Jouw wereld. Ons domein.

Update Registrar Score Card
+
IPv6 inventarisatie

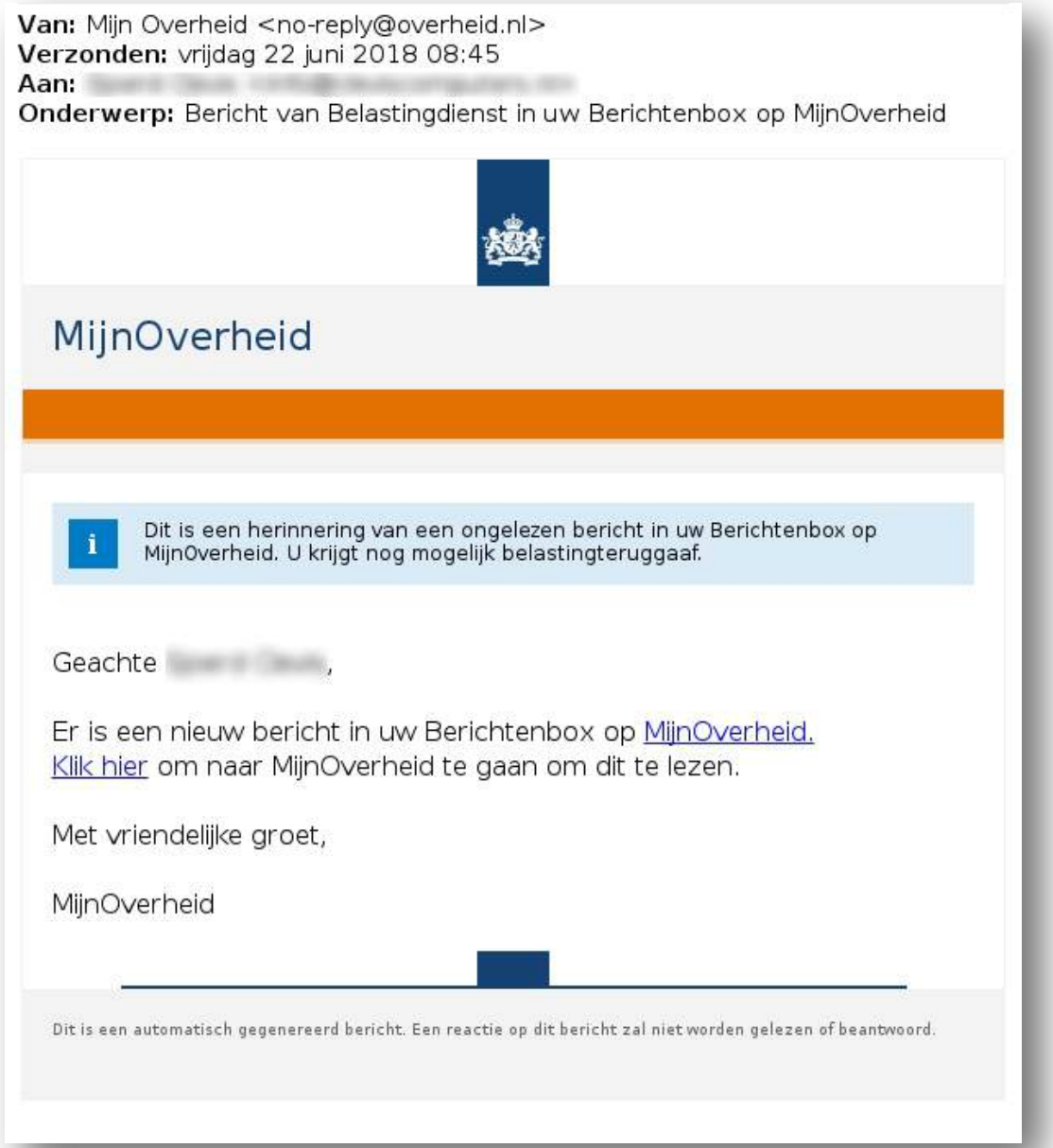
Marco Davids | Platform Internetstandaarden

29 oktober 2018

Klassieke SMTP is kwetsbaar

- *Plain text*, dus gemakkelijk mee te lezen
- Geen afzender-validatie, dus gemakkelijk als ander voor te doen
- Geen inhoud-validatie, dus gemakkelijk te manipuleren
- Geen verzender-validatie, iedereen kan zich als verzender voordoen

Recent voorbeeld



Van: Mijn Overheid <no-reply@overheid.nl>
Verzonden: vrijdag 22 juni 2018 08:45
Aan: [redacted]
Onderwerp: Bericht van Belastingdienst in uw Berichtenbox op MijnOverheid

MijnOverheid

Dit is een herinnering van een ongelezen bericht in uw Berichtenbox op MijnOverheid. U krijgt nog mogelijk belastingteruggaaf.

Geachte [redacted],

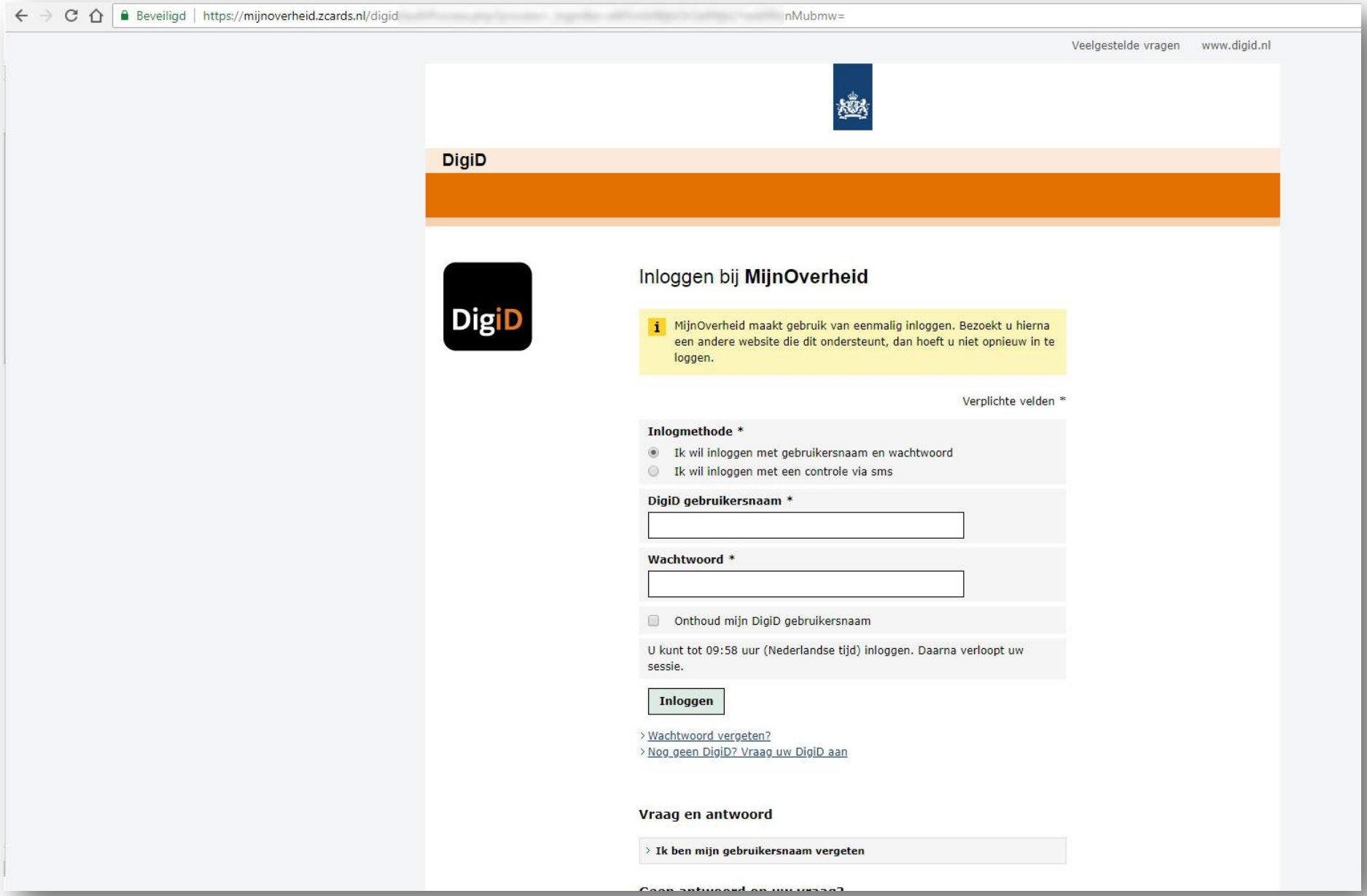
Er is een nieuw bericht in uw Berichtenbox op MijnOverheid.
Klik hier om naar MijnOverheid te gaan om dit te lezen.

