Halfjaarlijkse meting Informatieveiligheidsstandaarden BFS – Begin 2017

Achtergrond

Sinds 2015 biedt het Platform Internet Standaarden[1] de mogelijkheid om via de website internet.nl domeinen te toetsen op het gebruik van internet- en beveiligingsstandaarden die op de 'pas toe of leg uit'-lijst van Forum Standaardisatie staan. In datzelfde jaar is Forum Standaardisatie gestart met een halfjaarlijkse meting van overheidsdomeinen op het voldoen aan deze standaarden.

Die metingen hebben ertoe geleid dat het Nationaal Beraad in februari 2016 de ambitie uitsprak deze standaarden versneld te willen adopteren.[2] Dit betekent concreet dat voor deze standaarden niet het tempo van 'pas-toe-of-leg-uit' wordt gevolgd (i.e. wachten op een volgend investeringmoment en dan de standaarden implementeren), maar dat actief wordt ingezet op implementatie van de standaarden op de korte termijn[3]. Voorliggende notitie bevat de resultaten van de meest recente meting van begin 2107

Om welke standaarden gaat het

Het Nationaal Beraad heeft bovengenoemde afspraken gemaakt met betrekking tot de volgende standaarden[4]:

- DNSSEC: Domeinnaambeveiliging
- TLS[5] : Beveiligde verbinding
- DKIM: Anti-Phishing
- SPF: Anti-Phishing
- DMARC[6]: Anti-Phishing (rapportages)

Om welke domeinen gaat het

In totaal zijn in deze meting 548 domeinen getoetst, bestaande uit:

- Domeinen die horen bij de deelnemers van het Nationaal Beraad
- De domeinen die horen bij voorzieningen van de Generieke Digitale Infrastructuur.
- De 25 best bezochte domeinen van Rijksoverheden (en uitvoerders)
- De domeinen van de andere partijen die direct of indirect vertegenwoordigd zijn in het Nationaal Beraad, zoals:
    - uitvoerders (de Manifestpartijen)
    - gemeenten
    - provincies en waterschappen
    - partijen die behorend tot Klein LEF

Bij de eerdere metingen werd bij de presentatie alleen het onderscheid tussen gemeenten en 'niet-gemeenten' gemaakt. Bij deze meting wordt eerst het totaal gepresenteerd en vervolgens de scores van de volgende overheden: Rijk, uitvoerders, provincies, waterschappen en gemeenten.

Hoe wordt gemeten

De meting geeft de stand van zaken weer op de peildatum in januari (gemeenten) en februari(overige domeinen) 2017. De meting laat zien of een domein de gemeten standaarden ondersteunt. De meting

---

[1] Platform Internet Standaarden is een gezamenlijk initiatief van Forum Standaardisatie, het Ministerie van Economische zaken en het Nederlandse internet gemeenschap. Zie https://internet.nl/about/

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

[3] Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. Om die reden is de halfjaarlijkse meting vanaf dit jaar onderdeel van de Monitor Open standaarden beleid.

[4] Zie: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit

[5] Voor TLS geldt dat het Nationaal Beraad de ambitie uitsprak deze tenminste voor die domeinen toe te passen waar burgers en bedrijven mogelijk privacy -gevoelige gegevens invoeren (een zogenaamde transactiesite). Overheden worden opgeroepen om dergelijke domeinen, die nog niet getoetst worden, bij Forum Standaardisatie te melden, zodat deze onderdeel kunnen worden van de halfjaarlijkse toetsing.

[6] DMARC is positief getoetst maar nog niet opgenomen op de pas-toe-of-leg-uit lijst. DMARC hangt echter dermate sterk samen met de toepassing van DKIM en SPF, dat het Nationaal Beraad besloot DMARC alvast onderdeel te maken van de 'versnelde adoptie set'.

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.

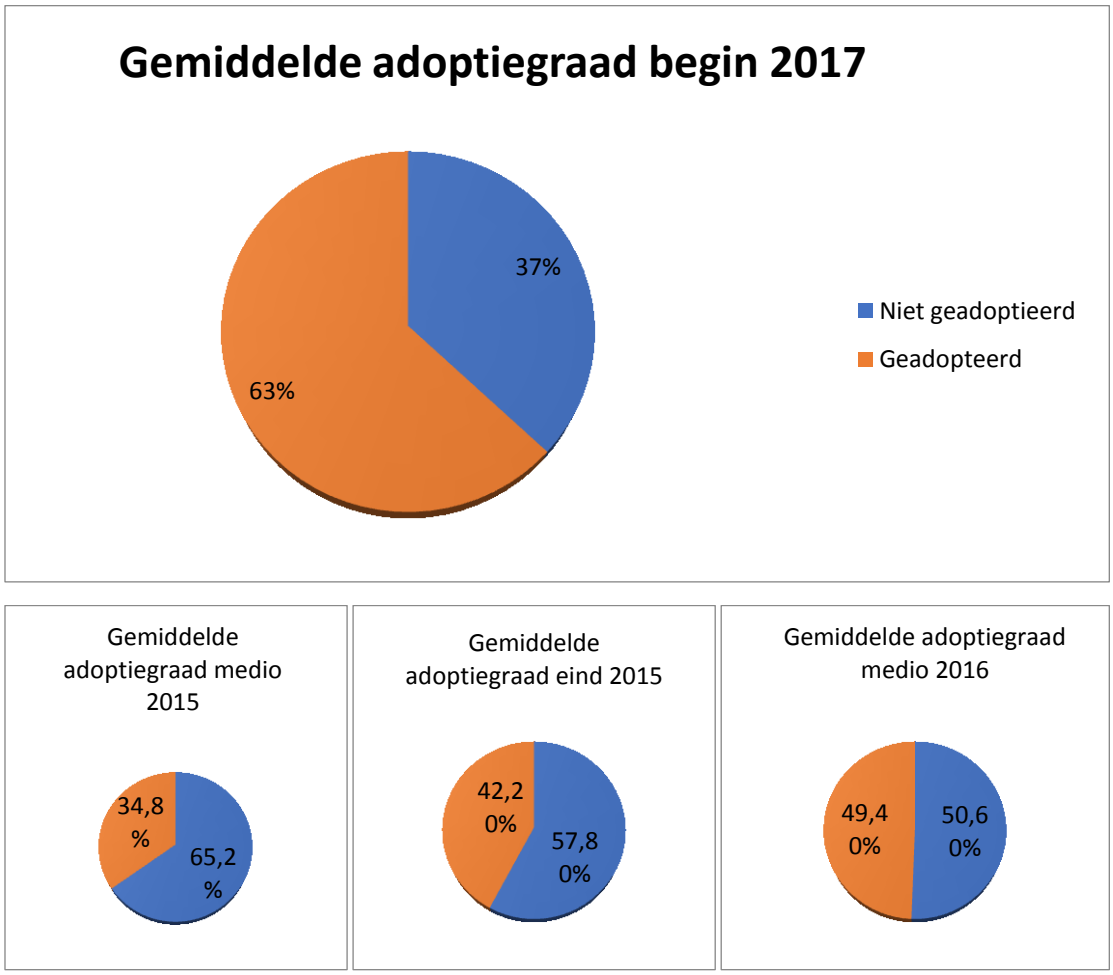
Ten aanzien van de meting van specifieke standaarden merken wij het volgende op:

