Zorgeloos online

SIDN LABS

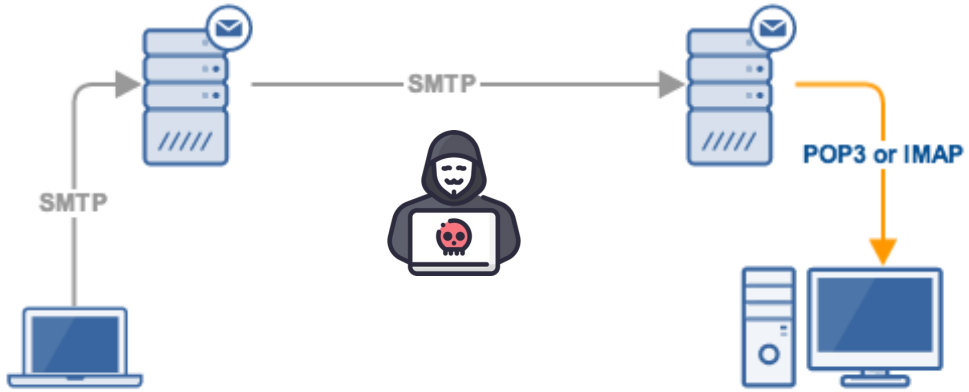
DANE (voor e-mail)

Kennissessie e-mailbeveiliging op basis van open standaarden

Marco Davids | 17 februari 2023 | 11:45 – 12:15 u.

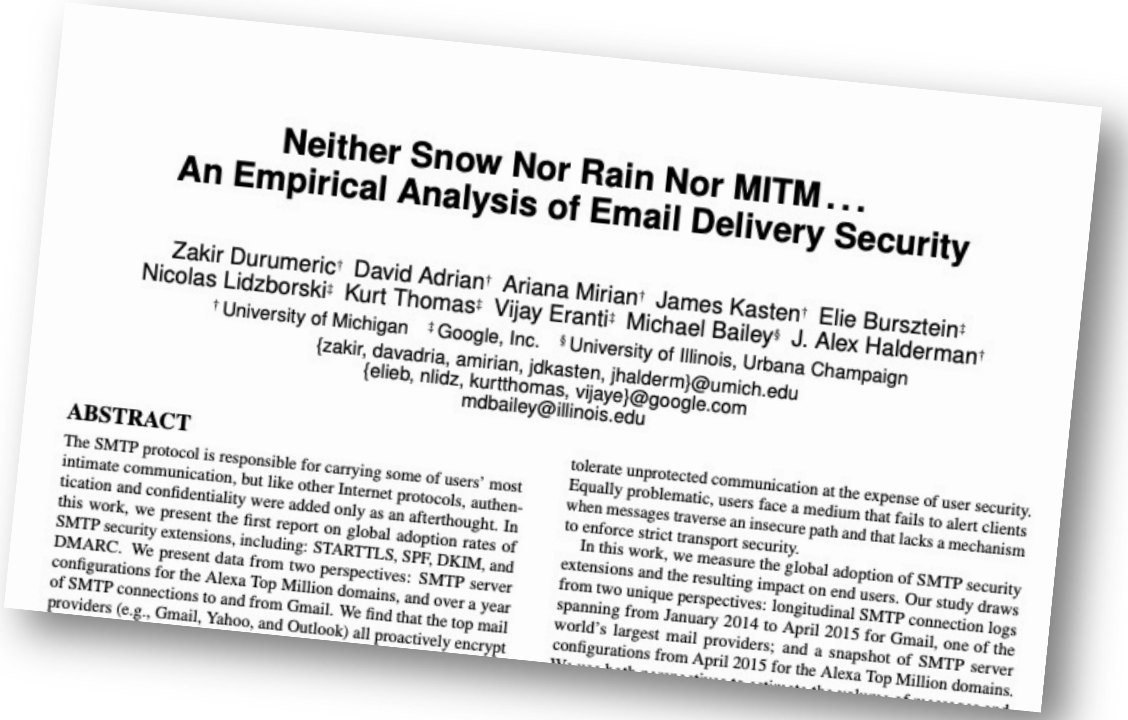
Wat is het probleem?

- Klassieke e-mail is niet versleuteld (plaintext)



Wat is het probleem?

- Misbruik komt daadwerkelijk voor



Neither Snow Nor Rain Nor MITM . . .
An Empirical Analysis of Email Delivery Security

Zakir Durumeric† David Adrian† Ariana Mirian† James Kasten† Elie Bursztein‡
Nicolas Lidzborski‡ Kurt Thomas‡ Vijay Eranti‡ Michael Bailey§ J. Alex Halderman†
†University of Michigan ‡Google, Inc. §University of Illinois, Urbana Champaign
{zakir, davadria, amirian, jdkasten, jhalderm}@umich.edu
{elieb, nlidz, kurtthomas, vijaye}@google.com
mdbailey@illinois.edu

