Forum Standaardisatie
Standaard Samenwerken

Meting Informatieveiligheidstandaarden overheid voorjaar 2022

Inclusief IPv6

Datum document: 26 augustus 2022

Status document: Definitief t.b.v. SO OBDO

02-11-2022: plaatsing figuren op pagina's 6 en 7 gecorrigeerd (omgewisseld)

08-11-2022: aanvullende correcties in enkele grafieken, opmaak en spelfouten

Inhoudsopgave

Leeswijzer 3

1. Samenvatting 4

1.1. Adviezen 4

1.2. Websitestandaarden 6

1.2.1. Totaalbeeld websites per overheidscategorie (incl. IPv6) 6

1.2.2. Websitebeveiligingsstandaarden (excl. IPv6) 7

1.3. E-mailstandaarden 8

1.3.1. Totaalbeeld e-mail per overheidscategorie (incl. IPv6) 8

1.3.2. E-mailstandaarden voor bestrijding van phishing (excl. IPv6) 9

1.3.3. E-mailstandaarden voor vertrouwelijk e-mailverkeer (excl. IPv6) 10

2. Adoptie per websitebeveiligingsstandaard 13

3. Adoptie per e-mailbeveiligingsstandaard 14

3.1. E-mailstandaarden voor bestrijding van phishing 14

3.2. E-mailstandaarden voor vertrouwelijk e-mailverkeer 14

4. Adoptie IPv6 voor websites en e-mail 16

4.1. IPv6 voor webverkeer per overheidscategorie 16

4.2. IPv6 voor webverkeer per ministerie 16

4.3. IPv6 voor e-mailverkeer per overheidscategorie 17

4.4. IPv6 voor e-mailverkeer per ministerie 18

5. Adoptie per overheidscategorie 19

5.1. Centrale overheid 19

5.2. Provincies 20

5.3. Waterschappen 21

5.4. Gemeenten 22

5.5. Gemeenschappelijke regelingen 23

6. Adoptie per ministerie 24

6.1. Totaalbeeld websitestandaarden (incl. IPv6) 24

6.2. Totaalbeeld e-mailstandaarden (incl. IPv6) 24

6.3. Ministerie van Algemene Zaken 26

6.4. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 27

6.5. Ministerie van Buitenlandse Zaken 28

6.6. Ministerie van Defensie 29

6.7. Ministerie van Economische Zaken en Klimaat 30

6.8. Ministerie van Financiën 31

6.9. Ministerie van Infrastructuur en Waterstaat 32

6.10. Ministerie van Justitie en Veiligheid 33

6.11. Ministerie van Landbouw, Natuur en Voedselkwaliteit 34

6.12. Ministerie van Onderwijs, Cultuur en Wetenschap 35

6.13. Ministerie van Sociale Zaken en Werkgelegenheid 36

6.14. Ministerie van Volksgezondheid, Welzijn en Sport 37

7. Achtergrond 38

7.1. Om welke standaarden gaat het 38

7.2. Om welke internetdomeinen gaat het 39

7.3. Hoe wordt gemeten 39

7.4. Wat wordt niet gemeten 40

7.5. Over de standaarden 40

7.5.1. Webstandaarden 40

7.5.2. E-mailstandaarden 42

Bijlage: individuele resultaten per internetdomein

Leeswijzer

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

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

Hoofdstuk 7 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 mei 2022.

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.

De meting laat zien dat bij 53% van de internetdomeinen alle verplichte websitestandaarden correct zijn toegepast. Het gaat om belangrijke beveiligingsstandaarden voor vertrouwelijk webverkeer, en IPv6 voor duurzame bereikbaarheid van online diensten.

Bij 44% van de internetdomeinen zijn alle verplichte e-mailstandaarden correct toegepast. 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.

Met de meting zijn in totaal 2584 overheidsdomeinen gecontroleerd. Dat is een uitbreiding ten opzichte van voorgaande metingen, in de voorgaande meting zijn 559 overheidsdomeinen gecontroleerd. De 2584 overheidsdomeinen zijn slechts een deelwaarneming van alle overheidsdomeinen, 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

Zeven jaar na het maken van de eerste streefbeeldafspraak, en ruim twee jaar na het maken van de laatste, is geen van de streefbeelden voor de overheid als geheel gehaald. Het ontbreekt aan effectieve sturingsmechanismen om overheidsbrede afspraken eenduidig te laten landen en nageleefd te krijgen binnen individuele overheidsorganisaties. Zodra de Wet Digitale Overheid van kracht wordt kunnen standaarden wettelijk worden verplicht, zoals

reeds is voorgenomen met HTTPS en HSTS. Ook hier speelt de vraag hoe deze verdergaande verplichtingen de operationele werkvloer bereiken, en hoe vervolgens gestuurd wordt op naleving van de verplichtingen.

Advies 1: onderzoek welke sturingsmechanismen kunnen worden ingezet om overheidsbrede architectuurafspraken en kwaliteitseisen (beleid) – bijvoorbeeld in de vorm van gemeenschappelijke standaarden en streefbeeldafspraken – effectief te laten landen in de uitvoering bij de individuele overheidsorganisaties (implementatie).

Positieve uitschieters binnen overheidscategorieën en tussen ministeries zijn vaak te verklaren vanuit proactieve sturing (regie) op de toepassing van standaarden, bijvoorbeeld vanuit een CIO- of CISO-office (voorbeelden: CIO BZK en CISO VWS). Proactieve sturing op de omvang en kwaliteitsaspecten van het internetdomeinportfolio is noodzakelijk om risico's voor zowel organisaties als burgers te kunnen beheersen. Als handreiking 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.

Het komt regelmatig voor dat websites of e-maildiensten decentraal ingekocht worden, terwijl er centrale (overheids)dienstverlening bestaat waarmee dezelfde diensten efficiënter geleverd kunnen worden. Met regie op internetdomeinen kan er beter op gestuurd worden dat centrale dienstverlening ook wordt benut.

Advies 2: organiseer regie op internetdomeinen binnen ministeries en individuele overheidsorganisaties. Jaag dit initieel project- of programmamatig aan, en borg dit vervolgens in de lijnorganisatie.

Centralisering van dienstverlening heeft veelal een positief effect op de toepassing van standaarden. Wanneer een gemeenschappelijke dienstverlener een standaard consequent toepast heeft dit een hefboomeffect. Dit is zichtbaar bij diverse dienstverleningsconcepten; bijvoorbeeld de centrale registrarrol die de Dienst Publiek en Communicatie (AZ/DPC) vervult voor de Rijksoverheid, maar ook bij gemeenschappelijke dienstverleners voor web en e-maildiensten, zoals SSC-ICT, DICTU en diverse regionale dienstverleners.

Advies 3: verken of het centrale dienstverleningsconcept rond DNS-beheer van de Rijksoverheid ook kan worden ingezet bij decentrale overheden.

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

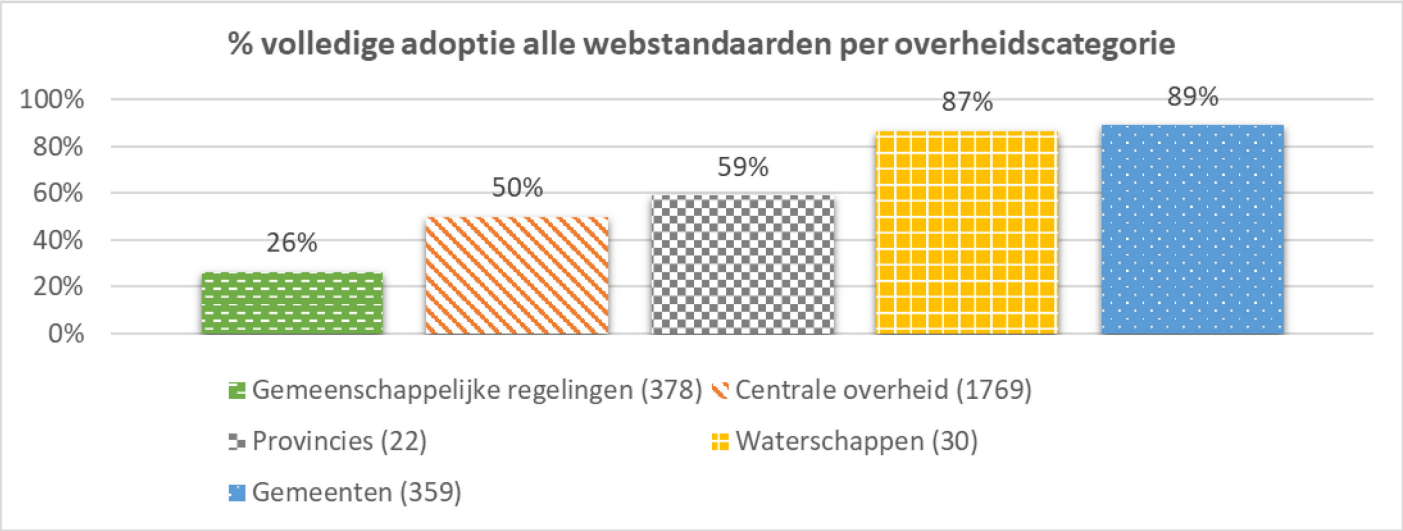
standaarden wel ondersteunt. Indien hiervan is afgeweken is het belangrijk dat overheden hun dienstverleners alsnog blijven vragen om ondersteuning van verplichte standaarden. Diverse dienstverleners geven in informele gesprekken aan dat een gebrek aan klantvraag een reden is om niet te investeren in ondersteuning van de voor overheid verplichte standaarden.

Advies 4: zorg ervoor dat naleving van IT-kwaliteitseisen – waaronder 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.

1.2. Websitestandaarden

1.2.1. Totaalbeeld websites per overheidscategorie (incl. IPv6)

Onderstaande cijfers laten zien in welke mate de 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. Waarschijnlijk zijn de streefbeeldafspraken niet doorgesijpeld naar deze instanties, hoewel zij in veel gevallen gefinancierd worden vanuit de andere overheden.



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

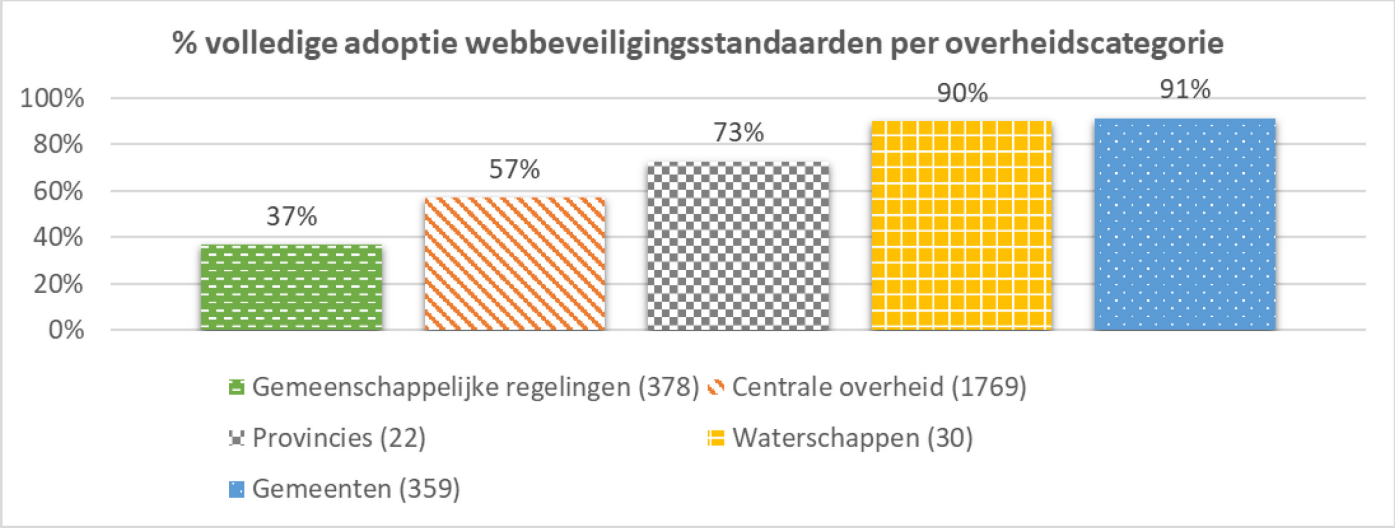
1.2.2. Websitebeveiligingsstandaarden (excl. IPv6)

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

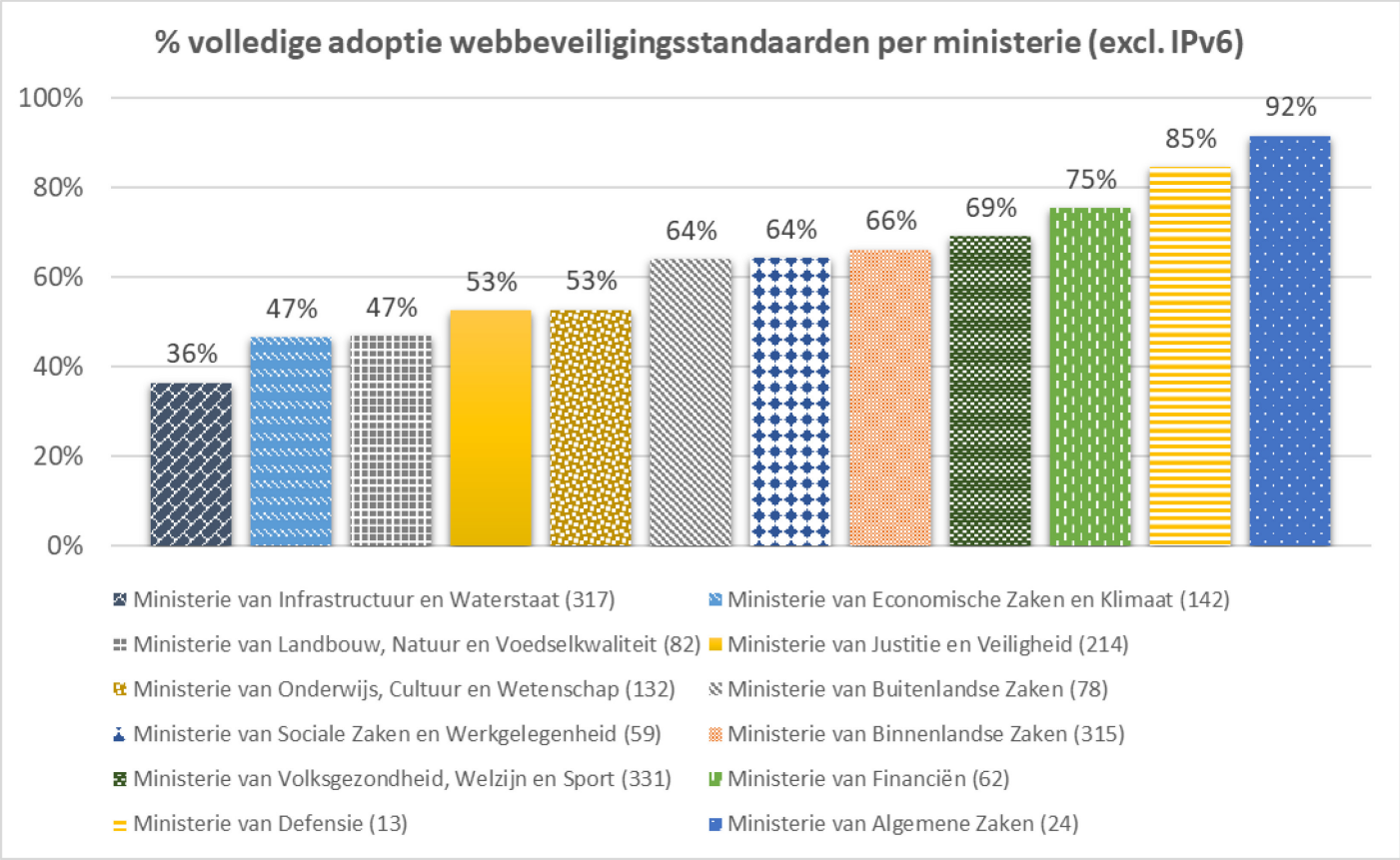
De achterblijvers zijn met name te vinden bij de centrale overheid en de gemeenschappelijke regelingen. De centrale overheid is getalsmatig oververtegenwoordigd in de meting doordat er veel secundaire internetdomeinen (campagnesites, projectsites, etc.) zijn meegenomen. Er is geen goed beeld van secundaire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



Voor meer details per overheidscategorie zie hoofdstuk 5.

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 Infrastructuur en Waterstaat (36%), Landbouw, Natuur en Voedselkwaliteit en Economische Zaken en Klimaat (beide 47%), en Justitie en Veiligheid en Onderwijs, Cultuur en Wetenschap (beide 53%) in negatieve zin op.

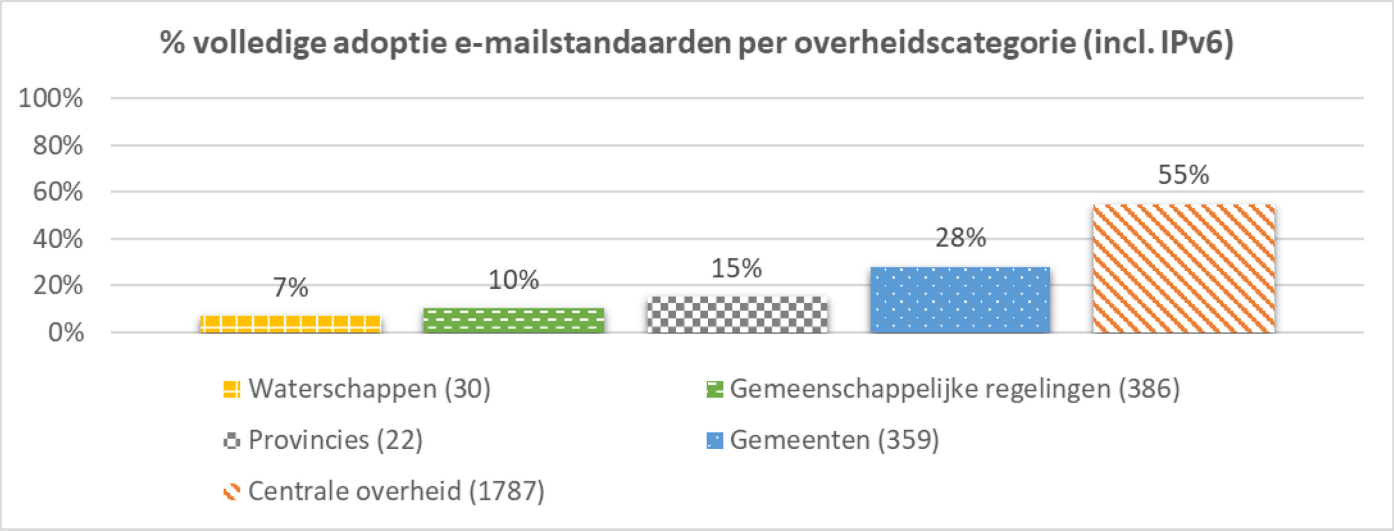


Voor meer details per ministerie zie hoofdstuk 6.

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 loopt 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. Lokale overheden lopen achter, 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 een rol spelen.



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

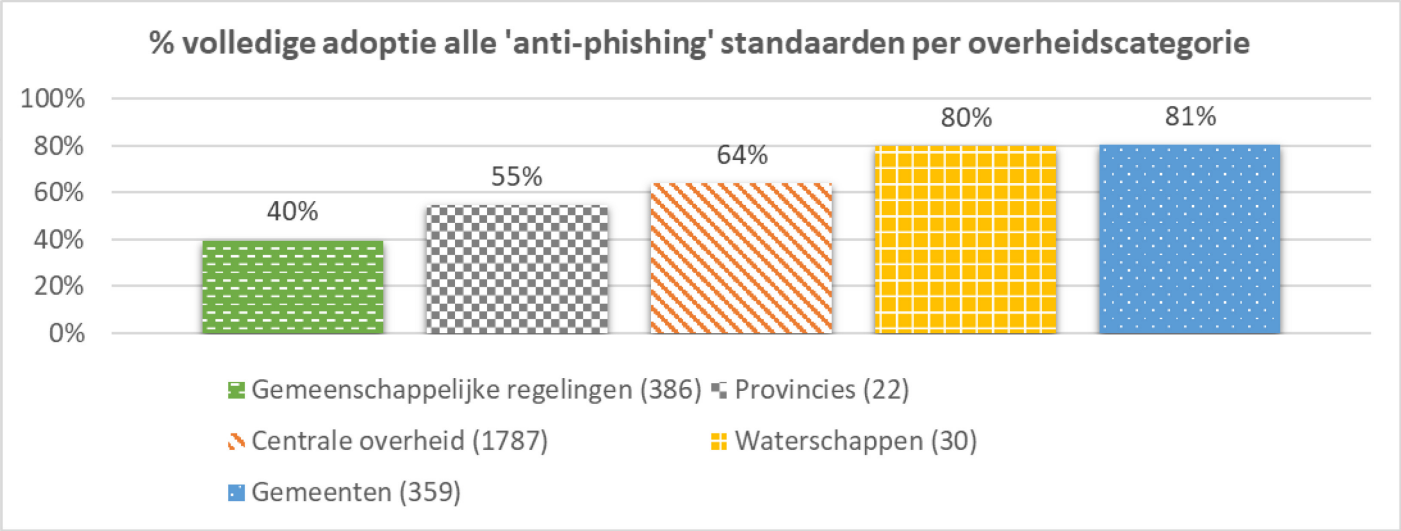
1.3.2. E-mailstandaarden voor bestrijding van phishing (excl. IPv6)

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

1.3.2.1. Adoptie per overheidscategorie

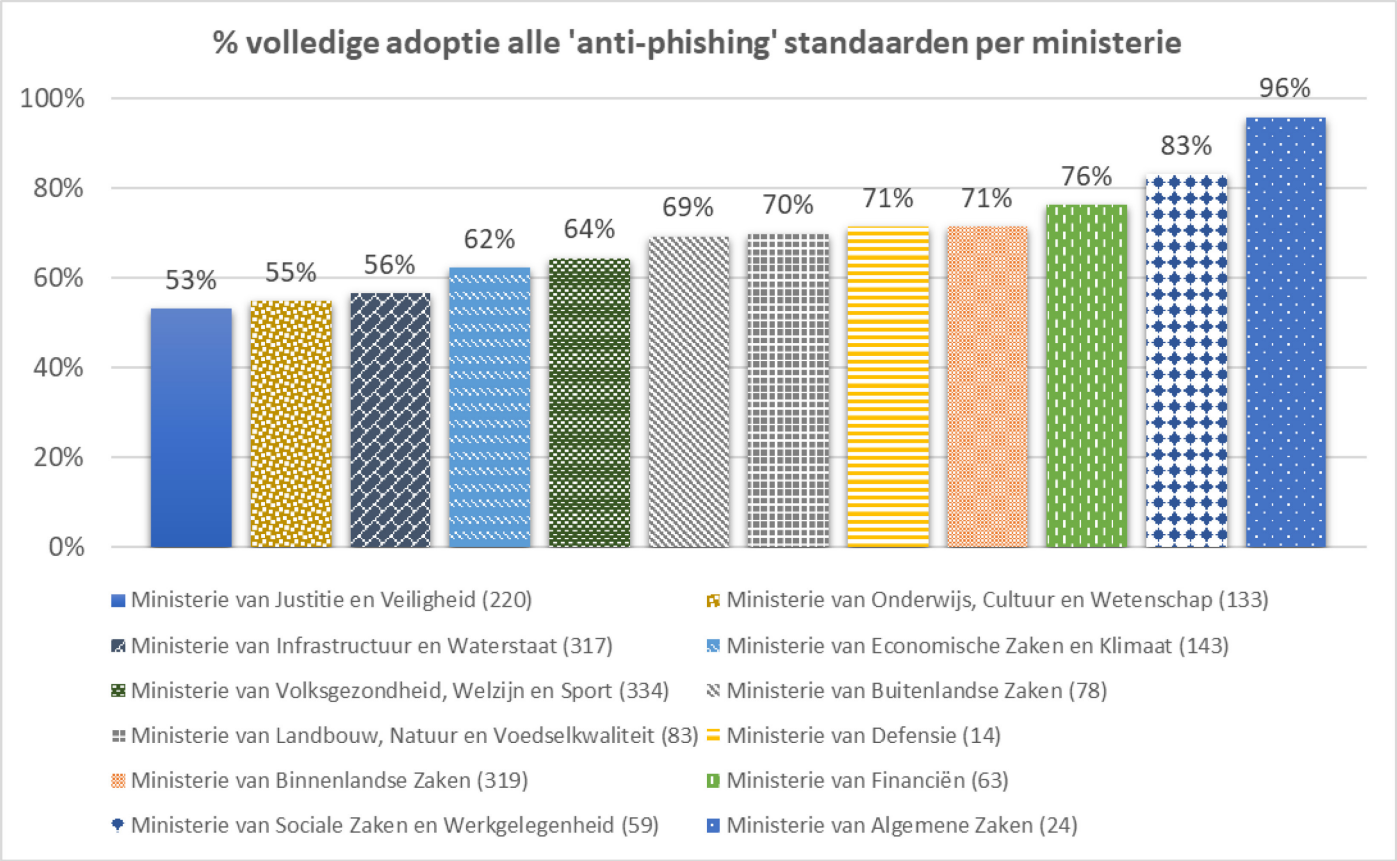
De waterschappen en gemeenten zijn positieve uitschieters in deze categorie. Wel gaat het bij deze categorieën voornamelijk om primaire domeinnamen. Er is geen inzicht in secundaire domeinnamen die in gebruik zijn, die waarschijnlijk gezamenlijk in de duizenden lopen. De gemeenschappelijke regelingen, waar lokale overheden vaak in participeren, scoren slecht met 40% goed geconfigureerde e-maildomeinen.