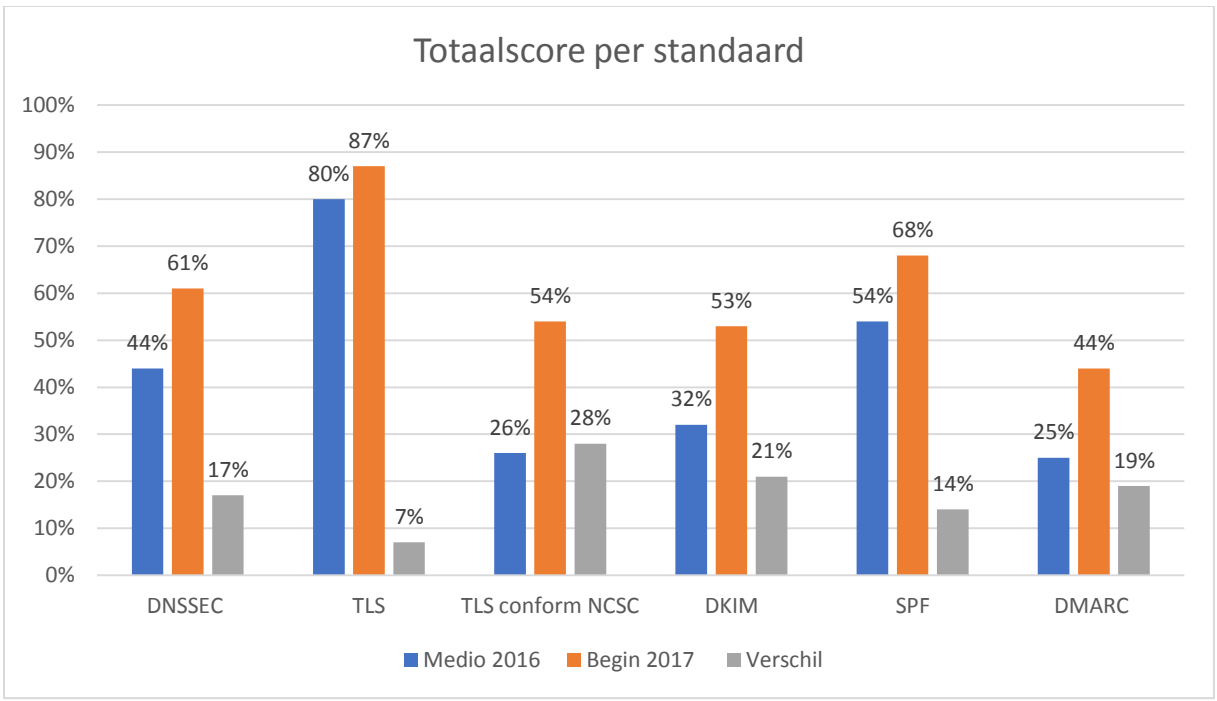
- Wij maken een onderscheid tussen 'TLS' en 'TLS conform NCSC' In het eerste geval wordt gebruik gemaakt van TLS en in het tweede geval is TLS bovendien zodanig geconfigureerd dat deze voldoet aan de aanbevelingen van het Nationaal Cyber Security Center (NCSC)[7].
- Wij maten het gebruik van TLS op alle (website)domeinen omdat wij onvoldoende informatie hebben over individuele domeinen om te weten of er op een website vertrouwelijke gegevens worden uitgewisseld.
- Bij gemeenten meten wij het gebruik van TLS alleen op het hoofddomein, omdat wij geen inzicht hebben in de overige domeinen die een gemeente voor verschillende doeleinden gebruikt. Wij roepen u daarom op om ons te wijzen op aanvullende transactiedomeinen die aanvullend gemeten zouden moeten worden.
- Wij meten het gebruik van e-mailbeveiligingsstandaarden (met name SPF) ook op domeinen waarvan een organisatie geen e-mail verstuurt. Dit is relevant omdat ook die domeinen worden misbruikt (burgers weten vaak niet dat ze niet (meer) worden gebruikt), en juist domeinen waarvandaan niet gemaild wordt, makkelijk kunnen worden geblokkeerd met SPF.
- TLS: Als een domein bereikbaar is via ipv6 dan wordt de toepassing van TLS getoetst via IPv4 én IPv6. De slechtste configuratie bepaald de eindscore.
- De gemeten 548 domeinen zijn bij lange na niet alle domeinen waar het Nationaal Beraad direct en indirect voor verantwoordelijk is. Een 100% score op deze domeinen garandeert geenszins dat hiermee alle overheidsdomeinen beschermt zijn tegen bijvoorbeeld phising.

In bijlage 1 worden alle individuele scores op de vijf genoemde standaarden weergegeven. Bij deze rapportage wordt de score van de webstandaarden DNSSEC en TLS weergegeven zoals getoetst op het 'www. Domein' De mailstandaarden zijn getoetst op hetzelfde domein zonder 'www.' .
(PM volgt nog, momenteel vindt toetsing van de conceptresultaten plaats bij o.a. gemeenten)