ABSTRACT

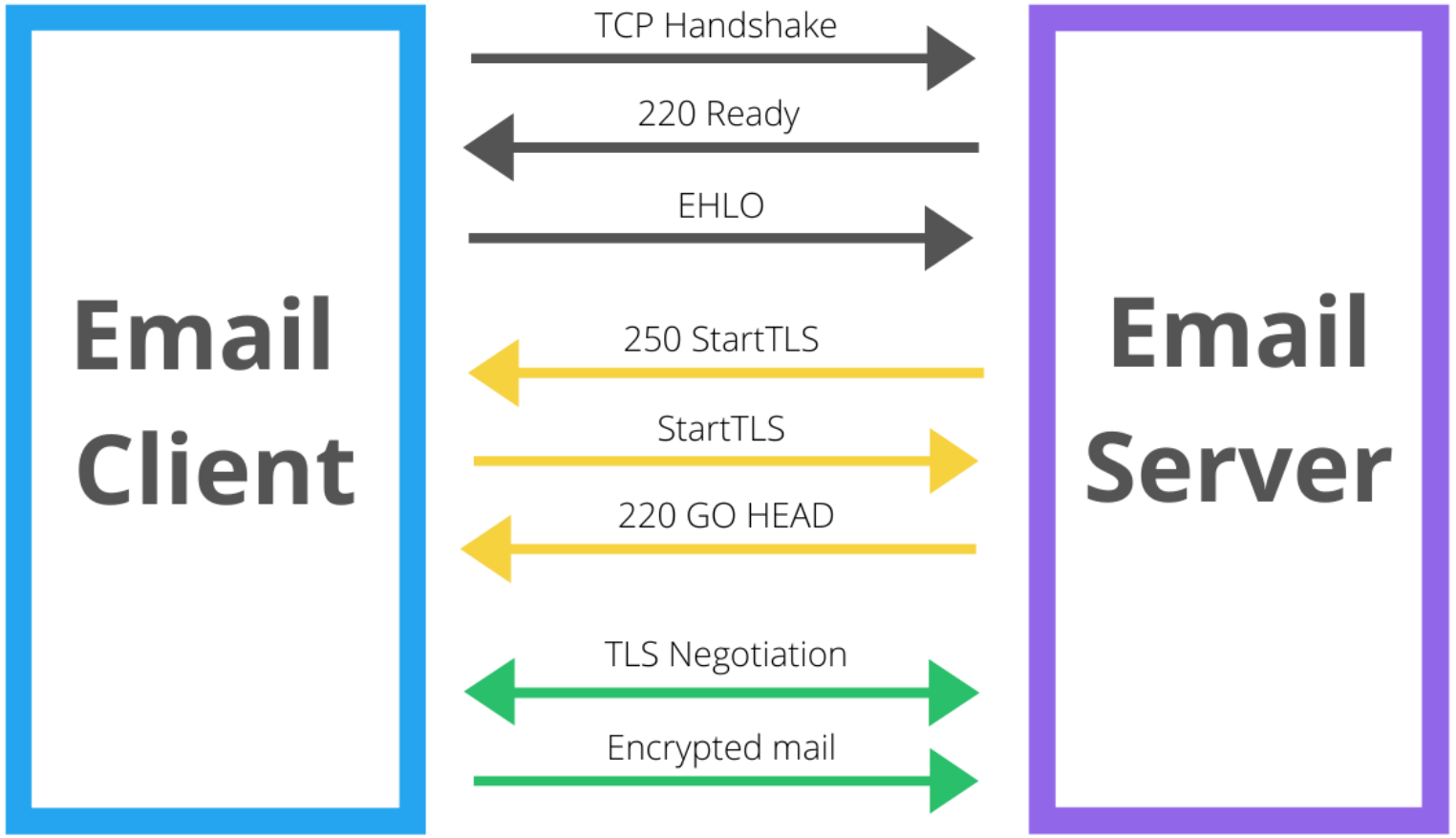
The SMTP protocol is responsible for carrying some of users' most intimate communication, but like other Internet protocols, authentication and confidentiality were added only as an afterthought. In this work, we present the first report on global adoption rates of SMTP security extensions, including: STARTTLS, SPF, DKIM, and DMARC. We present data from two perspectives: SMTP server configurations for the Alexa Top Million domains, and over a year of SMTP connections to and from Gmail. We find that the top mail providers (e.g., Gmail, Yahoo, and Outlook) all proactively encrypt tolerate unprotected communication at the expense of user security. Equally problematic, users face a medium that fails to alert clients when messages traverse an insecure path and that lacks a mechanism to enforce strict transport security.

