



notitie

Forum Standaardisatie

www.forumstandaardisatie.nl
forumstandaardisatie@logius.nl

Bureau Forum

Standaardisatie

gehuisvest bij Logius
Postadres
Postbus 96810
2509 JE Den Haag
Bezoekadres
Wilhelmina van Pruisenweg 52
2595 AN Den Haag
Bij bezoek aan Logius is
legitimatie verplicht

FORUM STANDAARDISATIE 19 oktober 2016

Meting Informatieveiligheidsstandaarden

Van:	Forum Standaardisatie
Aan:	Nationaal Beraad
Bijlagen:	Bijlage FS-20161019.04B1: NB-domeinen zonder gemeenten Bijlage FS-20161019.04B2: gemeentedomijnen

Half Jaarlijkse IV- standaardenmeting

Samenvatting

Uit de meest recente meting van 450 overheidsdomeinen op gebruik van de IV-standaarden blijkt dat, ondanks de ambitie van het Nationaal Beraad om deze standaarden versneld te adopteren, **de adoptie van de standaarden afgelopen half jaar niet is versneld**. Wordt de groei over het afgelopen jaar doorgezet in 2017 dat is **de gemiddelde adoptiegraag van deze standaarden eind 2017 ca. 70%**

Gevraagde actie

Leden van het nationaal Beraad worden opgeroepen deze standaarden versneld te adopteren

Uit de impactanalyse en verschillende factsheets die de IBD heeft laten opstellen voor deze standaarden¹ blijkt dat de kosten en inspanning om aan deze standaarden te voldoen geen belemmering vormen.

Bureau Forum Standaardisatie kan bovendien helpen als u contact opneemt via info@forumstandaardisatie.nl of 070 - 888 7776

¹ Zie <https://www.ibdgemeenten.nl/ibd-publiceert-factsheets-e-mailauthenticatie/> & <https://www.ibdgemeenten.nl/3619-2/>

Achtergrond

Sinds 2015 biedt het Platform Internet Standaarden² de mogelijkheid om via de website internet.nl domeinen te toetsten op het gebruik van de internet- en beveiligingsstandaarden die op de 'pas toe of leg uit' lijst van Forum Standaardisatie staan³. In datzelfde jaar is Forum Standaardisatie gestart met een halfjaarlijkse evaluatie van overheidsdomeinen op het voldoen aan deze standaarden. De evaluatierapportages hebben ertoe geleid dat het Nationaal Beraad eind 2015 de ambitie uitsprak deze standaarden versneld te willen adopteren. Dit betekent concreet dat voor deze standaarden niet het tempo van pas-toe-of-leg-uit wordt gevolgd – wachten op een volgend investeringmoment en dan de standaarden implementeren – maar dat actief wordt ingezet op implementatie van de standaarden op de korte termijn⁴. Voorliggende notitie bevat de resultaten van de meest recente meting van augustus 2016.

Om welke standaarden gaat het

Het Nationaal Beraad heeft bovengenoemde afspraken gemaakt met betrekking tot de volgende standaarden⁵:

- DNSSEC: Domeinnaambeveiliging
- TLS⁶ : Beveiligde verbinding
- DKIM: Anti-Phising
- SPF: Anti-Phising
- DMARC⁷: Anti-Phising (rapportages)

Om welke domeinen gaat het

Het gaat om de volgende groepen met domeinen: (152 niet-gemeenten)

- 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)
-

² 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/>

³ Uitgezonderd: webrichtlijnen en ISO 27001&27002

⁴ Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. Om die reden is de halfjaarlijkse voortgangsrapportage, vanaf dit jaar, ook onderdeel van voorliggende Monitor Open Standaarden.

⁵Zie: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit

⁶ 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.

⁷ 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'.

- De domeinen van de andere partijen die direct of indirect vertegenwoordigd zijn in het nationaal beraad, zoals:
 - o Uitvoerders (de Manifestpartijen)
 - o Provincies en Waterschappen
 - o Partijen die behorend tot Klein LEF

Gemeenten

Omdat VNG/KING ten tijde van de afspraak in het Nationaal Beraad een impact-assessment uitvoerde op de standaarden, is er niet eerder gerapporteerd over de gemeentedomijnen. Het gaat om 398 unieke gemeentedomijnen. In deze rapportage worden de scores van de gemeentedomijnen wel meegenomen. Om de rapportage makkelijk vergelijkbaar te houden met de eerdere halfjaarlijkse rapportages, worden de gemeentescores afzonderlijk weergegeven.

