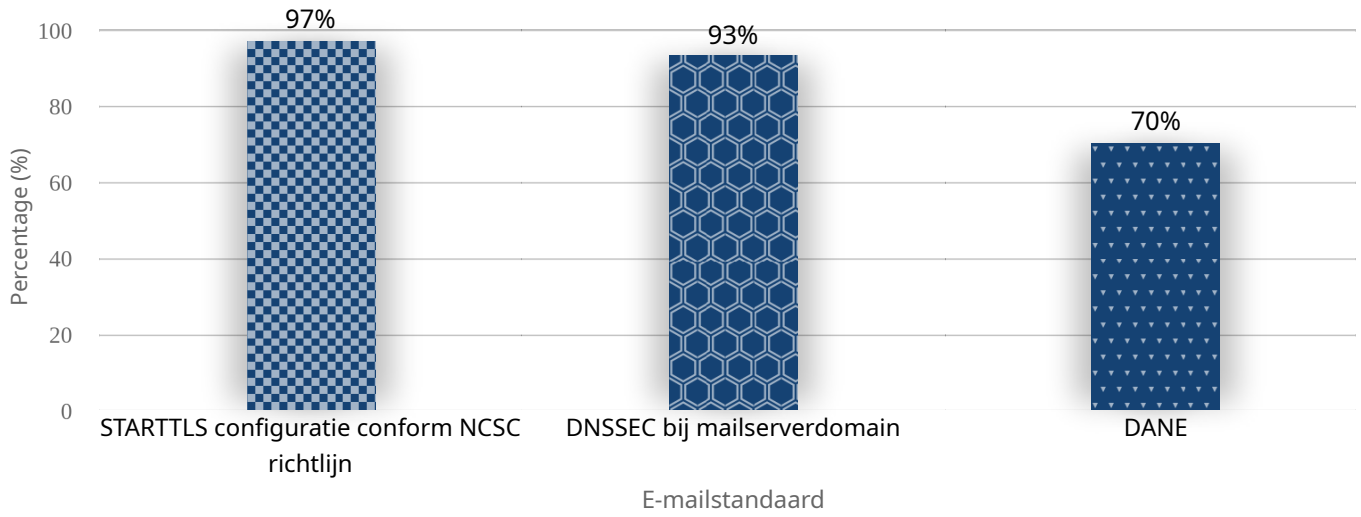
Grafiek 44: Adoptie per webbeveiligingsstandaard ministerie van Binnenlandse Zaken en Koninkrijksrelaties (n=1243)



Grafiek 45: Adoptie per 'anti-phishing' standaard ministerie van Binnenlandse Zaken en Koninkrijksrelaties (n=1311)

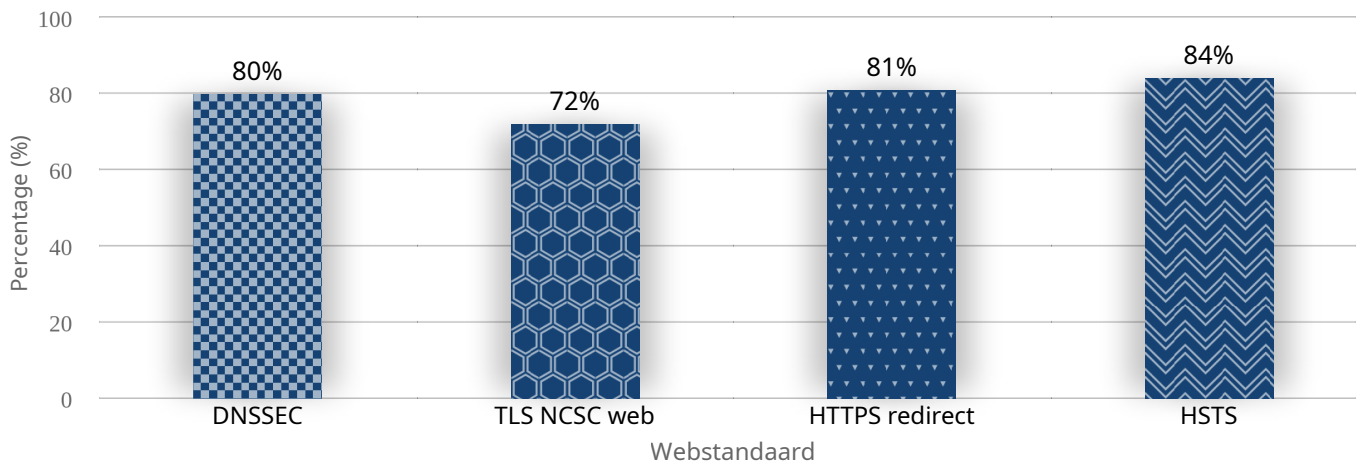


Grafiek 46: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (n=165)

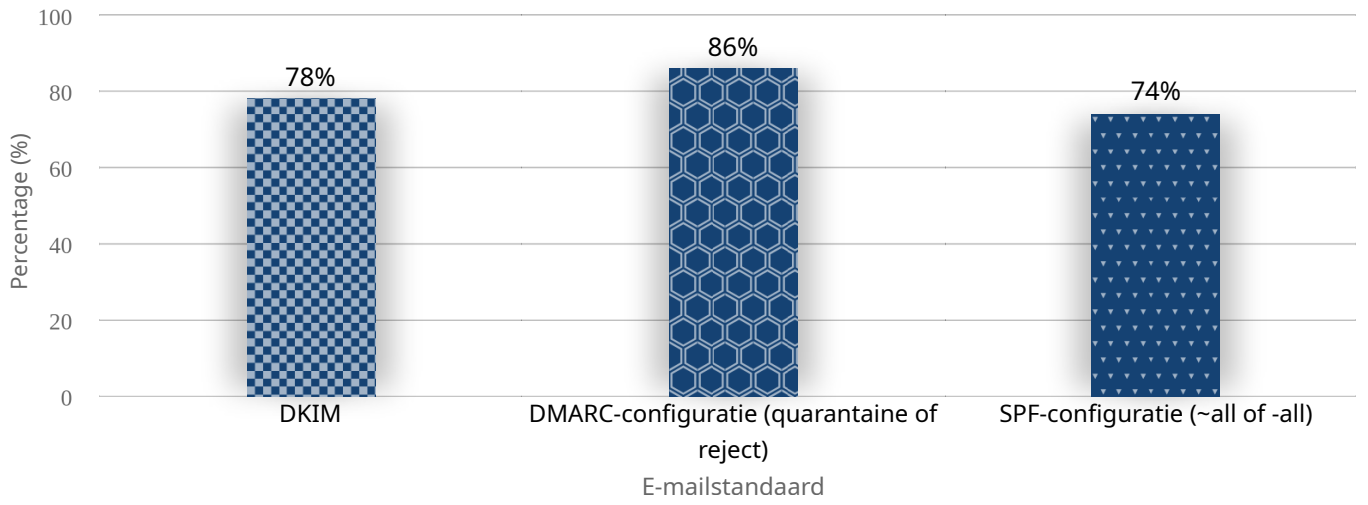


7.5. Ministerie van Buitenlandse Zaken

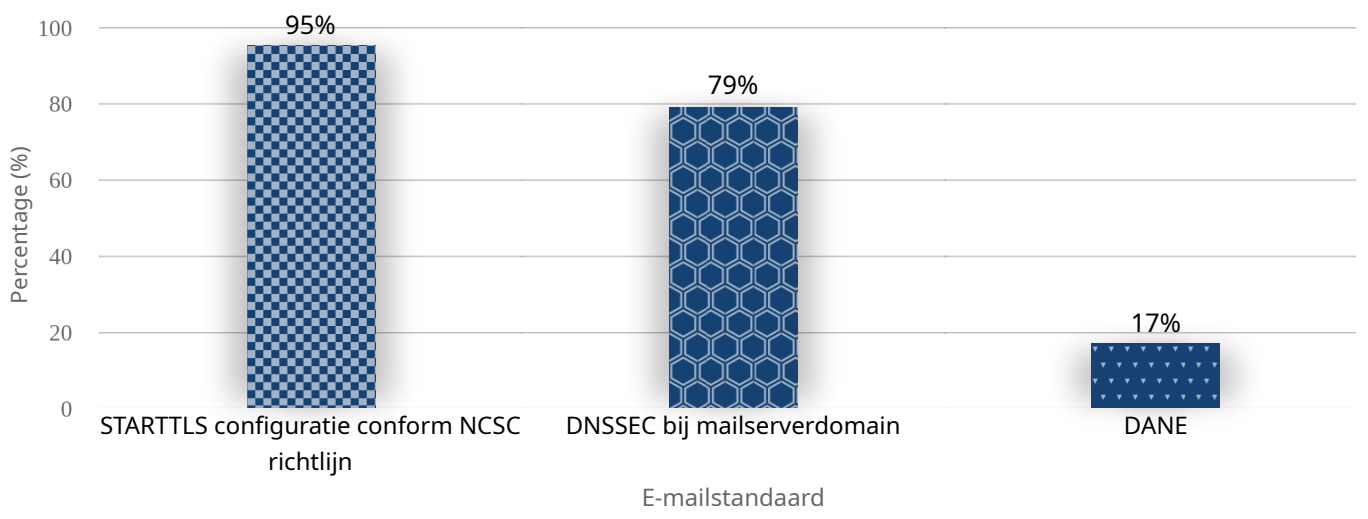
Grafiek 47: Adoptie per webbeveiligingsstandaard ministerie van Buitenlandse Zaken (n=289)