Voor meer details per overheidscategorie zie hoofdstuk 5.

1.3.2.2. Adoptie per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan vallen de ministeries van Algemene Zaken (96%) en Sociale Zaken en Werkgelegenheid (83%) positief op. Bijna alle ministeries met een portfolio kleiner dan 100 internetdomeinen scoren rond de 70% en hoger. Positieve opvaller met een portfolio groter dan 100 internetdomeinen is het ministerie van Binnenlandse Zaken met 71% volledige adoptie van anti-phishing standaarden voor haar portfolio van 319 gecontroleerde internetdomeinen. De ministeries van Justitie en Veiligheid (53%), Onderwijs, Cultuur en Wetenschap (55%), en Infrastructuur en Waterstaat (56%), hebben nog veel werk te verzetten om e-mailvervalsing namens haar domeinnamen te voorkomen.



Voor meer details per ministerie zie hoofdstuk 6.

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.

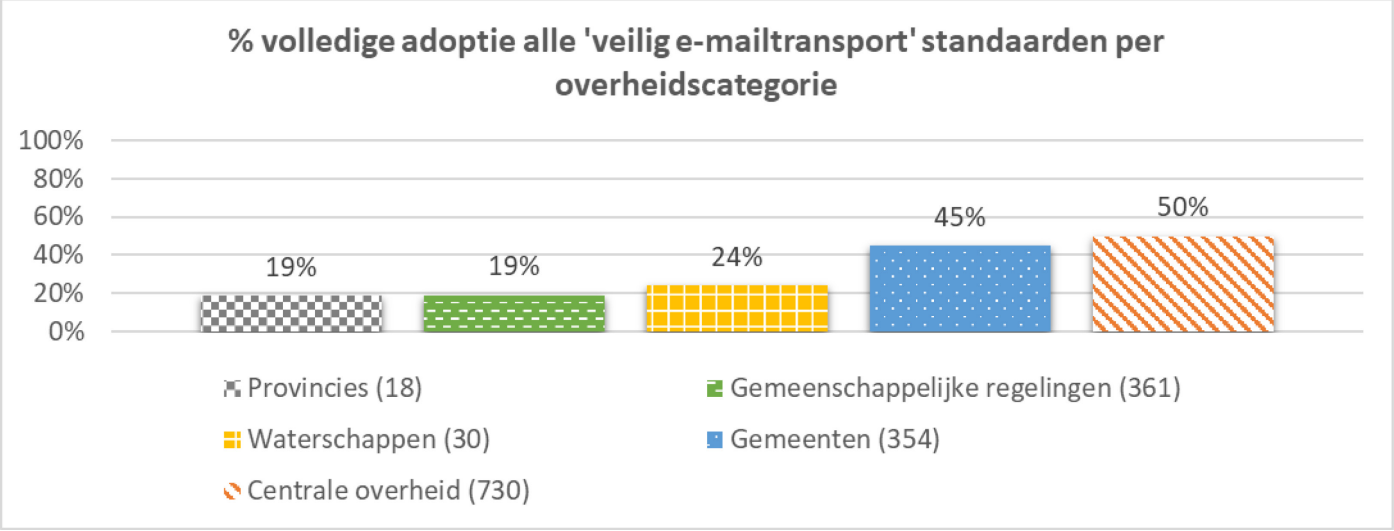
Omdat we alleen kunnen testen of de e-mailontvangst van de betreffende overheden voldoende veilig e-mailverkeer mogelijk maakt, hebben we internetdomeinen zonder een

ontvangende mailserver niet meegenomen in de statistieken. Hierdoor is het aantal gecontroleerde domeinen minder 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

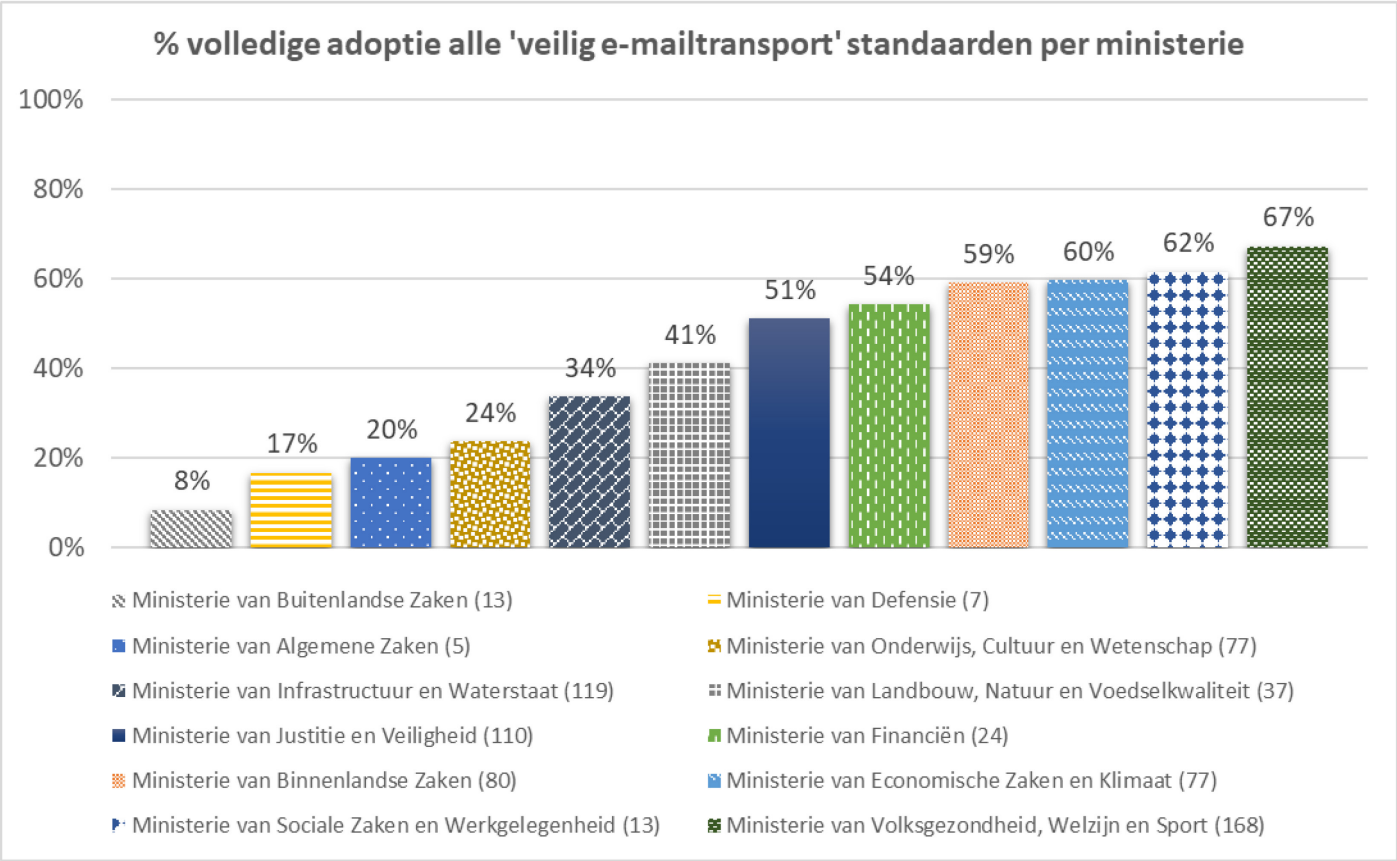
De centrale overheid en gemeenten scoren over het algemeen het beste op deze standaarden. Het gebruik van gemeenschappelijke e-maildienstverleners geeft daarbij een hefboomeffect. Lokale overheden maken veel meer gebruik van clouddiensten voor e-mailverkeer, die de standaarden DNSSEC en DANE over het algemeen niet ondersteunen. Dit is met name zichtbaar in de adoptiegraad bij provincies, gemeenschappelijke regelingen en waterschappen.



Voor meer details per overheidscategorie zie hoofdstuk 5.

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.



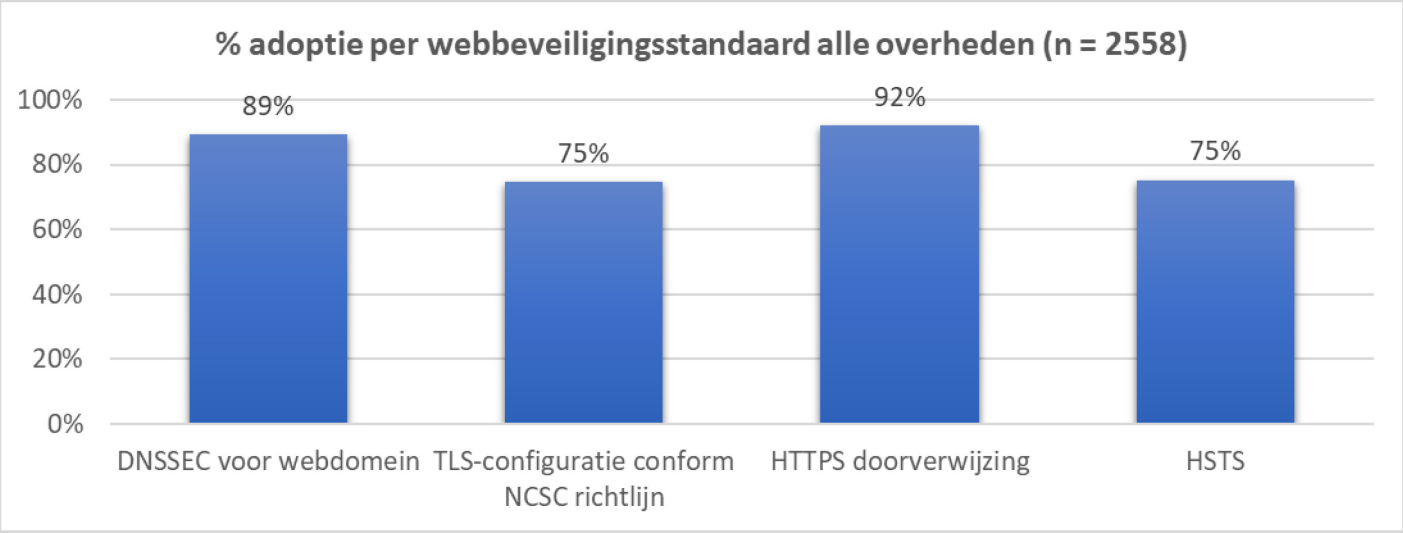
Voor meer details per ministerie zie hoofdstuk 6.

2. Adoptie per websitebeveiligingsstandaard

Dit hoofdstuk toont de algehele adoptiegraad per websitebeveiligingsstandaard.

Hoofdstukken 5 en 6 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.



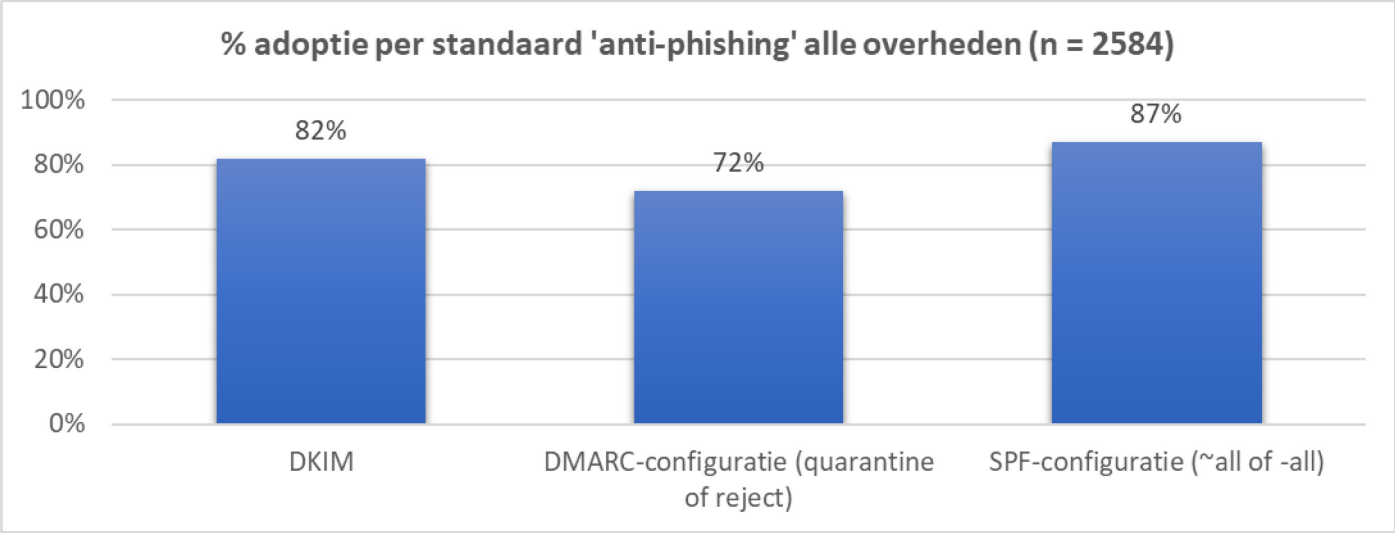
3. Adoptie per e-mailbeveiligingsstandaard

Dit hoofdstuk toont de algehele adoptiegraad per e-mailbeveiligingsstandaard.

Hoofdstukken 5 en 6 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 28% van de internetdomeinen nog een strikt DMARC-beleid worden ingesteld. Het streefbeeld was om dit eind 2019 voor elkaar te hebben.

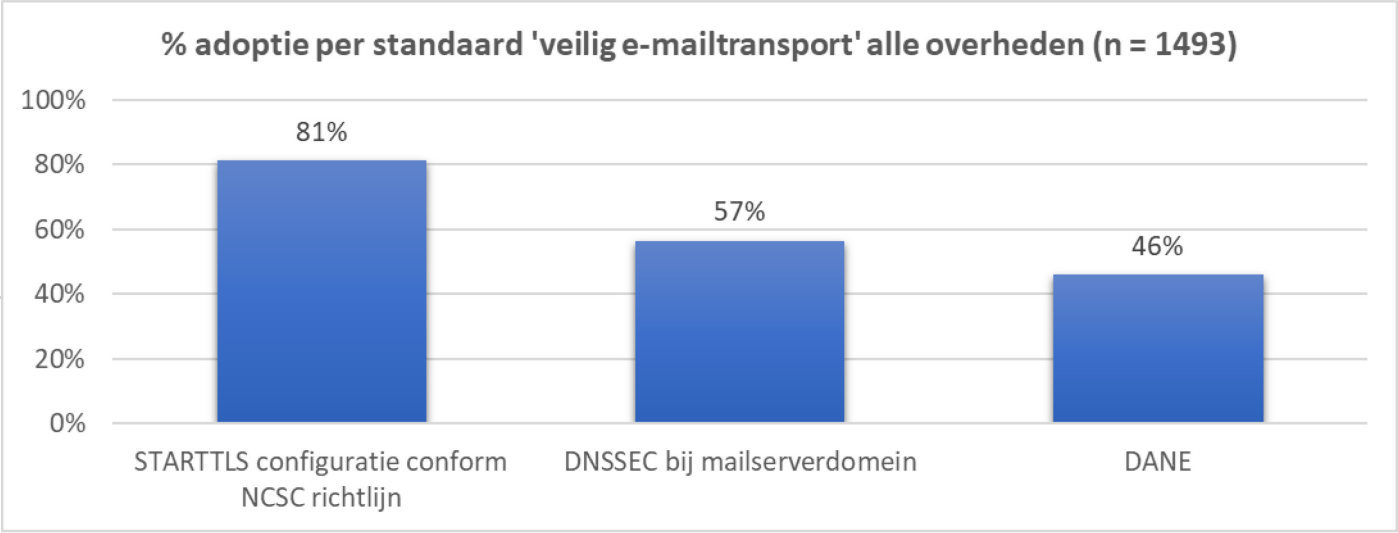


3.2. E-mailstandaarden voor vertrouwelijk e-mailverkeer

Bij één op de vijf 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 geauthenticeerde 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

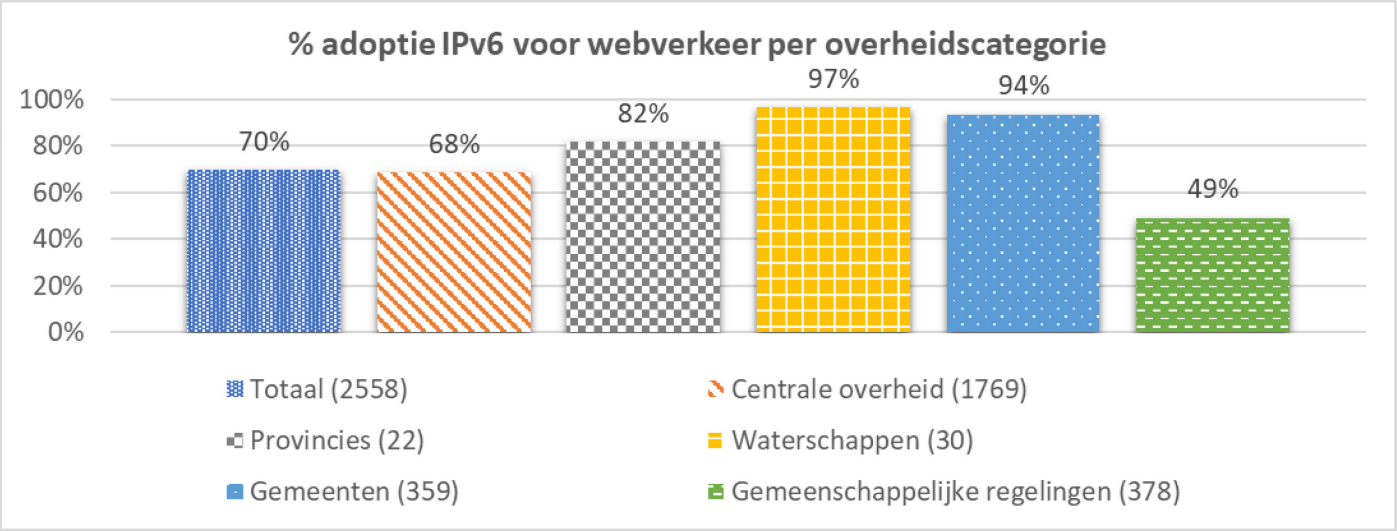
IPv6 is de open internetstandaard die iedere internetgebruiker nodig heeft om ook in de toekomst onbelemmerd gebruik te kunnen maken van internet. Er zijn verschillende goede redenen om voor IPv6 te kiezen, juist ook als overheid: groei en innovatie van internet, directere en snellere dienstverlening,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

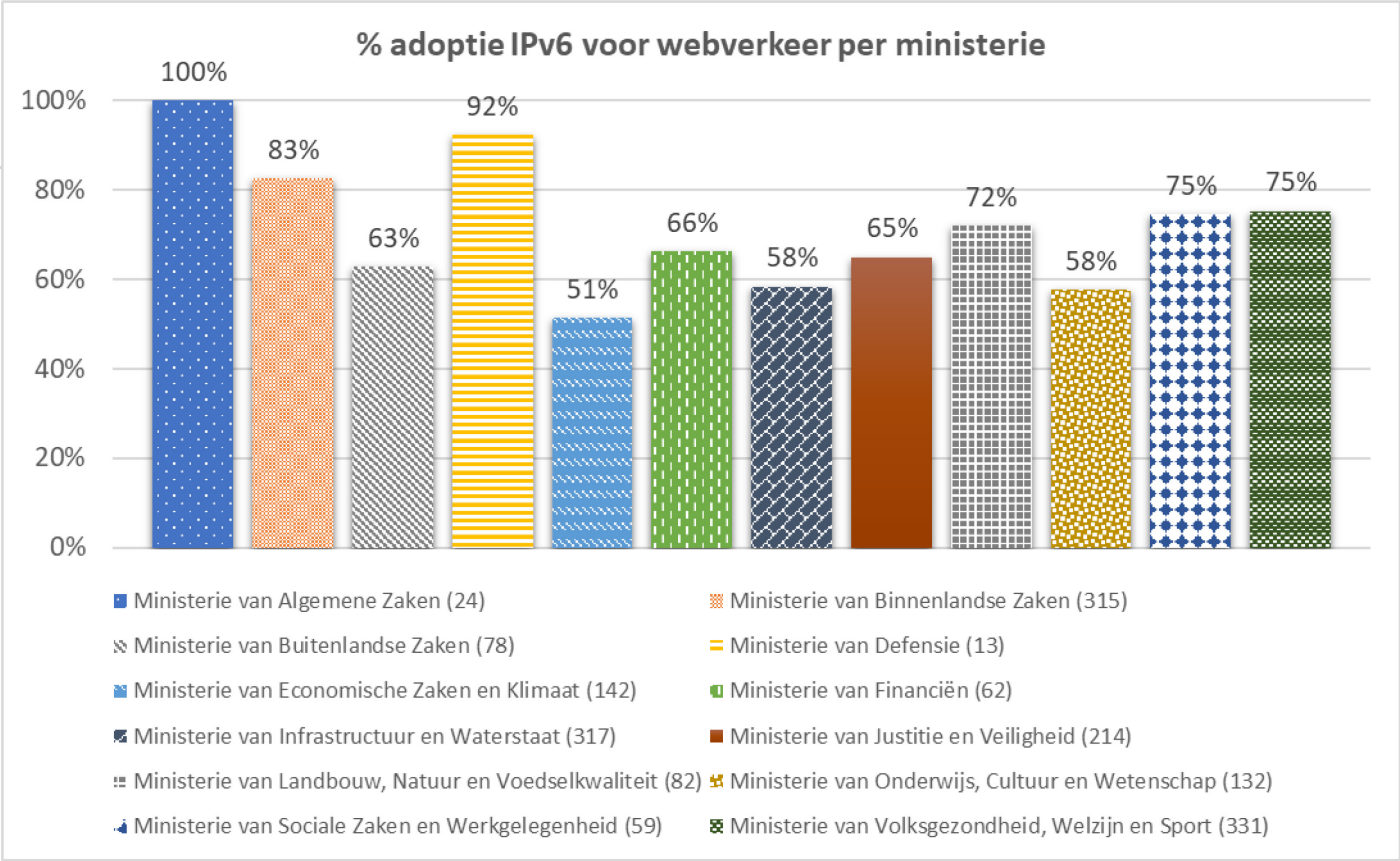
De gemeenschappelijke regelingen scoren ver onder de maat bij het gebruik van IPv6 voor webverkeer. De overheidsbrede afspraken hebben onvoldoende doorwerking gehad naar deze instanties, ondanks dat zij meestal gefinancierd worden vanuit de andere overheden.