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

Resultaten





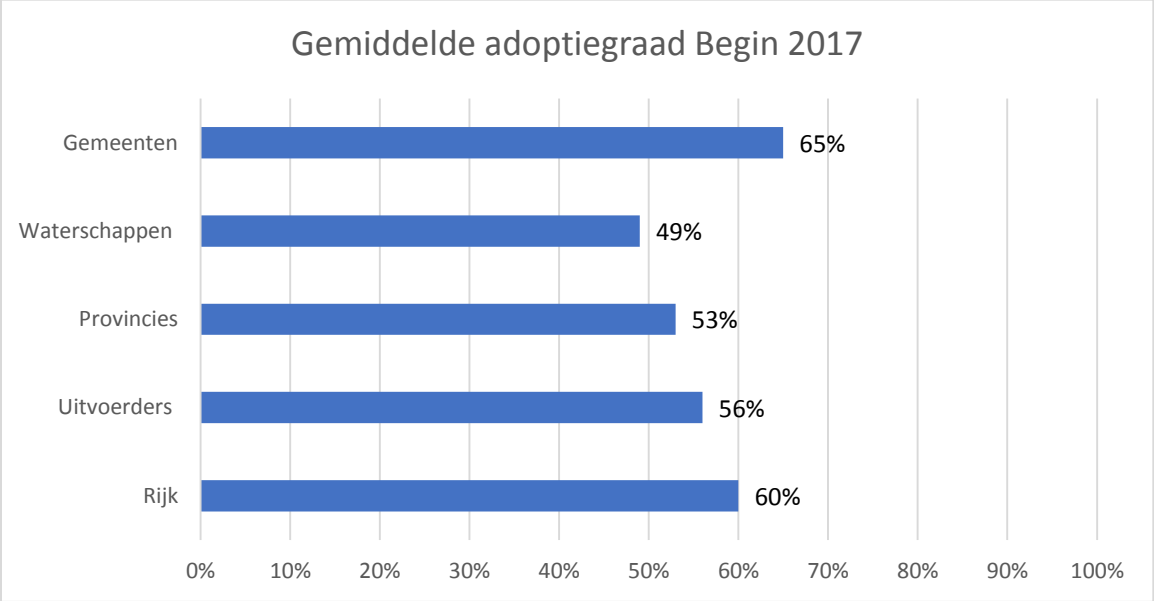
Figuur 1. Adoptiegraad van de standaarden over alle getoetste domeinen.

Wat valt op:

- De Toepassing van alle standaarden is het afgelopen half jaar gegroeid.
- De groei is met name bij TLS beperkt, maar tegelijk is de adoptiegraad van TLS het hoogst van alle standaarden (87%)
- Het aantal keer dat TLS conform de richtlijnen van het NCSC wordt toegepast is het afgelopen halve jaar flink toegenomen, maar heeft tegelijk nog een aardige weg te gaan.
- De toepassing van DMARC blijft achter bij de overige standaarden, al is de groei over het afgelopen halfjaar aangetrokken t.o.v. het jaar daarvoor.

Hoe scoren de verschillende domeinen?

Zoals gezegd wordt er in deze rapportage voor het eerst een onderscheid gemaakt tussen de overheden: Rijk, uitvoerders, provincies, waterschappen en gemeenten. De verschillende 'overheidslagen' hebben begin 2017 allemaal een andere gemiddelde adoptiegraad. Bovendien verschilt de gemiddelde groei t.o.v. de Medio 2016 meting flink.

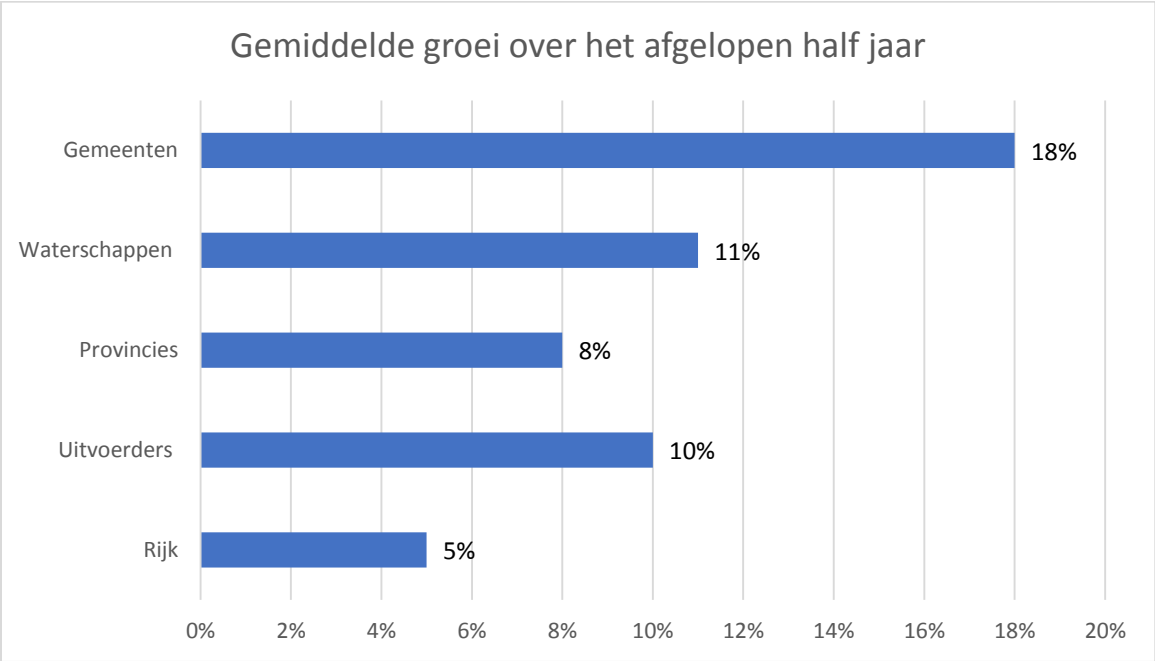


Figuur 2. De gemiddelde adoptiegraad van alle vijf de standaarden per 'overheidslagen'.

Wat valt op:

- Begin 2017 is de gemiddelde adoptiegraad bij gemeenten het hoogst.
- Het Rijk (begin 2016 nog koploper) is een goede tweede.
- De waterschappen scoren gemiddeld het slechtst.