Met vriendelijke groet,

MijnOverheid

Dit is een automatisch gegenereerd bericht. Een reactie op dit bericht zal niet worden gelezen of beantwoord.

Recent voorbeeld



Recent voorbeeld

Van:
Datum: 23-10-18 15:26 (GMT+01:00)
Aan:
Onderwerp: Attention: Your Email Has Been Hacked.

Hello my nickname in darknet is *****.
I'll begin by saying that I hacked this mailbox ****** (please look on 'from' in your header) more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

Even if you changed the password after that – it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history. Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

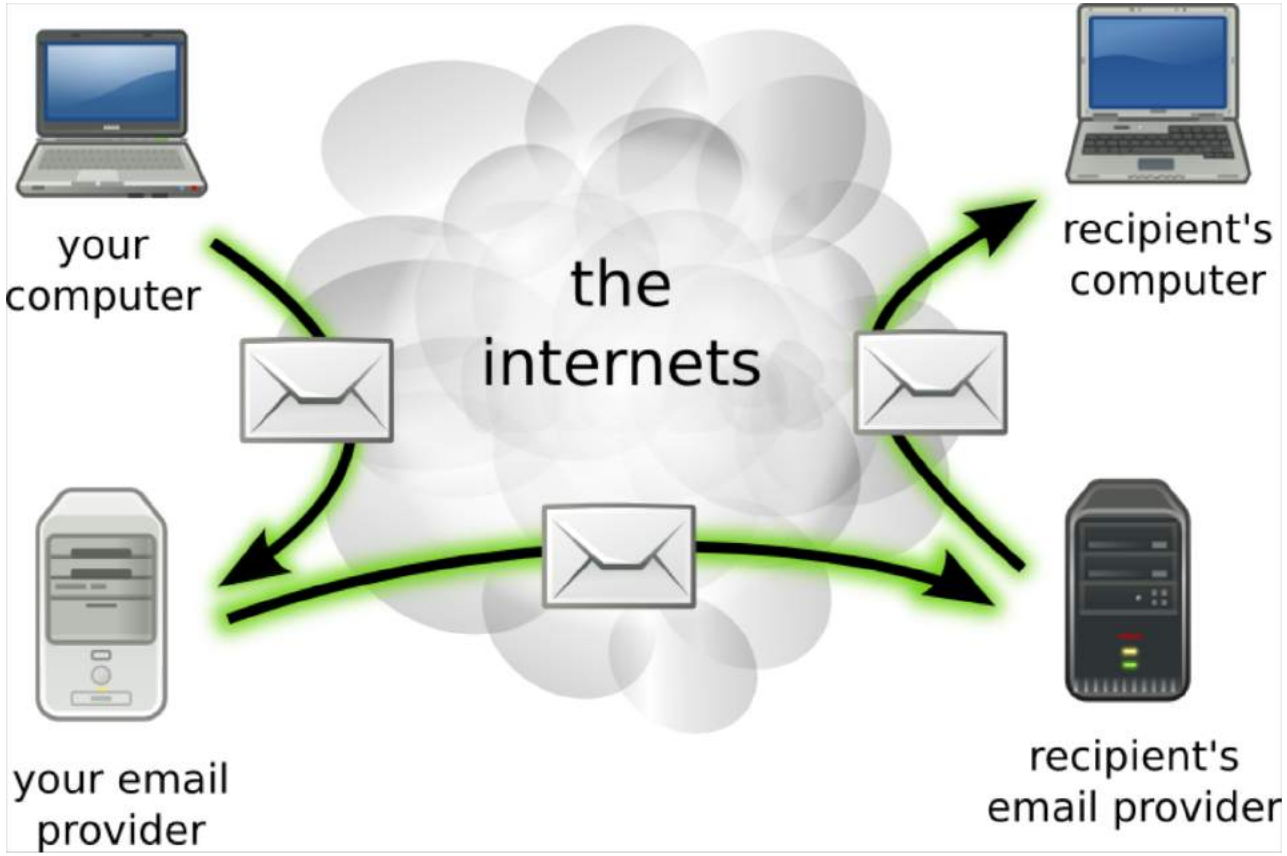
I was most struck by the intimate content sites that you occasionally visit. You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching. Oh my god! You are so funny and excited!