De centrale overheid scoort relatief lager dan de andere lokale overheden. Dat komt doordat er onevenredig veel secundaire webdomeinen in deze categorie zijn meegenomen. Deze secundaire webdomeinen zijn vaak gehost bij externe dienstverleners die niet goed aangestuurd zijn op het toepassen van IPv6 voor websites en webapplicaties.



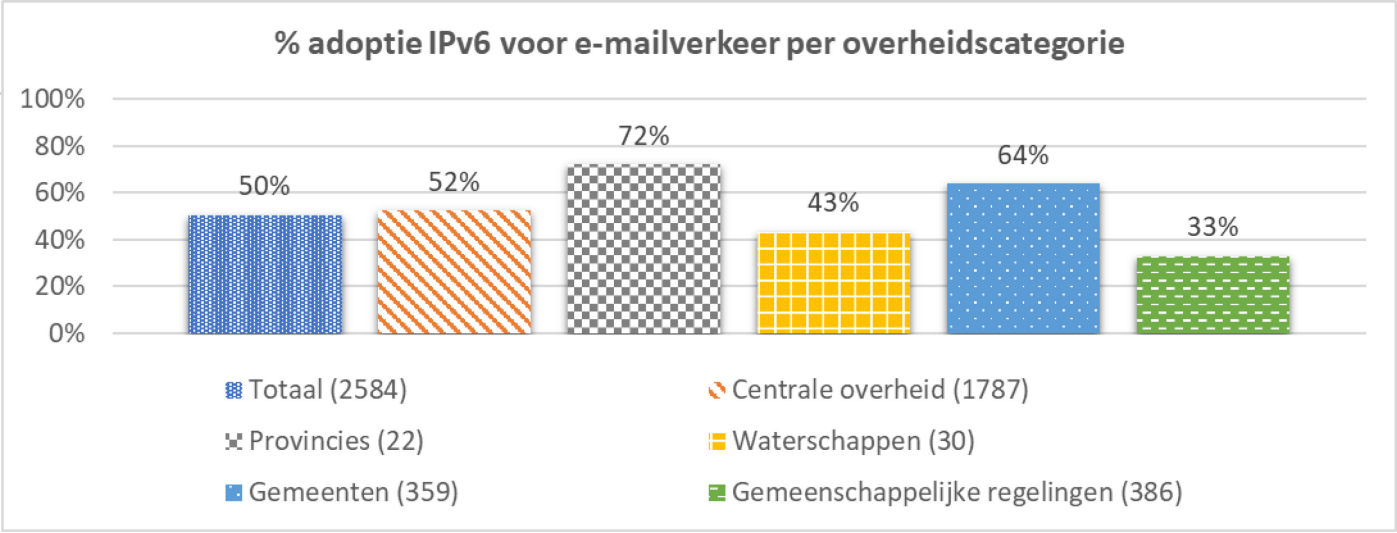
4.2. IPv6 voor webverkeer per ministerie

Positieve uitschieters – met een klein webportfolio – zijn de ministeries van Algemene Zaken (100%) en Defensie (92%). Negatieve opvaller is het ministerie van Economische Zaken (51%), terwijl dit beleidsmatig de aanjager is van IPv6 richting het bedrijfsleven. Dit ministerie heeft nog een uitdaging om de voorbeeldfunctie waar te maken.



4.3. IPv6 voor e-mailverkeer per overheidscategorie

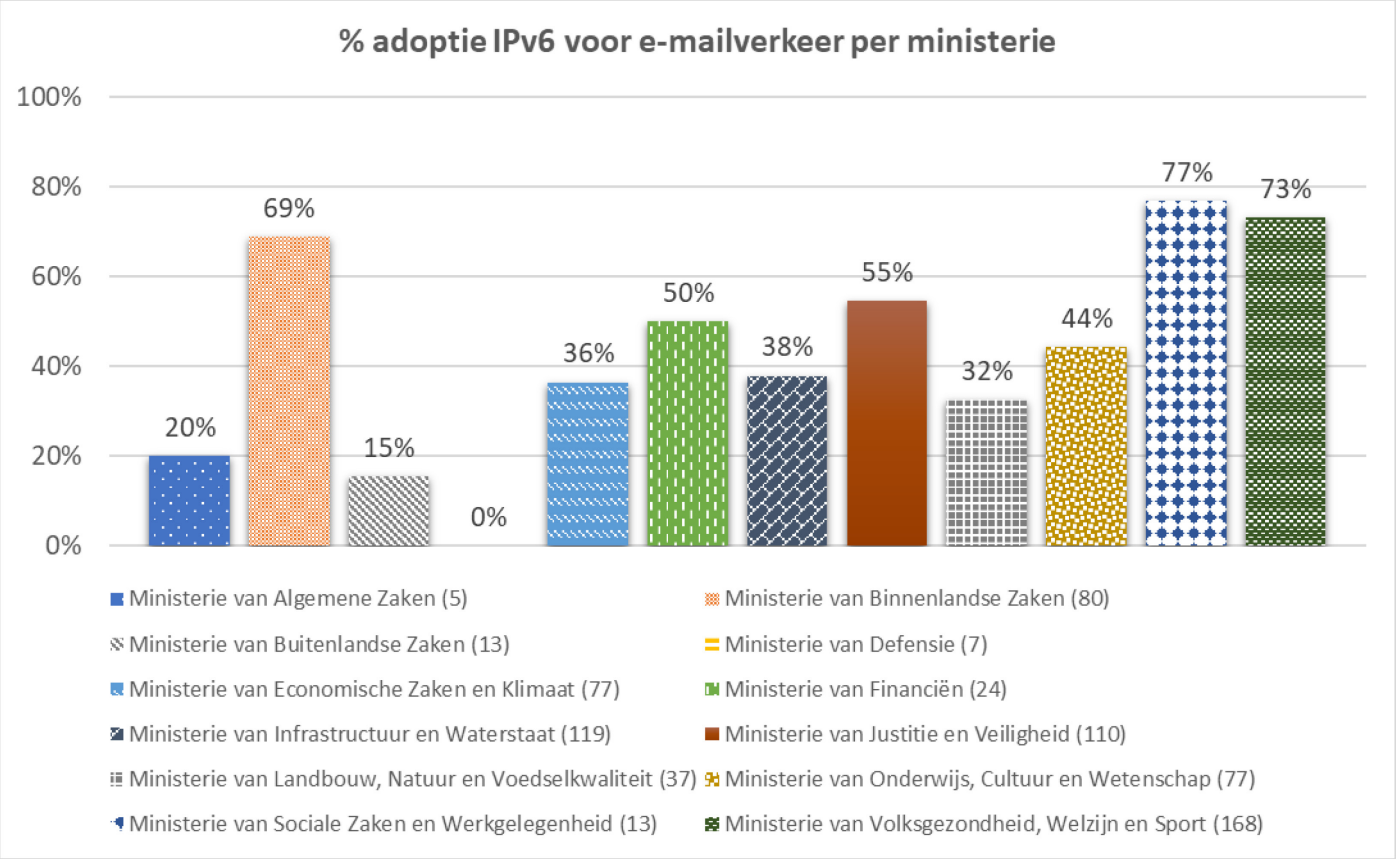
Ook bij het gebruik van IPv6 voor e-mailverkeer scoren de gemeenschappelijke regelingen ver onder de maat met een adoptiegraad van slechts 33%. Ook de waterschappen komen daar niet ver boven met 43%. Vermoedelijk zit er voor de centrale overheid (52%) nog rek in het adoptiepercentage door ongebruikte mailservers uit de domeinconfiguratie te verwijderen.



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 op, die helemaal geen IPv6 e-mailverkeer mogelijk maakt. Ook de ministeries van Buitenlandse Zaken (15%) en Algemene Zaken (20%) hebben ondanks een klein portfolio aan ontvangen e-maildomeinen een erg lage adoptiegraad.

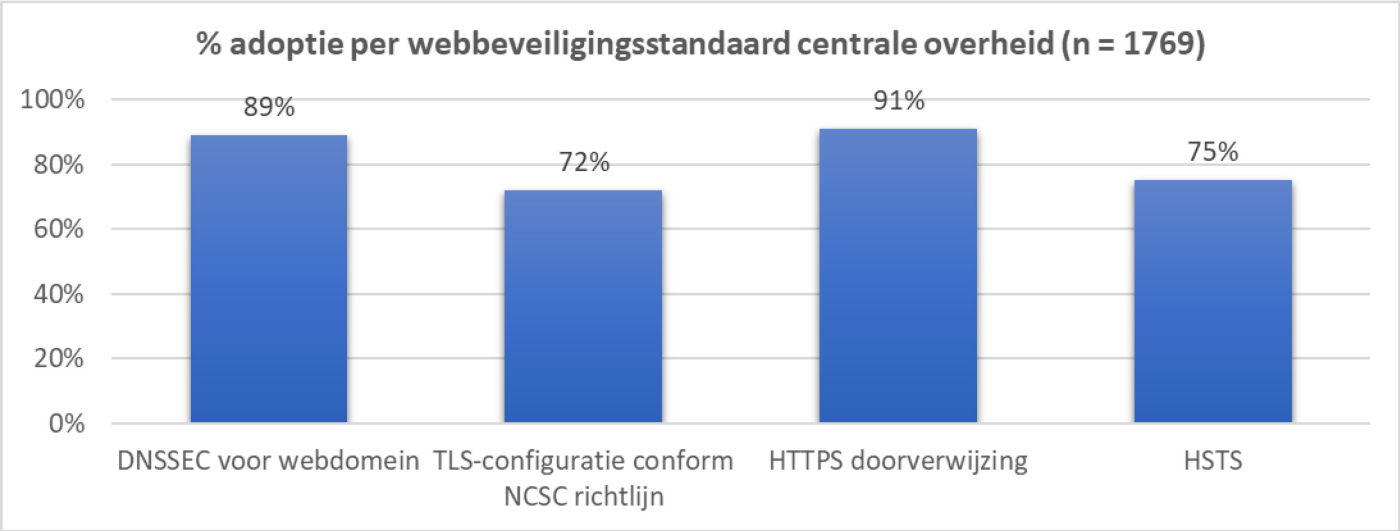
Positieve opvallers zijn de ministeries met een proactieve (projectmatige) sturing op toepassing van standaarden. Het gaat daarbij om de ministeries van Sociale Zaken en Werkgelegenheid (77%), Volksgezondheid, Welzijn en Sport (73%), en Binnenlandse Zaken en Koninkrijksrelaties (69%).

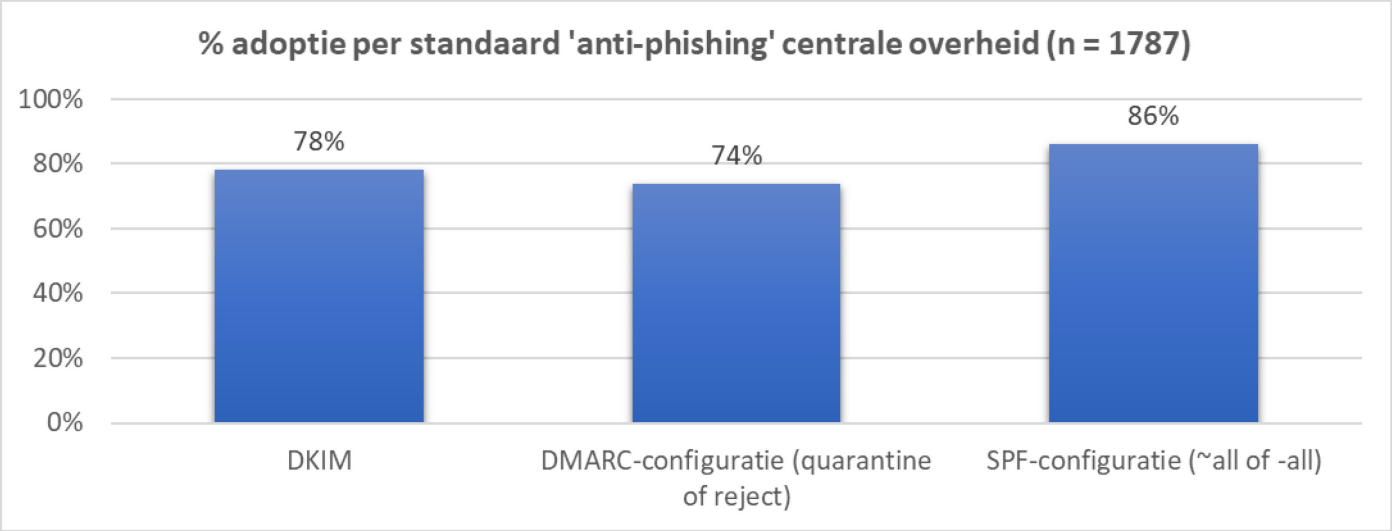


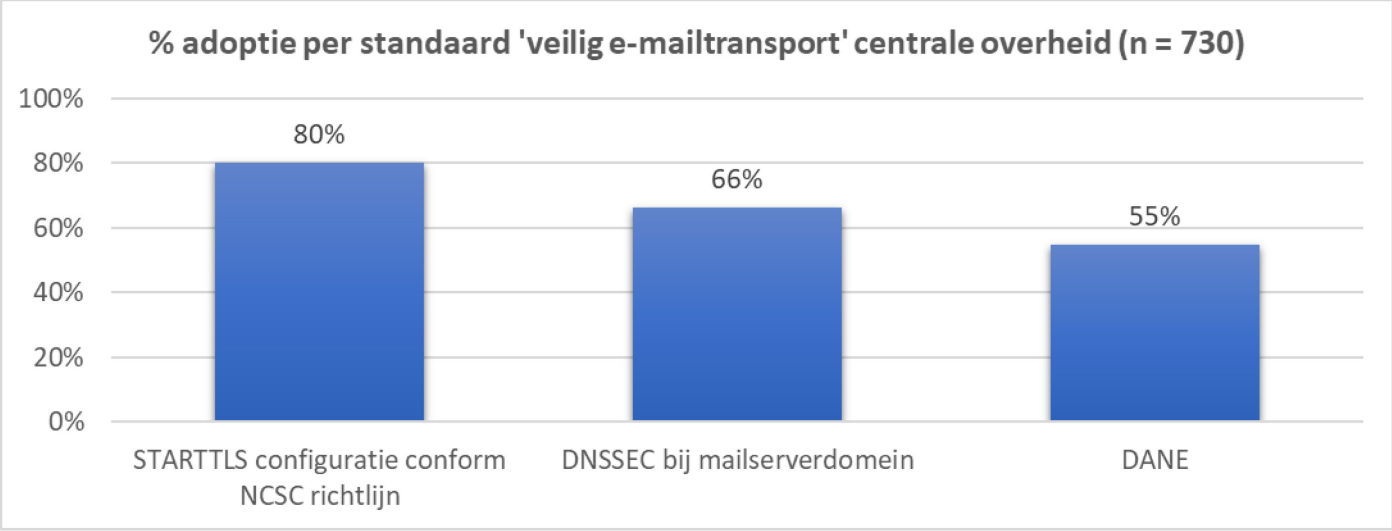
5. Adoptie per overheidscategorie

De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per overheidscategorie.