Grafiek 48: Adoptie per 'anti-phishing' standaard ministerie van Buitenlandse Zaken (n=316)

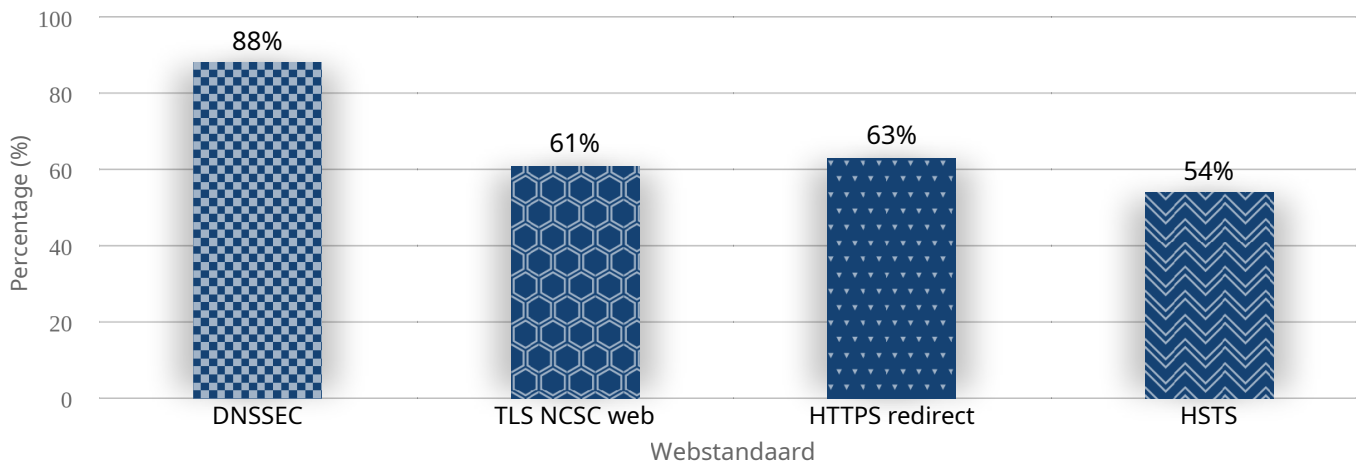


Grafiek 49: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Buitenlandse Zaken (n=44)

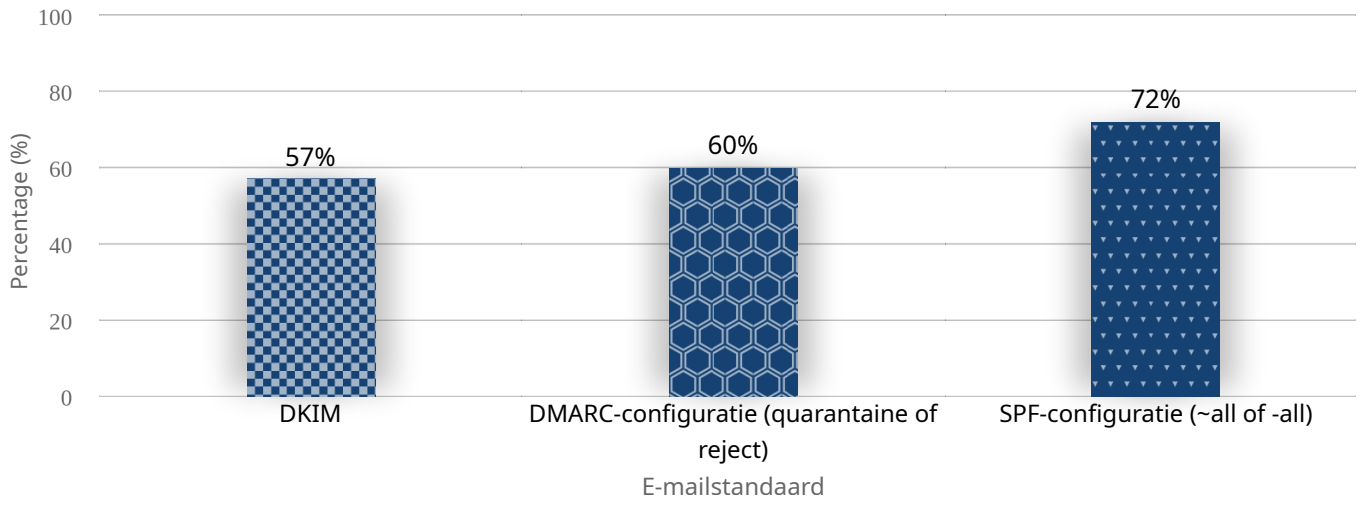


7.6. Ministerie van Defensie

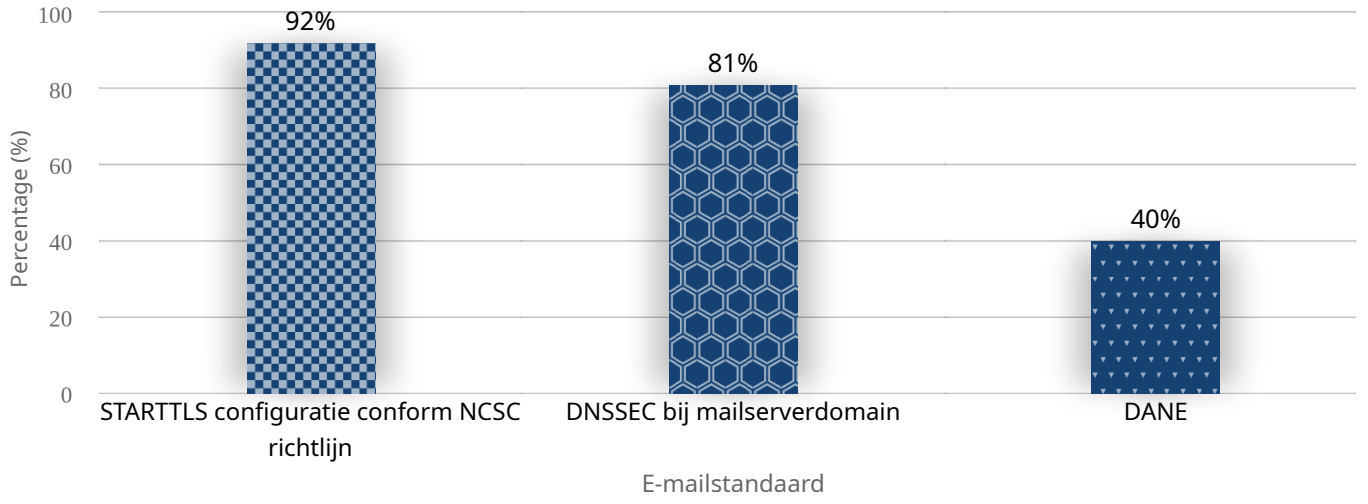
Grafiek 50: Adoptie per webbeveiligingsstandaard ministerie van Defensie (n=133)



Grafiek 51: Adoptie per 'anti-phishing' standaard ministerie van Defensie (n=151)

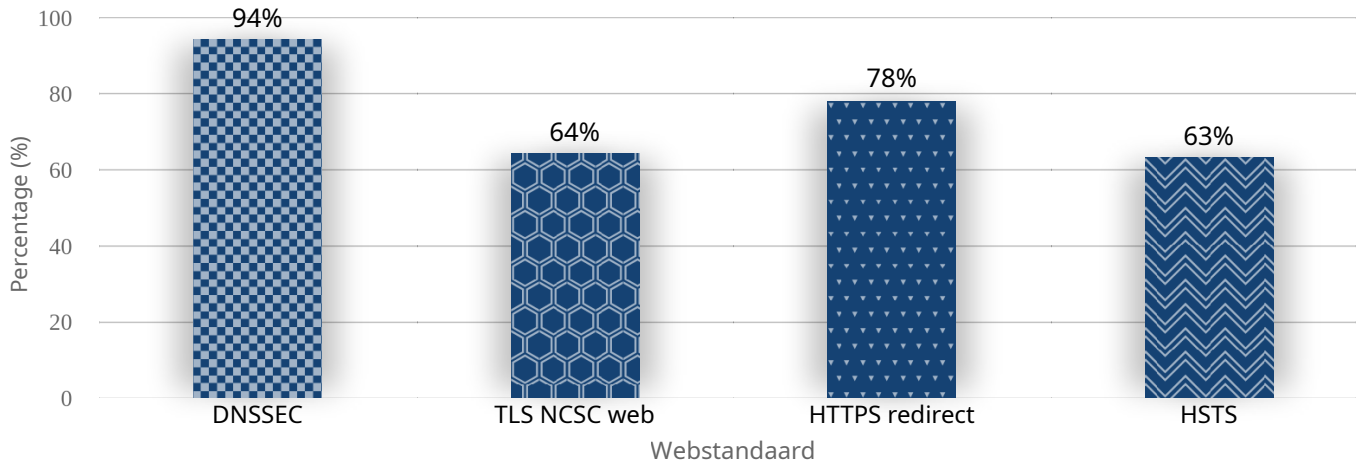


Grafiek 52: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Defensie (n=25)

