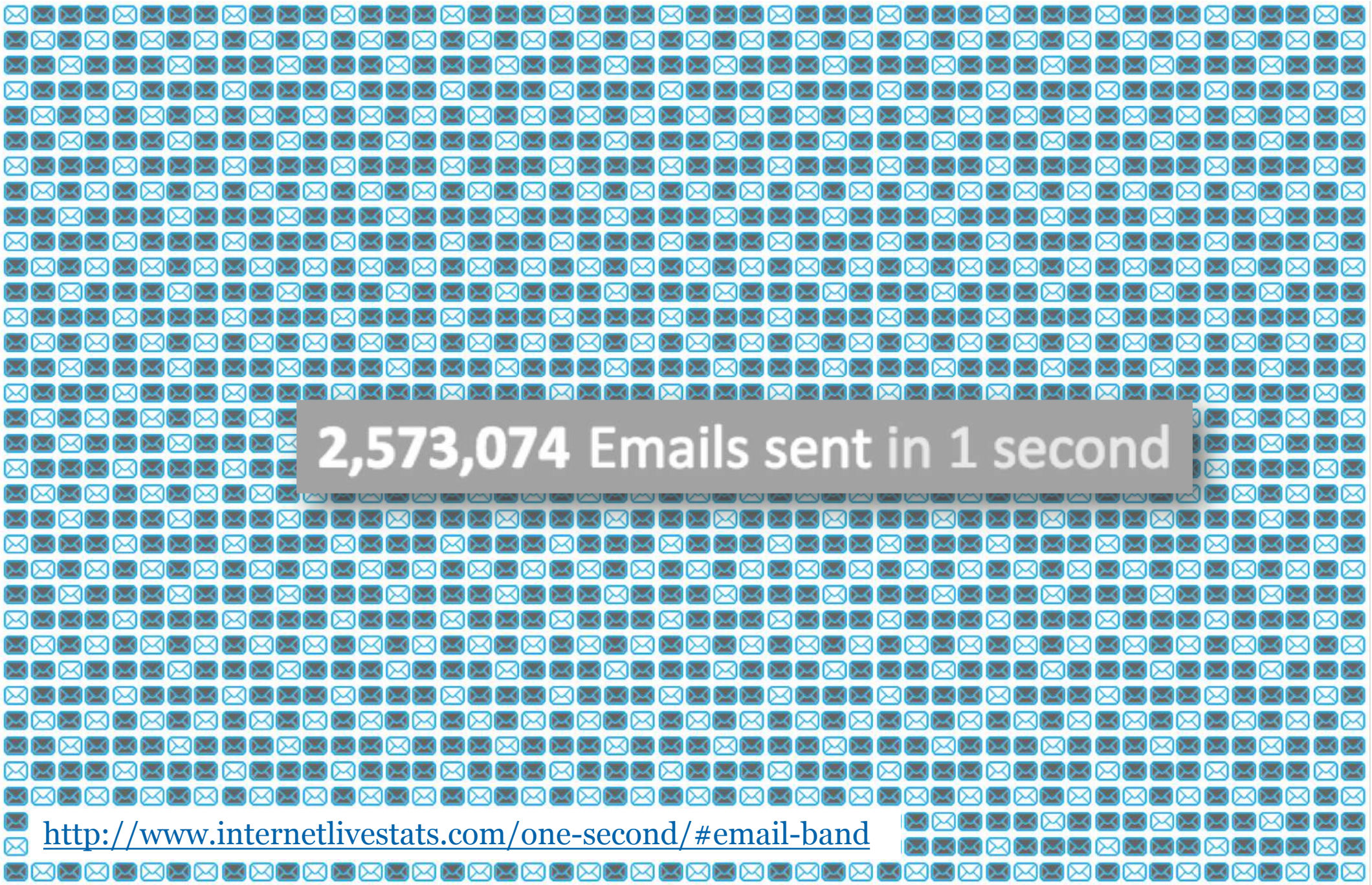
Moderne E-mailstandaarden
Veiliger e-mail

Marco Davids | RealHosting Partner Event

11 oktober 2018

SIDN LABS

TABLE OF CONTENTS



http://www.internetlivestats.com/one-second/#email-band

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

Gevolgen…

- Heel veel *spam* (50-98%)
- *Phishing* (= geld stelen)
- *Malware* (= ergernis en andere ellende)
- *Ransomware* (= is geld aftroggelen)