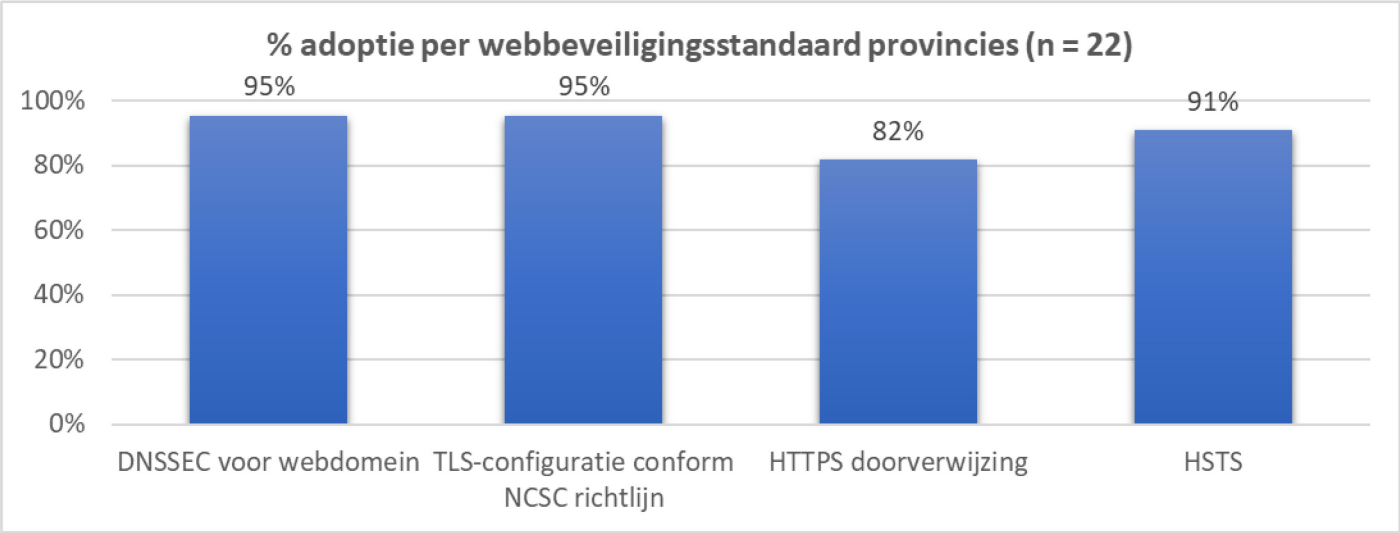
5.1. Centrale overheid

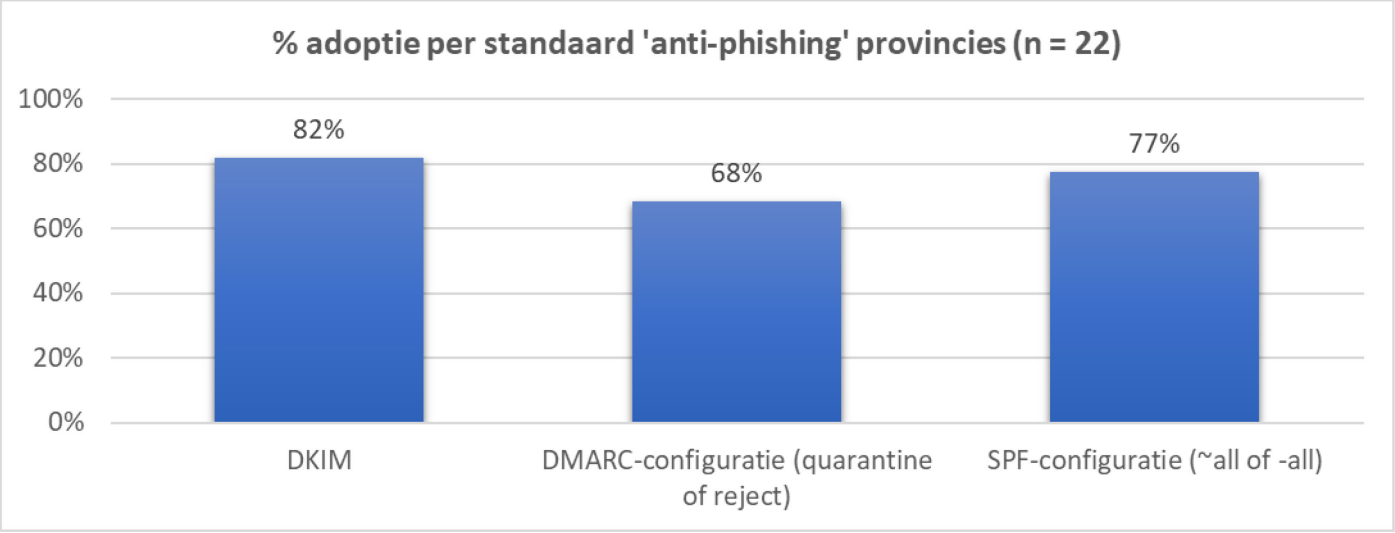


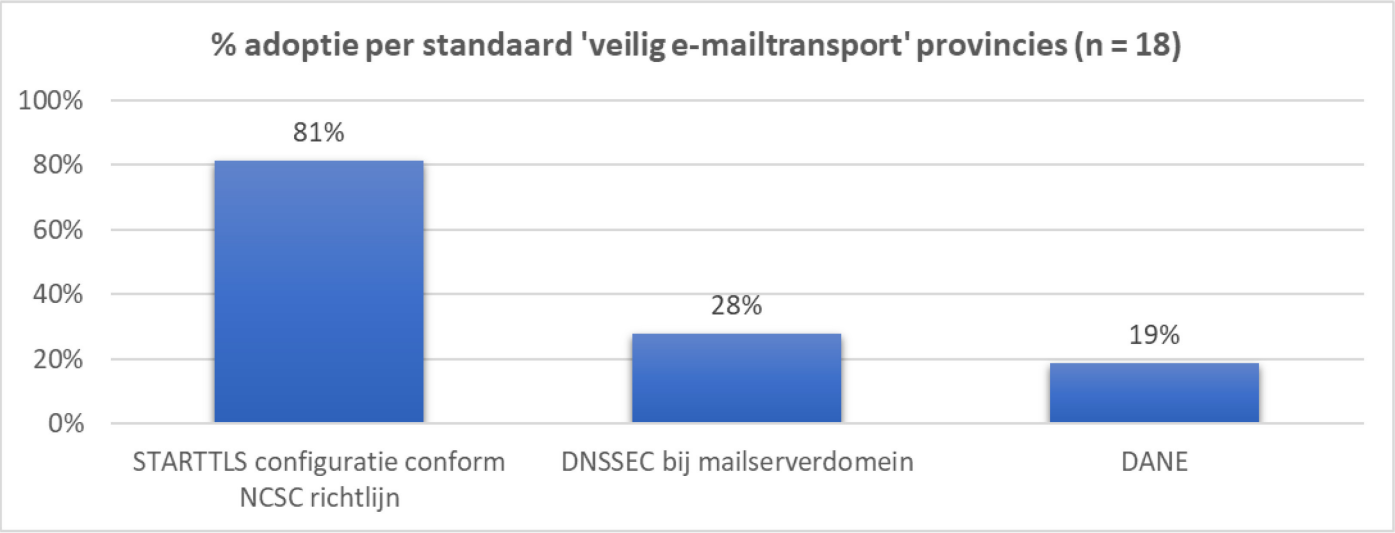




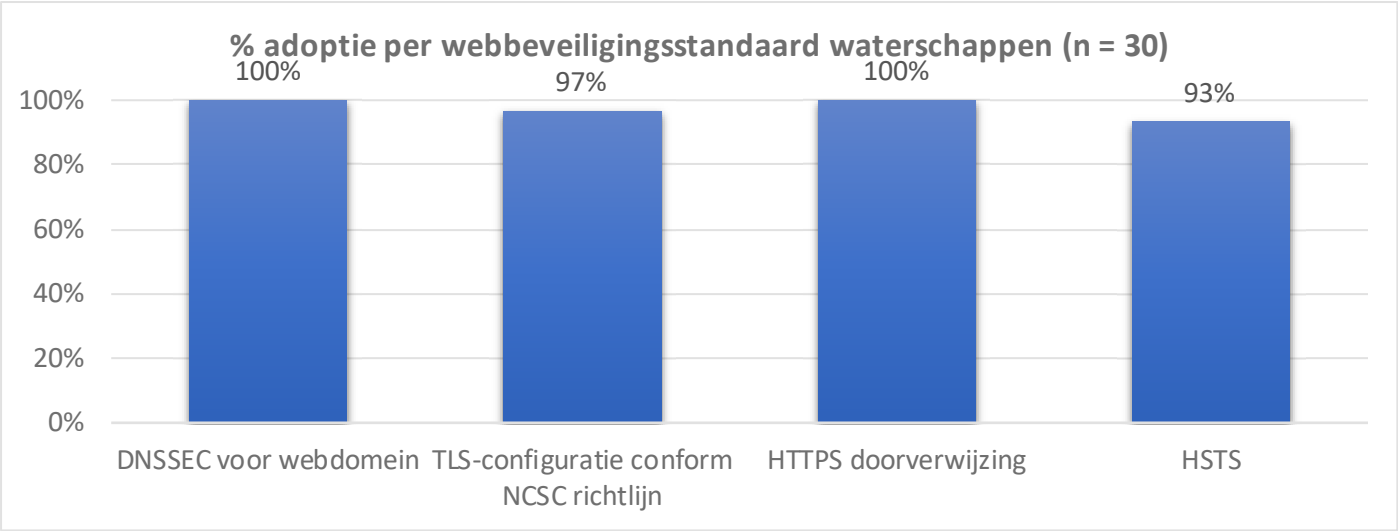
5.2. Provincies

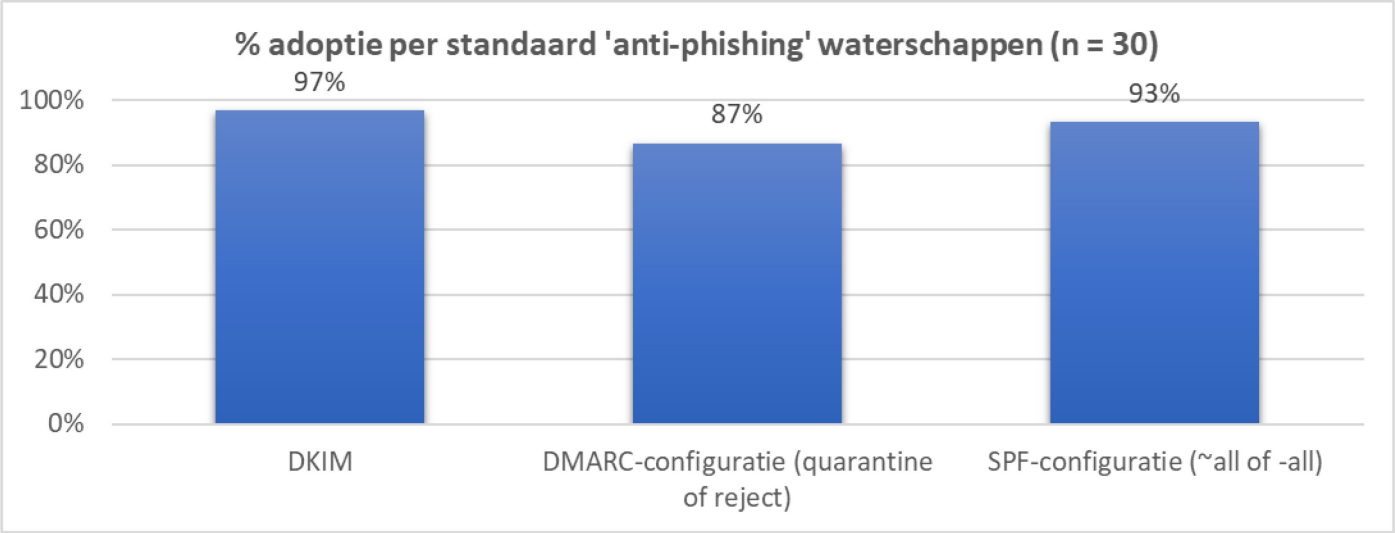


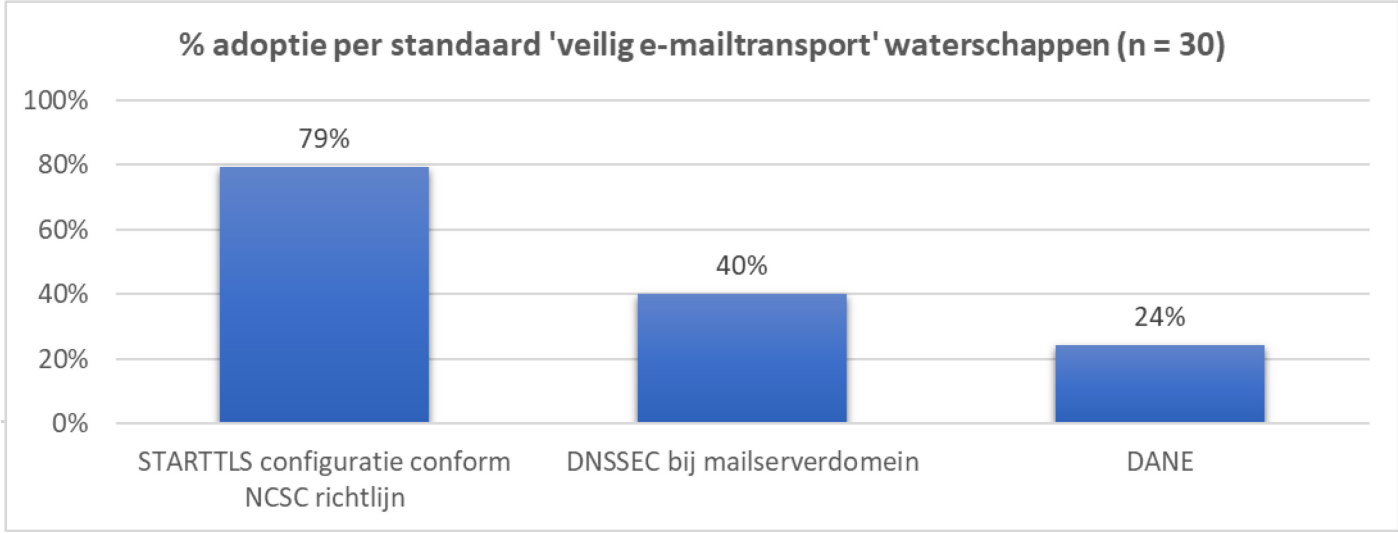




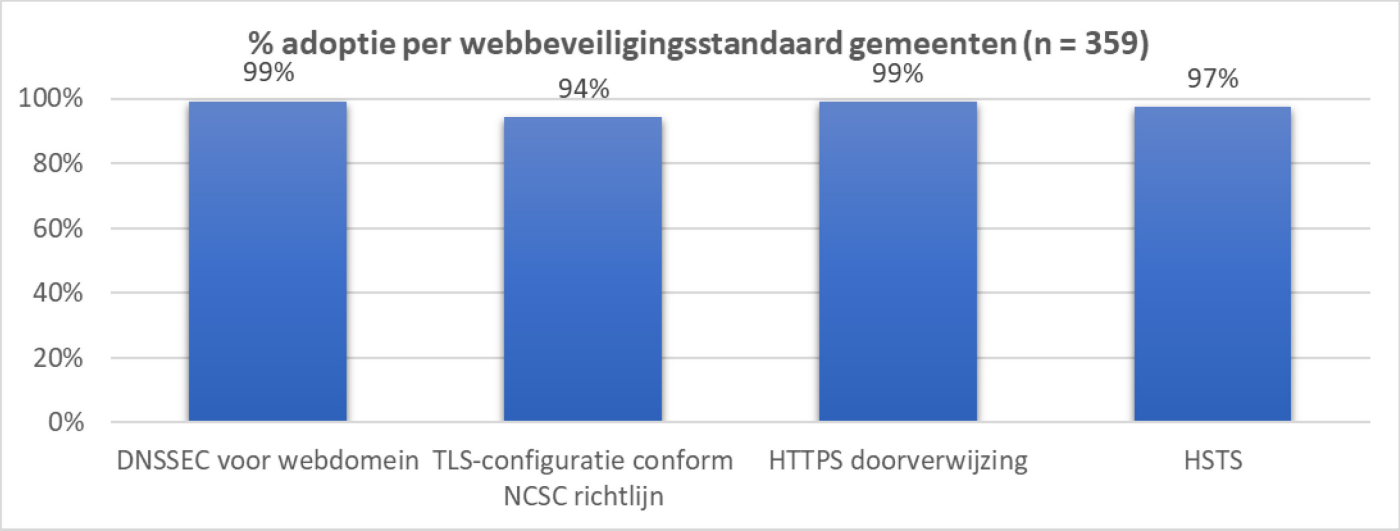
5.3. Waterschappen

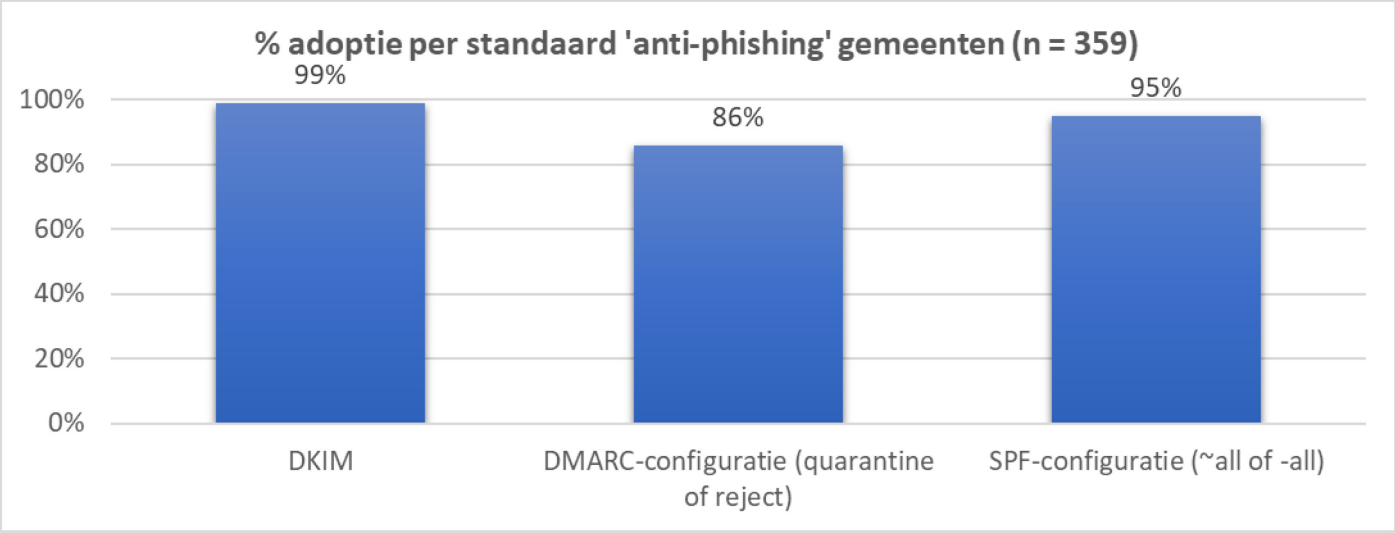


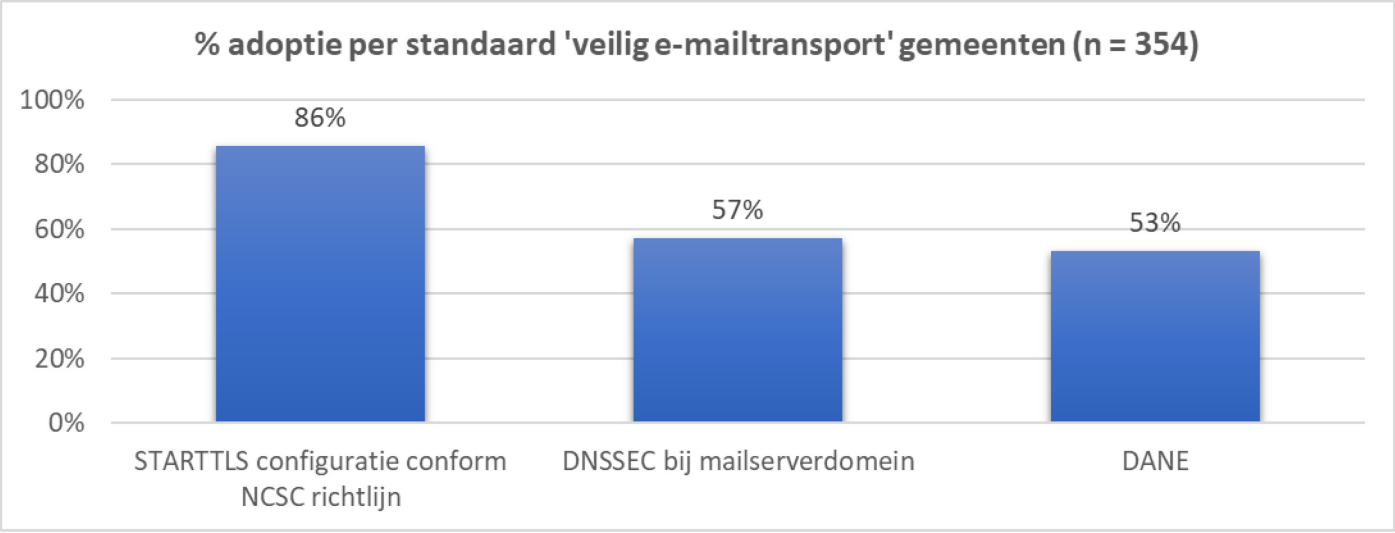




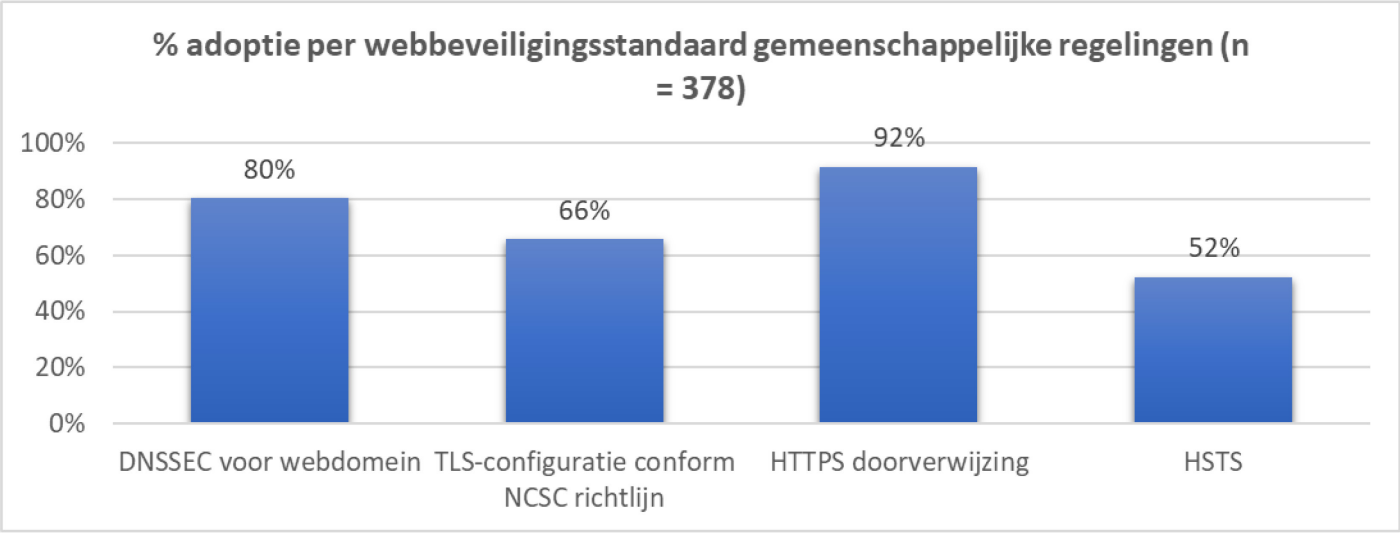
5.4. Gemeenten

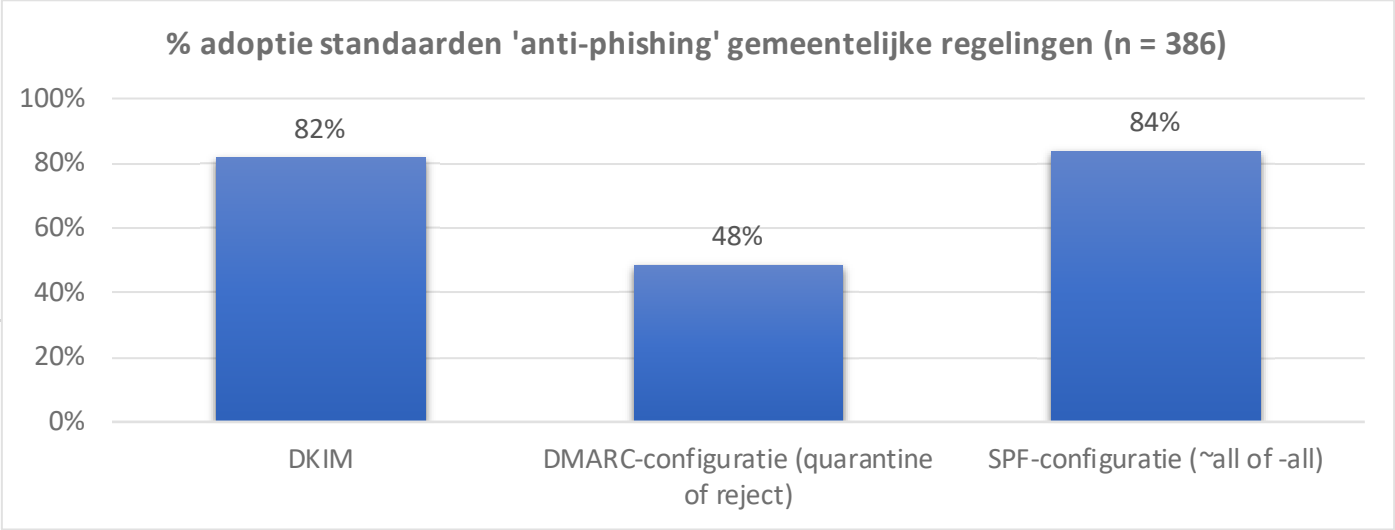


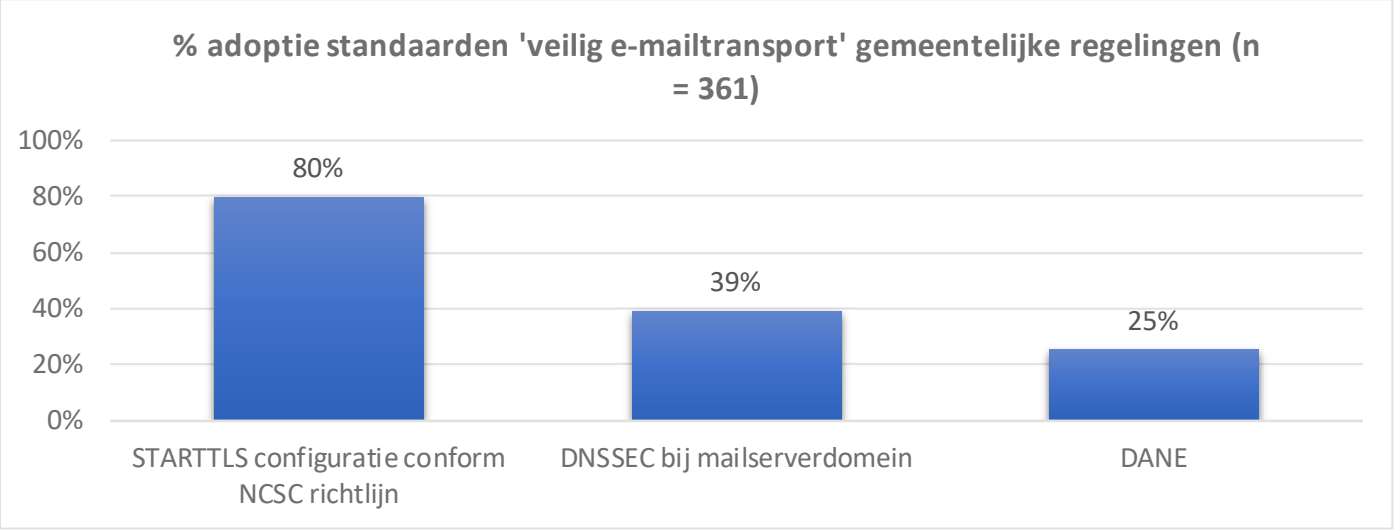




5.5. Gemeenschappelijke regelingen



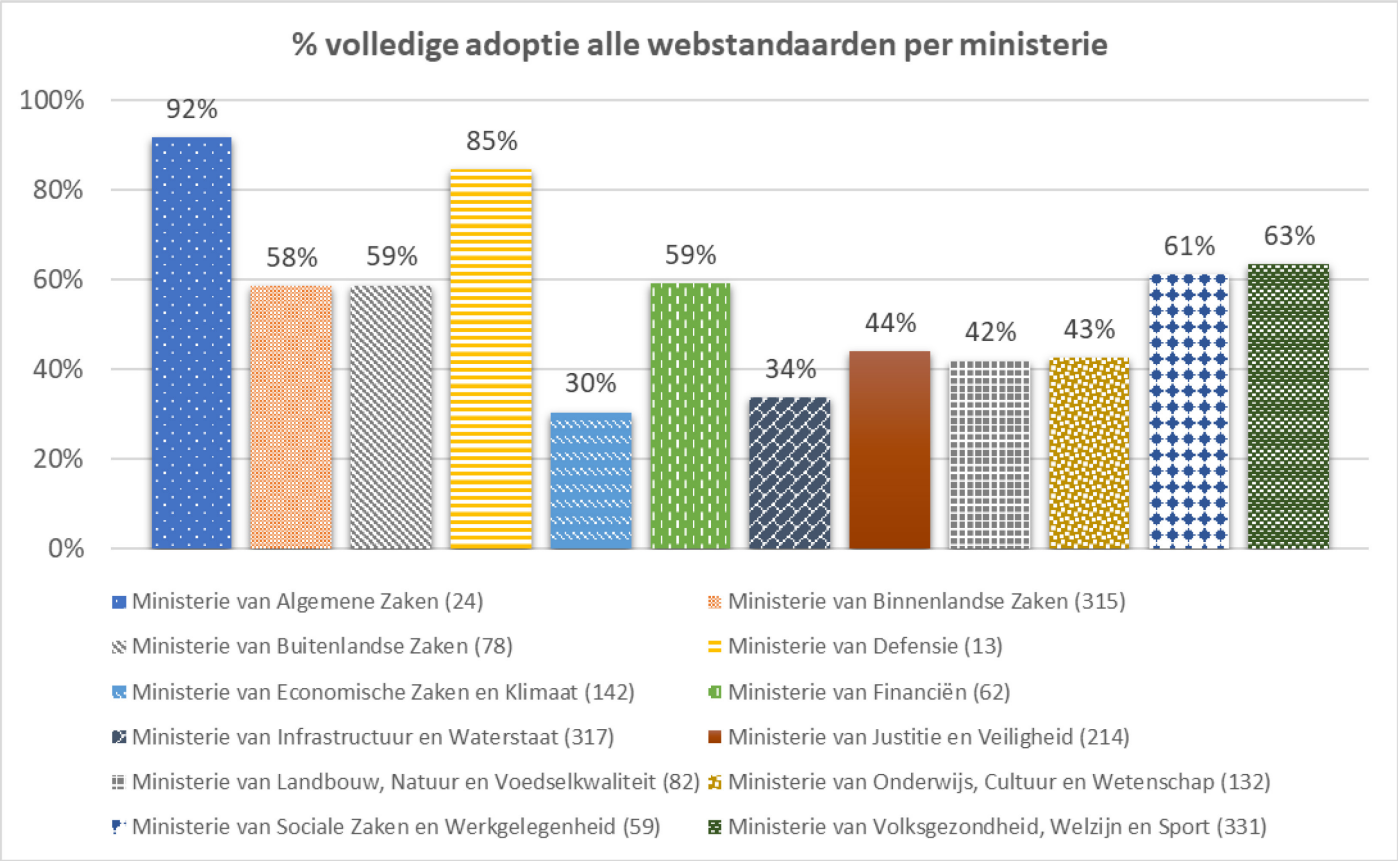




6. Adoptie per ministerie

6.1. Totaalbeeld websitestandaarden (incl. IPv6)

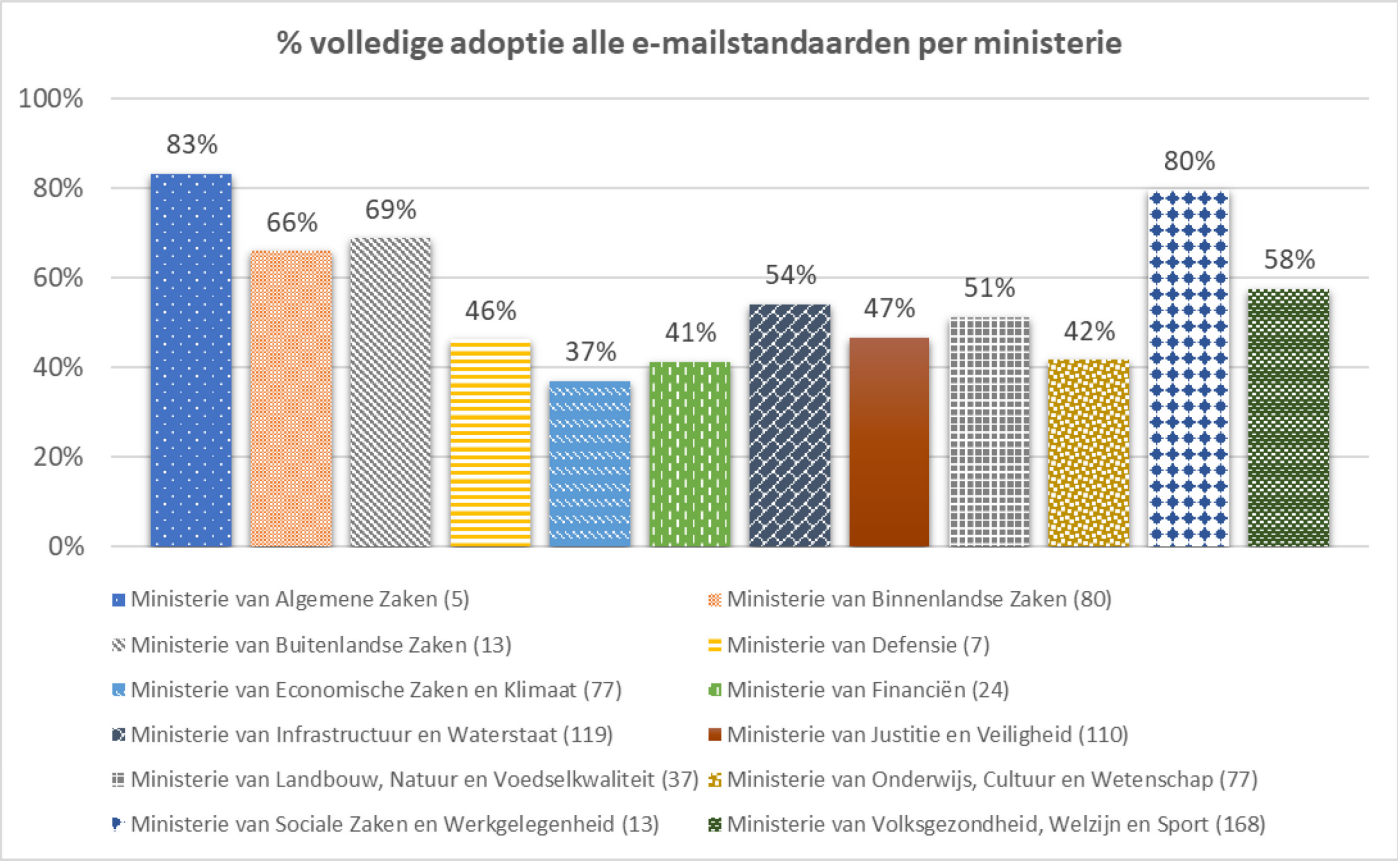
Onderstaande cijfers laten zien in welke mate de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – *alle* afgesproken websitestandaarden voor veilig en modern webverkeer toepassen (inclusief IPv6).