Groei sinds Medio 2016



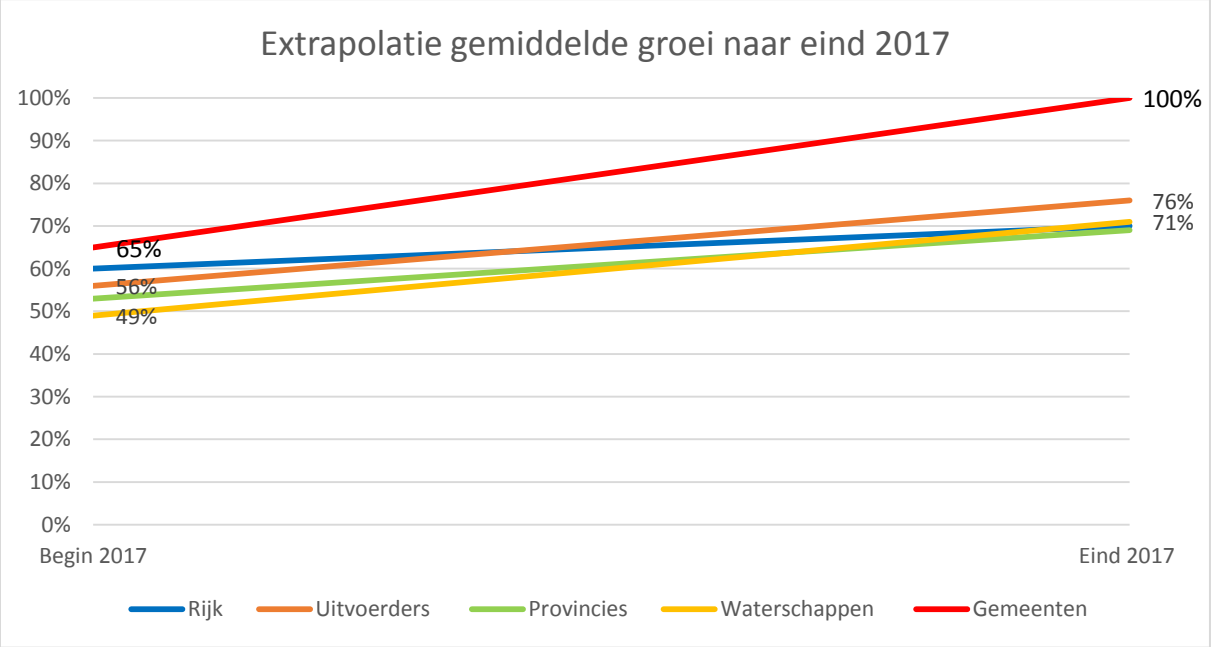
Figuur 3: De groei van de gemiddelde adoptiegraad over de afgelopen 6 maanden

Wat valt op:

- Gemeenten hebben begin 2017 niet alleen de hoogste gemiddelde adoptie. Het verschil t.o.v. de Medio 2016 meting is ook het grootst. Dit komt mogelijk door de aandacht die VNG/KING en IBD gemeenten in de tweede helft van vorig jaar aan deze standaarden gegeven hebben.
- Waar de gemiddelde adoptiegraad van het Rijk op 60% ligt en daarmee alleen de gemeenten voor moet laten gaan, is de groei van de gemiddelde adoptie bij het Rijk het afgelopen half jaar wederom vertraagd.
- Gezien de gemiddelde adoptiegraad van de overheden begin 2017 en waargenomen groei over de laatste zes maanden, is een flinke versnelling nodig om eind 2017 het streefbeeld te kunnen halen dat het Nationaal Beraad zichzelf als ambitie heeft gesteld.

Verwachting voor eind 2017

Net als bij voorgaande rapportages hebben we de groei over de afgelopen periode genomen en deze geëxtrapoleerd naar eind 2017.



Figuur 4: Extrapolatie gemiddelde groei verschillende overheden.

Wat valt op:

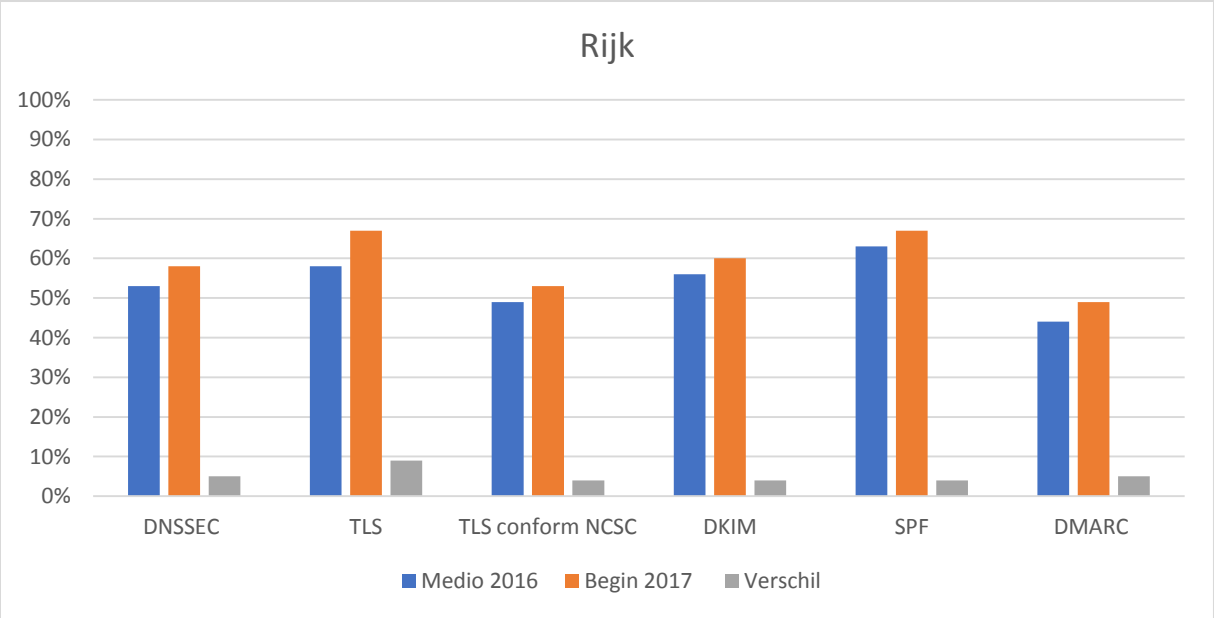
- Als de groei over het afgelopen halfjaar wordt doorgezet in 2017, hebben alleen de gemeenten gemiddeld genomen kans om aan het streefbeeld van het Nationaal Beraad te voldoen eind 2017.
- Voor de overige overheidslagen geldt dat deze gemiddeld blijven steken tussen de 70% (Rijk) en 76% (Uitvoerders) gemiddelde adoptiegraad.
- Bij gelijkblijvende groei wordt het Rijk in 2017 aan alle kanten ingehaald door de overige overheidslagen.