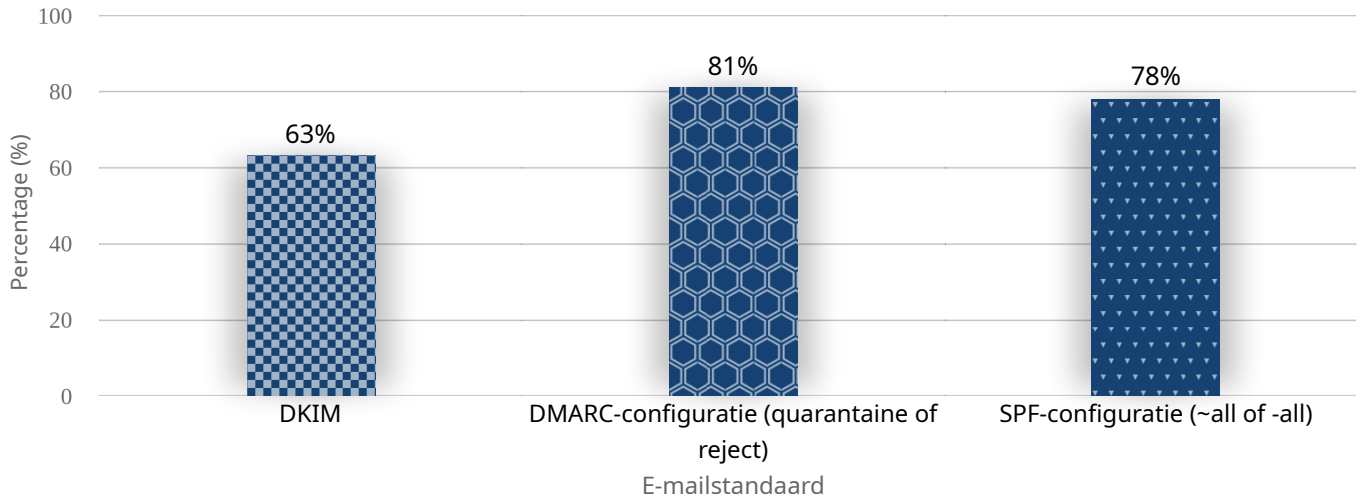


7.7. Ministerie van Economische Zaken en Klimaat

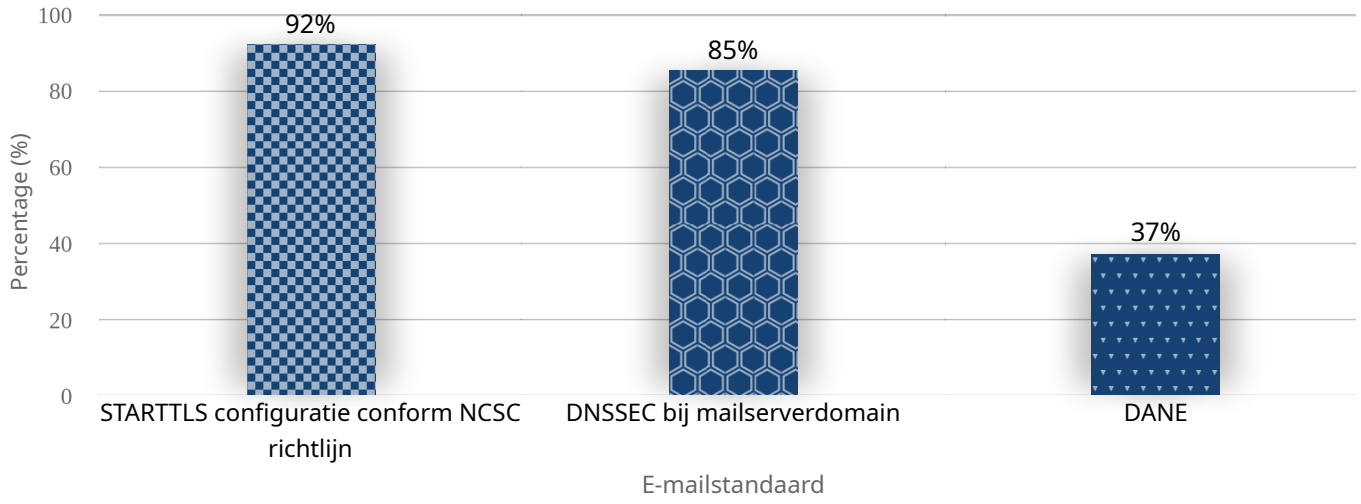
Grafiek 53: Adoptie per webbeveiligingsstandaard ministerie van Economische Zaken en Klimaat (n=721)



Grafiek 54: Adoptie per 'anti-phishing' standaard ministerie van Economische Zaken en Klimaat (n=886)

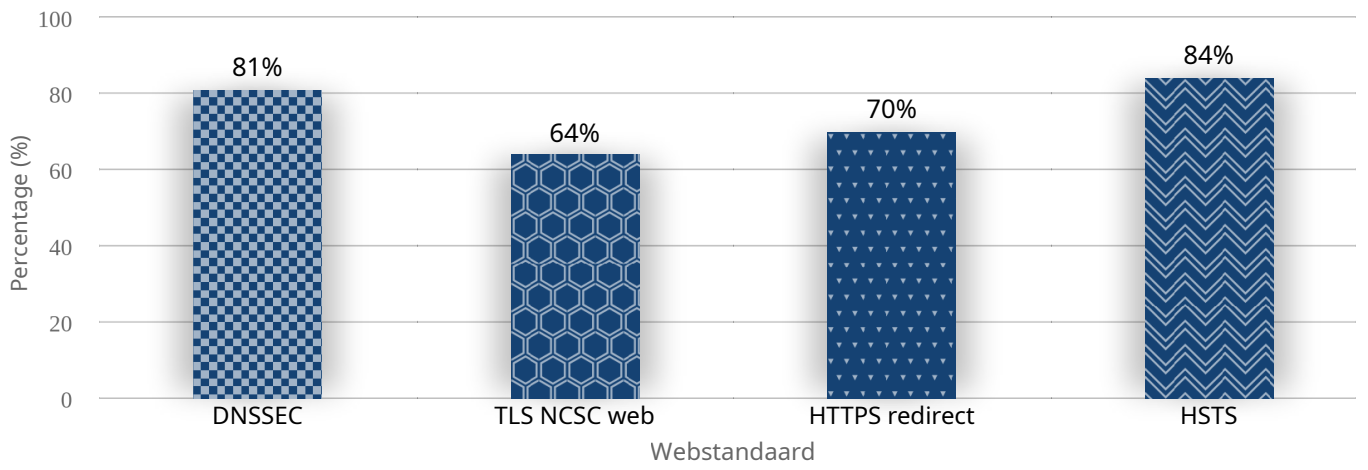


Grafiek 55: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Economische Zaken en Klimaat (n=297)