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. De ministeries van Binnenlandse Zaken en Volksgezondheid hebben een relatief hoge adoptiegraad afgezet tegen de hoge omvang van hun portfolio. Dit komt omdat zij in de voorgaande jaren actief (projectmatig) hebben gestuurd op toepassing van standaarden.

6.2. Totaalbeeld e-mailstandaarden (incl. IPv6)

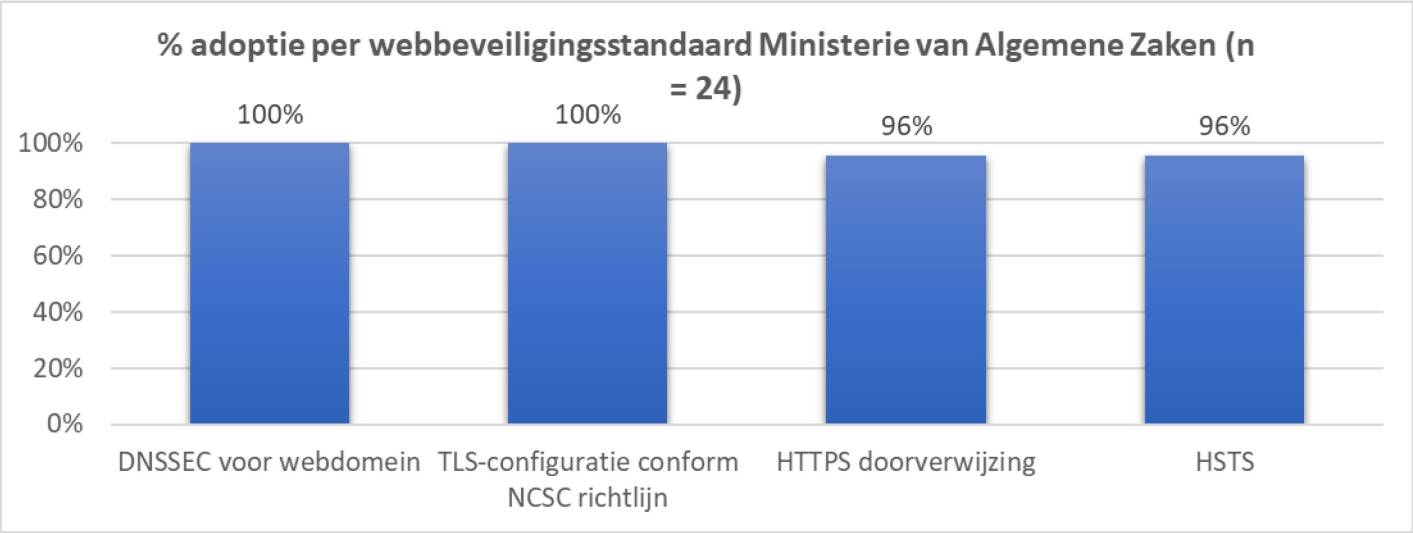
Onderstaande cijfers laten zien in welke mate de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – *alle* afgesproken e-mailstandaarden voor veilig en modern e-mailverkeer toepassen (inclusief IPv6).

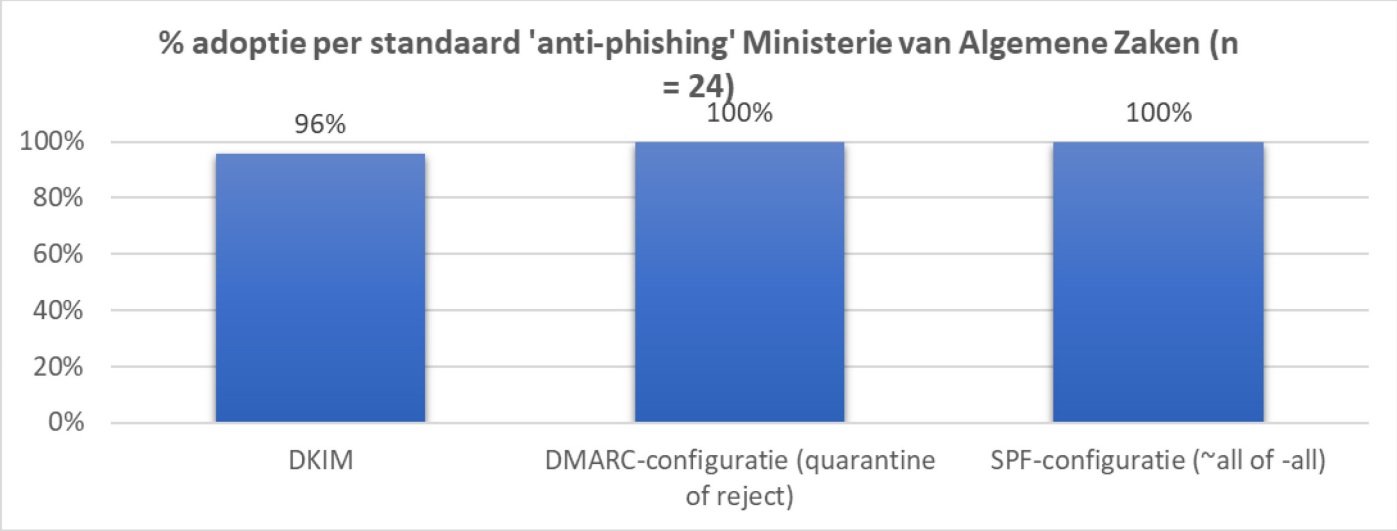


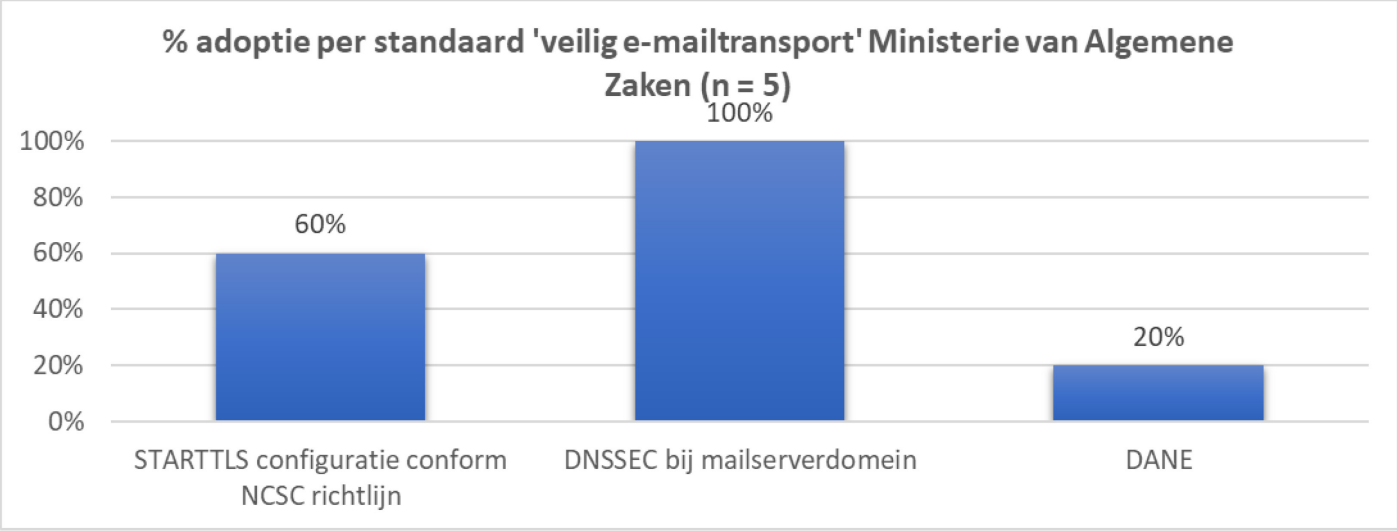
Vergelijkbaar met de adoptie van websitestandaarden, zien we dat ministeries met een beperkt portfolio, of actieve sturing op toepassing van standaarden, over het algemeen een hogere adoptiegraad bereiken.

De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per ministerie.

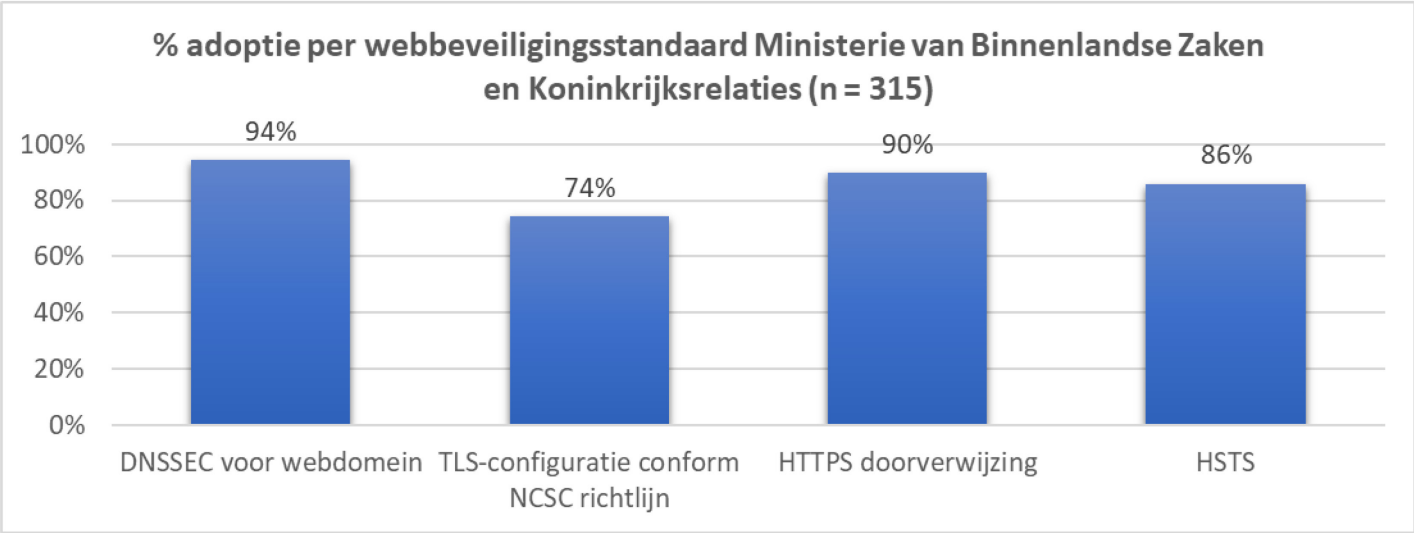
6.3. Ministerie van Algemene Zaken

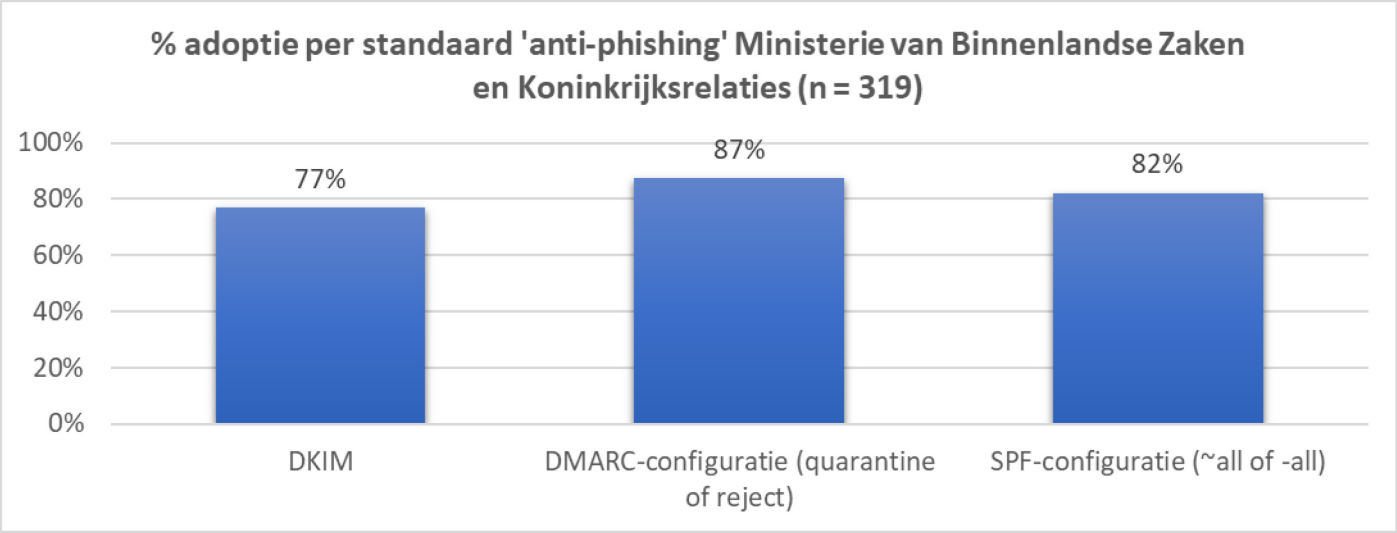


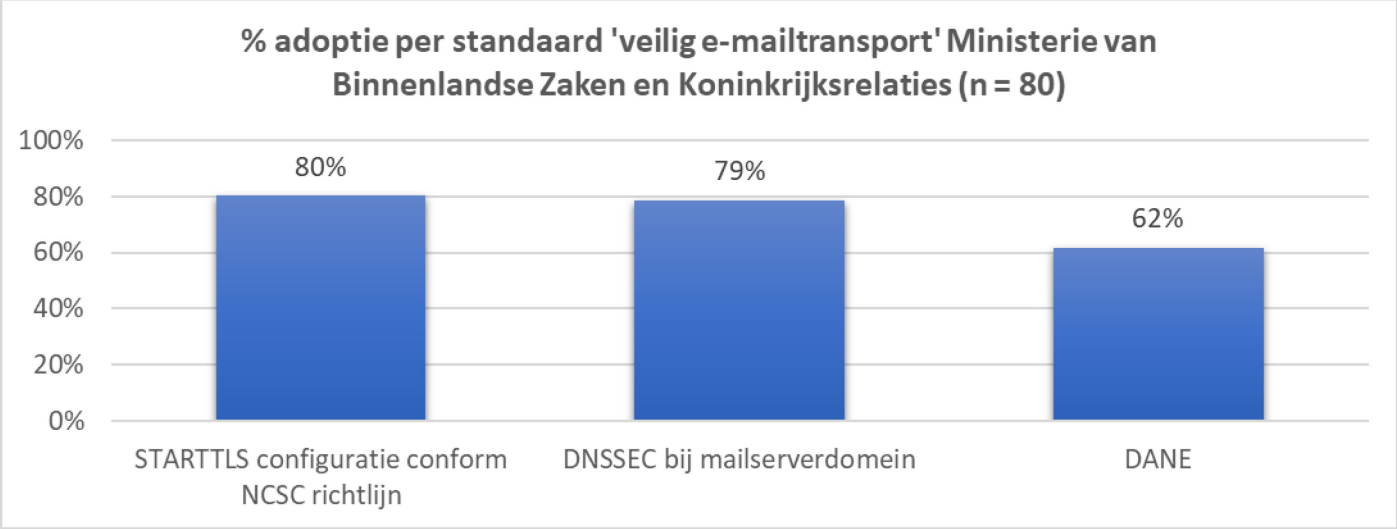




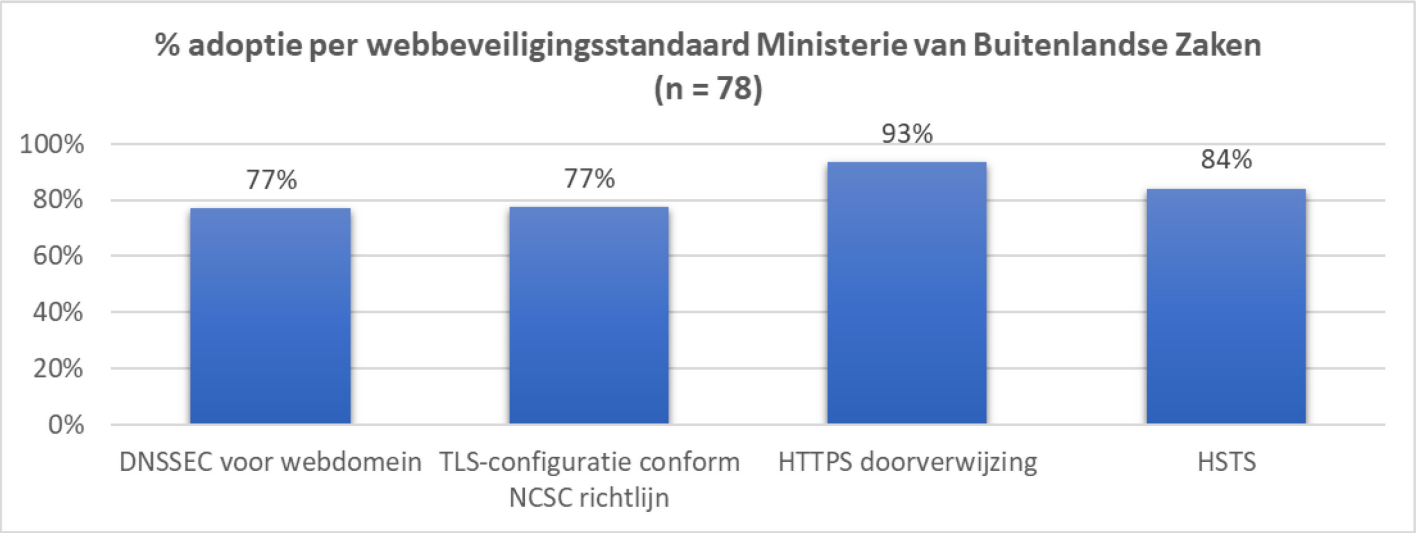
6.4. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