Antwoord:

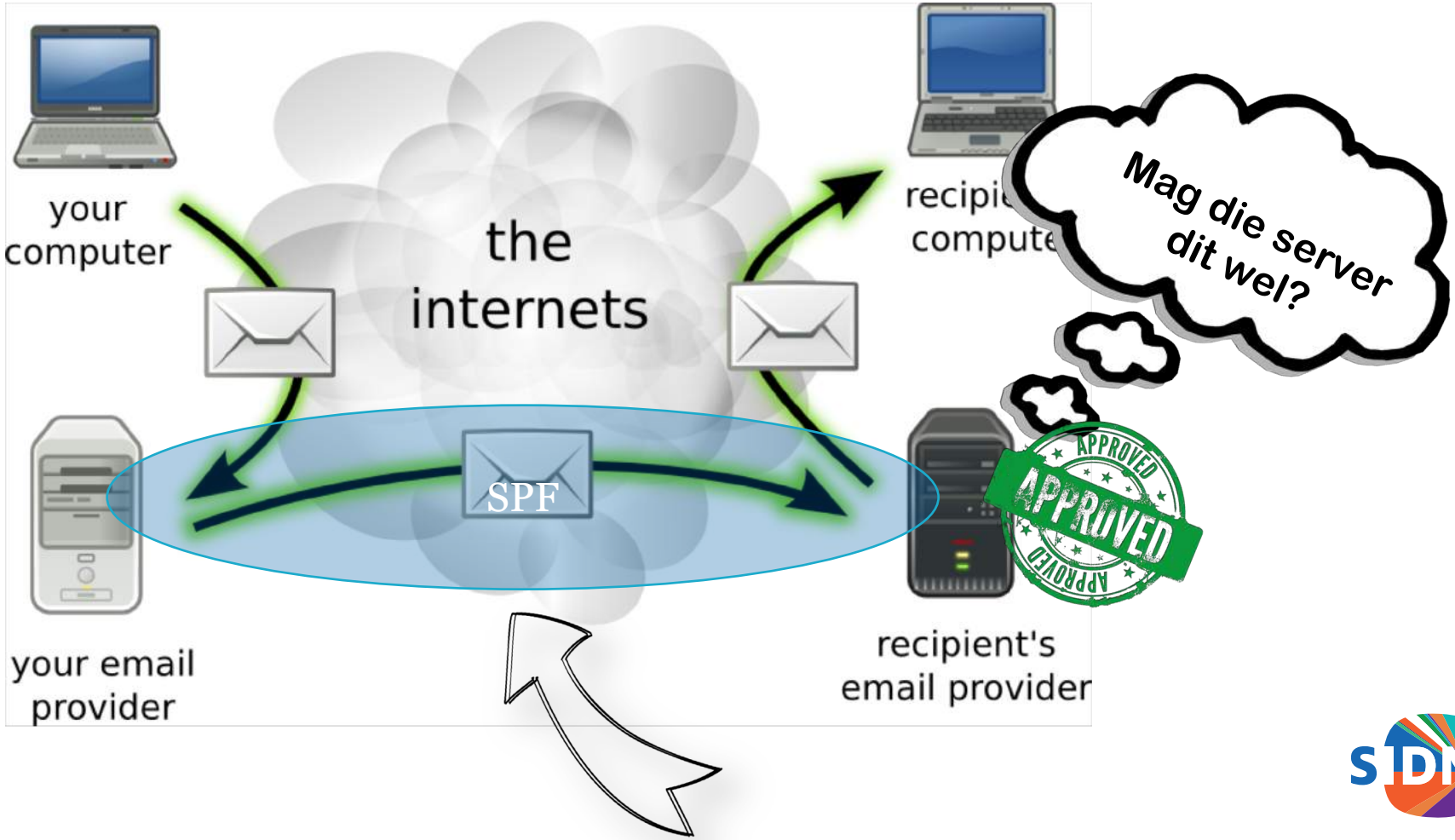
- SPF,
- DKIM,
- DMARC,
- STARTTLS

Mailflow


your
computer
the
internets
recipient's
computer
your email
provider
recipient's
email provider

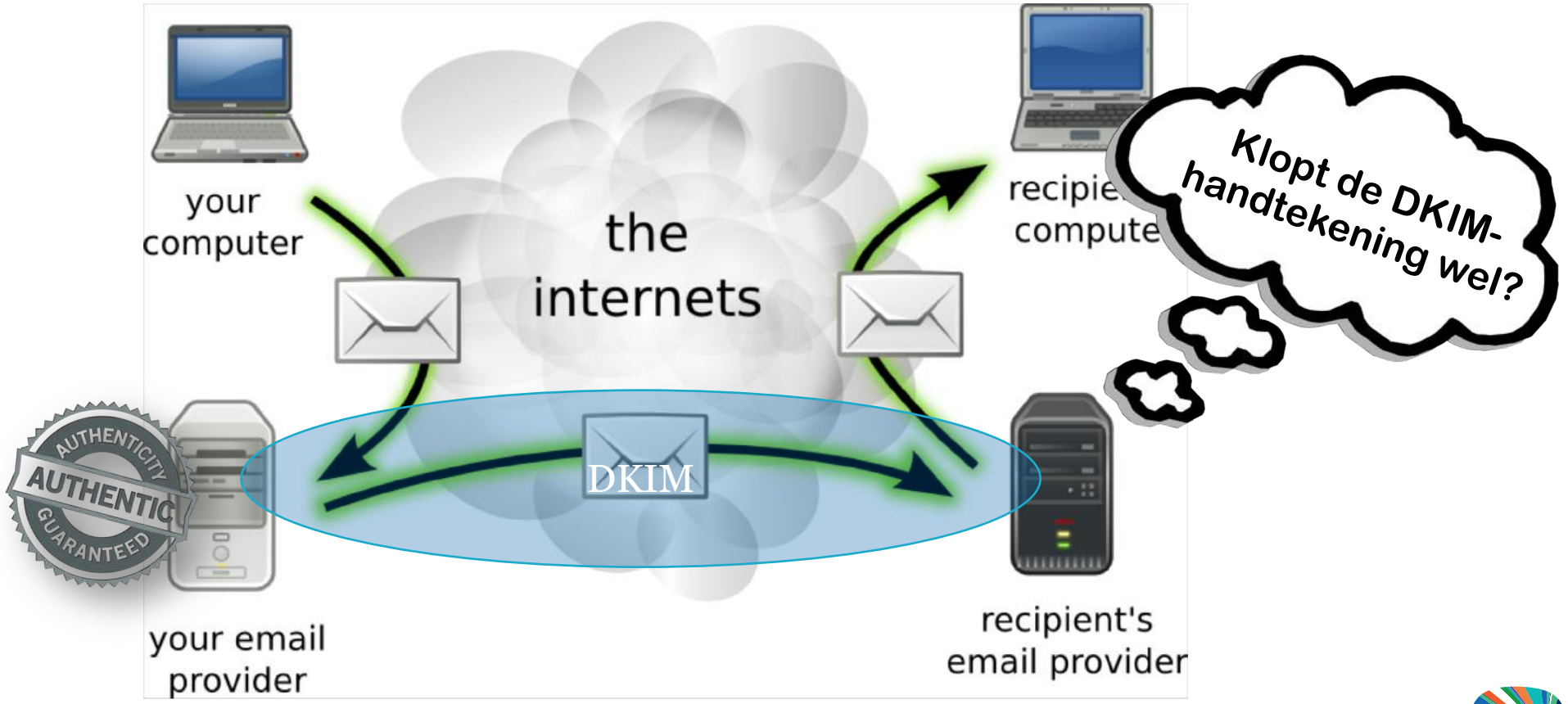
SPF (Sender Policy Framework)

Mailflow:



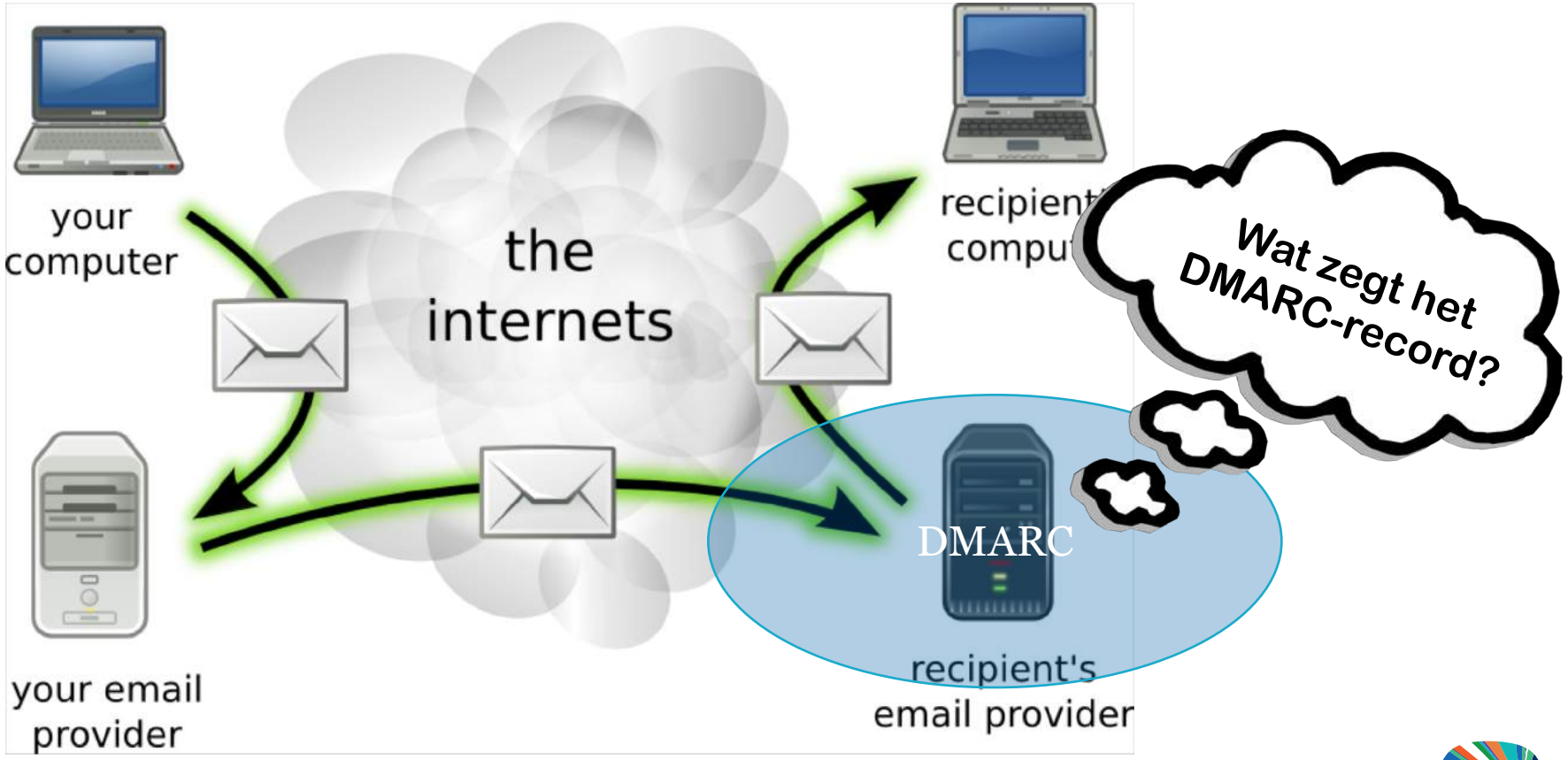
DKIM (DomainKeys Identified Mail)

Mailflow:



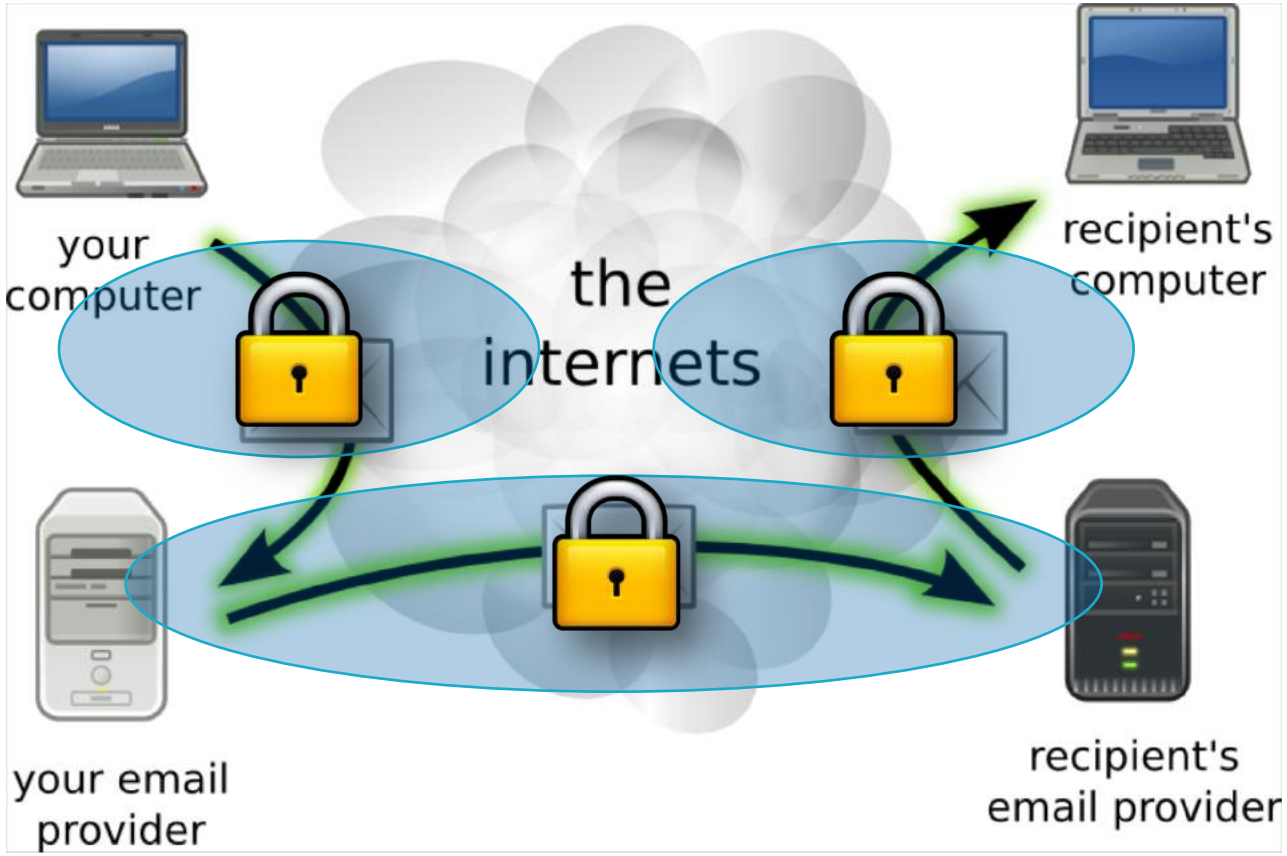
DMARC (Domain-based Message Authentication, Reporting and Conformance)

Mailflow:



STARTTLS

Mailflow:



En als ik nooit mail?