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],

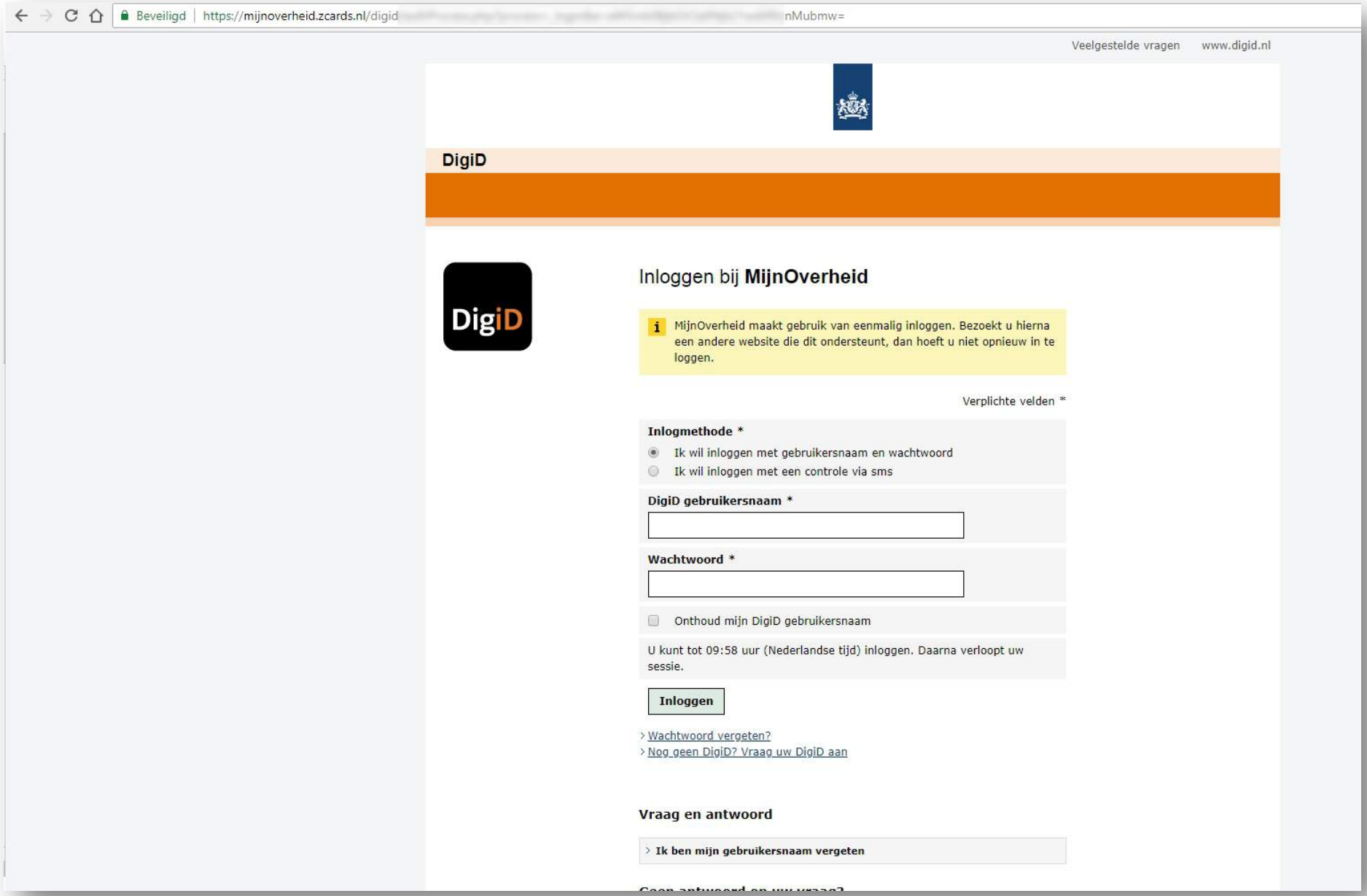
Er is een nieuw bericht in uw Berichtenbox op MijnOverheid.
Klik hier om naar MijnOverheid te gaan om dit te lezen.

Met vriendelijke groet,

MijnOverheid

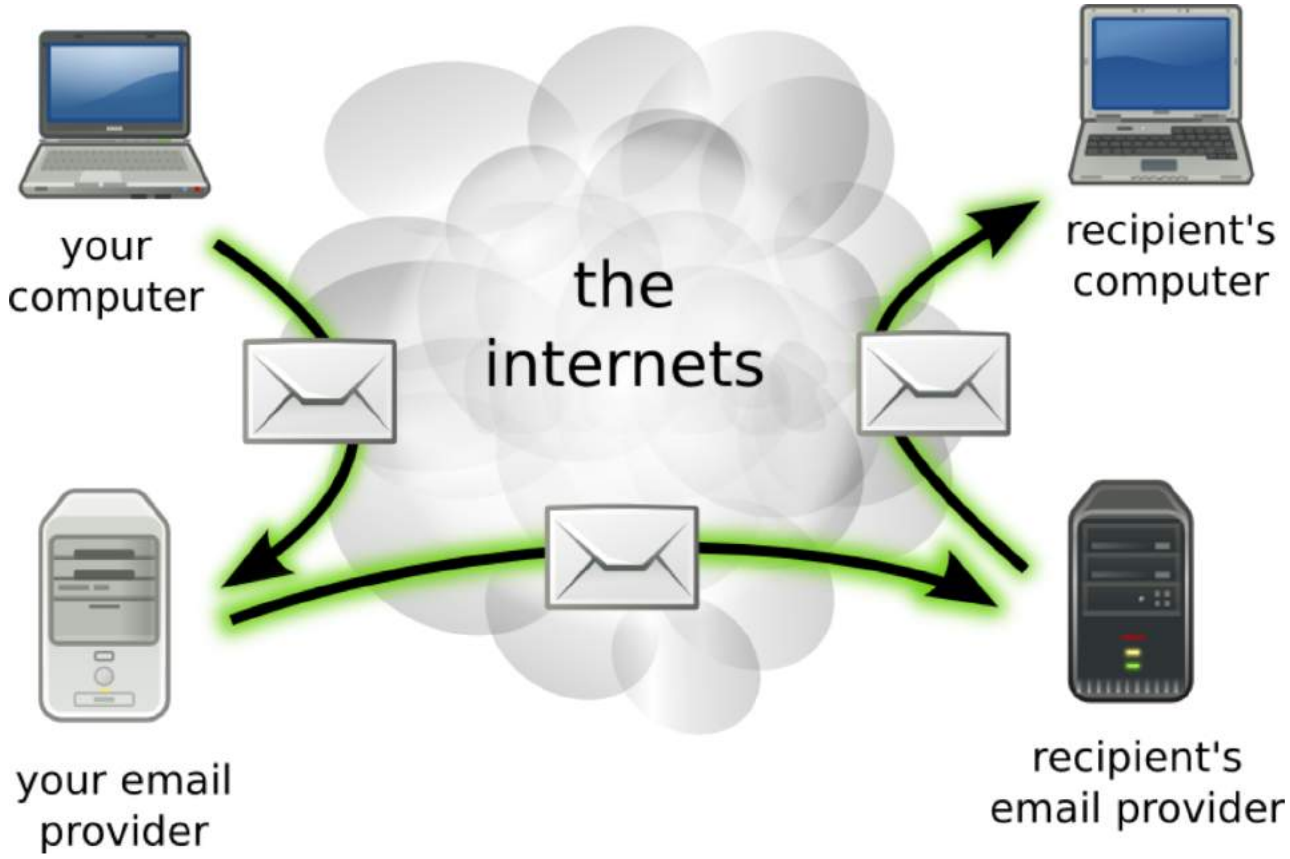
Dit is een automatisch gegenereerd bericht. Een reactie op dit bericht zal niet worden gelezen of beantwoord.