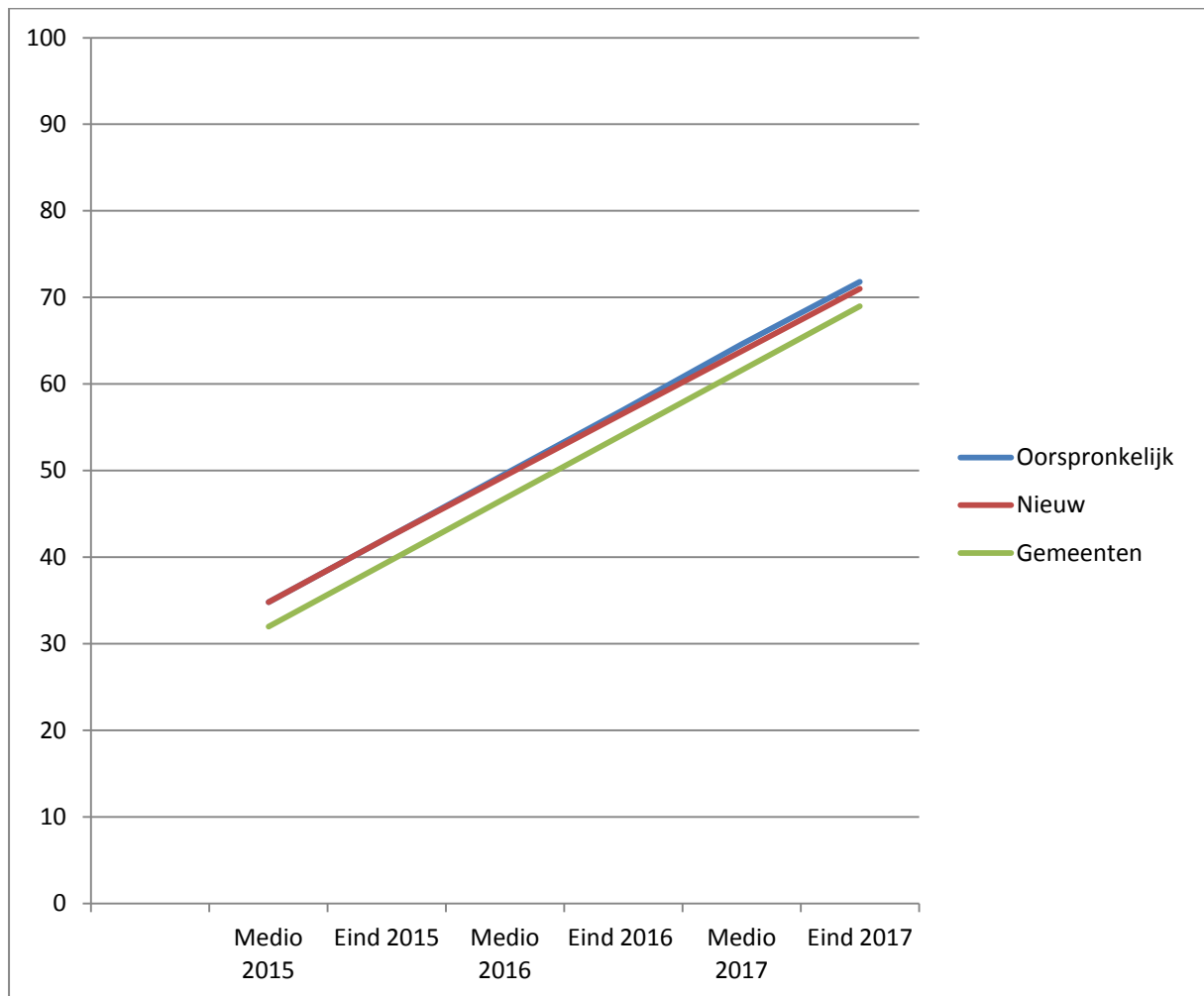
Resultaten

De trend en verwachting

Bij de eerste meting medio 2015 was de gemiddelde adoptiegraad van de 5 standaarden op de toen getoetste set van grofweg 150 Nationaal Beraad domeinen **34,8 %**. Aan het einde van het jaar stond dit percentage op **42,2 %** en medio 2016 op **49,4 %**. Dit betekent dat ondanks de uitgesproken ambitie van het Nationaal Beraad de groei het afgelopen halve jaar zelfs iets is afgenomen (**7,4%** naar **7,2%**).

Als dit groeipercentage wordt geëxtrapoleerd naar het einde van 2017 (einde mandaatperiode van Forum