- DKIM/DMARC/SPF-settings zijn ook nuttig voor domeinnamen die nooit zullen mailen of mail hoeven te ontvangen
- In dat geval ook ‘Null MX’-record toevoegen (RFC7505)

```
MX   0 .
TXT "v=spf1 -all”
TXT "v=DMARC1; p=reject"
```

https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12.pdf

SIDN LABS

Samenvattend

- Klassieke e-mail is een probleem
- Er zijn nieuwe standaarden die hier een oplossing bieden.
- Deze standaarden zijn volwassen genoeg voor '*deployment*'
- Ze worden (m.u.v. DANE) dan ook al grootschalig toegepast
- We belonen het gebruik ervan via de RSC! 😊

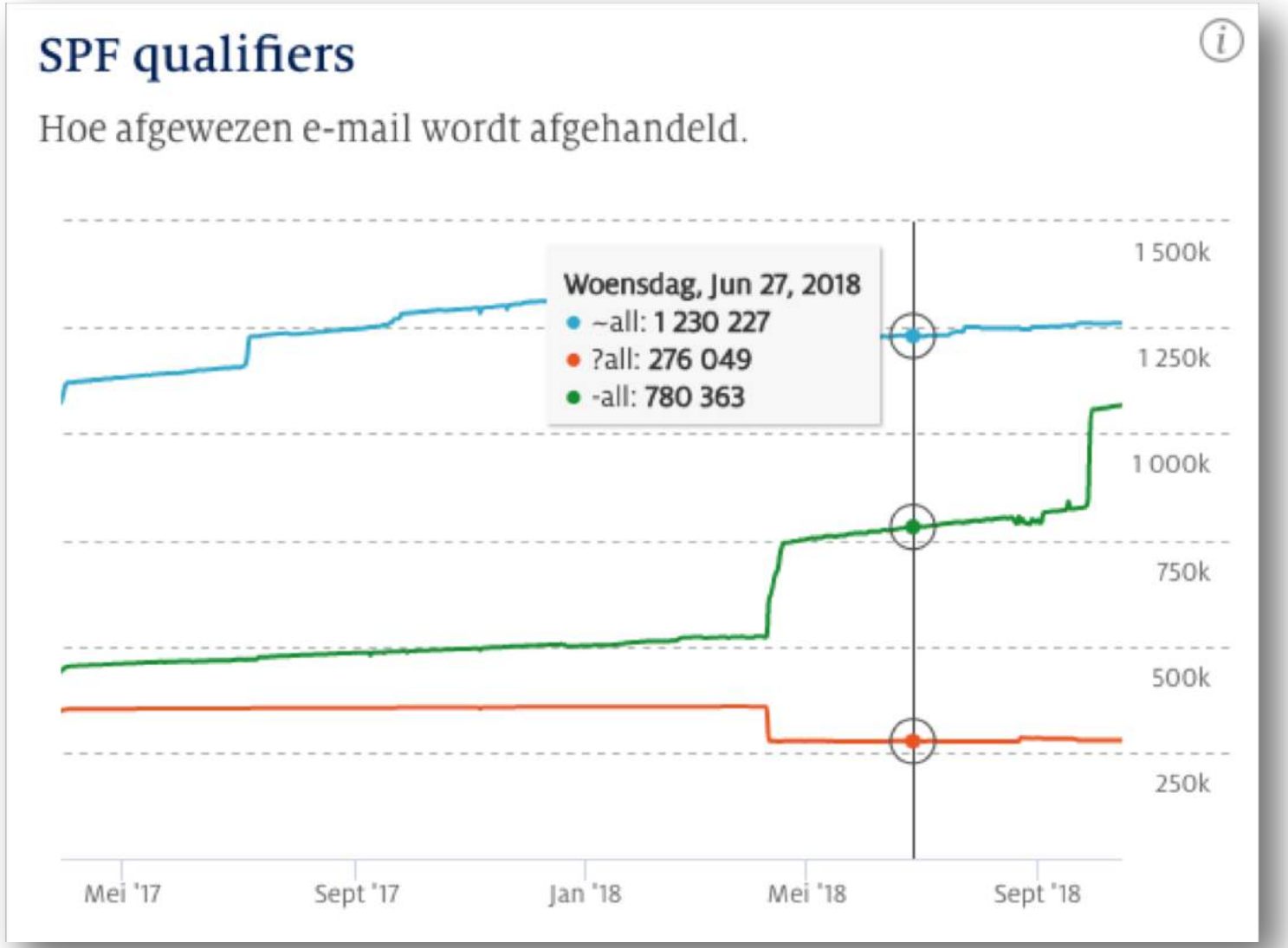
Meetmethodiek e-mail

Veilige e-mail meetmethodiek (1)

- STARTTLS: MX-record: ontdubbel eerst op IP-adres
  - Controleer of STARTTLS wordt ondersteund
  - Sla per mailserver resultaat op, voorkomt onnodig verkeer en blacklisting
- SPF: TXT-record van de apex opvragen, 8 evaluatie-resultaten mogelijk:
  - 1: *none*; geen SPF gevonden of geen goede domeinnaam uit SMTP-sessie kunnen halen
  - 2: *pass*; (+all) accepteer alles
  - 3: *hard fail*; (-all) accepteer het bericht niet, als SPF niet klopt
  - 4: *soft fail*; (~all) accepteer het bericht eventueel, maar markeer dit als verdacht
  - 5: *neutral*; (?all) accepteer het bericht, markeer het niet
  - 6: *permanent error*: permanente fout, bijvoorbeeld syntax-error
  - 7: *temporary error*: tijdelijke fout, bijvoorbeeld time out
  - 8: *unknown*: Al het andere, komt nauwelijks voor, was dan bijv. bugje in software