Recent voorbeeld



Antwoord: DKIM, DMARC en SPF en STARTTLS

Mailflow:



Aanpak:

- SPF,
- DKIM,
- DMARC,
- STARTTLS

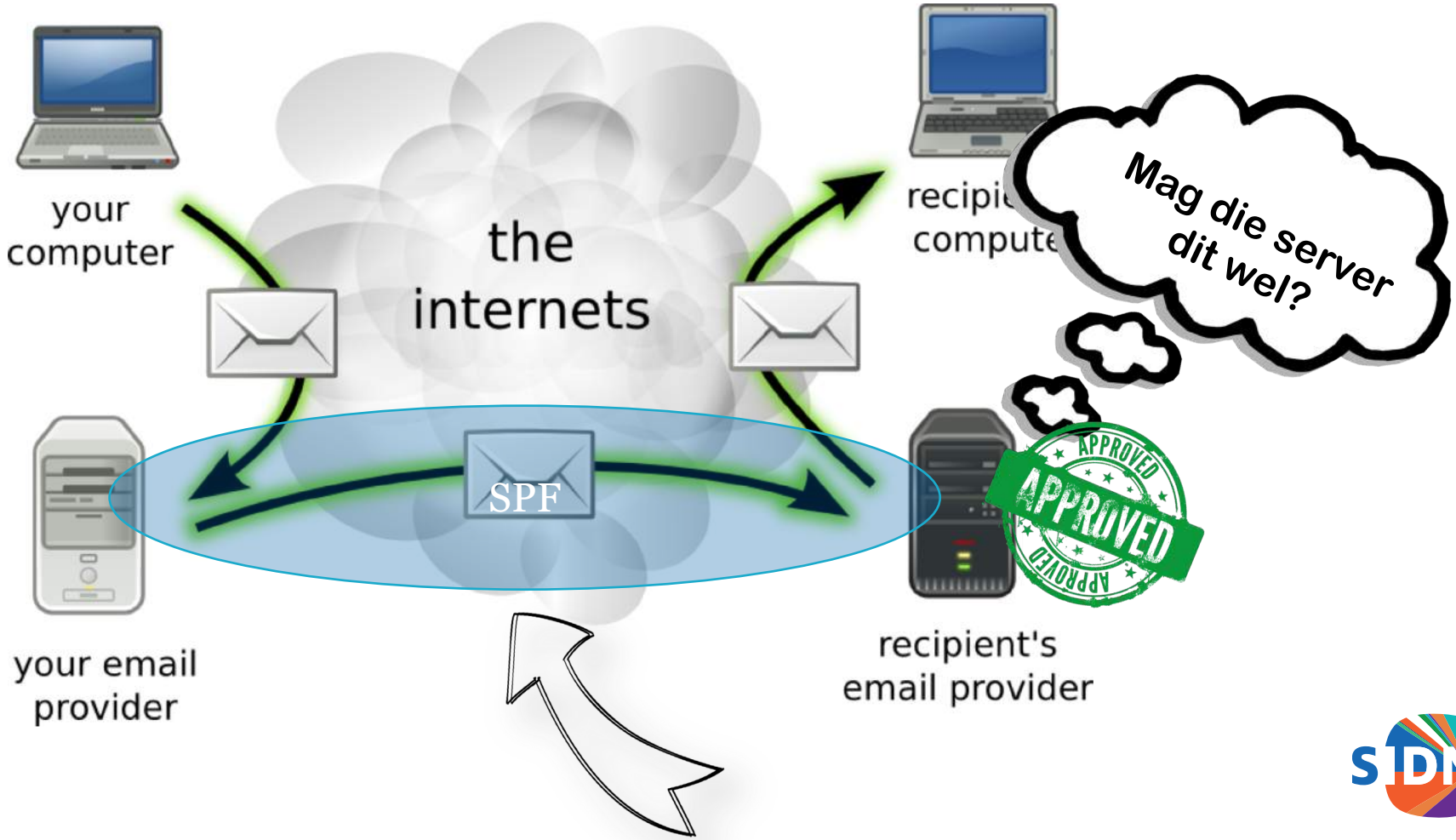
SPF (Sender Policy Framework)

Werking:

- Het SPF-record is een TXT-record in het DNS
- In het SPF-record staat aangegeven welke systemen mail mogen sturen voor het betreffende domein:

SPF (Sender Policy Framework)

Mailflow:



SPF (Sender Policy Framework)

Voordelen:

- Minder ‘valse’ mail
- Betere controle over mailstromen, betere e-mail reputatie

Aandachtspunt:

- *Forwarding* kan problemen geven (vandaar ‘*softfail*’)

DKIM (DomainKeys Identified Mail)

Werking:

- In het DNS staat een publieke sleutel (TXT-record)
- Verzendende MTA beschikt over een private sleutel
- Verzendende MTA voegt ‘DKIM-header’ toe aan uitgaande e-mails
- Ontv. MTA kan deze header controleren m.b.v. publieke sleutel