Standaardisatie), dan blijkt dat zonder aanvullende acties, de adoptiegraad op dat moment zal blijven steken op **71%** en daarmee ver achterblijft op het afgesproken streefbeeld om de standaarden eind 2017 – daar waar van toepassing – te hebben geïmplementeerd.

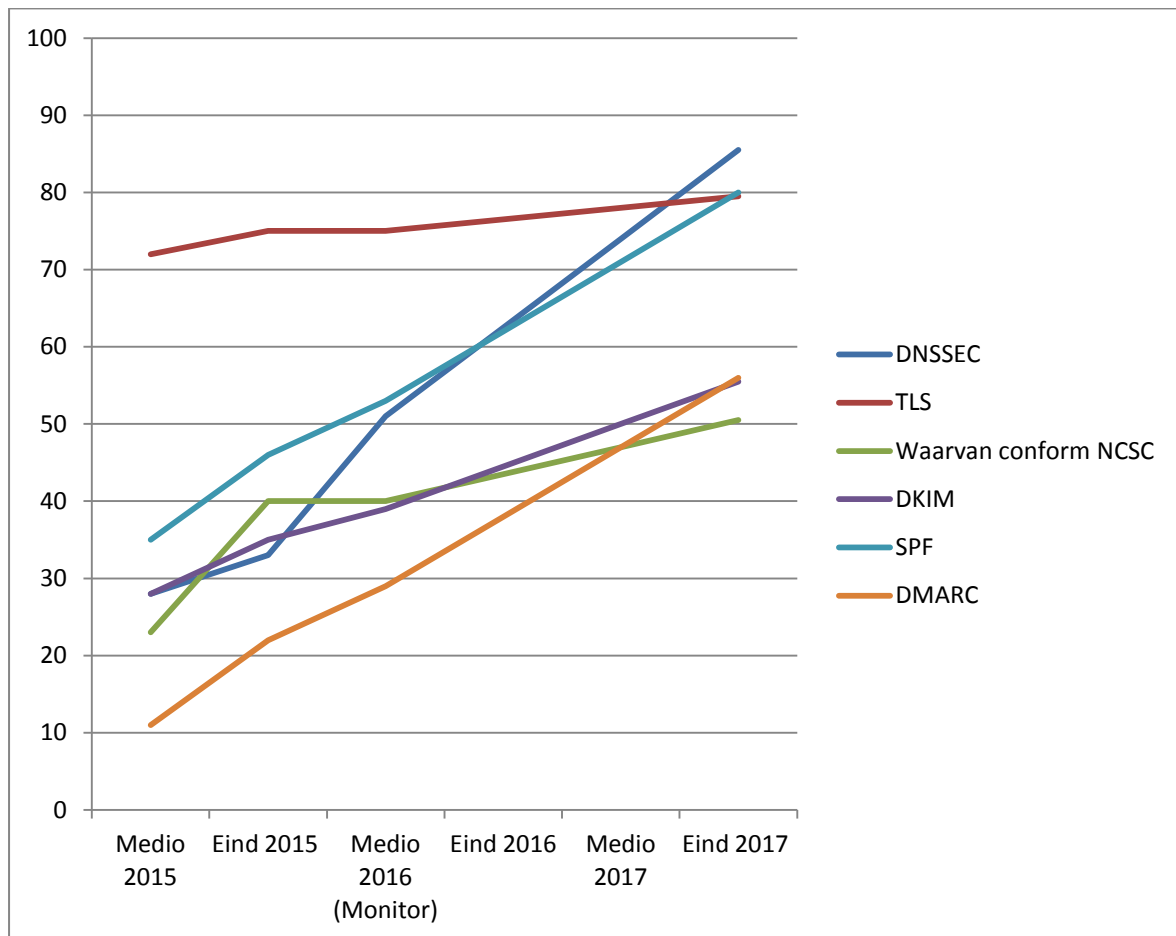
Daarbij valt op dat de groei bij gemeenten bijna praktisch hetzelfde is (7,4% per half jaar) t.o.v. de domeinen van de overige partijen in het Nationaal Beraad. Door de iets lagere adoptiegraad bij de eerste meting (32%) zal de adoptiegraad van gemeenten eind 2017 naar verwachting uitkomen op **69%**