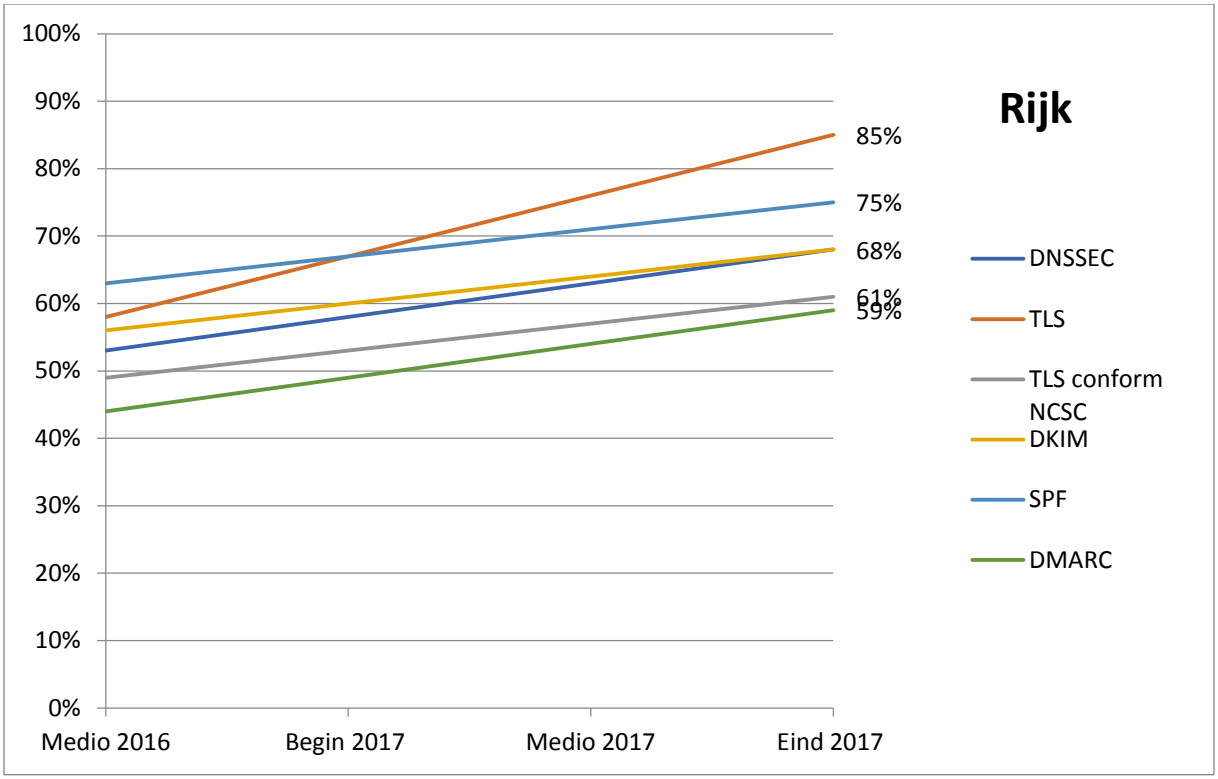
Adoptie van IV standaarden per 'overheidslaag'

Over de extrapolatie

Onderstaande grafieken laten zien hoe het gebruik van de verschillende standaarden naar verwachting zal toenemen in 2017 als de groei die we maten over het laatste halve jaar doorzet.

Deze groei verschilt flink per overheidsdomein en wordt daarom afzonderlijk voor het Rijk, uitvoerders, provincies, gemeenten en waterschappen weergegeven. Bij iedere extrapolatie worden de belangrijkste bevindingen vermeld.