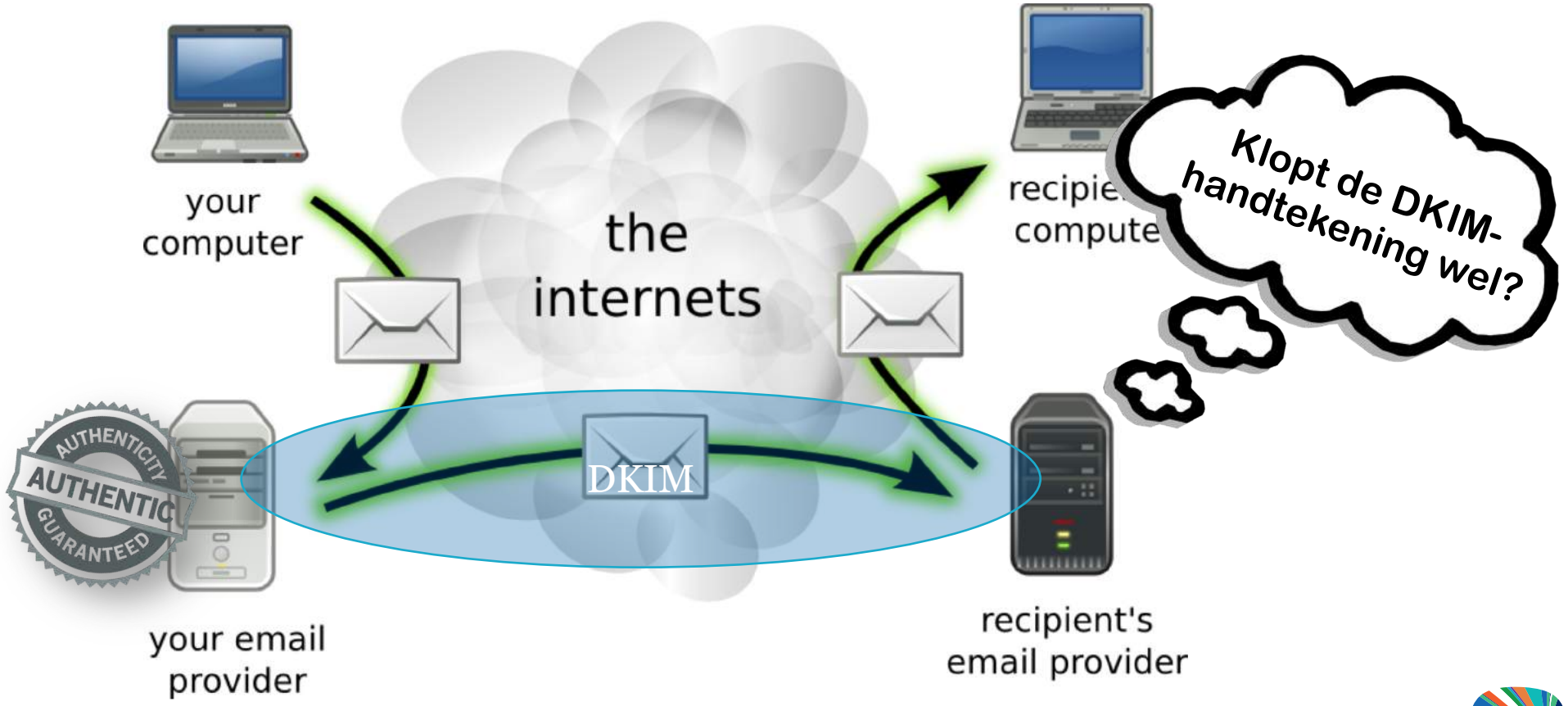
```
"v=DKIM1\; t=y\; k=rsa\; p=MIIB...MvGLmvwSYrPiEZIHoGggOVEtINi8Ucez2jVAZgzr"
```

DKIM is een e-mail authenticatie techniek die de ontvanger toestaat om te verifiëren of de e-mail echt verstuurd (en dus geautoriseerd) is door de eigenaar van het (DKIM)domein.
En of deze in oorspronkelijke staat aankomt.

SIDN LABS

DKIM (DomainKeys Identified Mail)

Mailflow:



DKIM (DomainKeys Identified Mail)

```
220 mail.example.net ESMTP
HELO mx.example.org
250 mail.example.net
MAIL FROM: <alice@example.org>
250 2.1.0 Ok
RCPT TO: <bob@example.net>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=example.org; s=2016;
        h=mime-version:from:date:message-id:subject:to;
        b=rr68DJxTrJcWlWD+Vx/gJvvzPjHsc7kRbbZc+jEtRuM=;
        H3WOsqwJ7BjiYXxp/sNAgyaVmUSMlKmhpmx+Jr2XwOBMoXopHFaEACapl/cbgUmNcc
        IqJgYilMbGFTZr+AOnpkBpu65fqTeTstLtKlmZvhCodMflrVSOgI6a9FjXPQli9US222
        ZATakL6nA3ClJOjqZabxgfItg4DIgITt8GDSnp2JxV4gjrJJH5zRD/R3E69bfDOAWz4
        /Pd/gZEnM6BYKlN9g3mzhJ1e3S/RsD6OUlVTR9zGaIGuC2o/RloWbbm2BEbMNYk8VkGA
        zloHRVXG30hql+7+VscrOl4PzMp+gwDE0aau/WWplPjuw2zhZnx0S1YUMEzZ6R9TU9PY
        aCPg==
From: alice@example.org
To: bob@example.net
Subject: demo

This is a small demo to show how email works.

Alice
.
250 2.0.0 Ok: queued as 766B0245619
QUIT
221 2.0.0 Bye
```

SDN LABS

DKIM (DomainKeys Identified Mail)

Voordelen:

- Verminderde kans op '*spoofing*'
- Verminderde kans op onderweg muteren van e-mail
- Betere e-mail reputatie

Aandachtspunten:

- Grotere beheerlast
- Toevoegingen door bijvoorbeeld mailinglists gooien roet in het eten