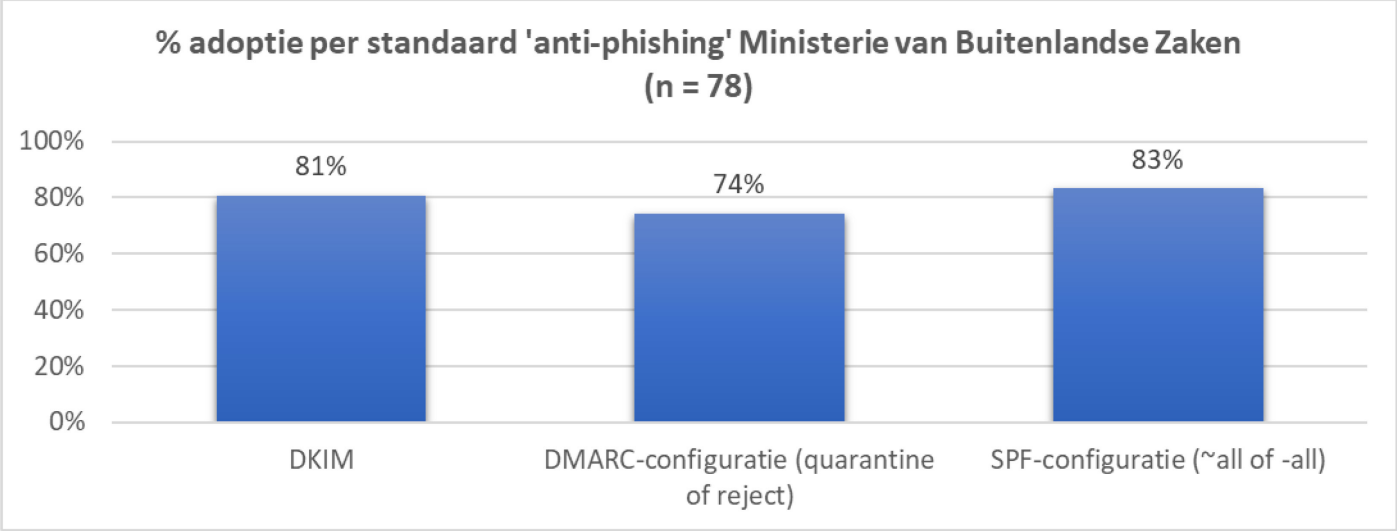


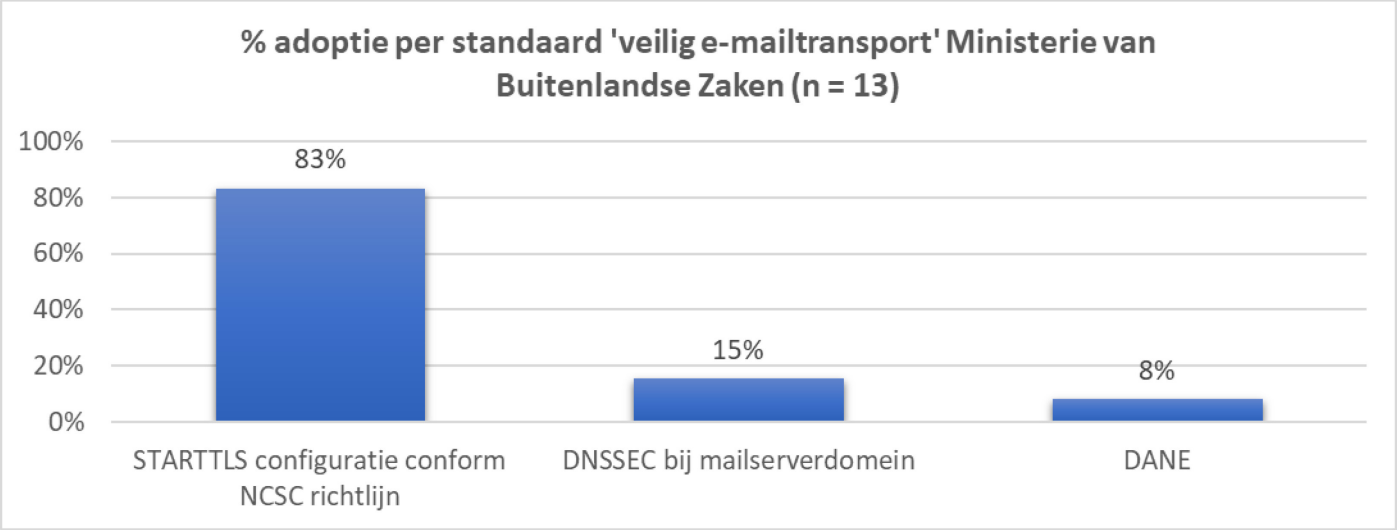




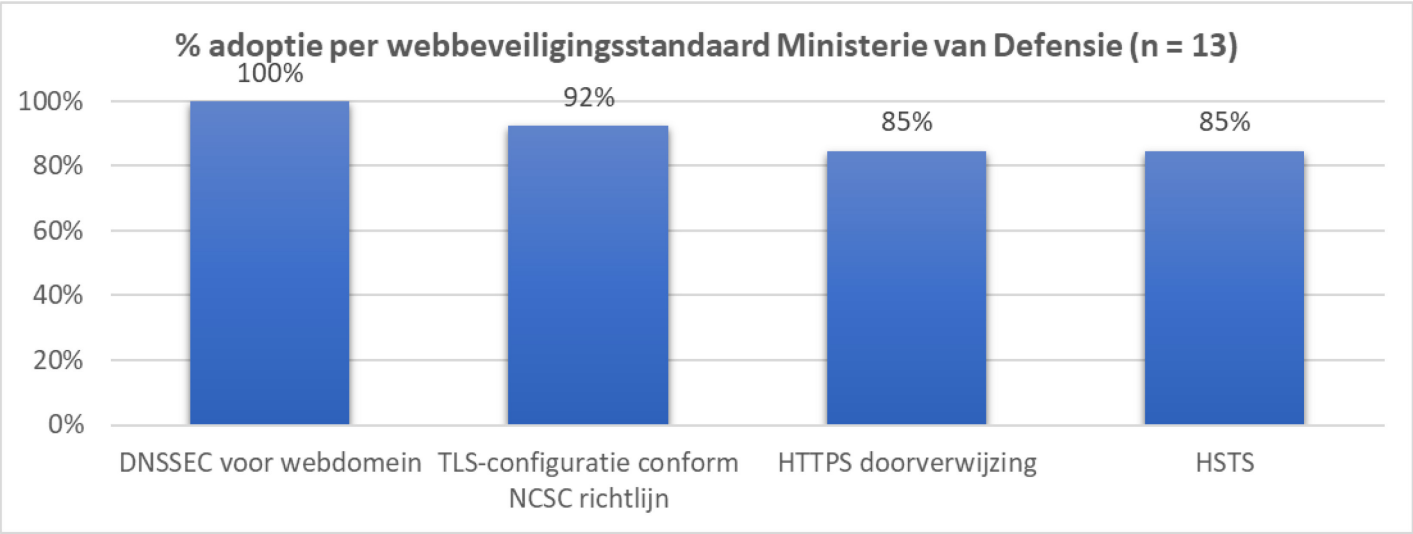
6.5. Ministerie van Buitenlandse Zaken

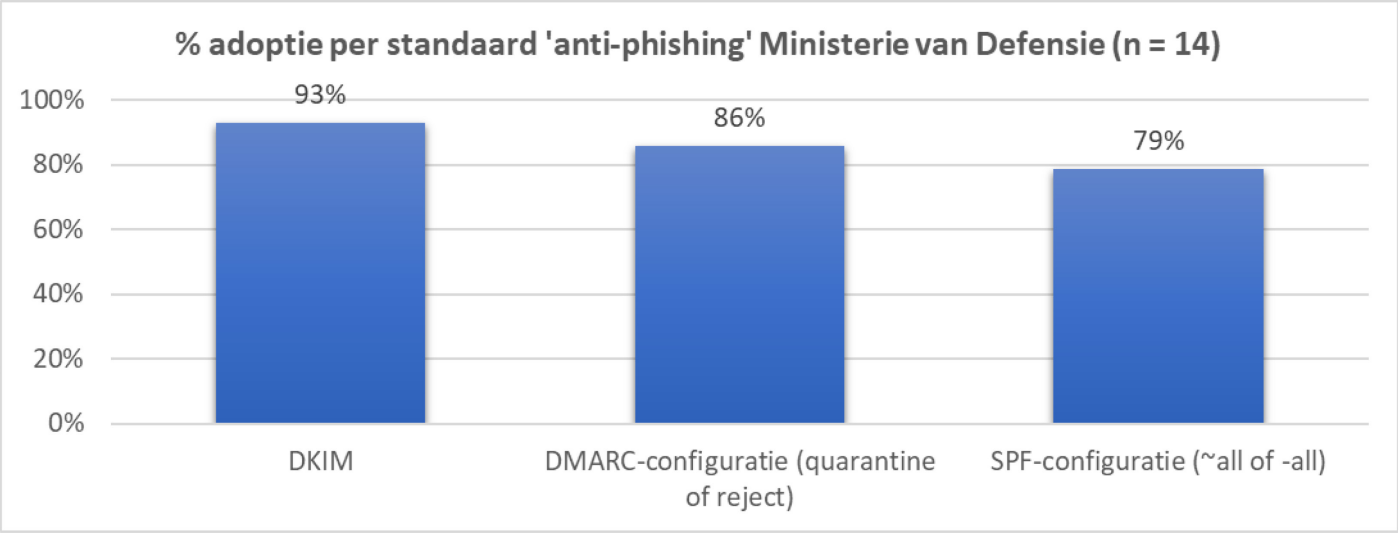


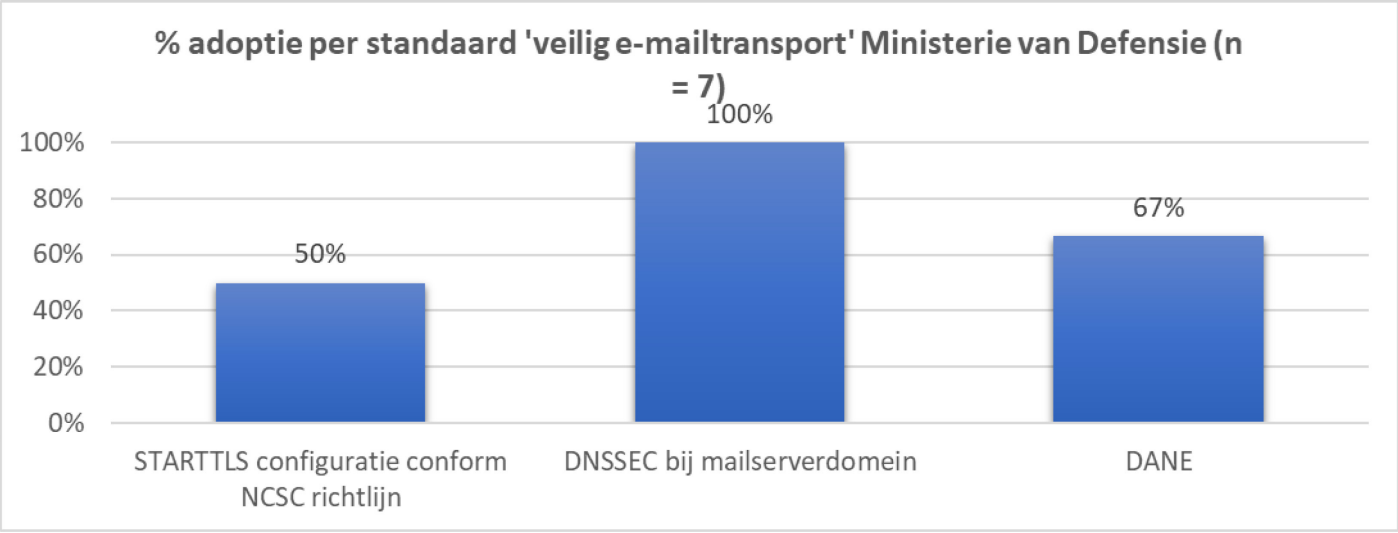




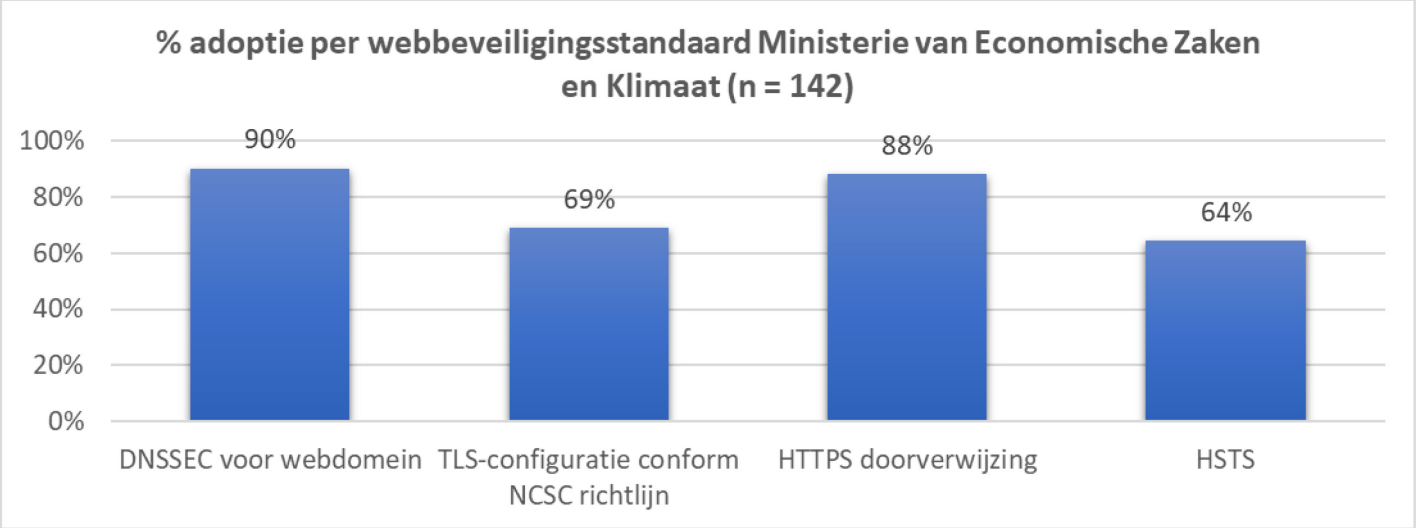
6.6. Ministerie van Defensie

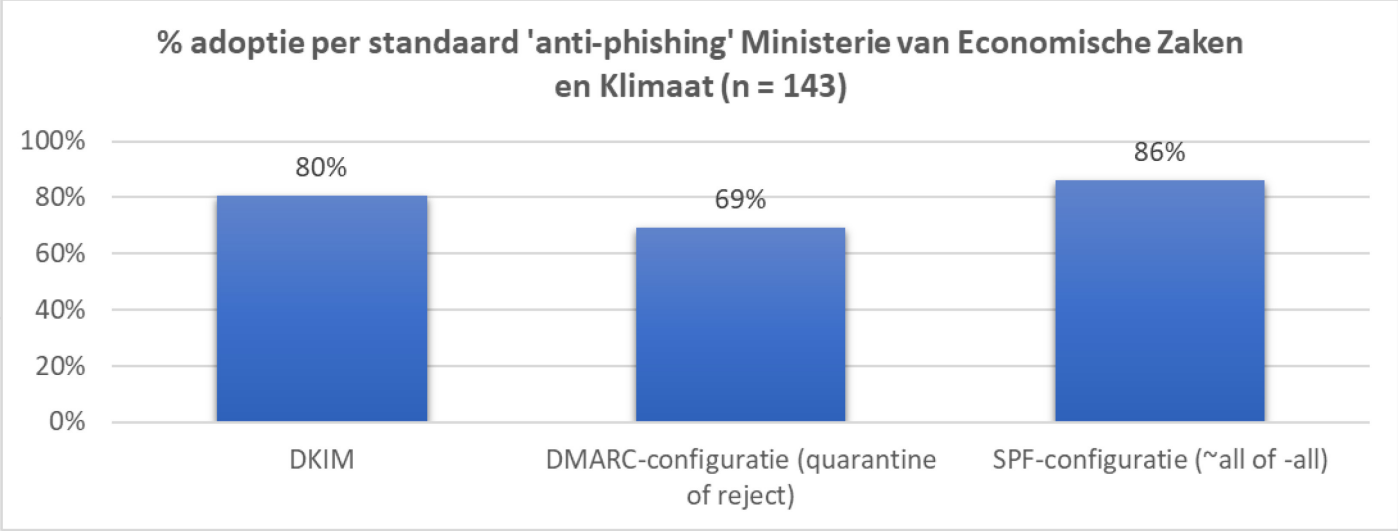


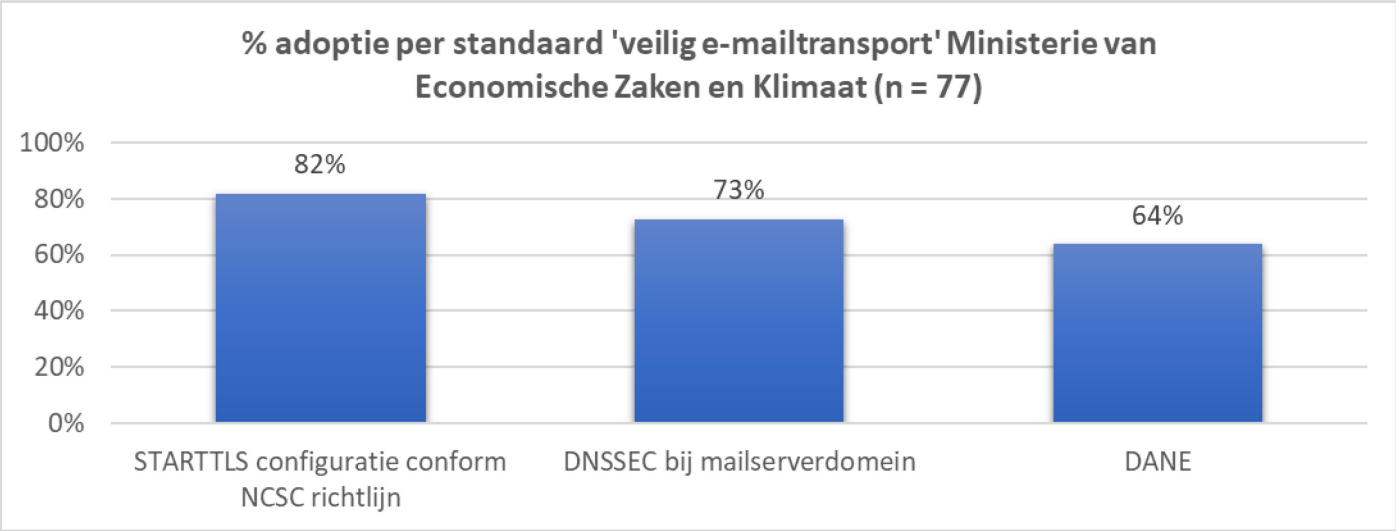




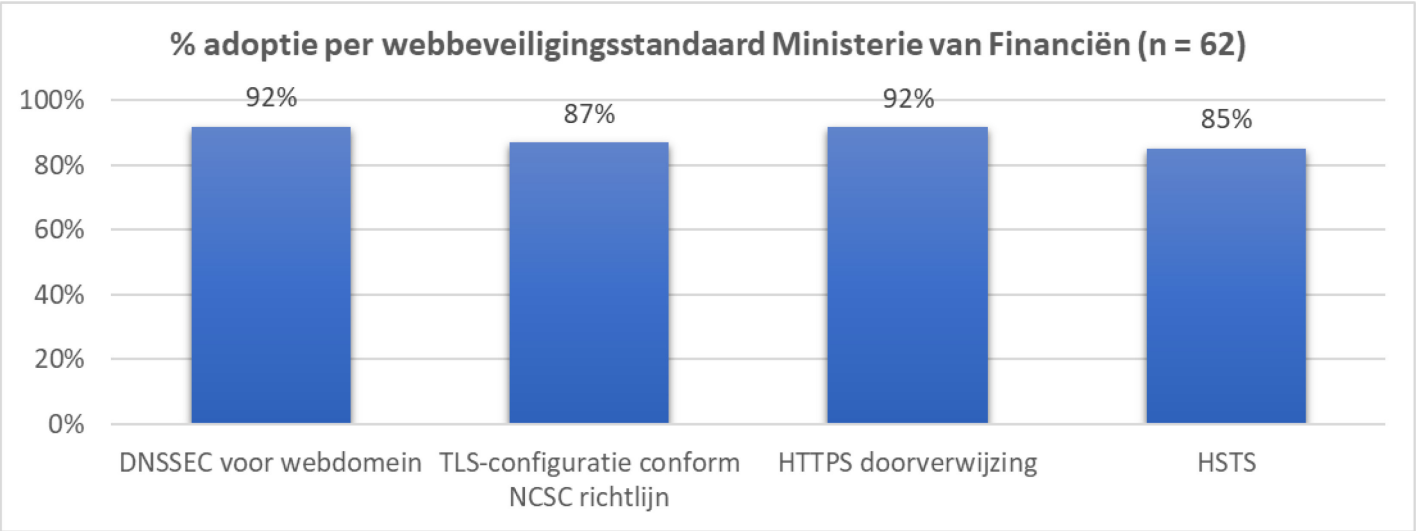
6.7. Ministerie van Economische Zaken en Klimaat