Groei geëxtrapoleerd naar eind 2017

Figuur 3. Groei geëxtrapoleerd naar eind 2017.

- Oorspronkelijk: verwachte groei adoptiegraad tot eind 2017 op basis van groei 2^e helft 2015
- Nieuw: verwachte groei adoptiegraad tot eind 2017 op basis van groei 1^e helft 2016
- Gemeenten: verwachte groei adoptiegraad op basis van groei afgelopen jaar.

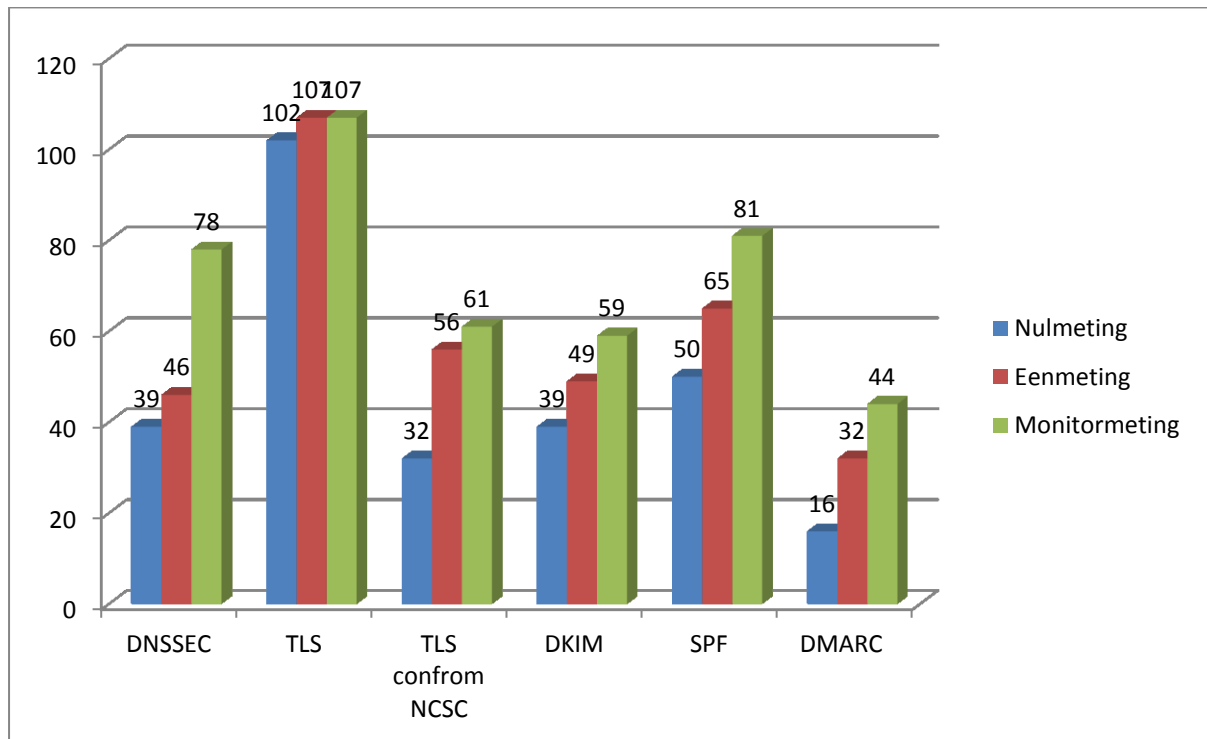
Per standaard ziet de verwachte groei er als volgt uit:



Figuur 4: Gemiddelde groei per standaard geëxtrapoleerd naar eind 2017 (zonder gemeenten)

De resultaten per standaard

Onderstaande scores hebben betrekking op de 152 getoetste niet-gemeentelijke domeinen. De scores per individueel domein zijn opgenomen in de bijlage.