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

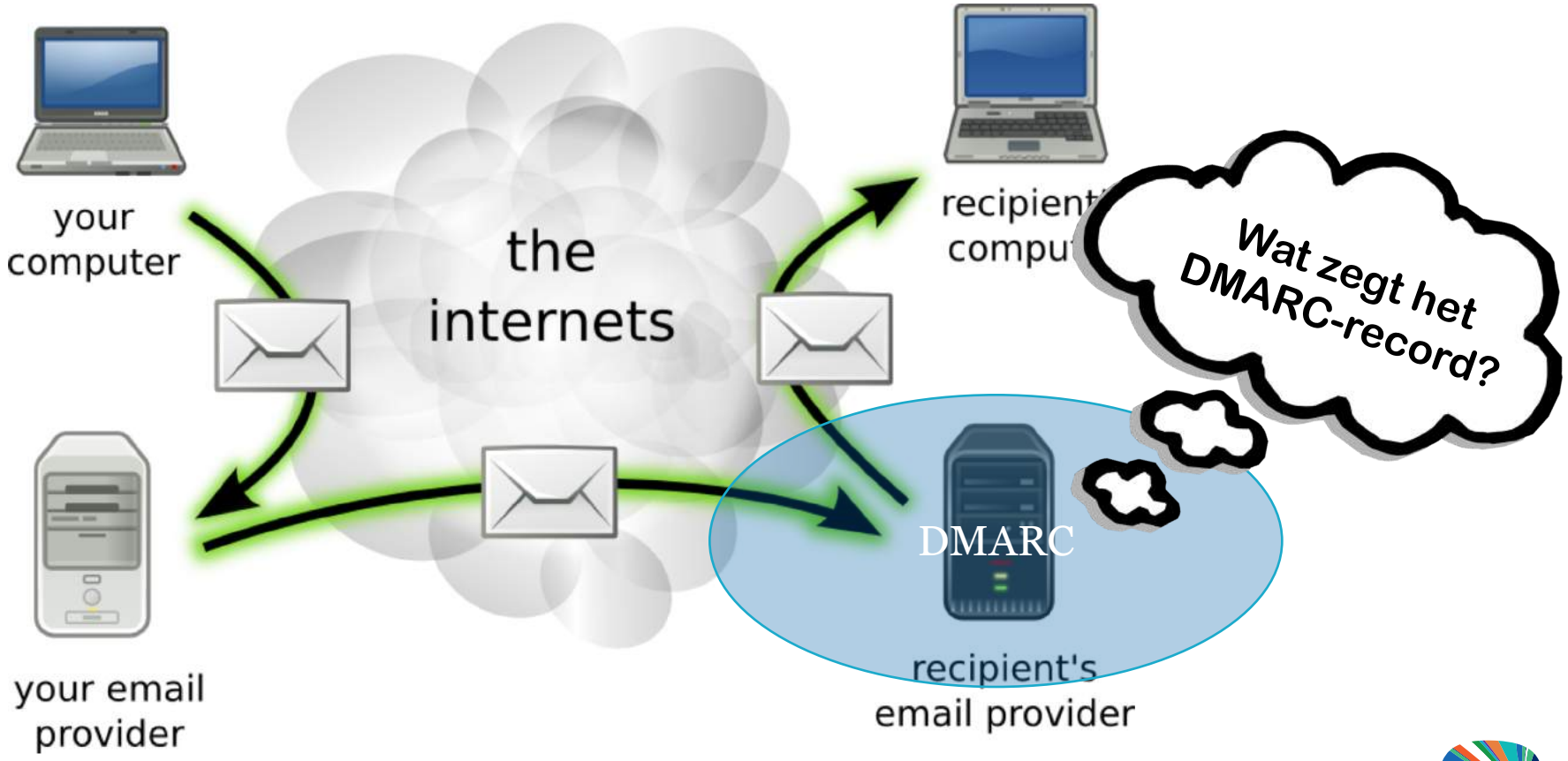
Werking:

- Het DMARC-record is een TXT-record in het DNS
- In het DMARC-record staat een *policy* aangegeven domein:

```
"v=DMARC1; p=none; rua=mailto:dmarc@example.nl; fo=0; adkim=r; aspf=r; pct=100; sp=none"
```

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

Mailflow:



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

Voordelen:

- Invloed op foute mail (weigeren, of in spamfolder bijv.)
- *Identifier alignment*
- Feedback-rapporten
- Betere e-mail reputatie

Aandachtspunten:

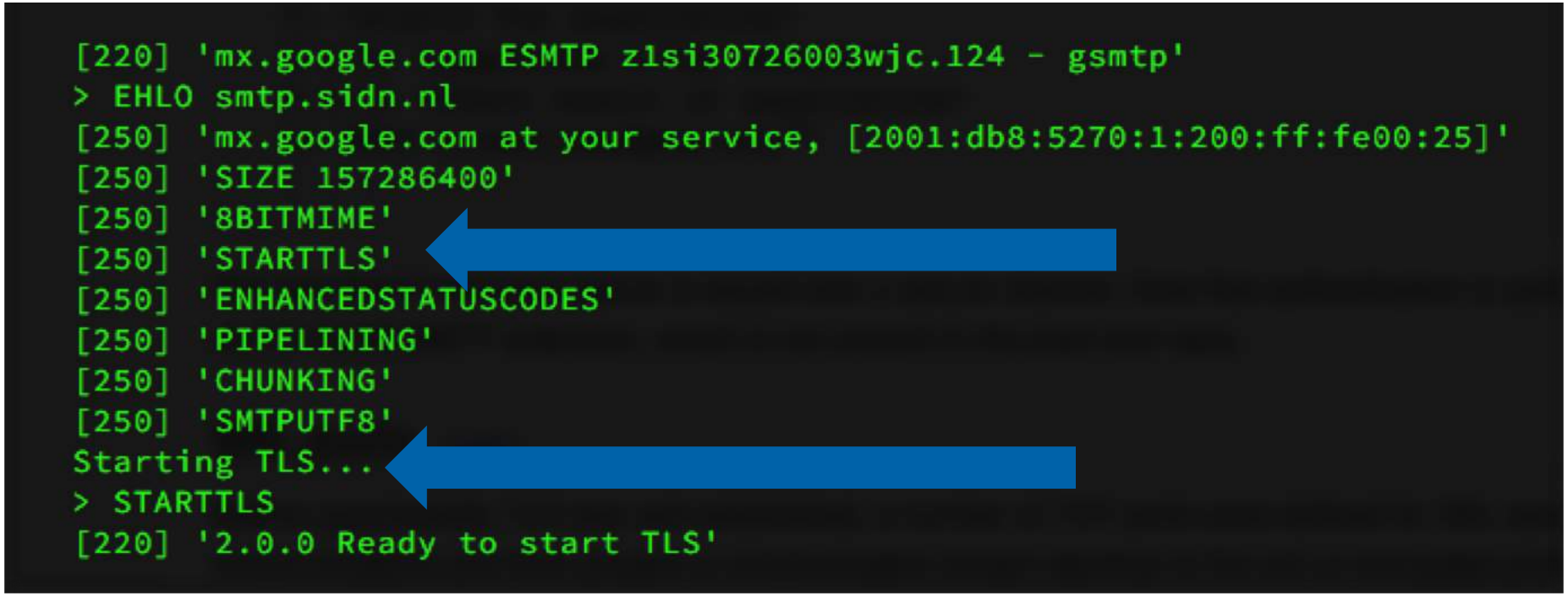
- Grotere beheerlast (met name rapporten)
- Ontvangende kant kan *overrulen*
- Privacy-issue in het ruf-rapport