SIDN LABS

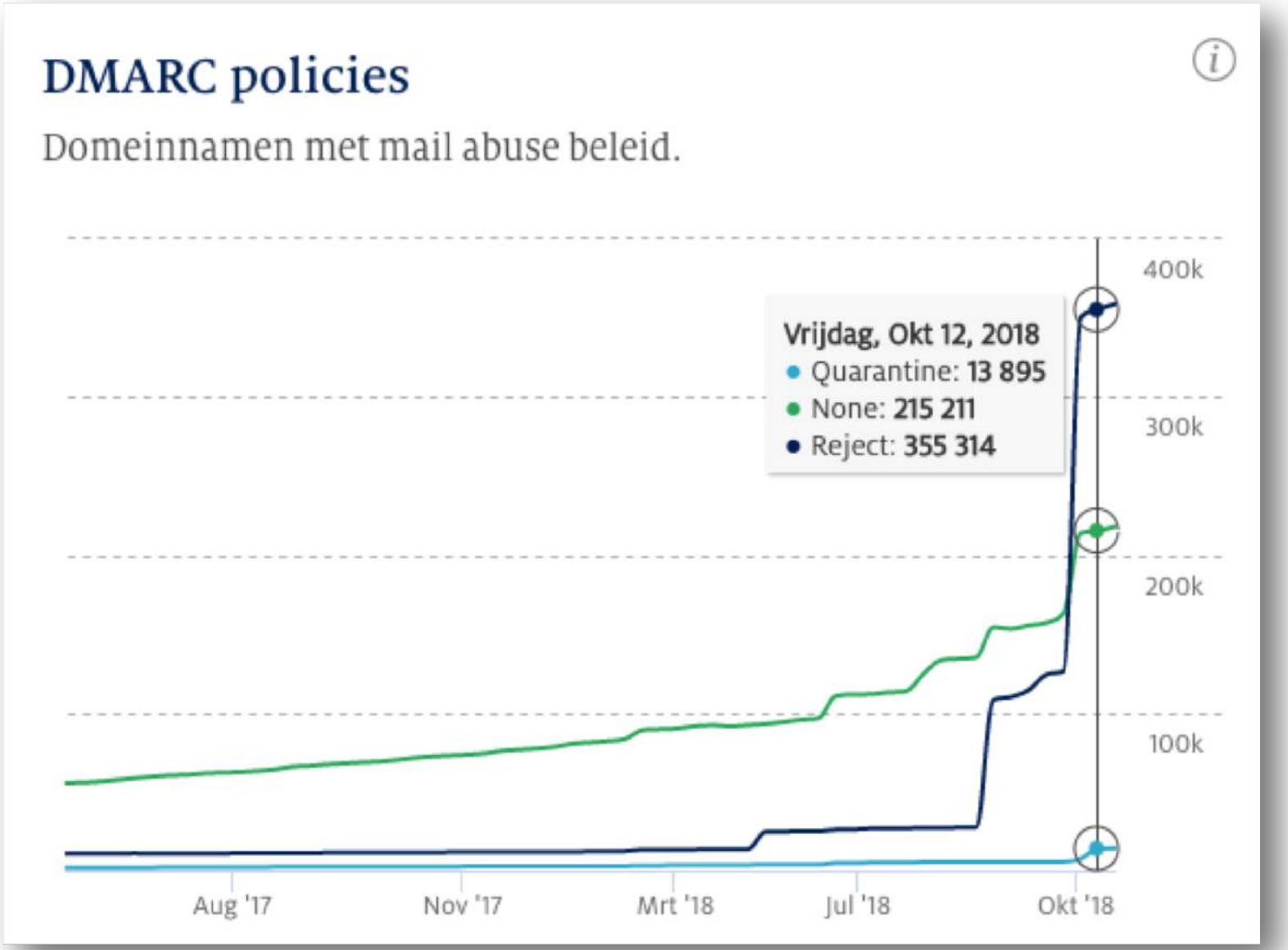
Veilige e-mail meetmethodiek (1)



Veilige e-mail meetmethodiek (2)

- DKIM: controle op de (onbekende) selector
  - Voorbeeld: `$eenlabel._domainkey.example.nl`
  - Empty non-terminal (_domainkey) aanwezig (NO DATA): dan aanname dat DKIM er is
  - Indien niet aanwezig (NX DOMAIN): dan aanname dat er geen DKIM is
- DMARC: controle op `_dmarc.example.nl`
  - Eenvoudig te meten
  - Let op: heb je SPF *–all* ingesteld? Dan moet je *p=reject* of *p=quarantaine*. DKIM is in dat geval niet noodzakelijk
  - Syntactisch juist, policy juist? Dan een incentive

Veilige e-mail meetmethodiek (2)



Veilige e-mail meetmethodiek (3)

- Starten met STARTTLS en DMARC (elke policy, dus ook *p=none*)
- Doorgroeien naar een strakkere policy voor DMARC
- Belonen op DMARC, niet specifiek op DKIM en SPF want die zijn randvoorwaardelijk aan DMARC-implementatie

- Toegelicht via SIDN Webinar over de RSC*
- Tevens uitgelegd via onze SIDN Academy over e-mailbeveiliging

*https://www.onlineseminar.nl/sidn/webinar/22325/ontwikkelingen-registrar-scorecard

SIDN LABS

Minimale duur per incentive

Incentives	H2- 2018	H1- 2019	H2-2019	H1-2020	H2- 2020
DPO	→				
DNSSEC	→ onderzoek naar incentive op DNSSEC-validatie				
IPV6	→	→	→		
Veilige e-mail	→	→	→		

Incentive overzicht H2 2018

- *Duurzame Portfolio Optimalisatie*, DPO (ongewijzigd)
- *IPV6* (ongewijzigd)
- *DNSSEC*, de incentive wordt verlaagd. Komende tijd onderzoek naar incentive op validatie DNSSEC
- *Datakwaliteit* komt te vervallen, maar ge-update informatie blijft beschikbaar op dashboard
- Nieuwe incentive: *veilige e-mailstandaarden;* DMARC, SPF, DKIM en STARTLS

IPv6 uitkering

- Uitkering op domeinnamen waarvan nameserver, webserver en/of e-mailserver via (IPv4 en) IPv6 te bereiken zijn.
- Basisprincipe: alles wat via v4 werkt, moet ook via v6 werken. En er moet minstens íets actiefs gebeuren op de domeinnaam: web of e-mail.
- Minimaal twee nameservers via IPv6 bereikbaar.
- Als website via v4 bereikbaar is, moet v6 ook bereikbaar zijn.
- Als e-mailserver via v4 bereikbaar is, moet v6 ook bereikbaar zijn.
- Is v4 niet bereikbaar, dan hoeft v6 ook niet bereikbaar te zijn.
- Hierbij geldt dat wel minstens één van beide (web of e-mail) moet werken.

Resultaten incentives

Incentives	Start bij start	Eind 2017	Huidige stand
DPO: Actief gebruik Netto groei	start medio 2017 23,1% 1%	 22,6% 0,85%	 21,4% 0,3%
DNSSEC	start medio 2012 0,32% 15.686	 49,27% 2.854.827	 52,16% 3.043.767
IPV6	start medio 2017 11,7% 669.709	 26,8%% 1.554.000	 28,38% 1.648.636
Datakwaliteit Adres Tel E-mail	Start medio 2015 70%*	 80,9% 84% 84,8%	 80,7% 84,9% 85,9%

SIDN LABS

Resultaten incentives

DKIM

reference_date	count
Thursday, 28 June 2018	364,693
Wednesday, 18 July 2018	384,830
Monday, 13 August 2018	871,350
Friday, 19 October 2018	995,355

STARTTLS

reference_date	count
Thursday, 28 June 2018	3,220,270
Wednesday, 18 July 2018	3,038,017
Monday, 13 August 2018	3,394,193
Wednesday, 12 September 2018	3,523,999
Friday, 19 October 2018	3,537,456