Figuur 3: Nationaal Beraad: De score per standaard in absolute aantallen.

- Nulmeting: medio 2015 (140 domeinen)
- Eenmeting: eind 2015 (152 domeinen)
- Monitormeting: medio 2016 (152 domeinen)

Nationaal Beraad	Nulmeting	Eenmeting	Mid 2016 meting	Vershil
DNSSEC	28%	33%	51%	23%
TLS	72%	75%	75%	3%
Waarvan conform NCSC	23%	40%	40%	17%
DKIM	28%	35%	39%	11%
SPF	35%	46%	53%	18%
DMARC	11%	22%	29%	18%

TLS was en is met afstand de meest toegepaste standaard (75%). Hierdoor is de relatieve groei van TLS beperkt. Daarentegen is het aantal sites dat TLS op de door het NCSC voorgeschreven veilige manier is geconfigureerd over het afgelopen jaar flink gestegen (23% naar 40%)⁸. De groei van DNSSEC was in de 2^e helft 2015 beperkt, maar is met name in de eerste helft van 2016 flink toegenomen. DMARC is een relatief nieuwe standaard die met name in 2015 nog niet veel werd toegepast (11%). DMARC laat over het afgelopen jaar wel de grootste relatieve groei zien (160%).

⁸ Zie: <https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html>)

Best scorende domeinen en grootste stijgers

Onderstaande domeinen behalen een maximale score op de 5 getoetste standaarden en hebben TLS bovendien geconfigureerd volgens de aanbevelingen van het NCSC.

Best scorende domeinen

Domein	Organisatie
www.cbpweb.nl	Autoriteit persoonsgegevens
www.cjib.nl	Centraal Justitieel Incasso Bureau
www.ibdgemeenten.nl	Informatiebeveiligingsdienst voor gemeenten
www.logius.nl	Logius (Min. BZK)
www.rechtspraak.nl	Min. V&J
www.rijksoverheid.nl	Rijksoverheid
www.werkenbijdefensie.nl	Min. Defensie
www.forumstandaardisatie.nl	Forum Standaardisatie
lijsten.forumstandaardisatie.nl	Forum Standaardisatie

Daarnaast zijn er bij veel domeinen aanzienlijke verbeteringen te melden. Twee domeinen hebben vier standaarden meer toegepast dan bij de eerste meting een jaar eerder. En nog eens vijftien domeinen laten een nog steeds indrukwekkende verbetering zien van drie standaarden t.o.v. de eerste meting.

Gestegen met 4 standaarden

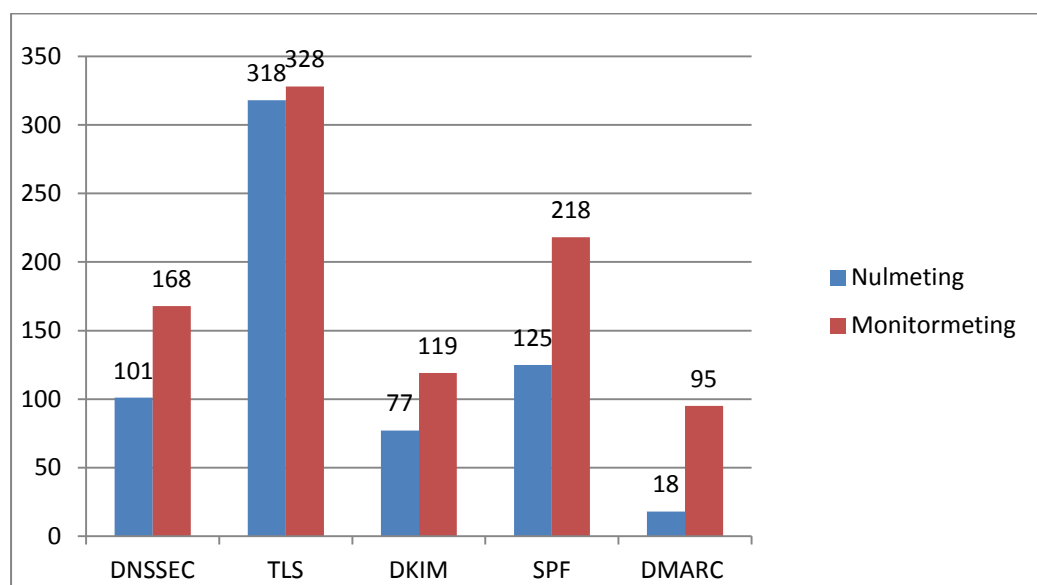
Domein	Organisatie
www.stelselcatalogus.nl	Logius (Min. BZK)
www.derbq.nl	Website van de Regionale Belastinggroep