SIDN LABS

STARTTLS

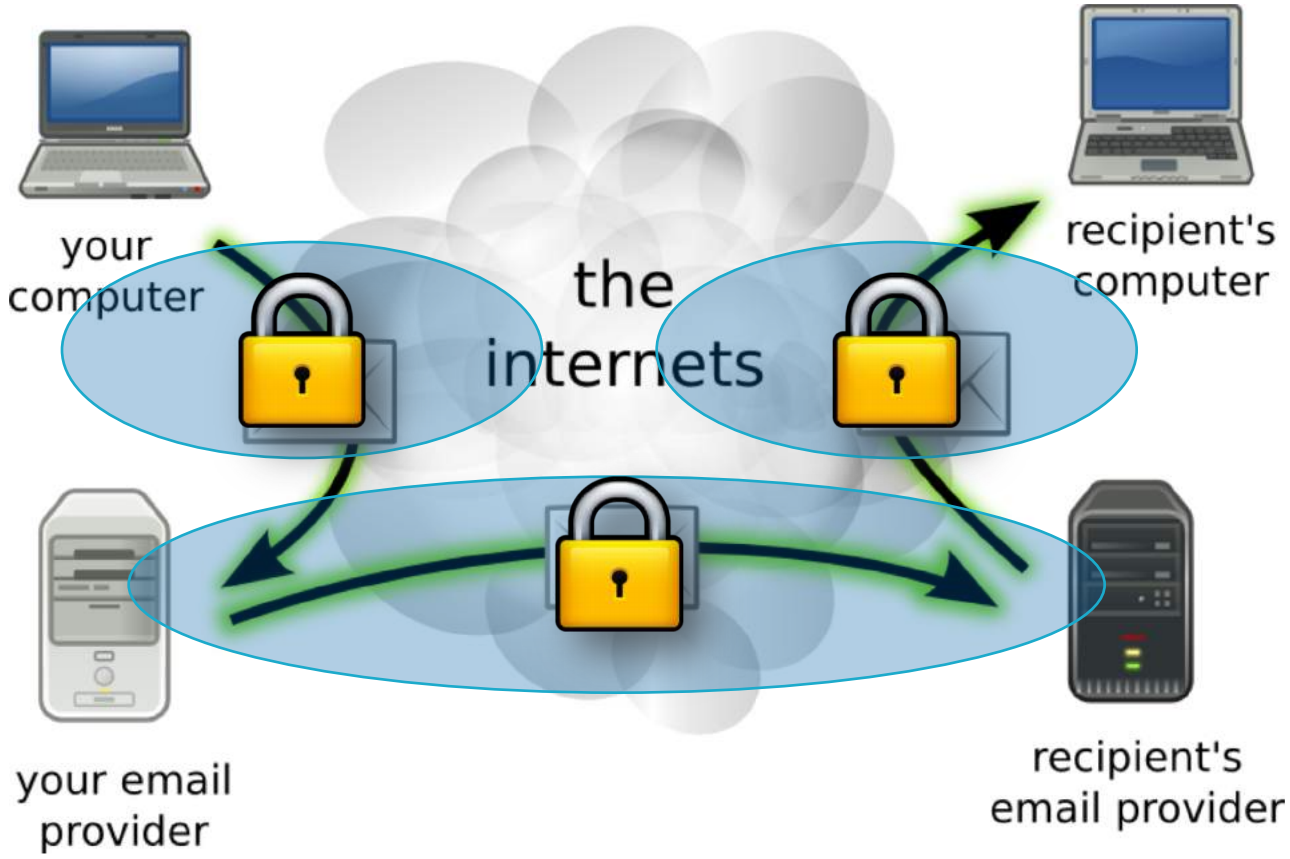
Werking:

- Ontvangende MTA geeft aan deze mogelijkheid te ondersteunen
- Verzendende MTA vraagt vervolgens om deze mogelijkheid
- Verkeer zal via TLS worden versleuteld



STARTTLS

Mailflow:



STARTTLS

Voordeel:

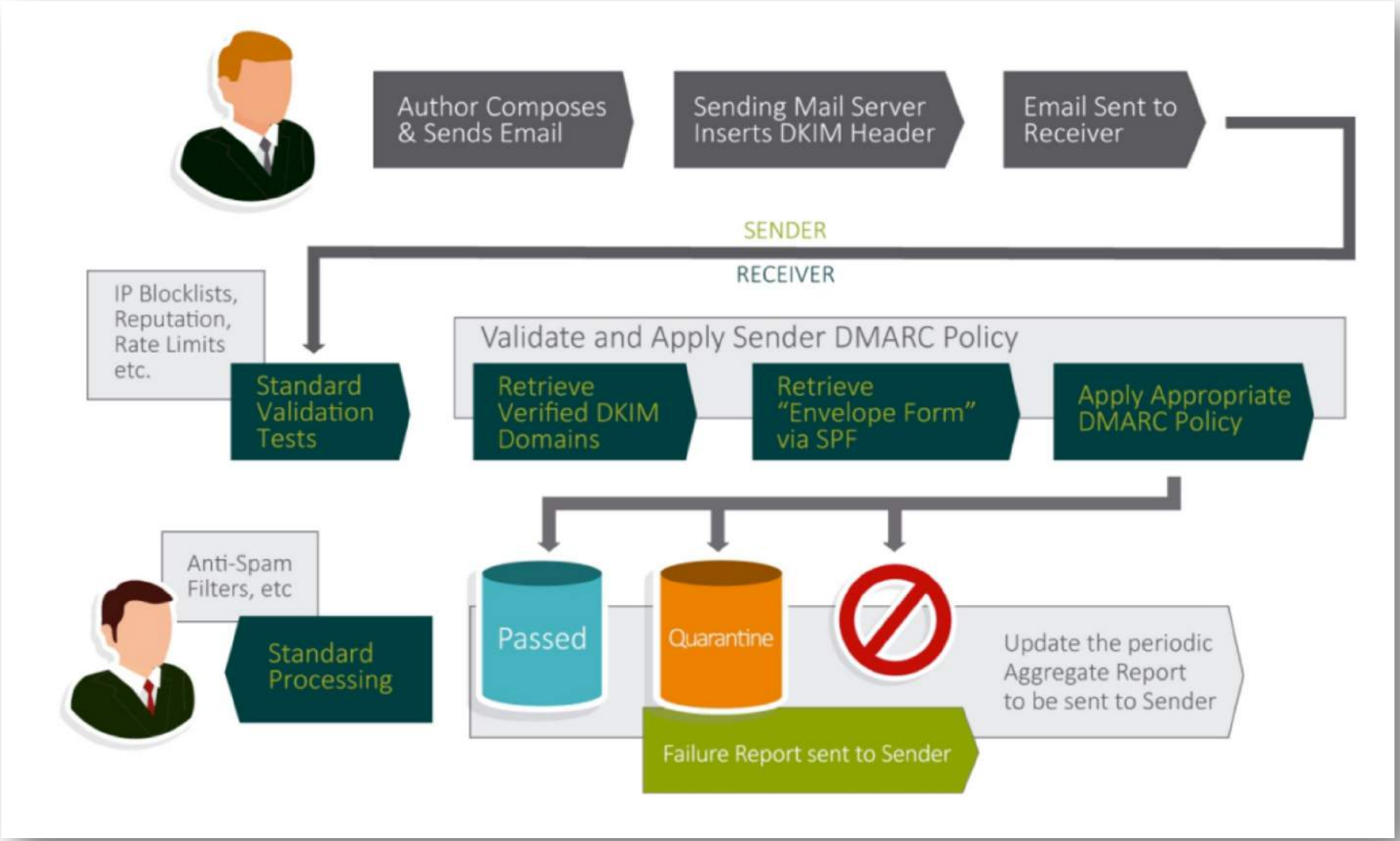
- E-mail verkeer is versleuteld, dus moeilijker af te luisteren

Tekortkoming:

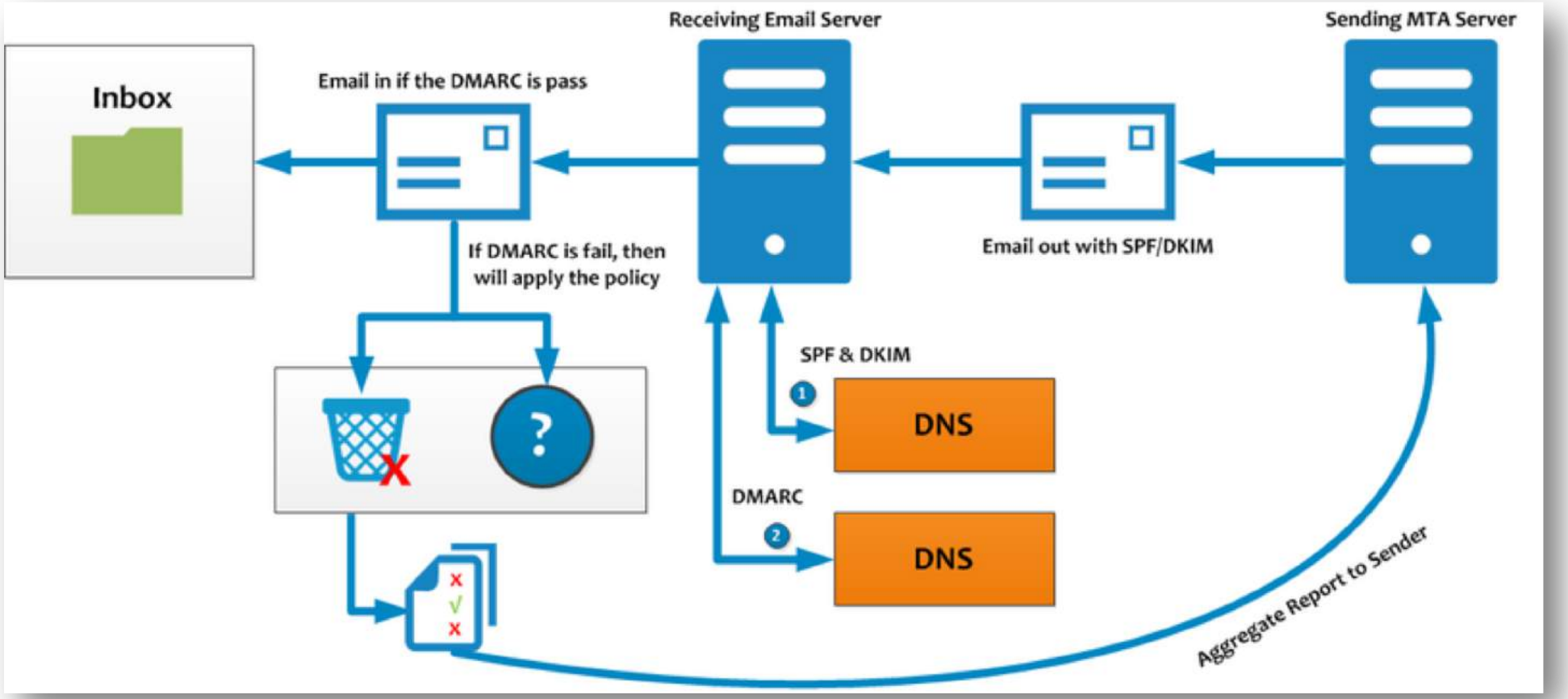
- Is '*opportunistic*' (oplossing: DANE*, RFC7672 en/of MTA-STS)