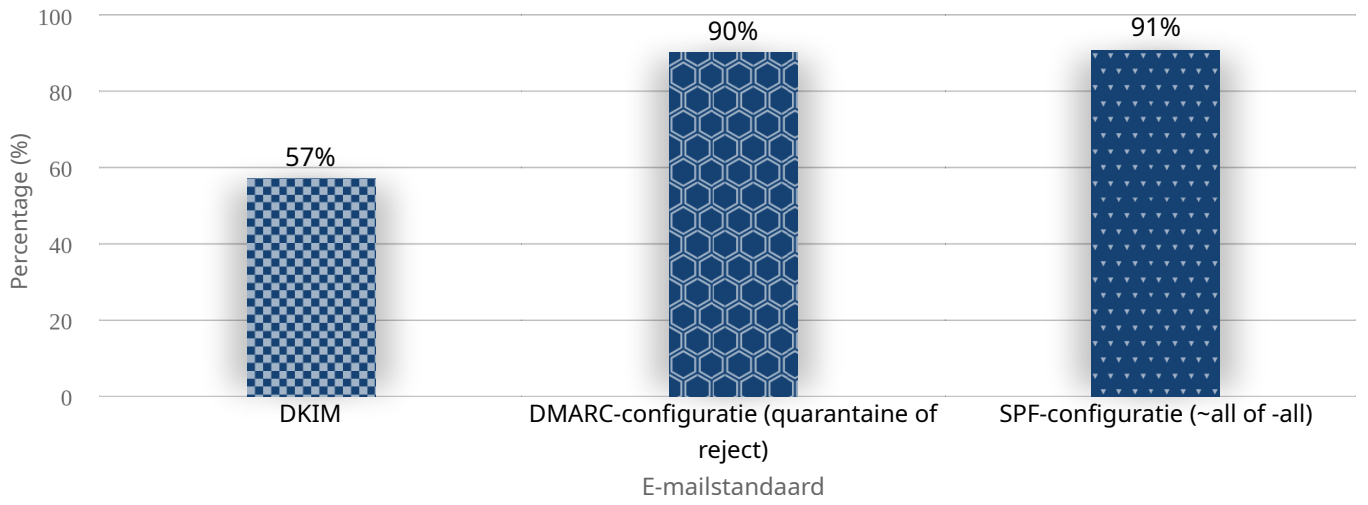


7.8. Ministerie van Financiën

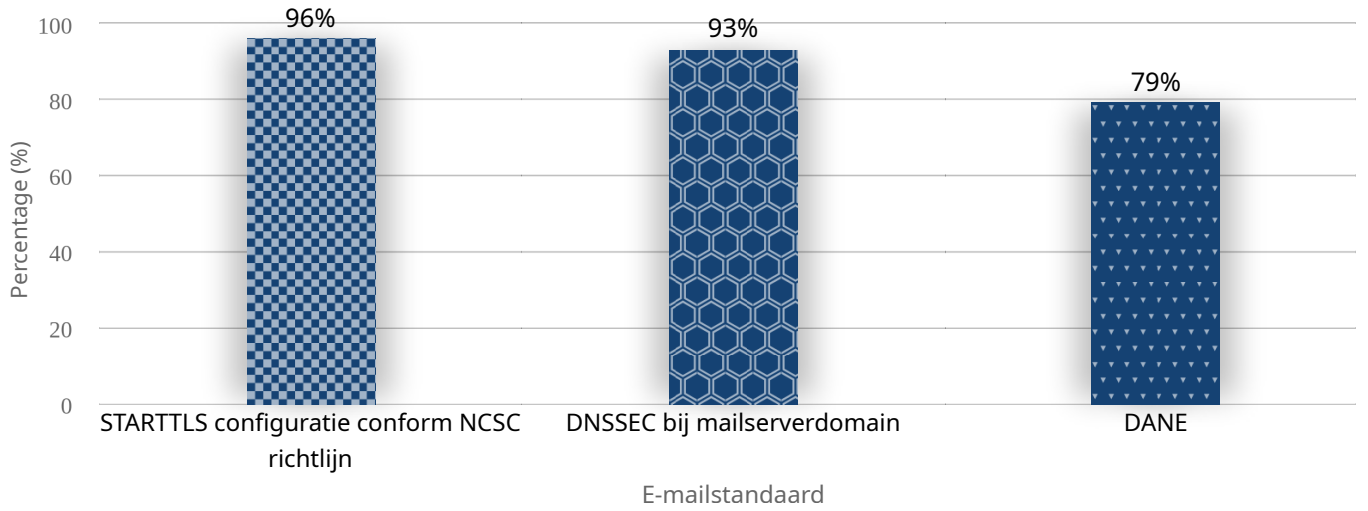
Grafiek 56: Adoptie per webbeveiligingsstandaard ministerie van Financiën (n=320)



Grafiek 57: Adoptie per 'anti-phishing' standaard ministerie van Financiën (n=410)

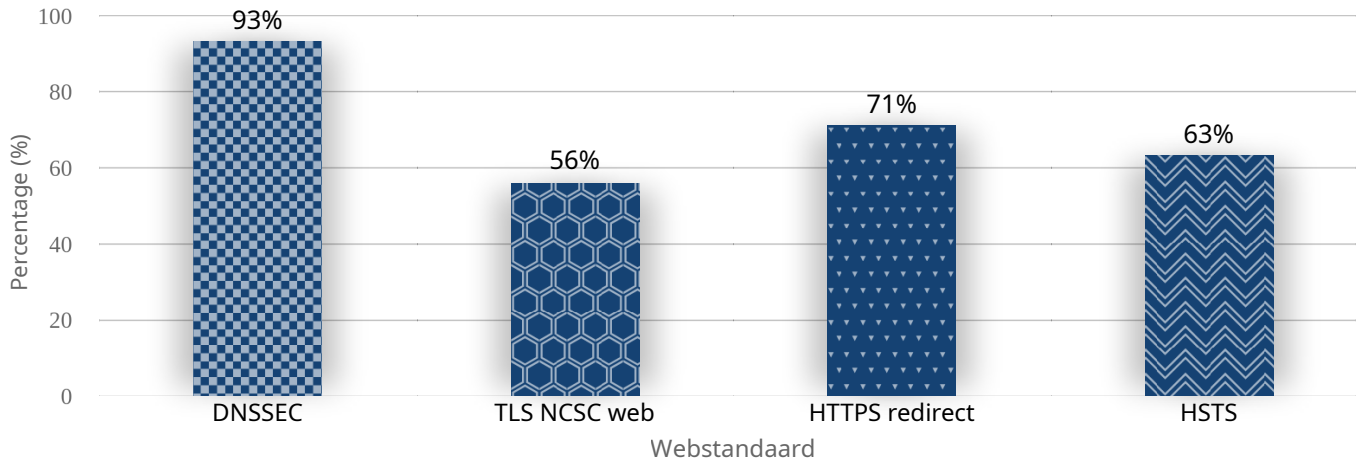


Grafiek 58: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Financiën (n=127)

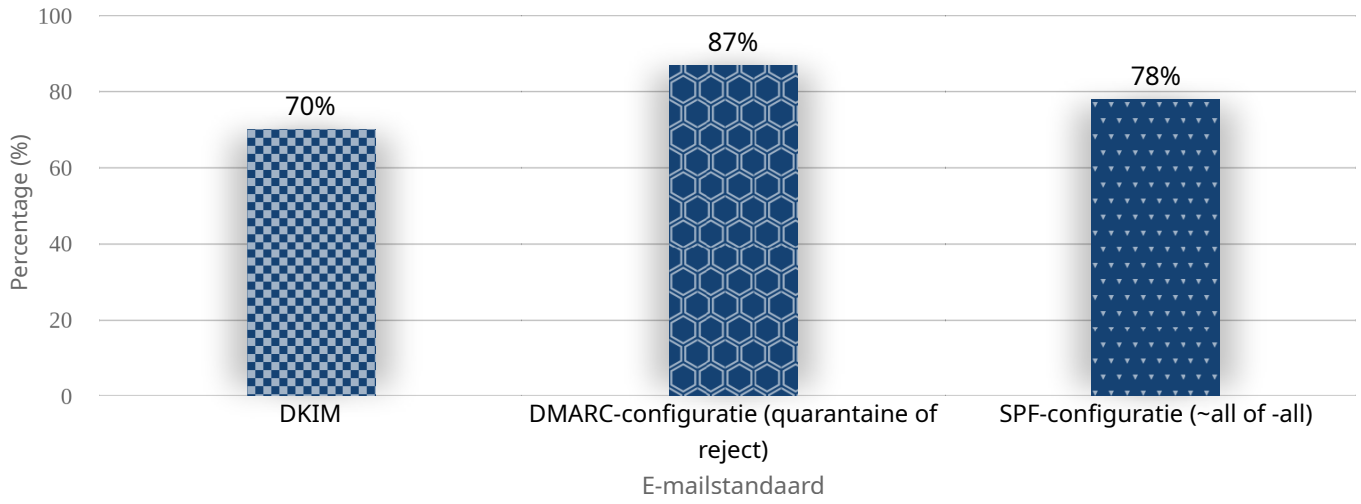


7.9. Ministerie van Infrastructuur en Waterstaat

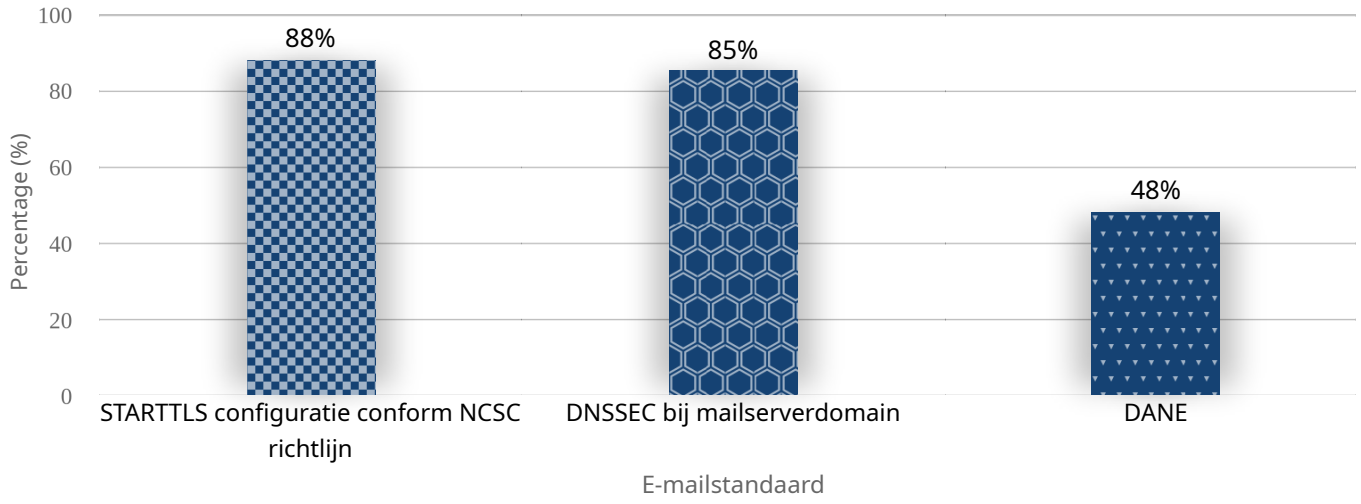
Grafiek 59: Adoptie per webbeveiligingsstandaard ministerie van Infrastructuur en Waterstaat (n=1398)



Grafiek 60: Adoptie per 'anti-phishing' standaard ministerie van Infrastructuur en Waterstaat (n=1528)