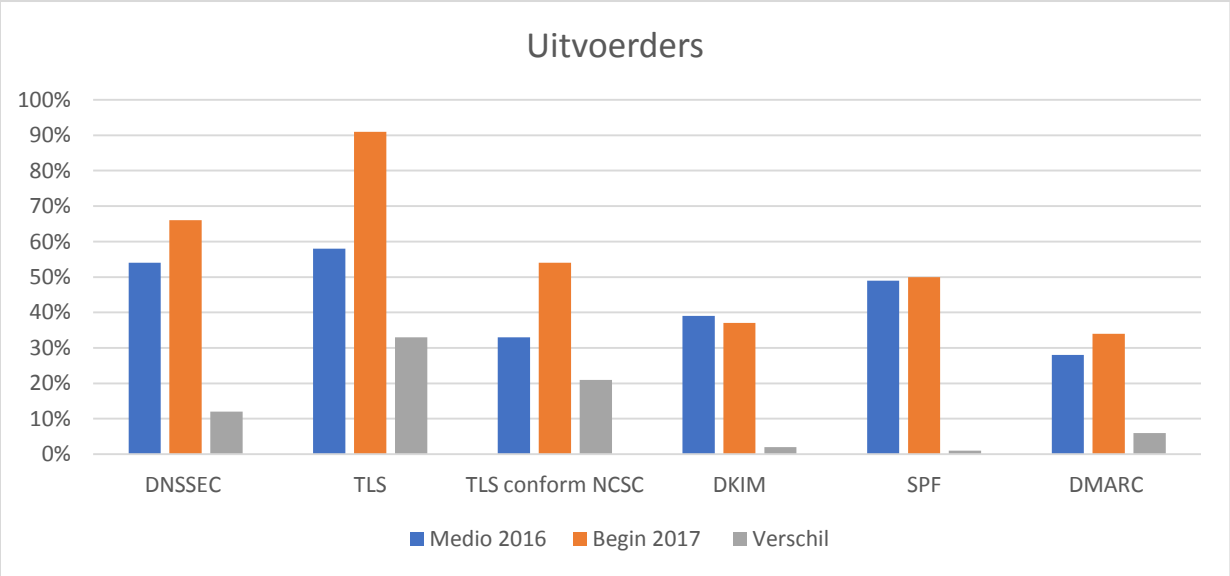


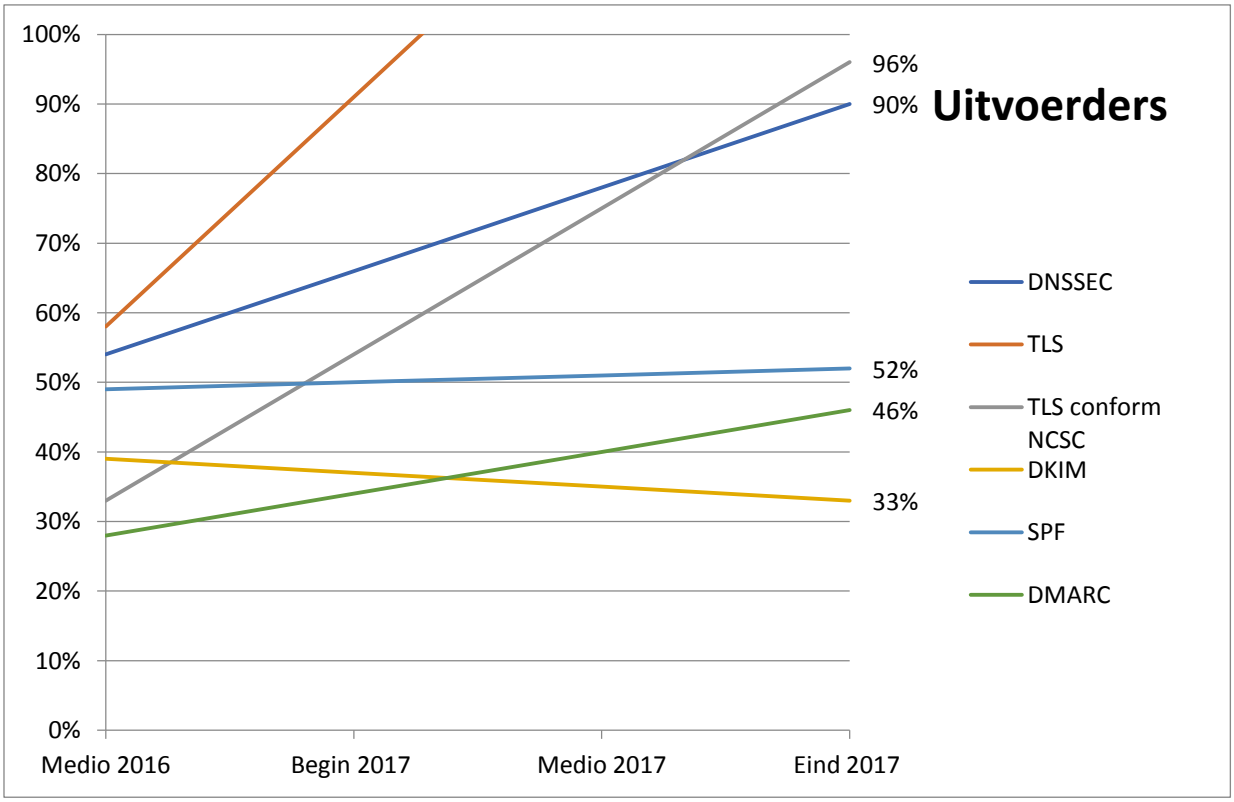
Wat valt op:

- Geen van de standaarden staat eind 2017 op 100%

- De groei is heel beperkt

- De groei is over alle standaarden ongeveer gelijk (TLS doet het iets beter)





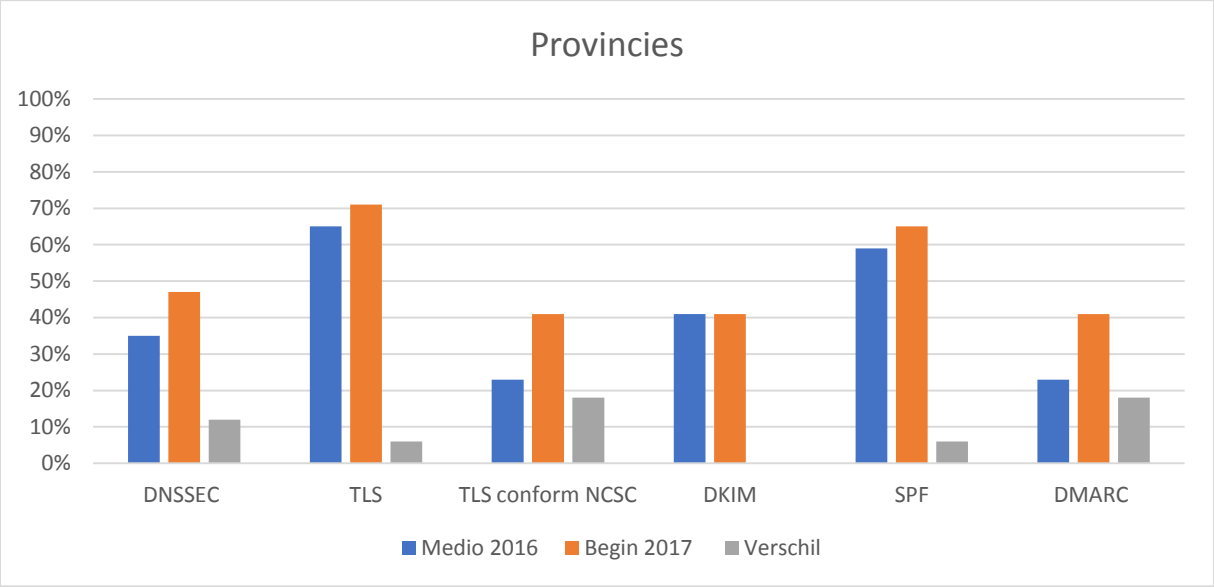
Wat valt op:

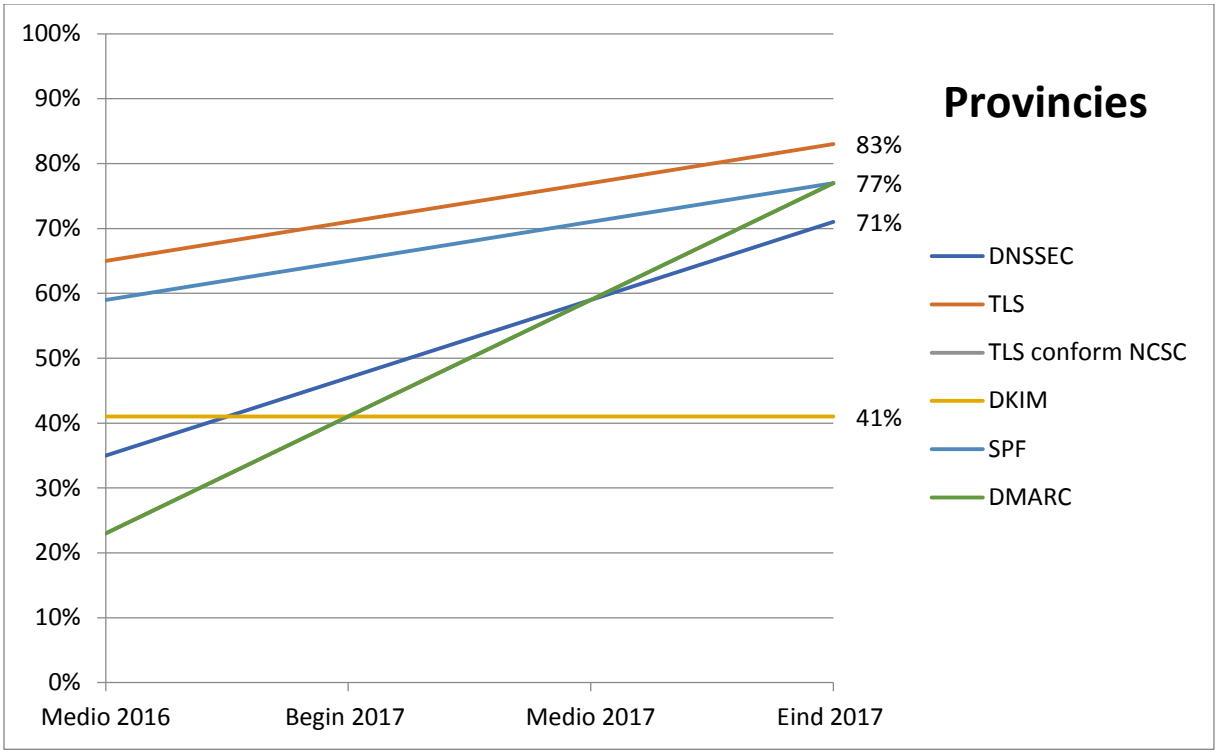
- Het gebruik van TLS is momenteel al heel groot en haalt, bij gelijke groei, al voor het midden van 2017 de 100%