DMARC (none, reject) + SPF 2

reference_date	count
Thursday, 28 June 2018	13,873
Wednesday, 18 July 2018	14,559
Monday, 13 August 2018	75,407
Friday, 19 October 2018	87,097

DMARC (all) + SPF 3&4

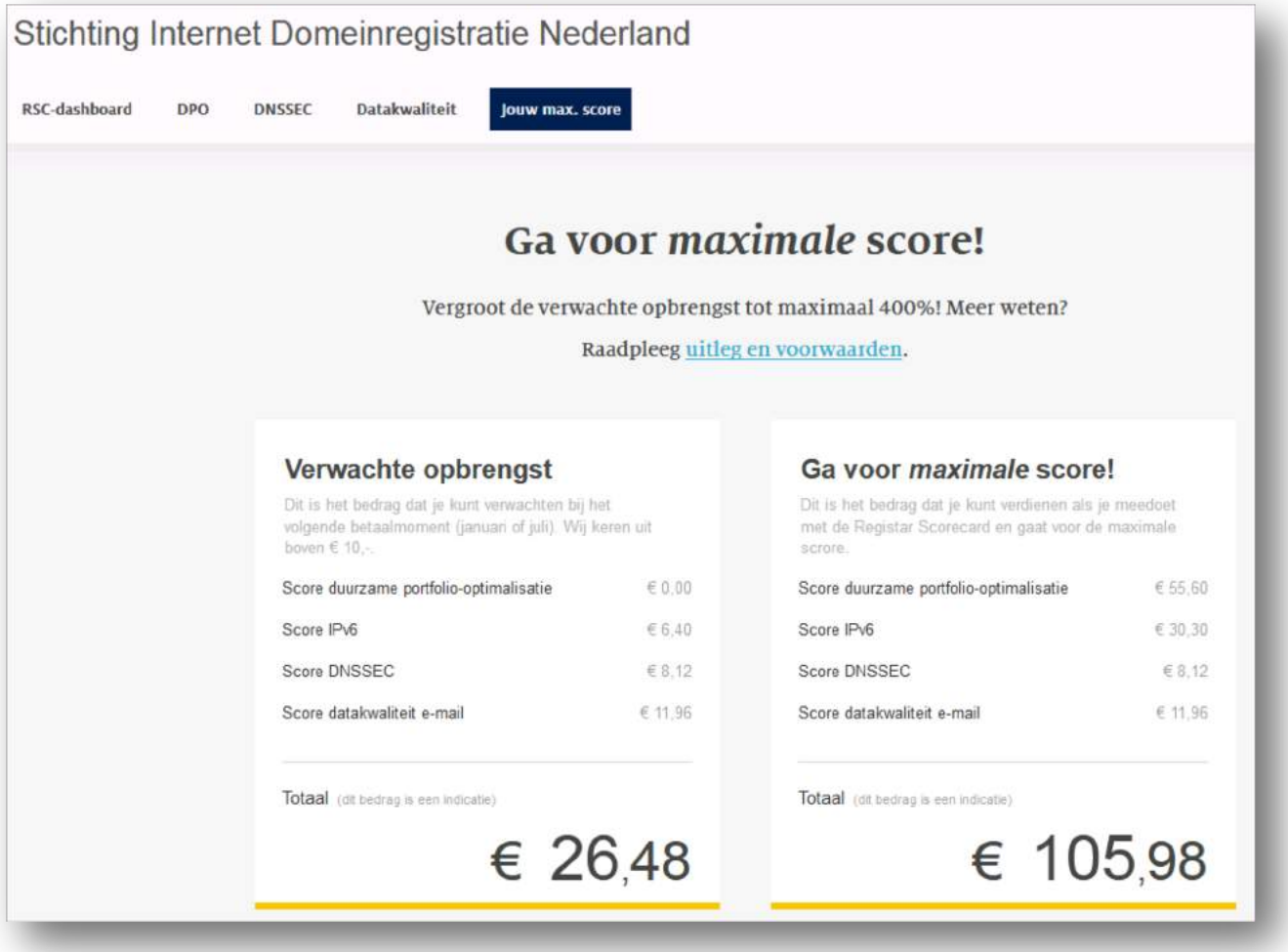
reference_date	count
Thursday, 28 June 2018	69,152
Wednesday, 18 July 2018	72,399
Monday, 13 August 2018	94,300
Wednesday, 12 September 2018	113,454
Friday, 19 October 2018	125,013

SIDN LABS

RSC dashboard

Informatieve meters (1)

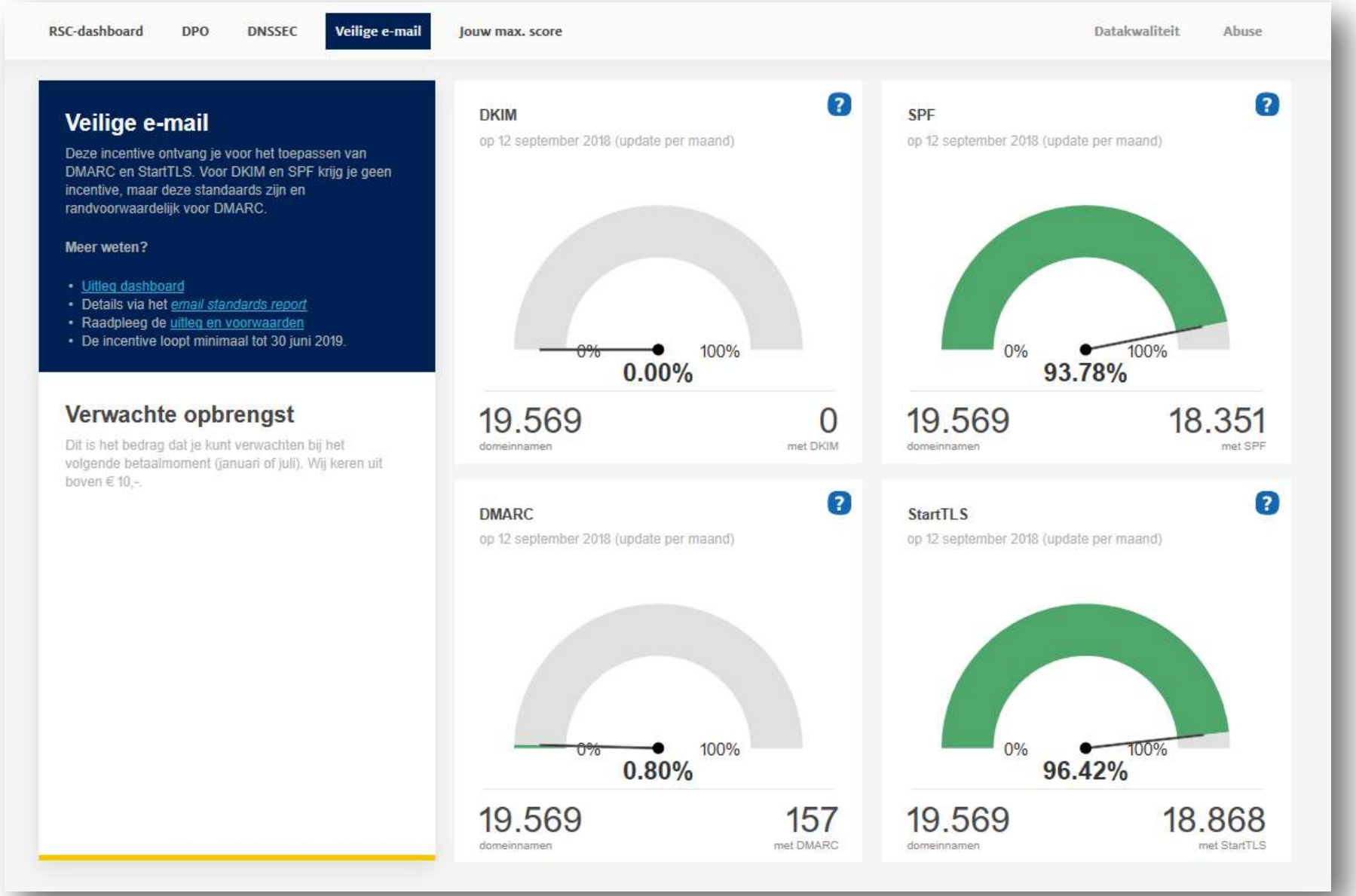
- Datakwaliteit blijft beschikbaar op dashboard
- Maximale score zichtbaar