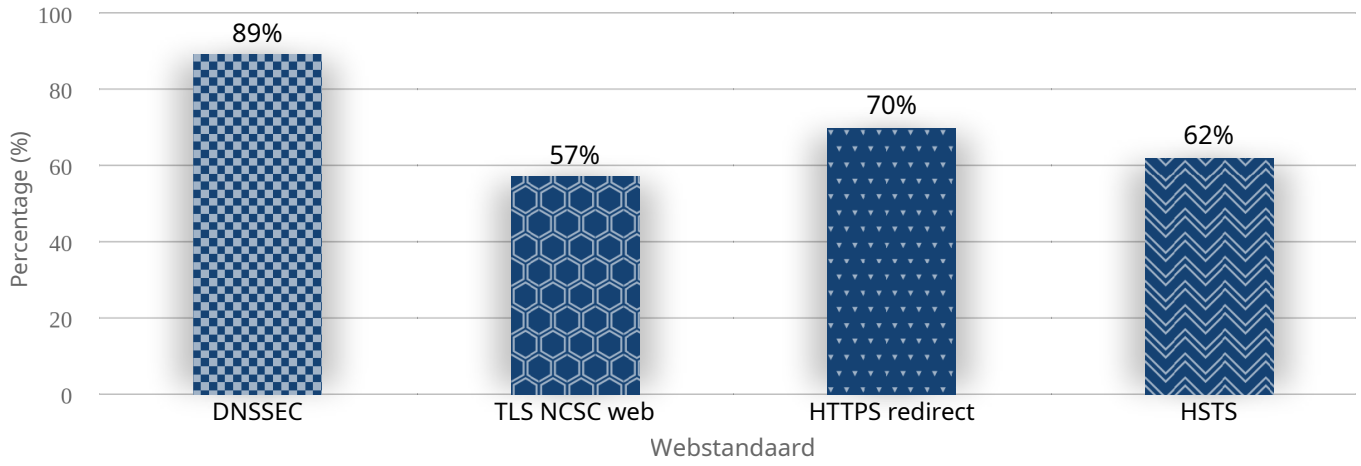


Grafiek 61: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Infrastructuur en Waterstaat (n=257)

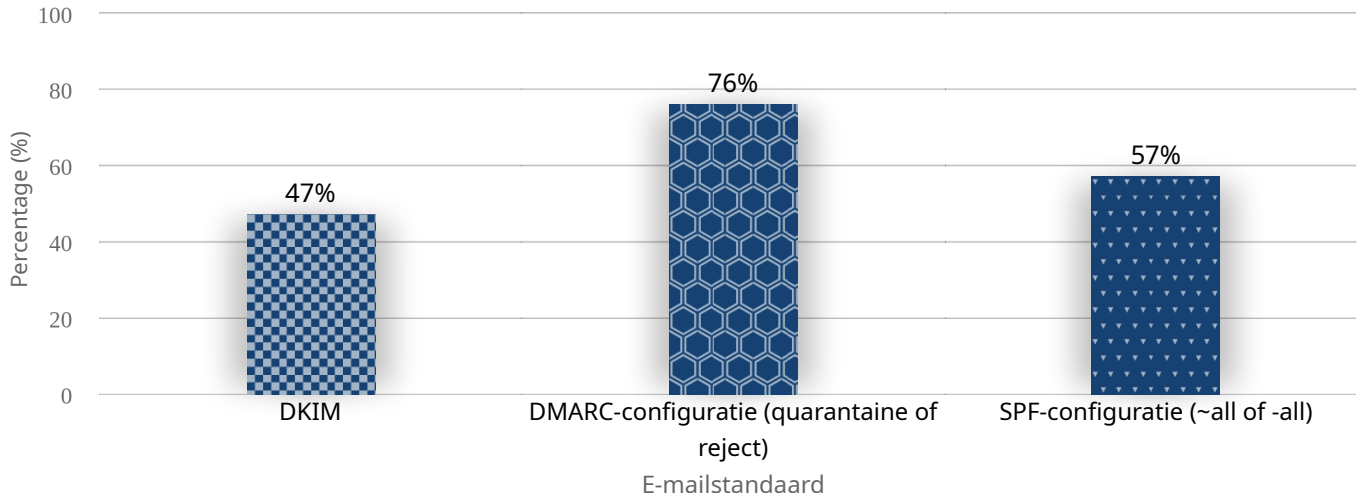


7.10. Ministerie van Justitie en Veiligheid

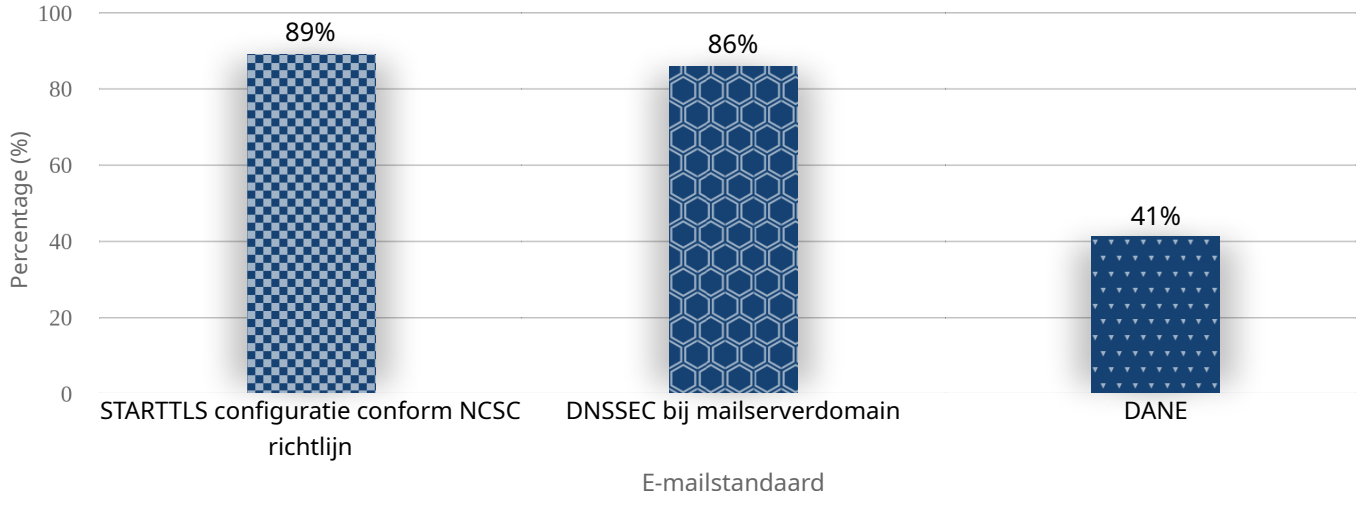
Grafiek 62: Adoptie per webbeveiligingsstandaard ministerie van Justitie en Veiligheid (n=1271)



Grafiek 63: Adoptie per 'anti-phishing' standaard ministerie van Justitie en Veiligheid (n=1388)

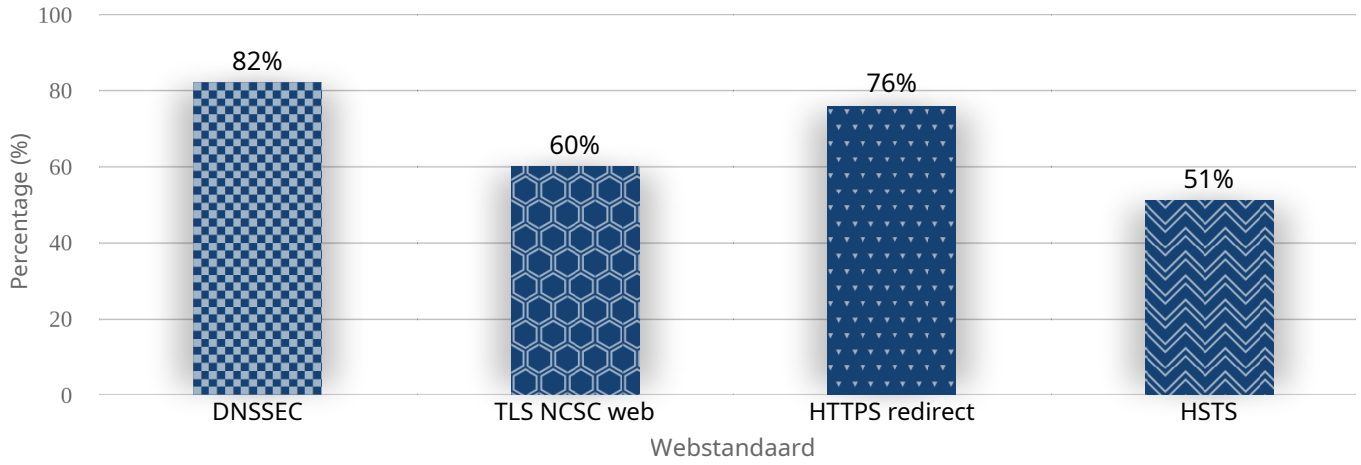


Grafiek 64: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Justitie en Veiligheid (n=329)