- De groei tussen de verschillende standaarden verschilt flink

- De mailstandaarden blijven achter t.o.v. de webstandaarden

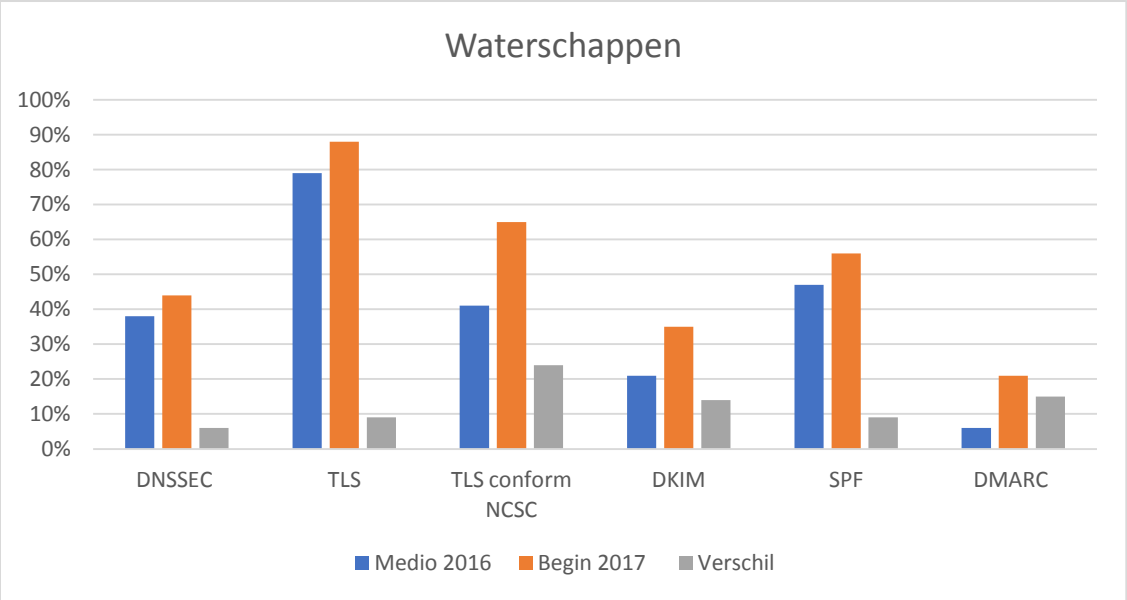
- Begin 2017 gebruikten minder domeinen DKIM dan in medio 2016 (scheelt één domein). Hier is geen duidelijke verklaring voor en betreft waarschijnlijk een tijdelijke teruggang. Het zorgt echter wel voor een negatieve extrapolatie.

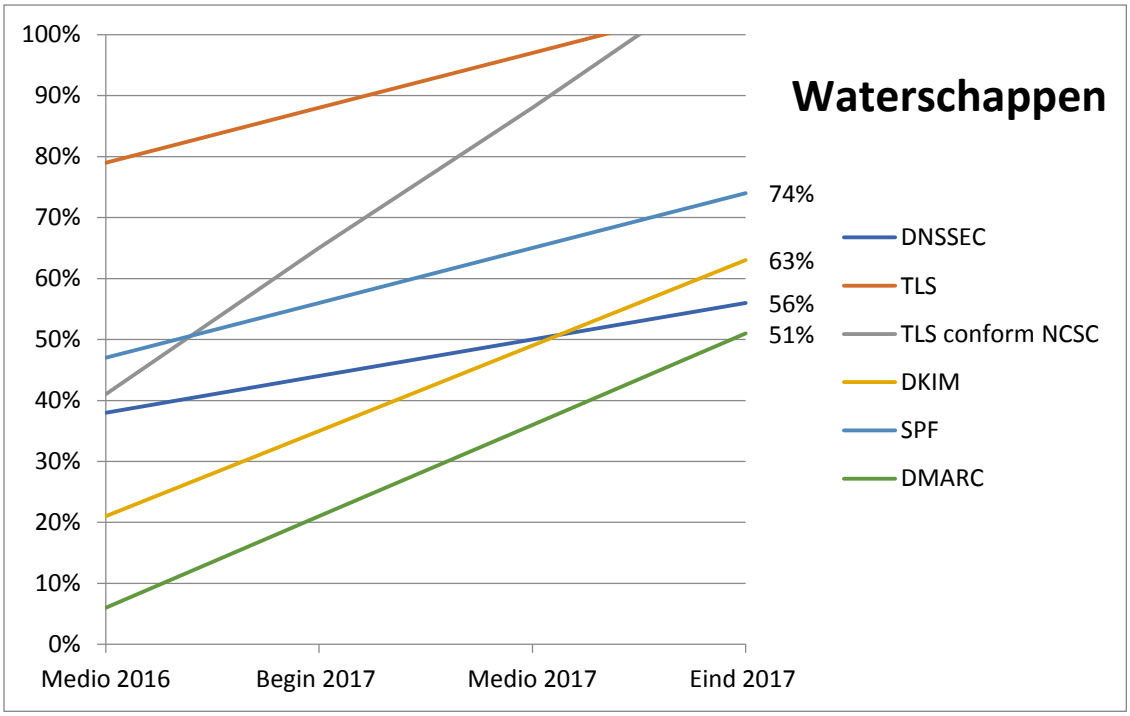




Wat valt op:

- Geen van de standaarden staat eind 2017 op 100%
- De uitgangspositie van de verschillende standaarden verschilt flink.
- Het gebruik van DKIM is niet toegenomen en zal daarom bij deze extrapolatie ook niet toenemen.