*Check de *factsheet van het NCSC over DANE+STARTTLS*.

In combinatie met elkaar

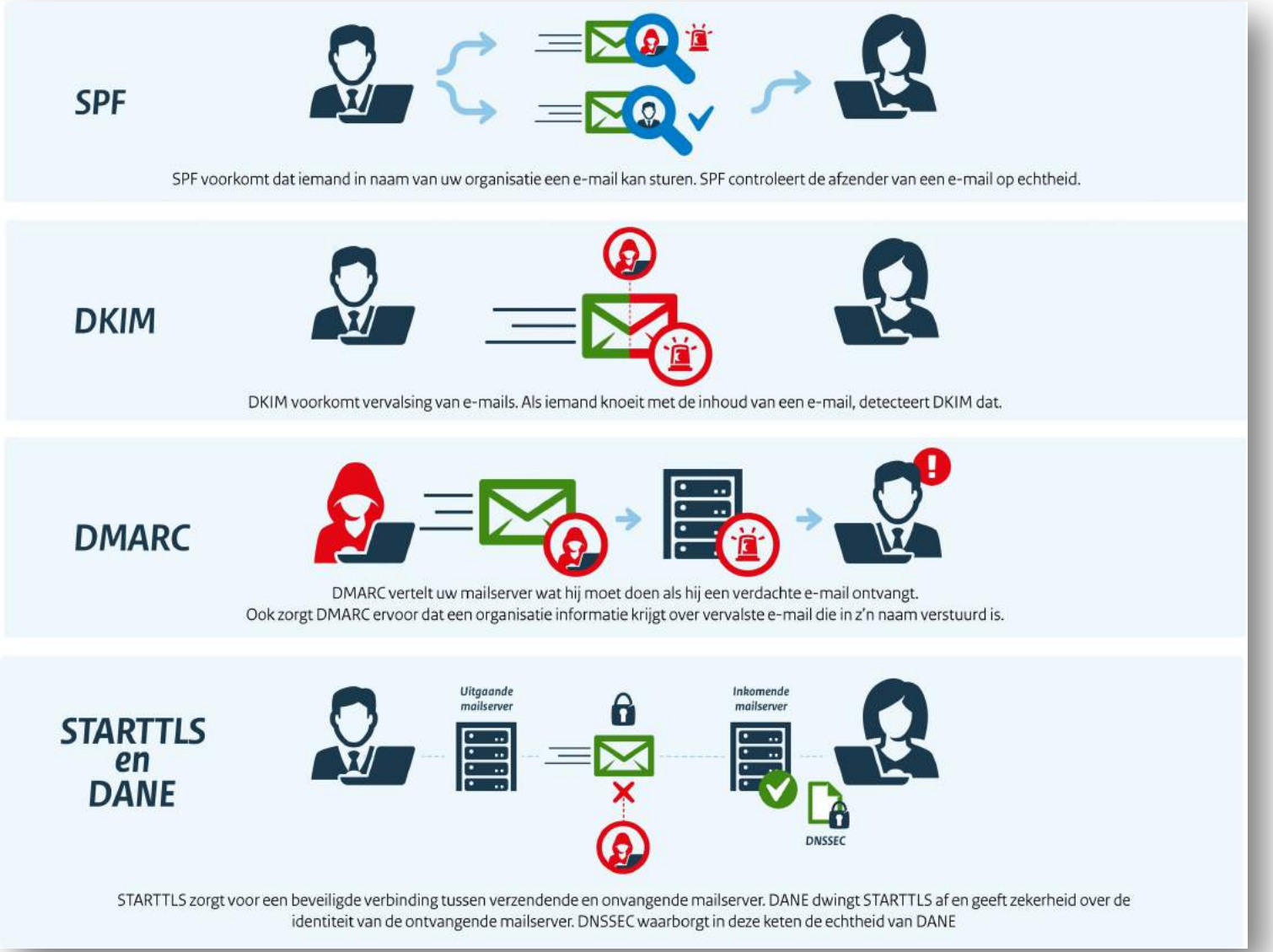


In combinatie met elkaar



Leestip:
https://www.ncsc.nl/actueel/factsheets/factsheet-bescherm-domeinnamen-tegen-phishing.html

In combinatie met elkaar (nog eens)



Bron: https://www.sidn.nl/a/veilig-internet/veilige-e-mail-coalitie-van-start

En als ik nooit mail?

- DKIM/DMARC/SPF-instellingen 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=DKIM1; p="
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 dan ook al grootschalig toegepast
- Maar nog meer is altijd beter
- Samen kunnen we E-mail veiliger maken! 😊

Bedankt
voor de aandacht!

Check het op: https://internet.nl/
Zie ook: https://stats.sidnlabs.nl/nl/mail.html

@marcodavids

SIDN LABS