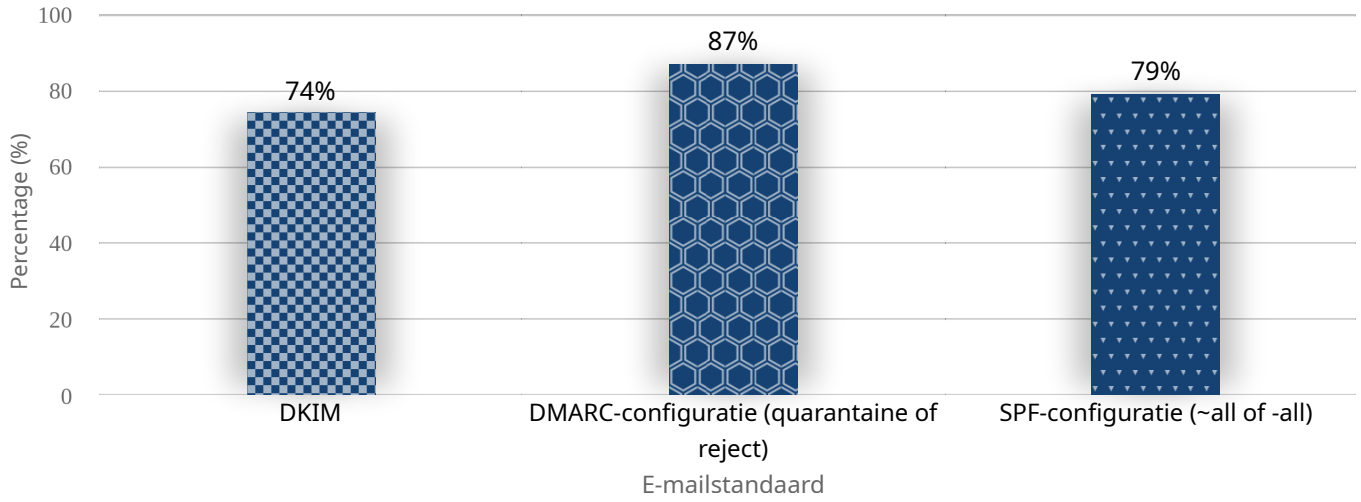


7.11. Ministerie van Landbouw, Natuur en Voedsel-kwaliteit

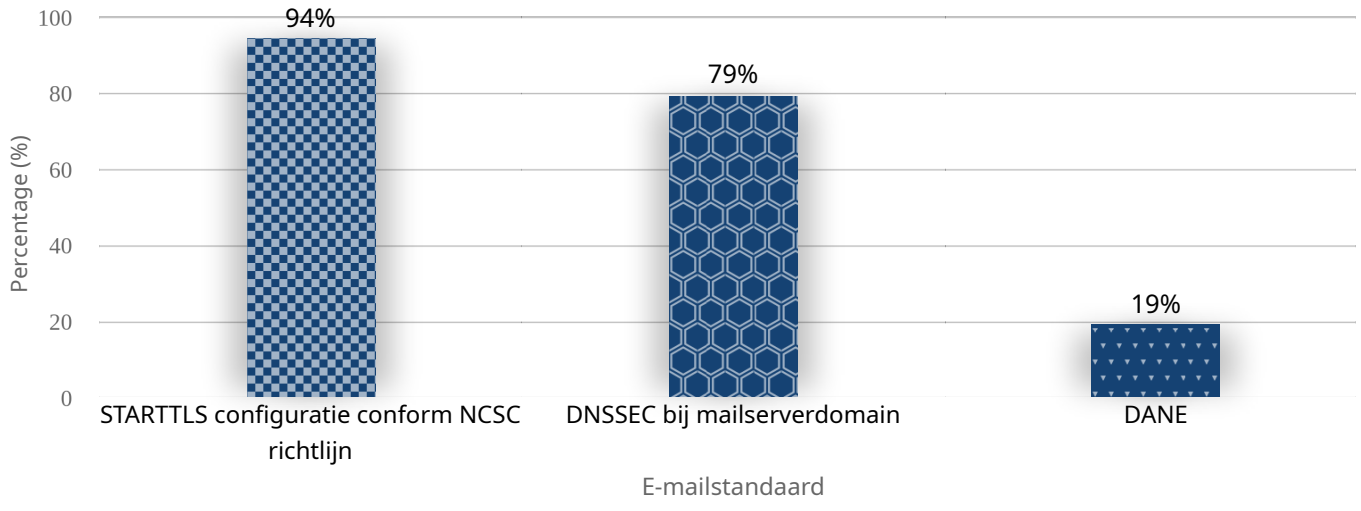
Grafiek 65: Adoptie per webbeveiligingsstandaard ministerie van Landbouw, Natuur en Voedsel-kwaliteit (n=397)



Grafiek 66: Adoptie per 'anti-phishing' standaard ministerie van Landbouw, Natuur en Voedsel-kwaliteit (n=449)

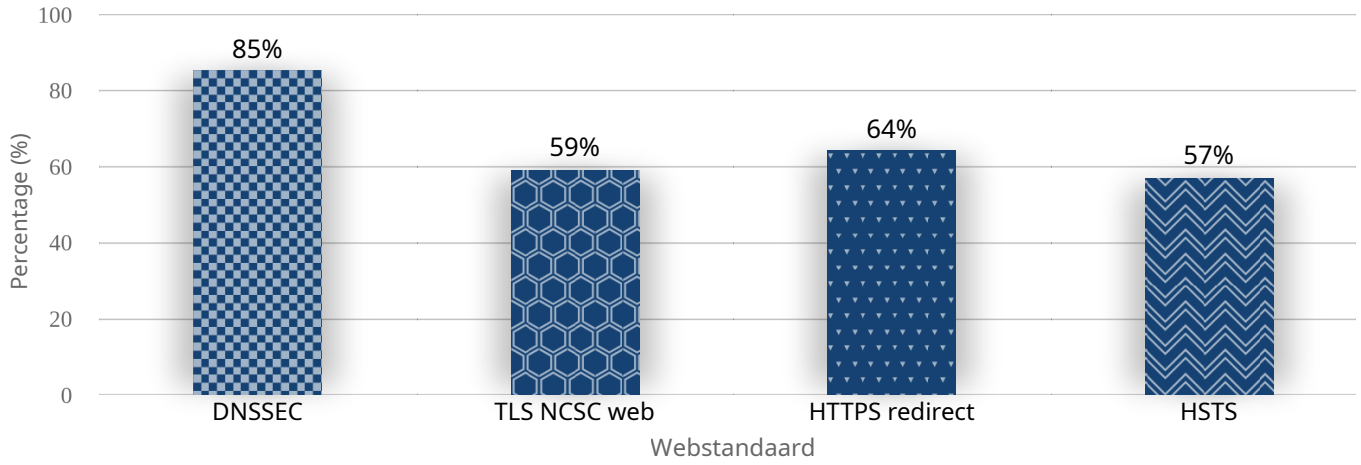


Grafiek 67: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Landbouw, Natuur en Voedselkwaliteit (n=80)