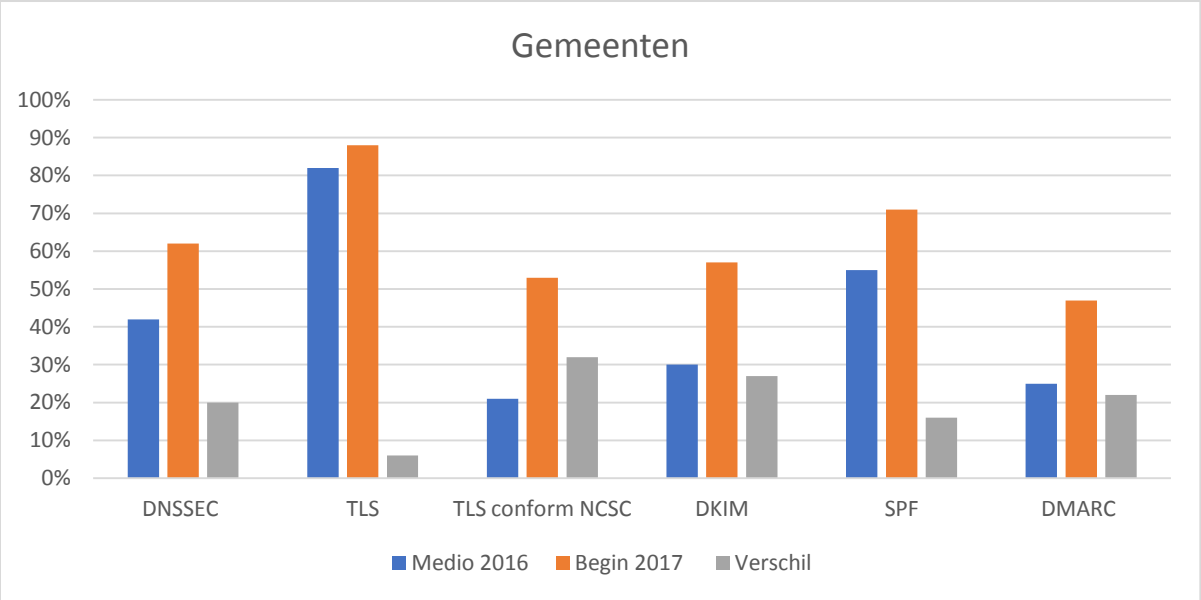


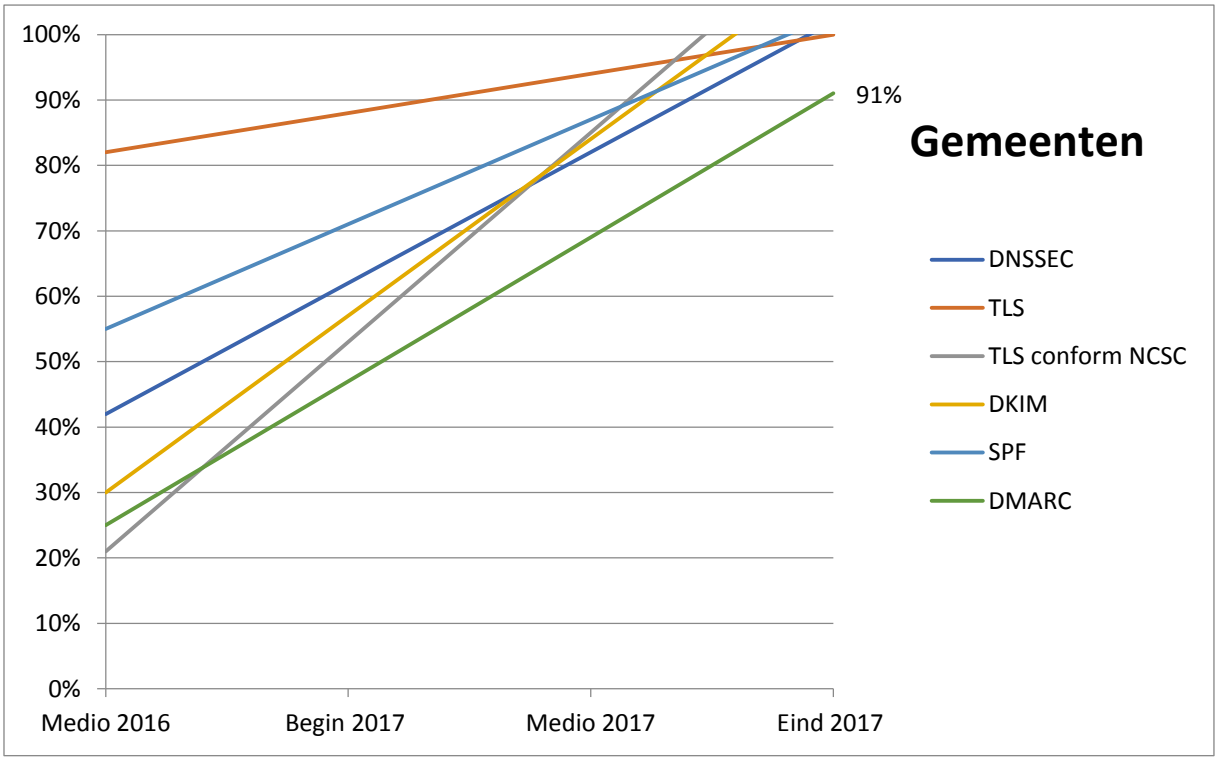
Wat valt op:

- Het gebuik van TLS zal, bij gelijke groei, naar verwachting voor eind 2017 op 100% zitten

- Bovendien zal het aantal domeinen dat TLS veilig continueert volgens de aanbevelingen van het NCSC ook voor eind 2017 de 100% bereiken.

- Het verschil in de uitgangspositie van de verschillende standaarden is bij de waterschappen het grootst.





Wat valt op:

- Als gemeenten dezelfde groei doorzetten die zij het afgelopen half jaar hadden, dan zullen bijna alle standaarden eind 2017 volledig gebuikt worden.

- Voor de webstandaarden geldt ene verwachting van 100%

- Voor de mailstandaarden geldt dat alleen DMARC naar verwachting iets achter blijft, maar met een verwachte adoptie van 91% is dat nog altijd ruim meer dan bij de andere overheden.