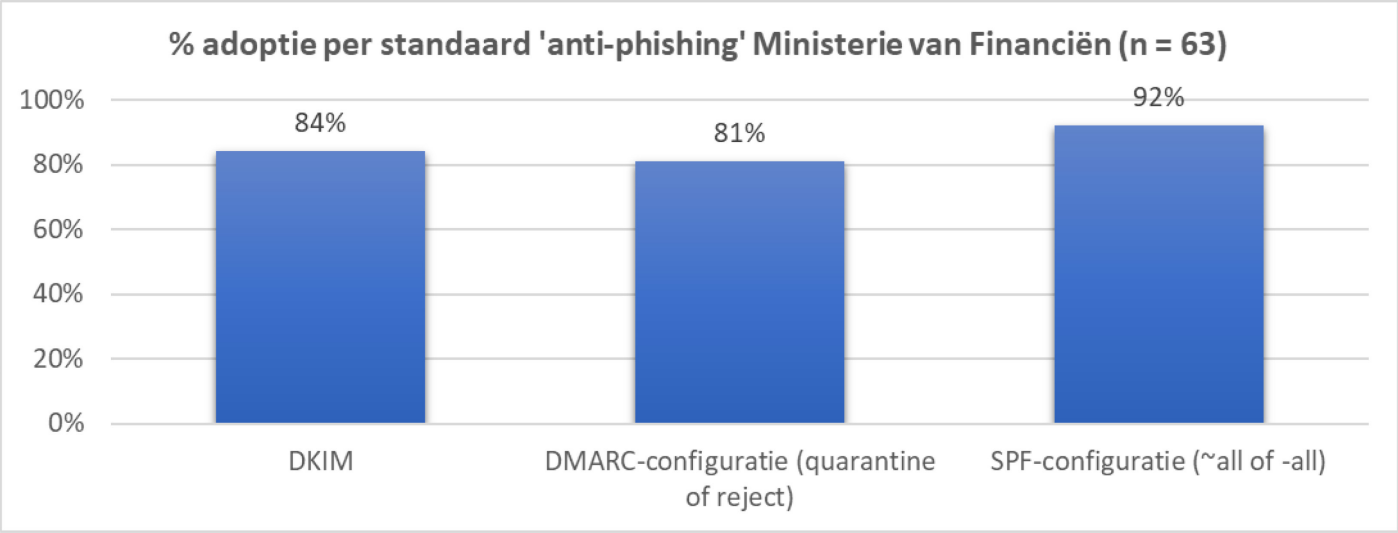


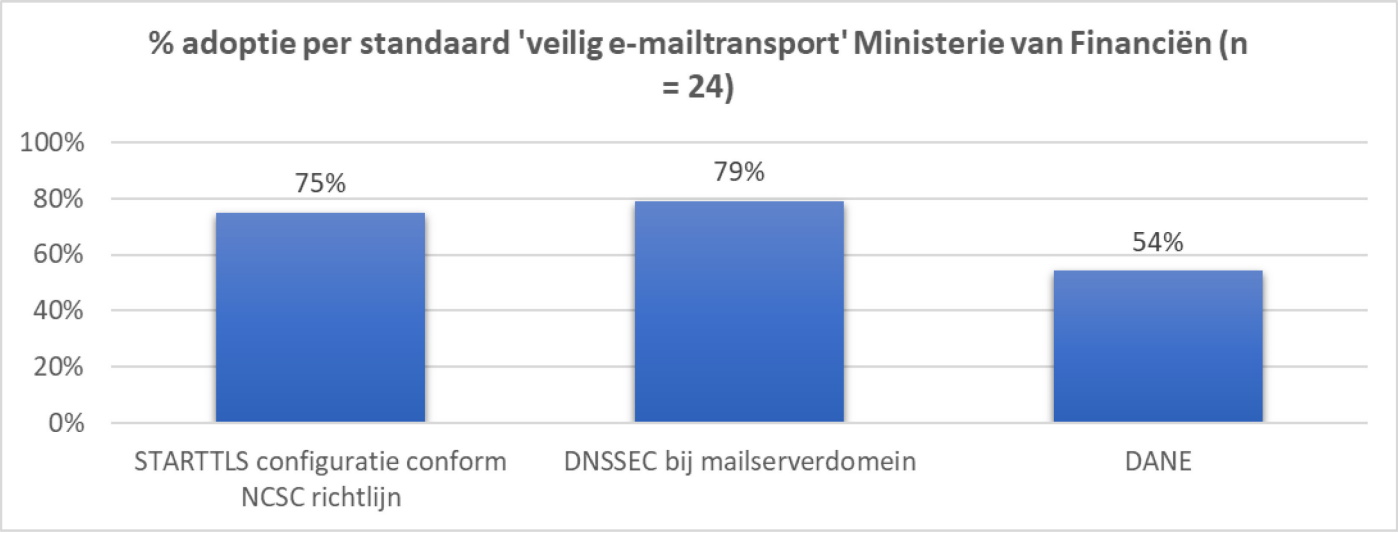




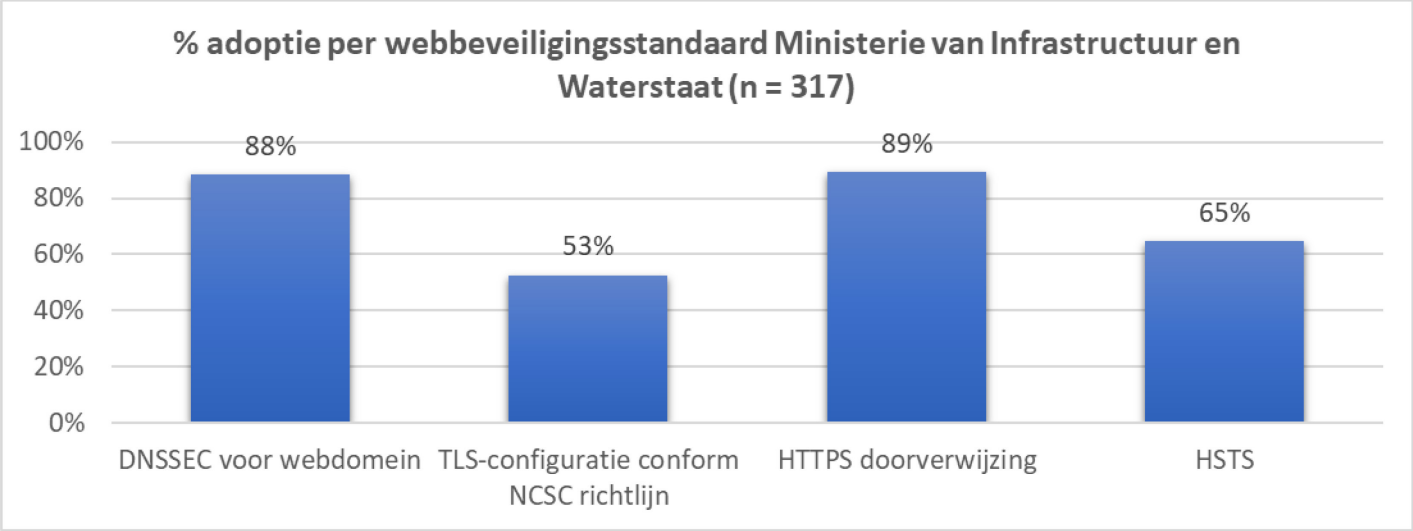
6.8. Ministerie van Financiën

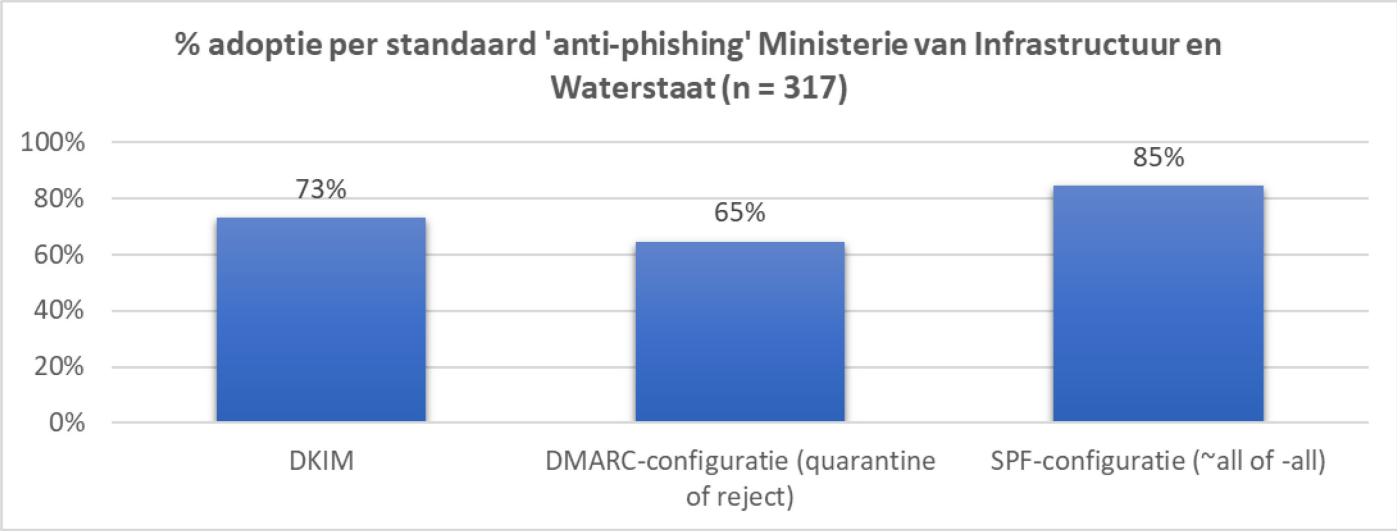


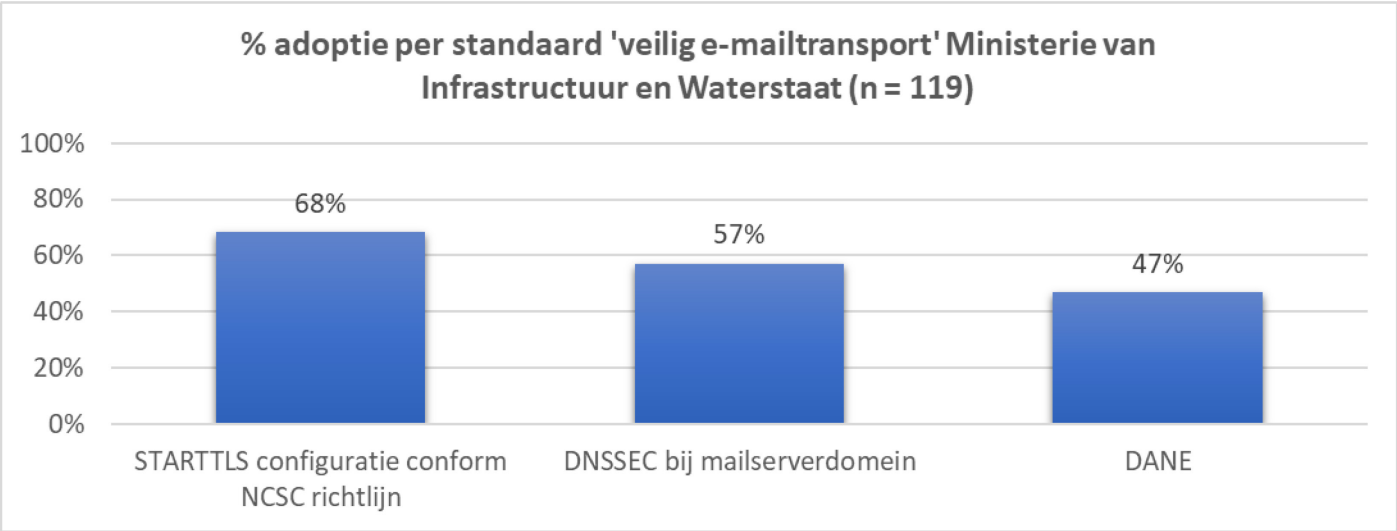




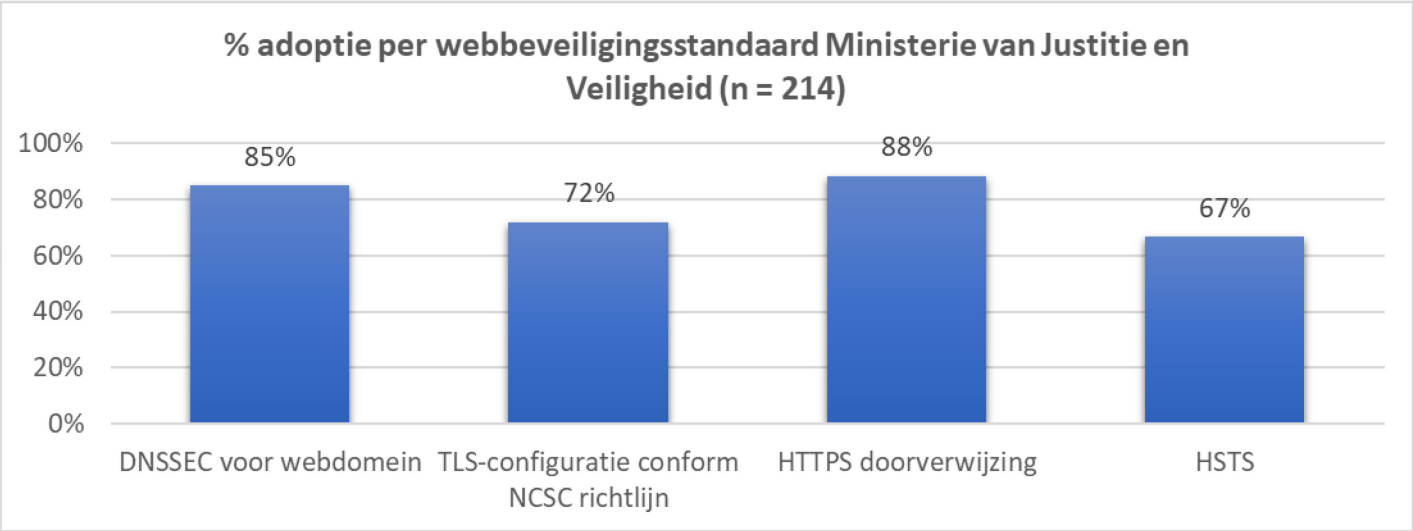
6.9. Ministerie van Infrastructuur en Waterstaat

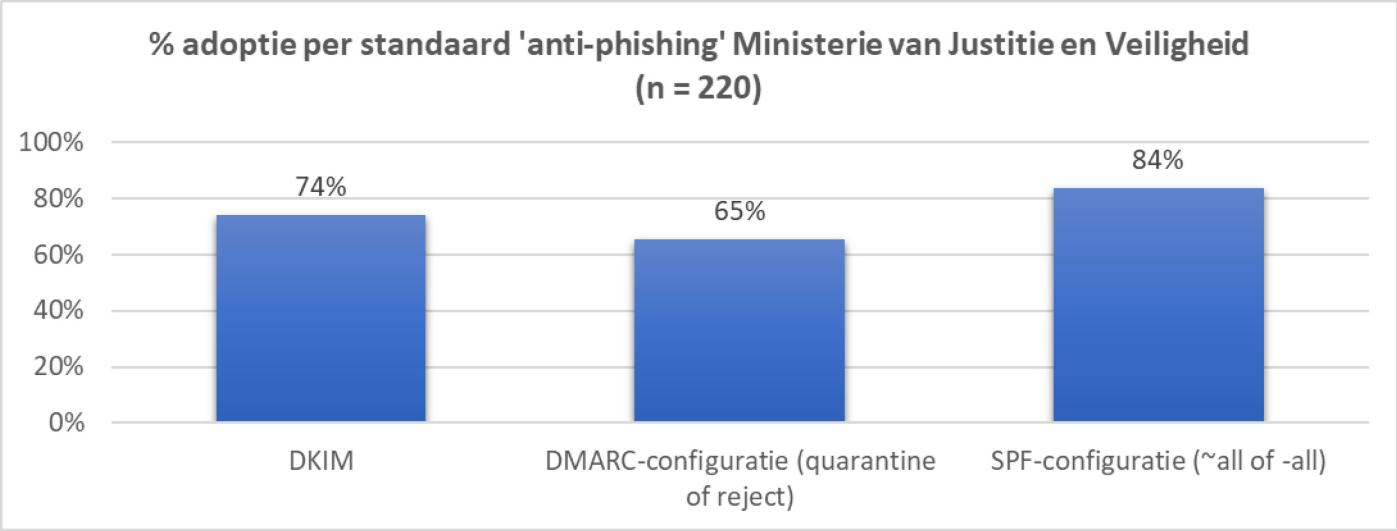


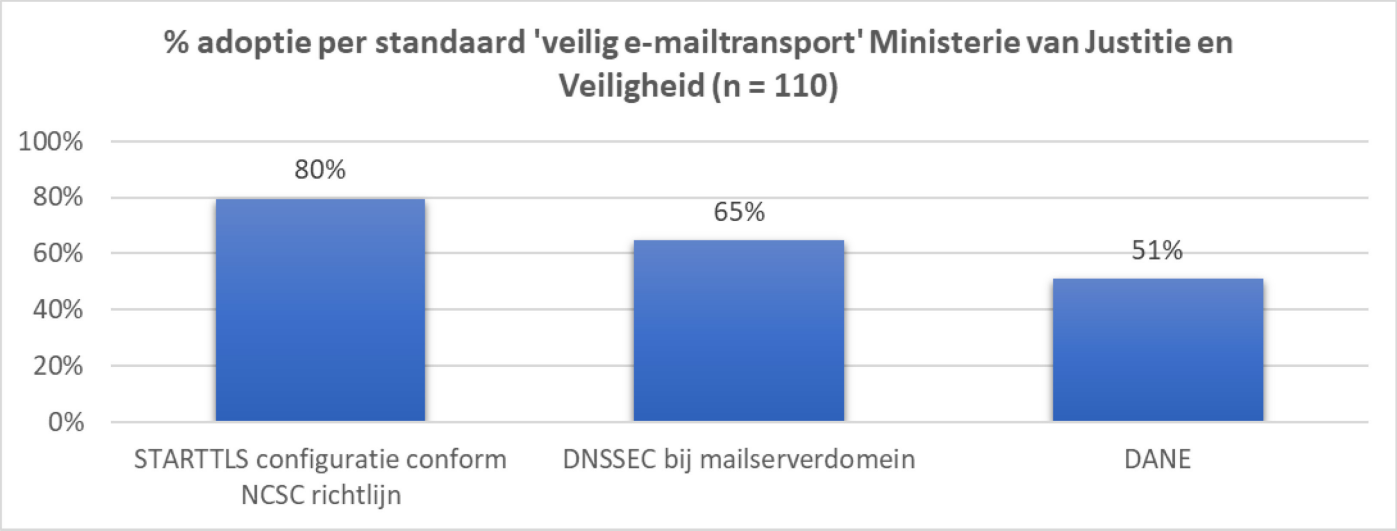




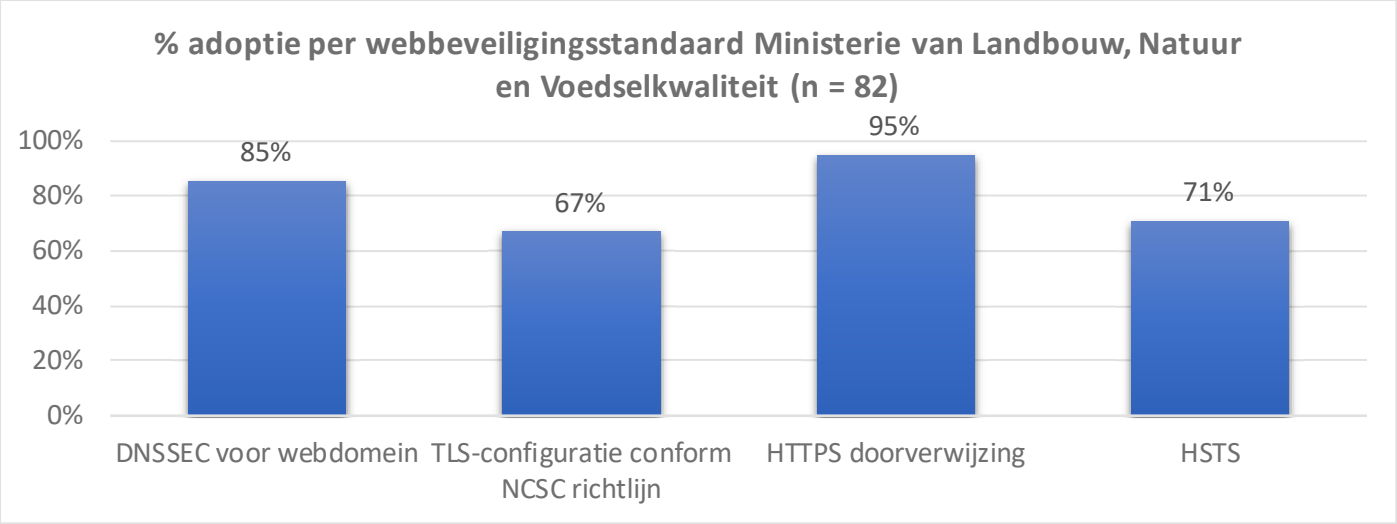
6.10. Ministerie van Justitie en Veiligheid

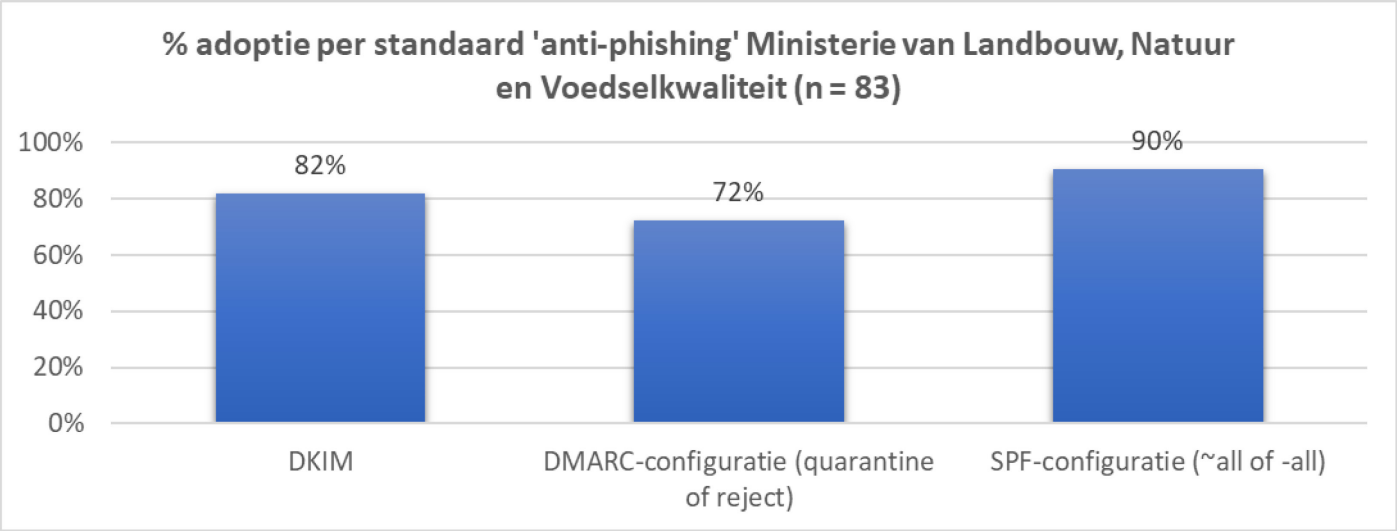


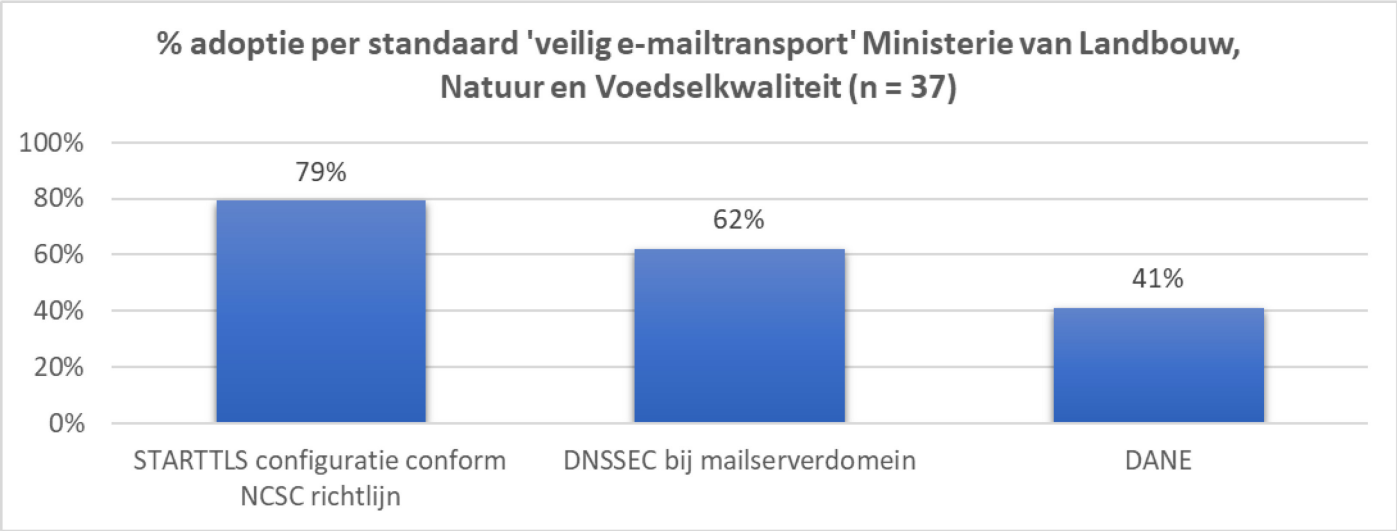




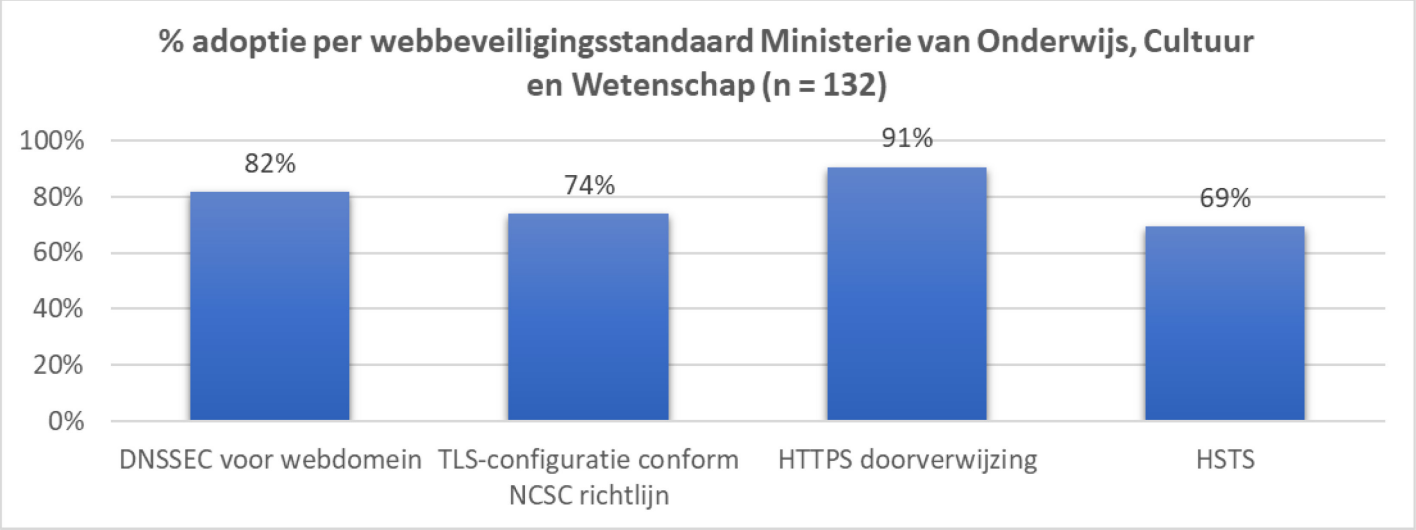
6.11. Ministerie van Landbouw, Natuur en Voedselkwaliteit