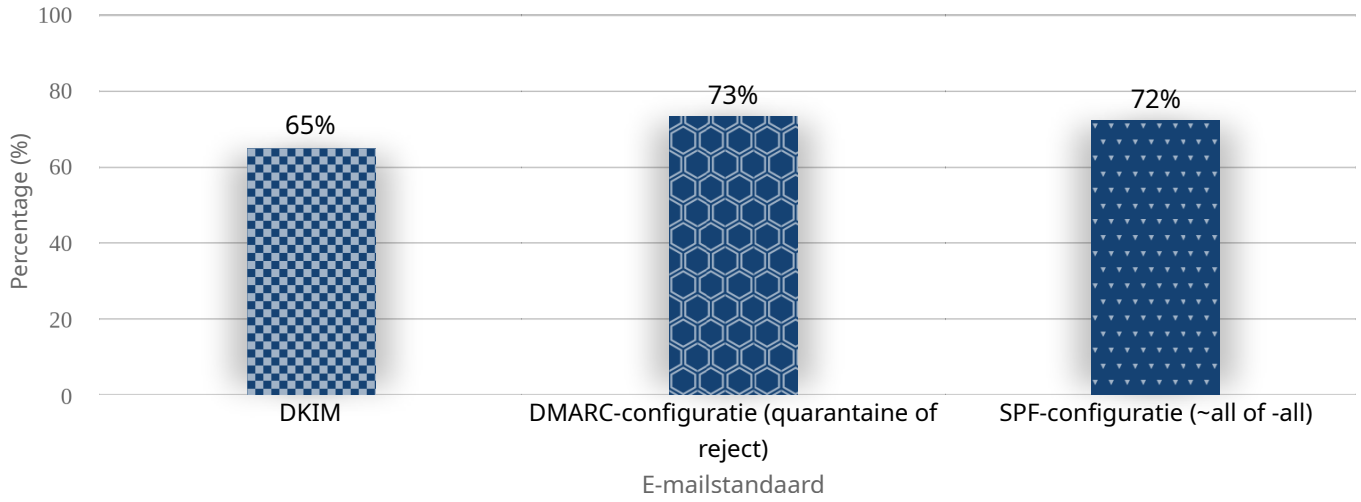


7.12. Ministerie van Onderwijs, Cultuur en Weten-schap

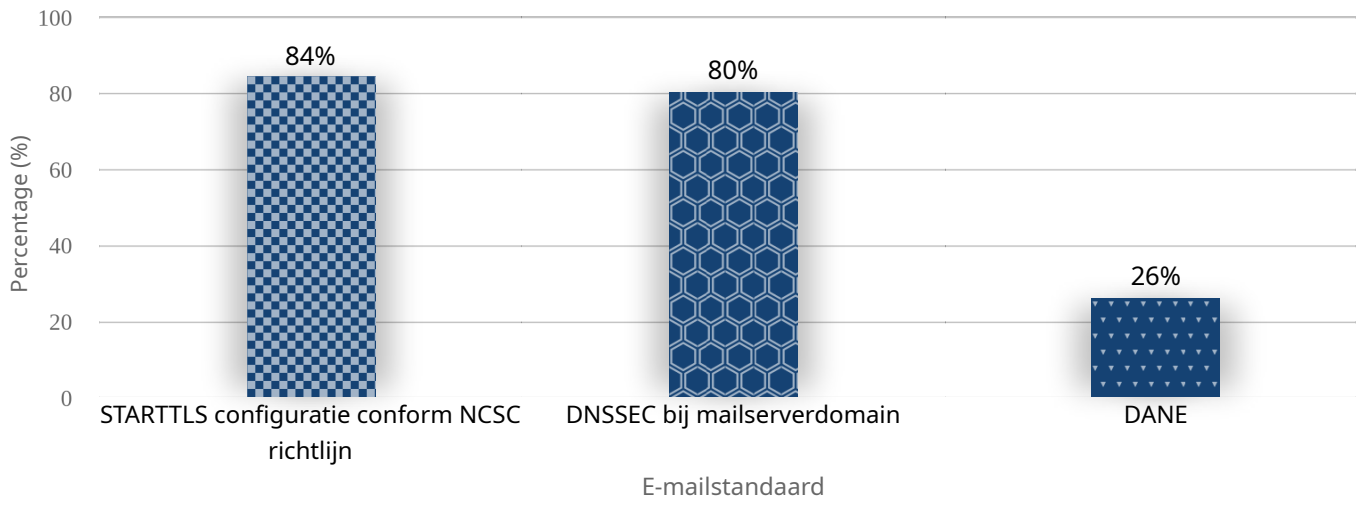
Grafiek 68: Adoptie per webbeveiligingsstandaard ministerie van Onderwijs, Cultuur en Weten-schap (n=792)



Grafiek 69: Adoptie per 'anti-phishing' standaard ministerie van Onderwijs, Cultuur en Weten-schap (n=927)

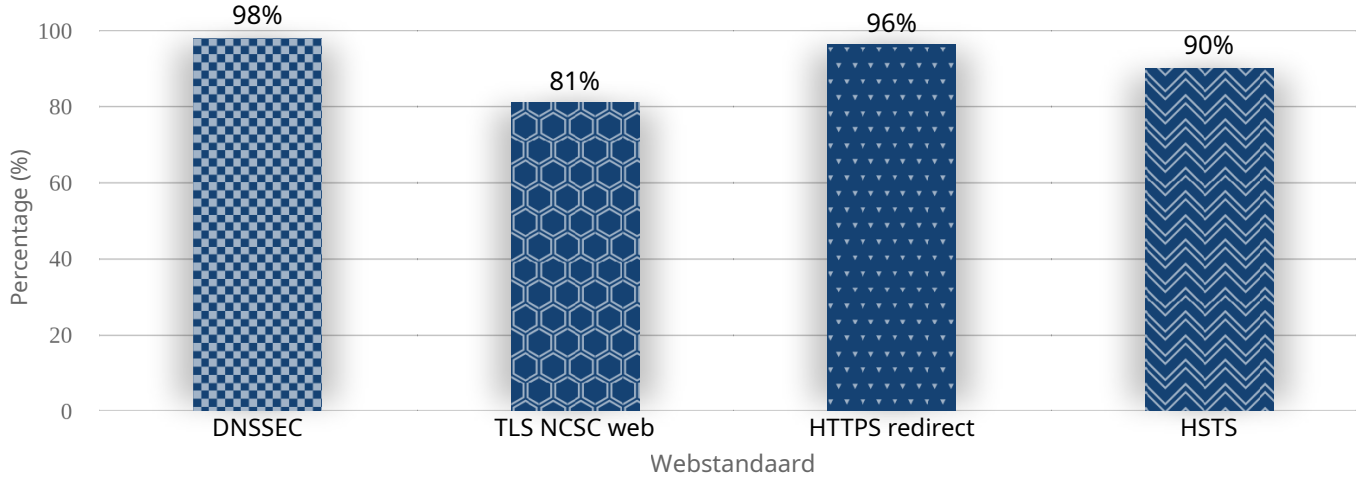


Grafiek 70: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Onderwijs, Cultuur en Wetenschap (n=180)

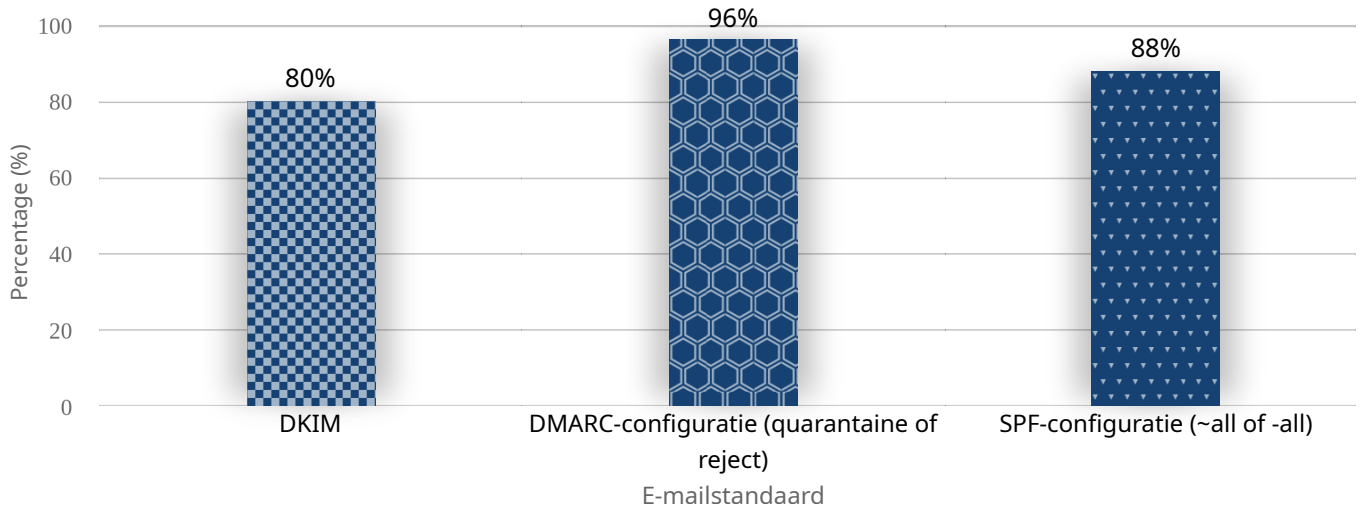


7.13. Ministerie van Sociale Zaken en Werkgelegenheid

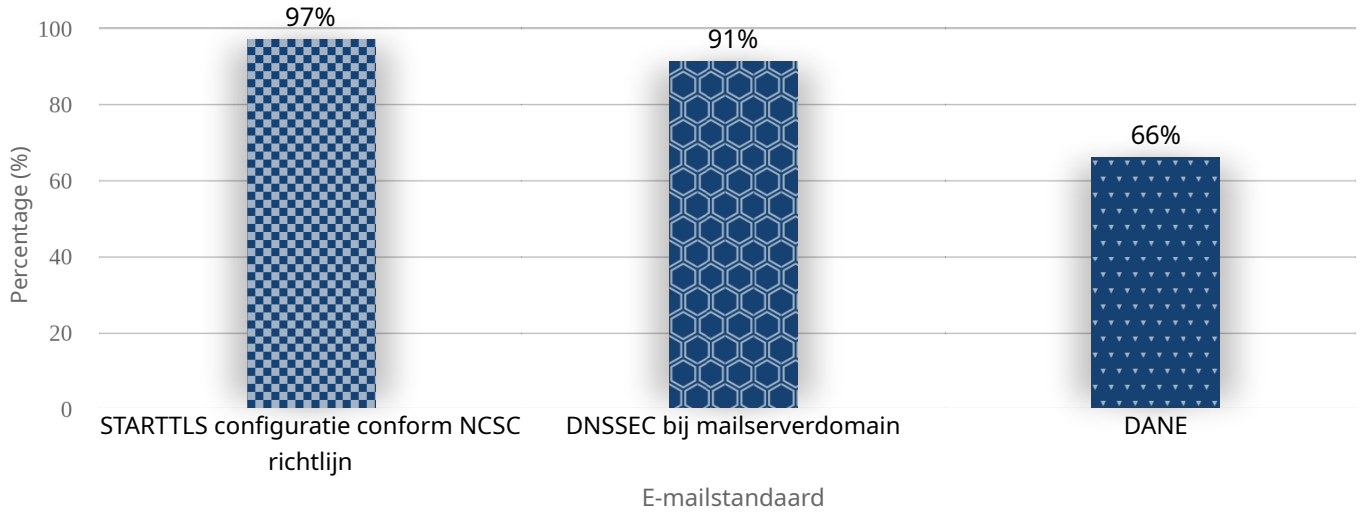
Grafiek 71: Adoptie per webbeveiligingsstandaard ministerie van Sociale Zaken en Werkgelegenheid (n=499)



Grafiek 72: Adoptie per 'anti-phishing' standaard ministerie van Sociale Zaken en Werkgelegenheid (n=526)