Informatieve meters (2)

- Nieuwe abuse-meter beschikbaar

Incentive-meters voor email



IPv6 onderzoek*

Medio 2018

*https://www.sidn.nl/a/over-sidn/achterblijven-implementatie-ipv6-schaadt-nederlands-innovatieklimaat

IPv6 Onderzoek SIDN – medio 2018

- Gericht op organisaties die kritieke rol spelen in infrastructuur
  - O.a. lijst ‘vitale aanbieders’ volgens ‘besluit meldplicht cybersecurity’
  - Verrijkt met andere sectoren
  - Drinkwaterbedrijven, netbeheerders, banken, telecom, ISP’s, haven Rotterdam, Schiphol, Brainport-regio Eindhoven, wegennet, vaarwegen, zorg, wetenschappelijk onderzoek, openbare orde & veiligheid, online media

IPv6 Onderzoek SIDN – medio 2018

- Getest met SIDN Lab's DMAP-crawler* en https://internet.nl/

onderdeel	geslaagd
DNS	2+ servers bereikbaar
web	1+ server bereikbaar (met of zonder www ervoor)
mail	1+ gateway bereikbaar (alleen als ook mail-domein)
totaal	geslaagd op alledrie onderdelen

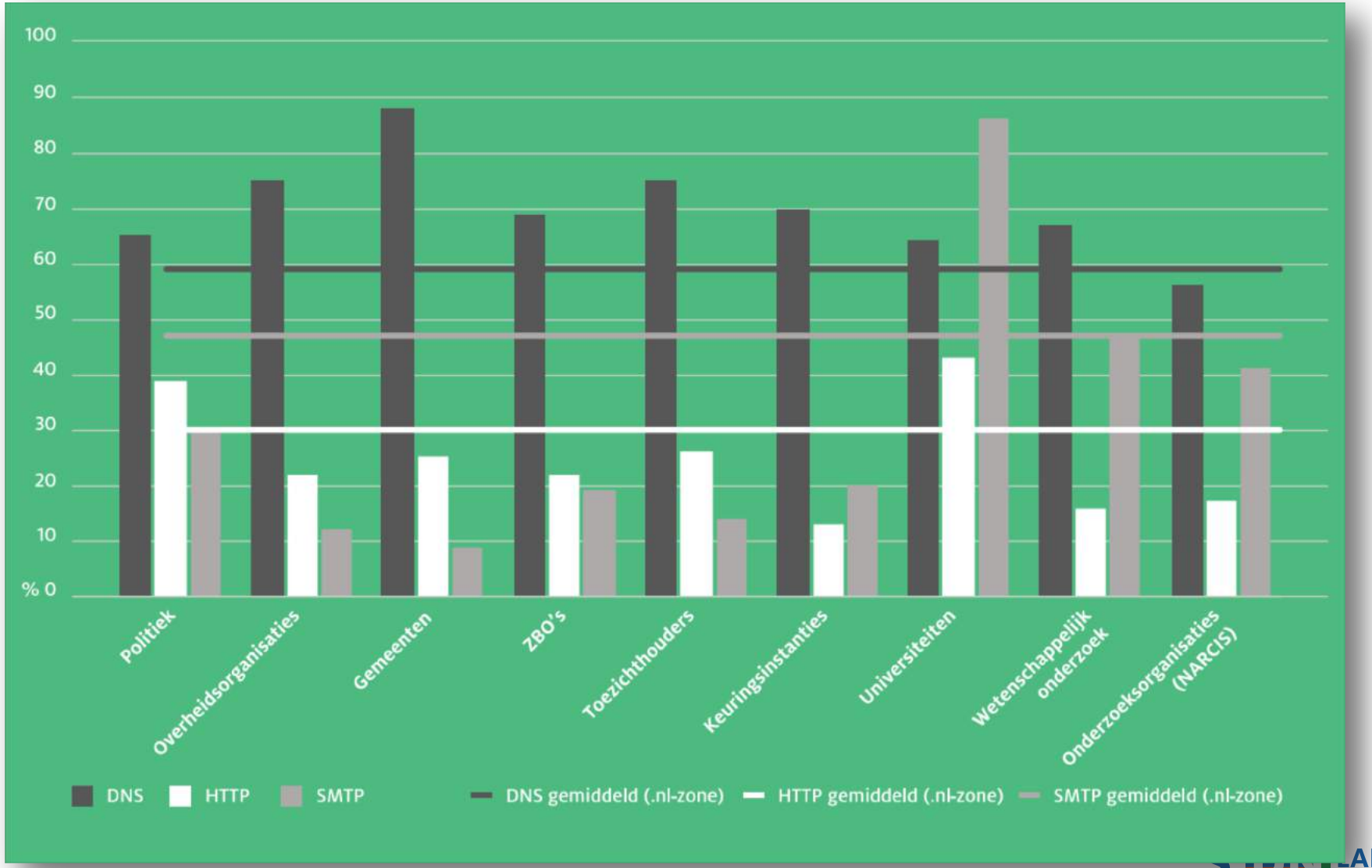
* https://dmap.sidnlabs.nl/

IPv6 Onderzoek SIDN – medio 2018

- DNS komt als beste uit de bus (effect van incentive-regeling?)
- Totaalscore valt erg tegen
- Geen helder beleid (IPv6 lijkt meer geluk dan wijsheid)
- Middelgrote partijen scoren het slechtst

IPv6 Onderzoek SIDN – medio 2018

Publieke sector:



IPv6 Onderzoek SIDN – medio 2018

Volledige rapport:

https://www.sidn.nl/downloads/reports/IPv6-inventarisatie%202018_270918.pdf

Bedankt voor de aandacht!

Check het op: https://stats.sidn.nl/

@marcodavids

SIDN LABS