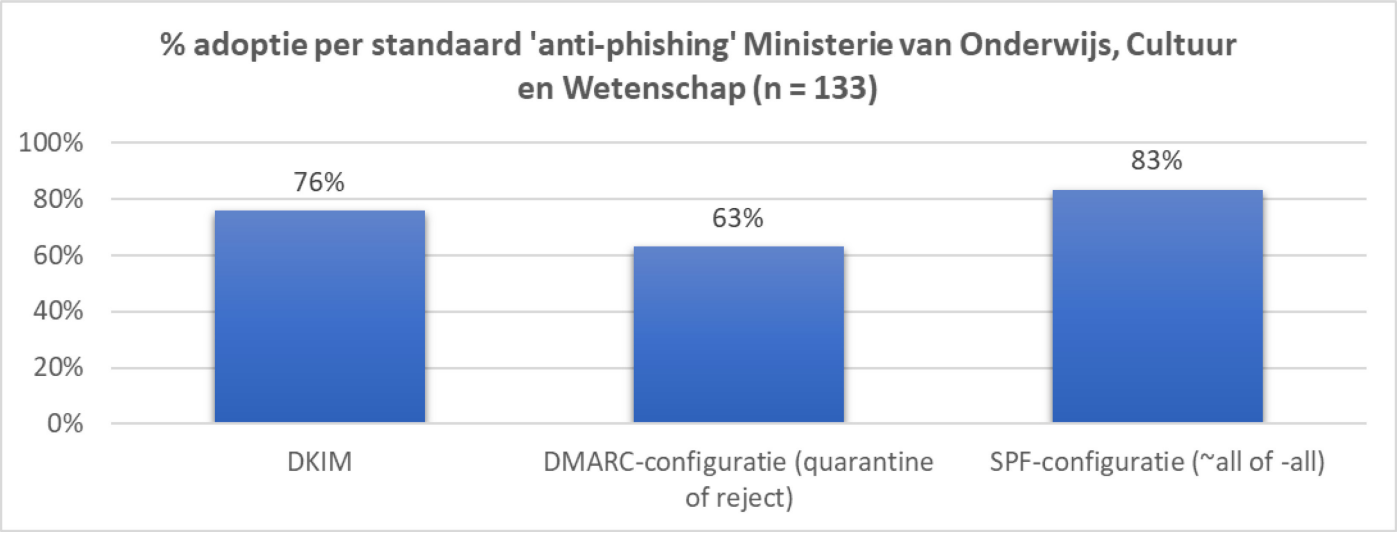


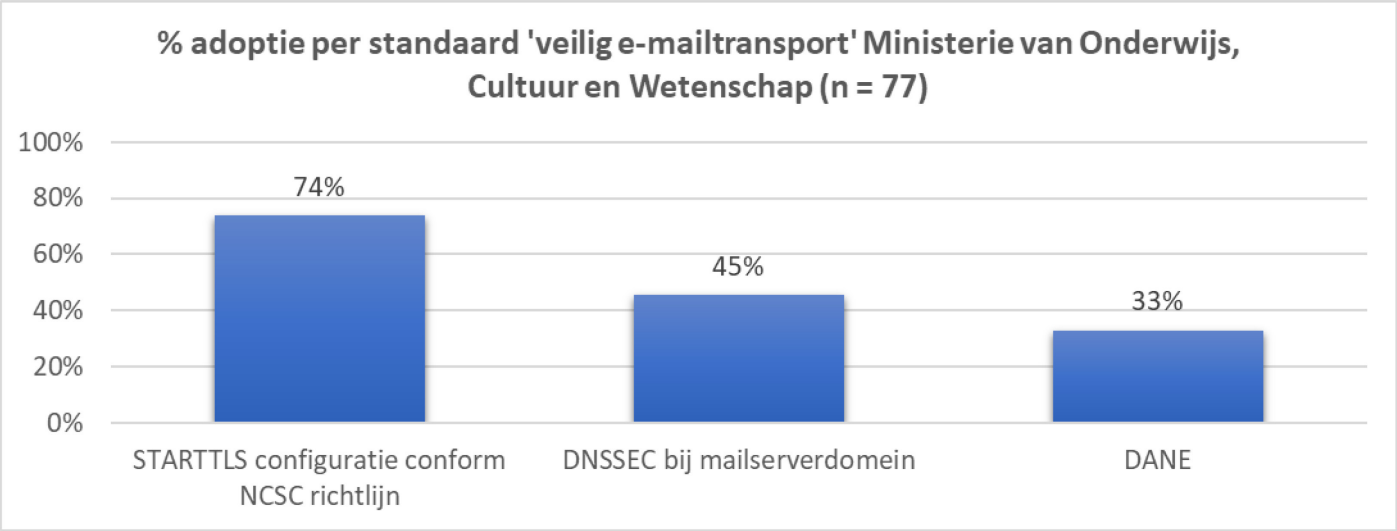




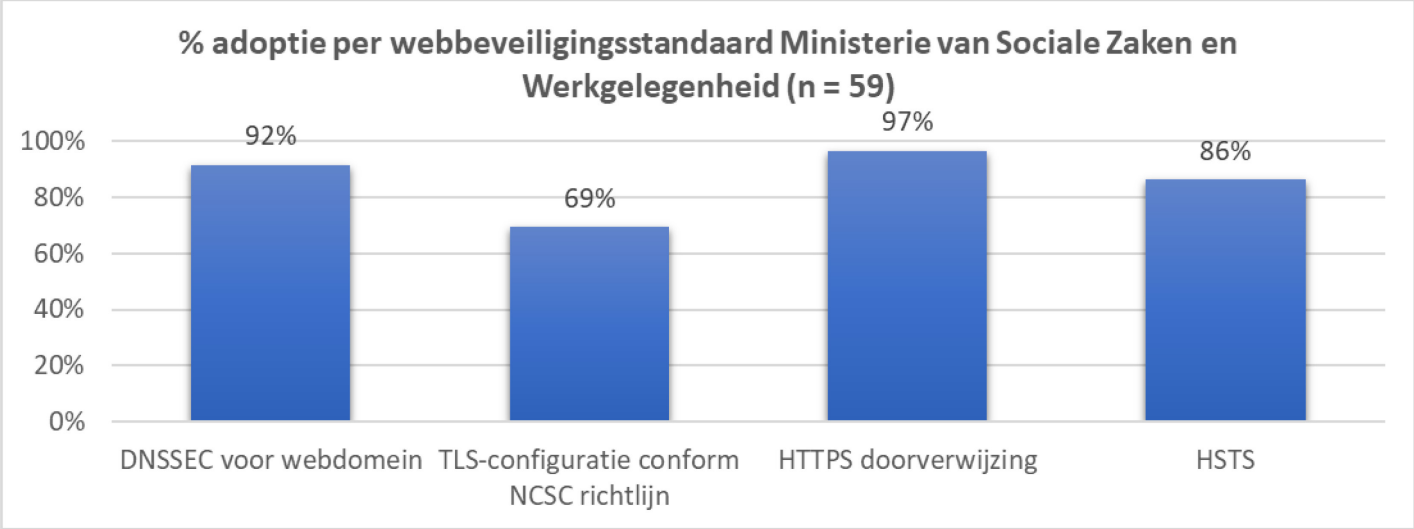
6.12. Ministerie van Onderwijs, Cultuur en Wetenschap

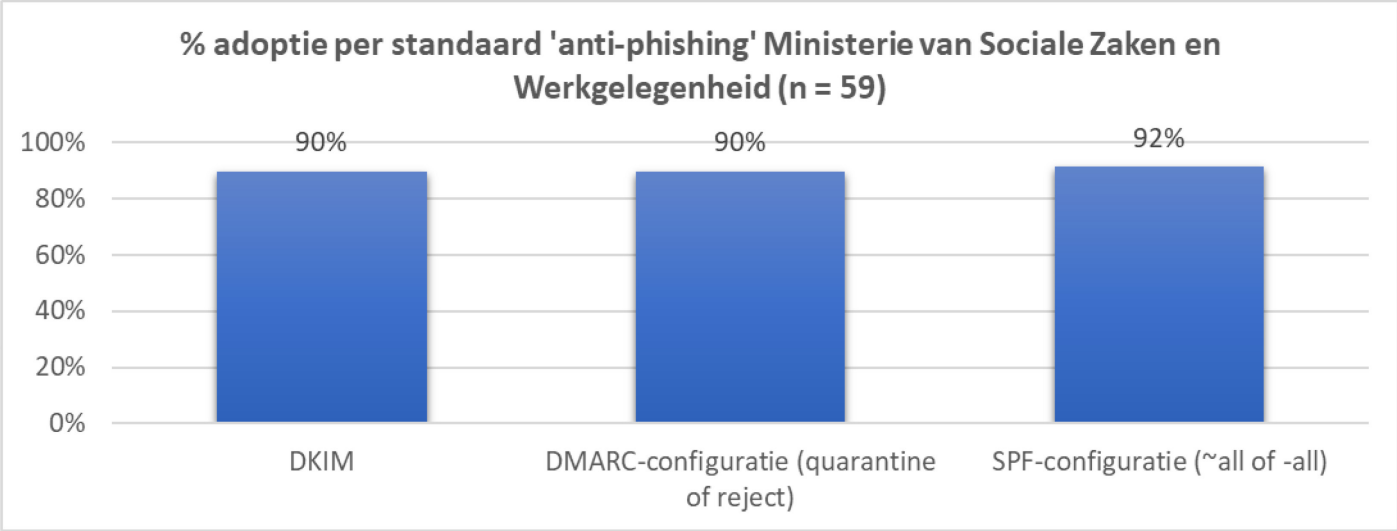


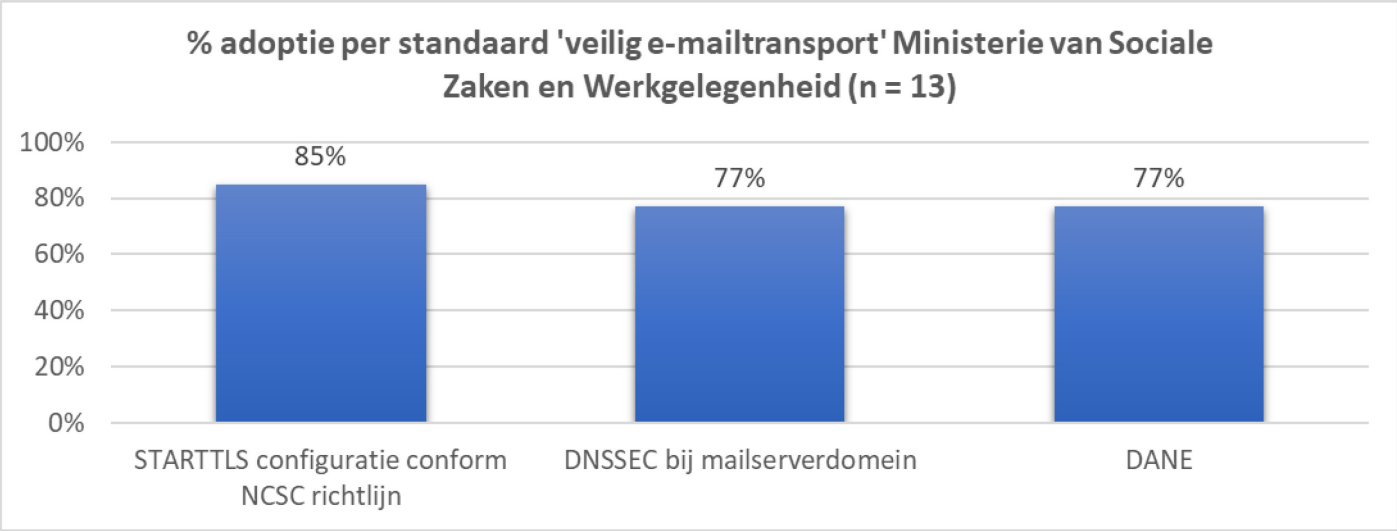




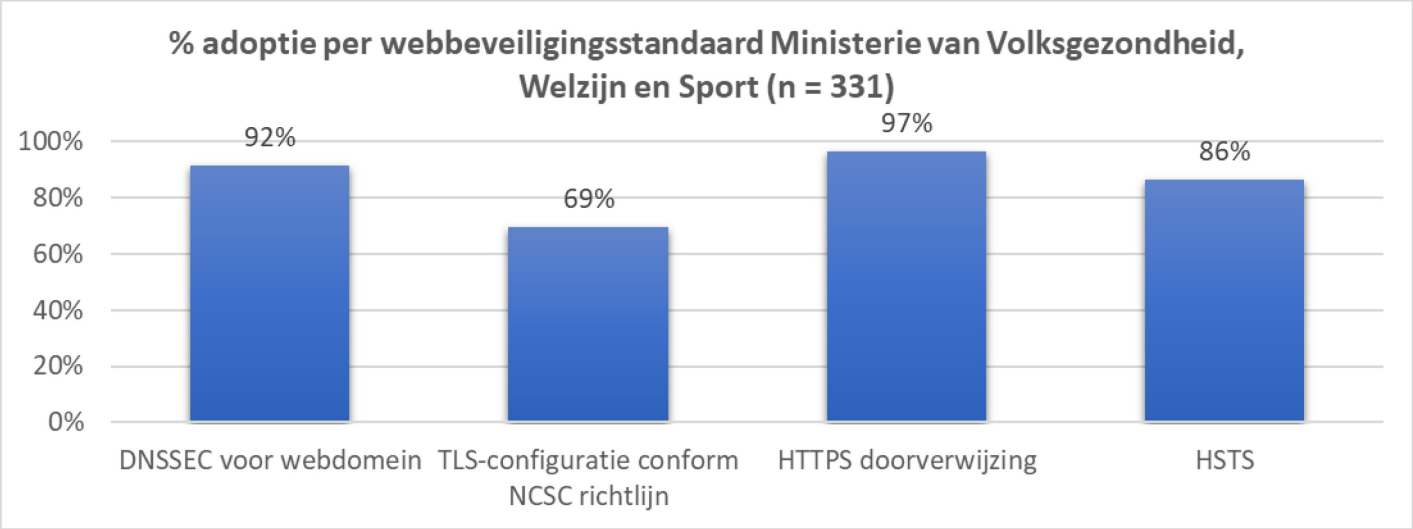
6.13. Ministerie van Sociale Zaken en Werkgelegenheid

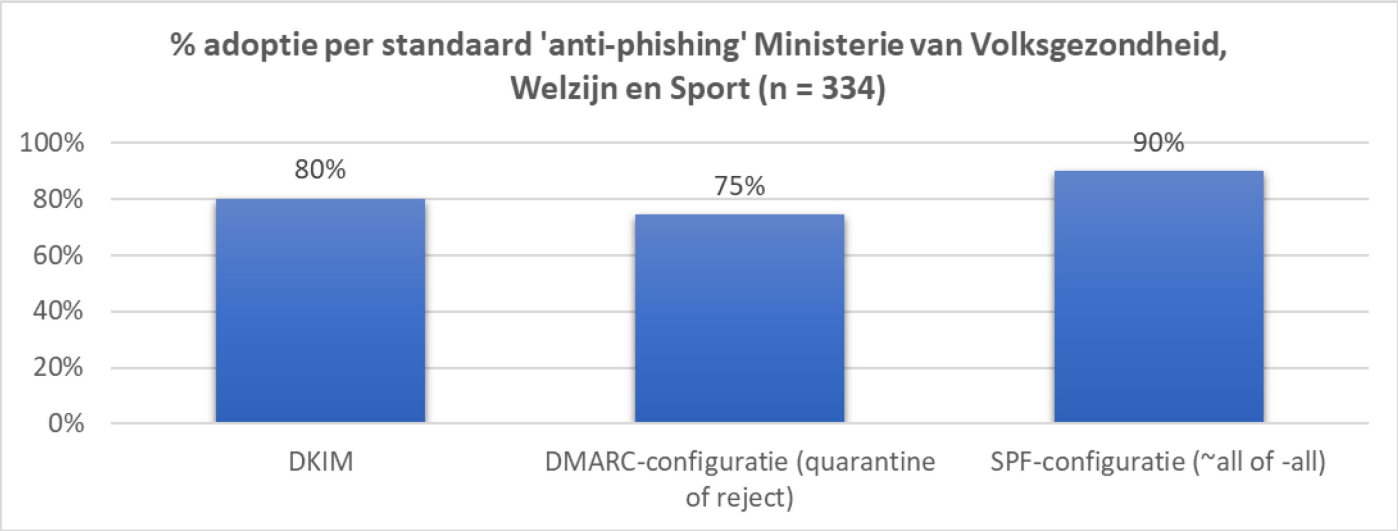


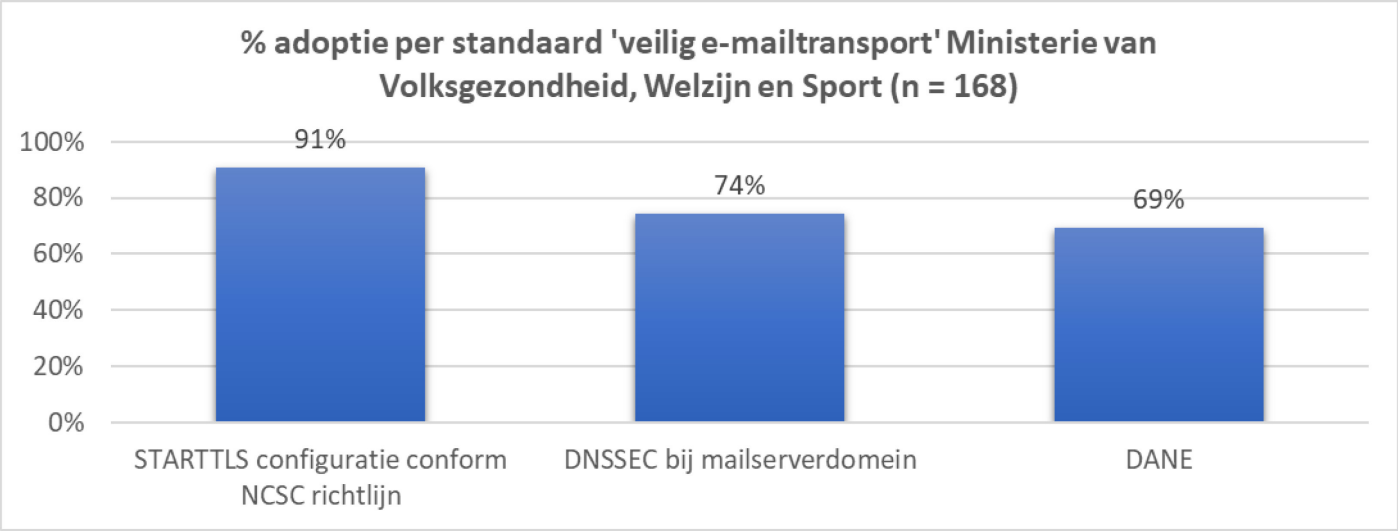




6.14. Ministerie van Volksgezondheid, Welzijn en Sport







7. 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) drie 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.

7.1. 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

7.2. Om welke internetdomeinen gaat het

In totaal zijn in deze meting 2584 internetdomeinen van overheidsorganisaties getoetst, bestaande uit:

- Alle internetdomeinen uit het Websiteregister Rijksoverheid;
- Alle internetdomeinen uit het Register van Overheidsorganisaties op organisaties.overheid.nl;
- Internetdomeinen uit voorgaande metingen.

De lijst betreft een selectie van alle overheidsdomeinnamen. De lijst is niet volledig en kan dat ook niet zijn omdat de overheid momenteel geen overzicht heeft over alle domeinnamen. De gemeten internetdomeinen zijn bij lange na niet alle domeinen waar het OBDO direct en indirect voor verantwoordelijk is. Zo heeft het ministerie van AZ zicht op meer dan 9.000 internetdomeinen van de Rijksoverheid waarvan het overzicht niet openbaar is gepubliceerd. Een 100%-score op de gemeten domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn tegen bijvoorbeeld phishing.

7.3. Hoe wordt gemeten

De meting geeft de stand van zaken weer van mei 2022. De meting laat zien of op een domeinnaam de standaarden worden toegepast. De resultaten zijn voorgelegd aan een aantal koepelorganisaties en stakeholders en begin juli geactualiseerd indien nodig.

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

Op Internet.nl is eenvoudig te testen of een website of e-mail een aantal moderne internetstandaarden ondersteunen, ook de standaarden waarover streefbeeldafspraken zijn gemaakt zijn onderdeel van de test. 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.

7.4. 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.

7.5. 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.

7.5.1. Webstandaarden

Wij meten het gebruik van de beveiligingsstandaarden en IPv6 voor het web ook op domeinen die alleen gebruikt worden voor mail omdat dit vaak wel domeinnamen zijn die re-directen naar het hoofddomein. Ook hiervoor moeten de standaarden juist worden toegepast en burgers weten vaak niet hoe deze domeinen worden gebruikt. Als redirects worden toepast dan moeten ook de doorverwijzende domeinen met HTTPS beveiligd zijn, anders is de beginschakel niet veilig en daarmee is ook de gehele keten onveilig. Dit geldt ook wanneer een zogenaamde 'parking page' wordt getoond. Alleen als een geregistreerd domein geen webpagina bevat dan is HTTPS niet nodig (en niet mogelijk).

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.

7.5.2. 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. (Opm: Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC) Er wordt gecontroleerd of de syntax van de DMARC-record correct is en of deze een voldoende strikte policy bevat. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
DKIM	Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven. Getest wordt of de domeinnaam DKIM ondersteunt. Voor non-mail domeinen waar dit goed is ingesteld heeft DKIM verder geen toegevoegde waarde. In de meting wordt dit weergegeven middels de score “NVT” (niet van toepassing) voor DKIM. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF 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.