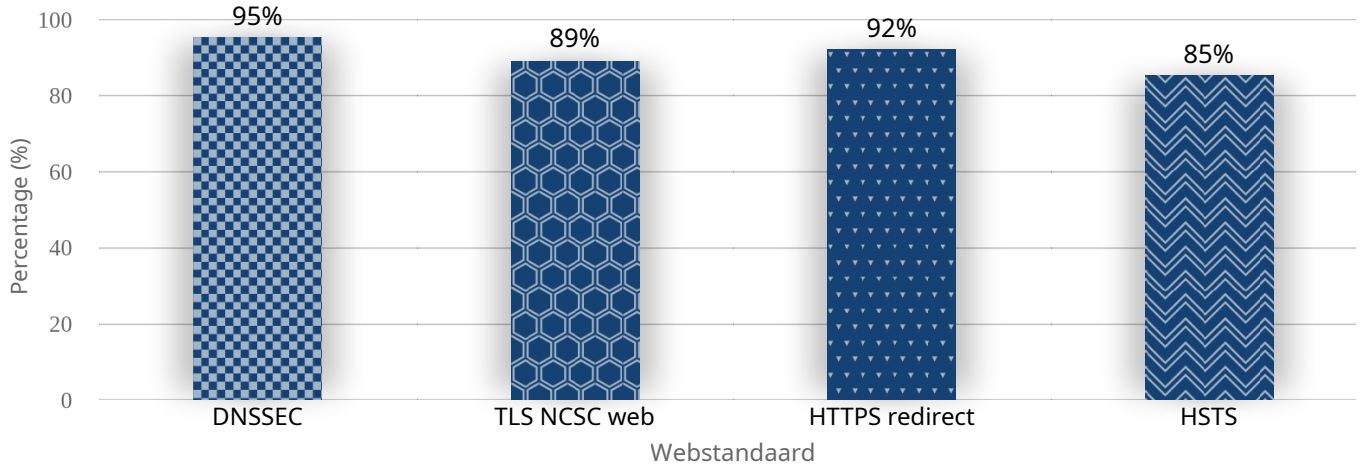


Grafiek 73: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Sociale Zaken en Werkgelegenheid (n=63)

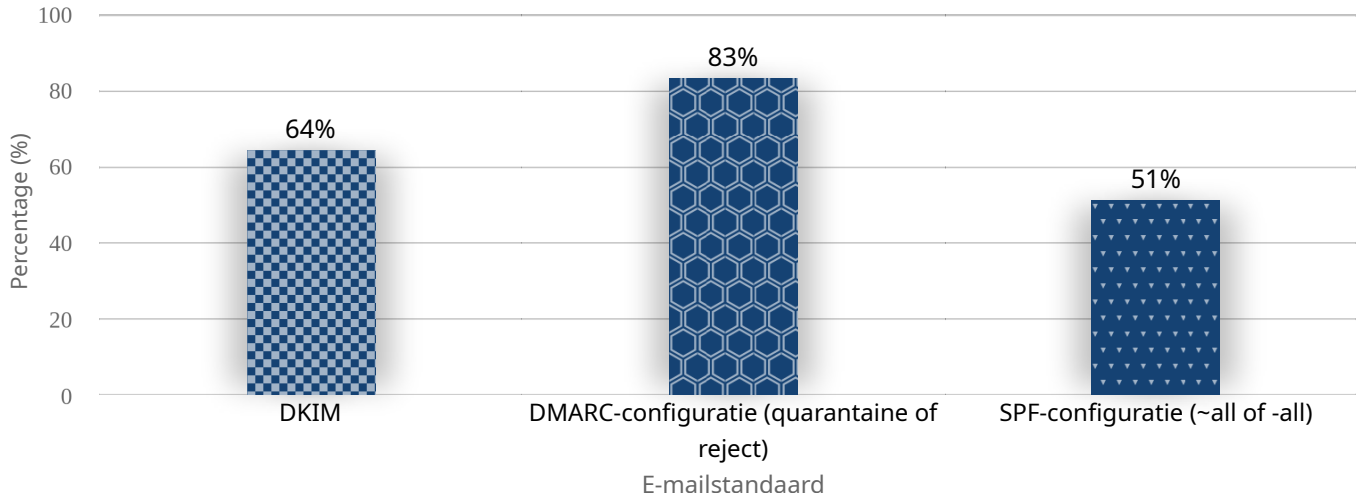


7.14. Ministerie van Volksgezondheid, Welzijn en Sport

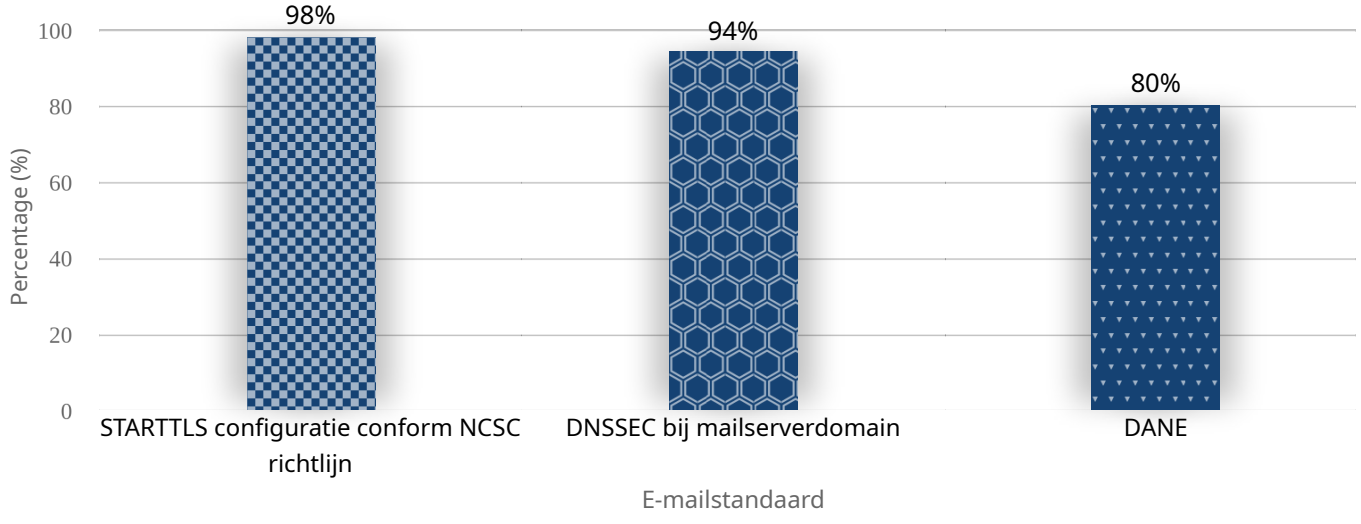
Grafiek 74: Adoptie per webbeveiligingsstandaard ministerie van Volksgezondheid, Welzijn en Sport (n=1801)



Grafiek 75: Adoptie per 'anti-phishing' standaard ministerie van Volksgezondheid, Welzijn en Sport (n=1881)



Grafiek 76: Adoptie per 'veilige e-mailtransport' standaard Ministerie van Volksgezondheid, Welzijn en Sport (n=488)



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 IMPLEMENTATIEDATUM	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 10959 internetdomeinen van overheidsorganisaties getoetst, bestaande uit:

- Alle internetdomeinen uit het Websiteregister Rijksoverheid;
- Alle internetdomeinen uit het Register van Overheidsorganisaties;
- Alle internetdomeinen uit het Register Internetdomeinen Overheid;
- 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. Een 100%-score op de gemeten domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn.

De organisaties zijn zelf verantwoordelijk voor de volledigheid, juistheid en actualiteit van de gegevens die zijn opgenomen in de drie genoemde registers.

8.2.1. Waarom worden anwb.nl en aanmelder.nl gemeten?

De Koninklijke Nederlandse Toeristenbond ANWB en anwb.nl staat in het Register van Overheidsorganisaties vanwege een wettelijke grondslag, het afgeven van het internationaal rijbewijs. De url aanmelder.nl/evenementenbureauvws is zowel in het Websiteregister Rijksoverheid opgenomen, als in het Register Internetdomeinen Overheid opgenomen.

8.3. Hoe wordt gemeten

De meting wordt uitgevoerd middels een bulktoets via de API van Internet.nl. Voor de webstandaarden wordt het hoofddomein getoetst, zowel zonder als met het subdomein www. (dus: forumstandaardisatie.nl én www.forumstandaardisatie.nl), omdat het gebruikelijk is dat de website daarop bereikbaar is. Voor de maildomeinen wordt primair getoetst zonder enig voorvoegsel omdat dat doorgaans gebruikt wordt als e-maildomein (dus: @forumstandaardisatie.nl), maar ook wordt gekeken of andere subdomeinen (zoals www, dus @www.forumstandaardisatie.nl) goed zijn geconfigureerd met SPF en DMARC. Dit is toegevoegd omdat het vaak wordt vergeten dat voor élk A en/of AAAA-record er een SPF record moet worden geplaatst. DMARC vereist namelijk SPF óf DKIM, als er géén SPF-record aanwezig is, de combinatie SPF none en DKIM fail kan alsnog voor een succesvolle bezorging zorgen.

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 vóór 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 vóór 2019 aan te voldoen.

STANDAARD	BESCHRIJVING
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.

STANDAARD	BESCHRIJVING
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).