Gestegen met 3 Standaarden

Domein	Organisatie
www.eidstelsel.nl	Logius (Min. BZK)
www.idensys.nl	Logius (Min. BZK)
register.digikoppeling.nl	Logius (Min. BZK)
www.rijksdienstvooridentiteitsgegevens.nl	Rijksdienst voor identiteitsgegevens (Min. BZK)
www.werk.nl	UWV (Min. SZW)
mijn.toeslagen.nl	Belastingdienst (Min. Fin)
www.duo.nl	DUO (Min OC&W)
siam.duo.nl	DUO (Min OC&W)
www.rijkswaterstaat.nl	Rijkswaterstaat (Min I&M)
www.cbs.nl	Centraal Bureau voor de Statistiek
www.crisis.nl	Nationaal Coördinator Terrorisme Bestrijding (MinV&J)
www.toeslagen.nl	Belastingdienst
www.provinciegroningen.nl	Provincie Groningen
www.prvlimburg.nl	Provincie Limburg
www.bsgw.nl	Belastingsamenwerking gem. en waterschappen Limburg

Gemeenten

In juni 2015 en in augustus 2016 zijn 398 unieke gemeentedomeinen getoetst d.m.v. internet.nl. Dit betreft de hoofddomeinen van de gemeenten. Veel gemeenten hebben daarnaast verschillende (sub)domeinen. Gemeente Den Haag hanteert bijvoorbeeld het domein mijn.denhaag.nl voor het deel van de website dat bedoeld is om als burger of bedrijf gegevens door te geven en diensten aan te vragen. Het is moeilijk om voor alle gemeenten te achterhalen welke domeinen men gebruikt naast het hoofddomein. Om die reden is gekozen alleen de hoofddomeinen te toetsen⁹.



Figuur 4: Gemeenten: De score per standaard in absolute aantallen.

- Nulmeting: medio 2015 (398 domeinen)
- Monitormeting: medio 2016 (398 domeinen)

Gemeenten	Nulmeting	Monitormeting	Vershil
DNSSEC	25%	42%	17%
TLS	80%	82%	2%
Waarvan conform NCSC	nb	21%	nvt
DKIM	19%	30%	11%
SPF	31%	55%	24%
DMARC	5%	25%	20%

Wat vooral opvalt is dat de initiële adoptiegraad van TLS midden 2015 al erg hoog lag (80%) en is gegroeid naar 82% in 2016. Daarbij kan wel worden opgemerkt dat, vergeleken met de niet-gemeentelijke domeinen, het aantal domeinen waarbij TLS is gefigureerd volgens de aanbevelingen van het NCSC¹⁰ relatief laag is (21%). Het gebruik van DNSSEC en met name SPF is flink toegenomen. Ook bij gemeenten bleef de adoptie van DMARC in 2015 achter, maar laat het inmiddels een flinke groei zien (400%).

⁹ Forum Standaardisatie roept gemeenten en overige overheden op om aanvullende domeinen aan te melden waarvan zij vinden dat die onderdeel moeten zijn van de toetsing.

¹⁰ zie <https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html>