In this work, we measure the global adoption of SMTP security extensions and the resulting impact on end users. Our study draws from two unique perspectives: longitudinal SMTP connection logs spanning from January 2014 to April 2015 for Gmail, one of the world's largest mail providers; and a snapshot of SMTP server configurations from April 2015 for the Alexa Top Million domains.

https://dl.acm.org/doi/pdf/10.1145/2815675.2815695

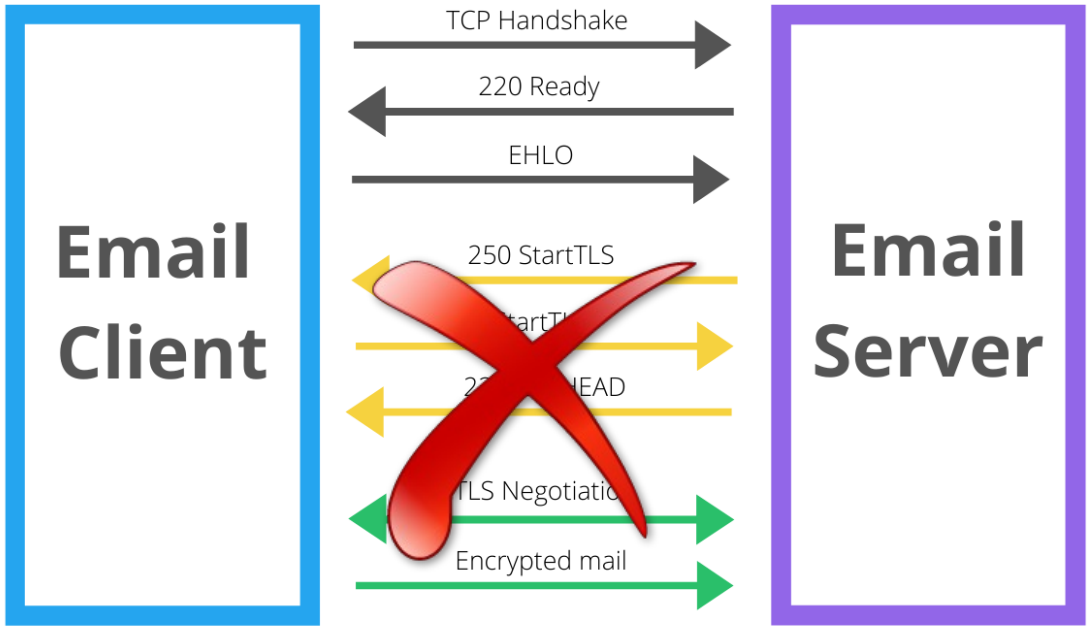
Oplossing?

- STARTLS (RFC3207) probeert dit op te lossen.



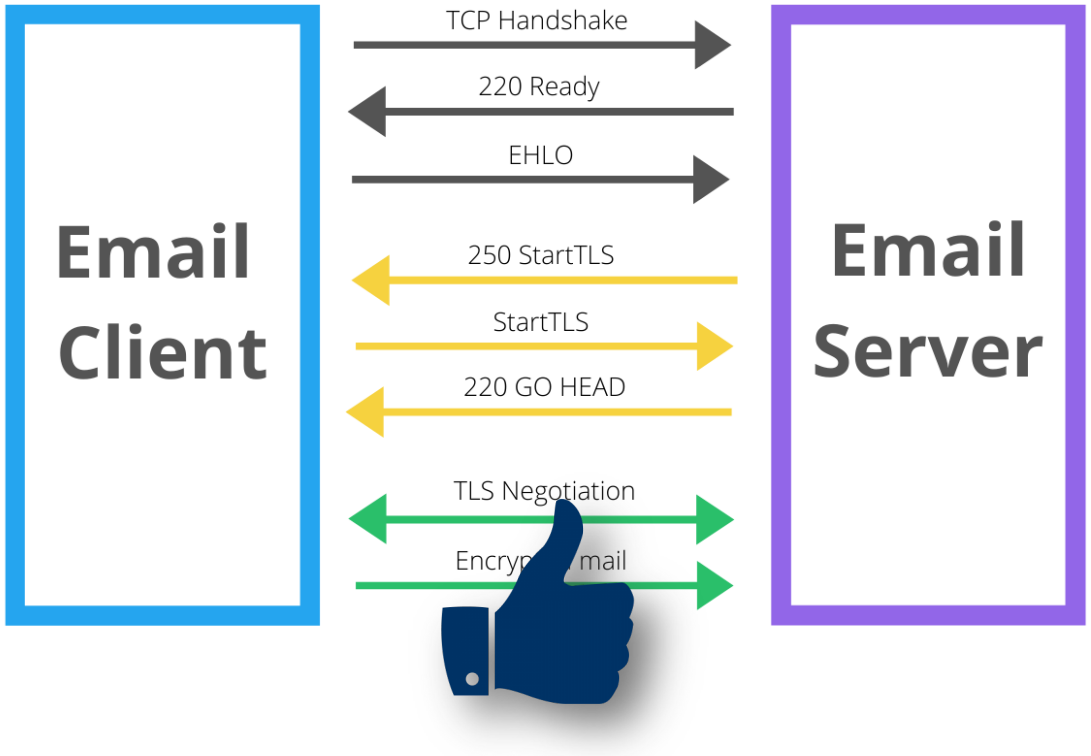
Wat is het probleem?

- STARTTLS (RFC3207) probeert dit op te lossen, maar…
  - Het STARTTLS-commando kan door MITM worden tegengehouden



Wat is het probleem?

- STARTLS (RFC3207) probeert dit op te lossen, maar…
  - Het certificaat wordt in de praktijk gewoon altijd vertrouwd



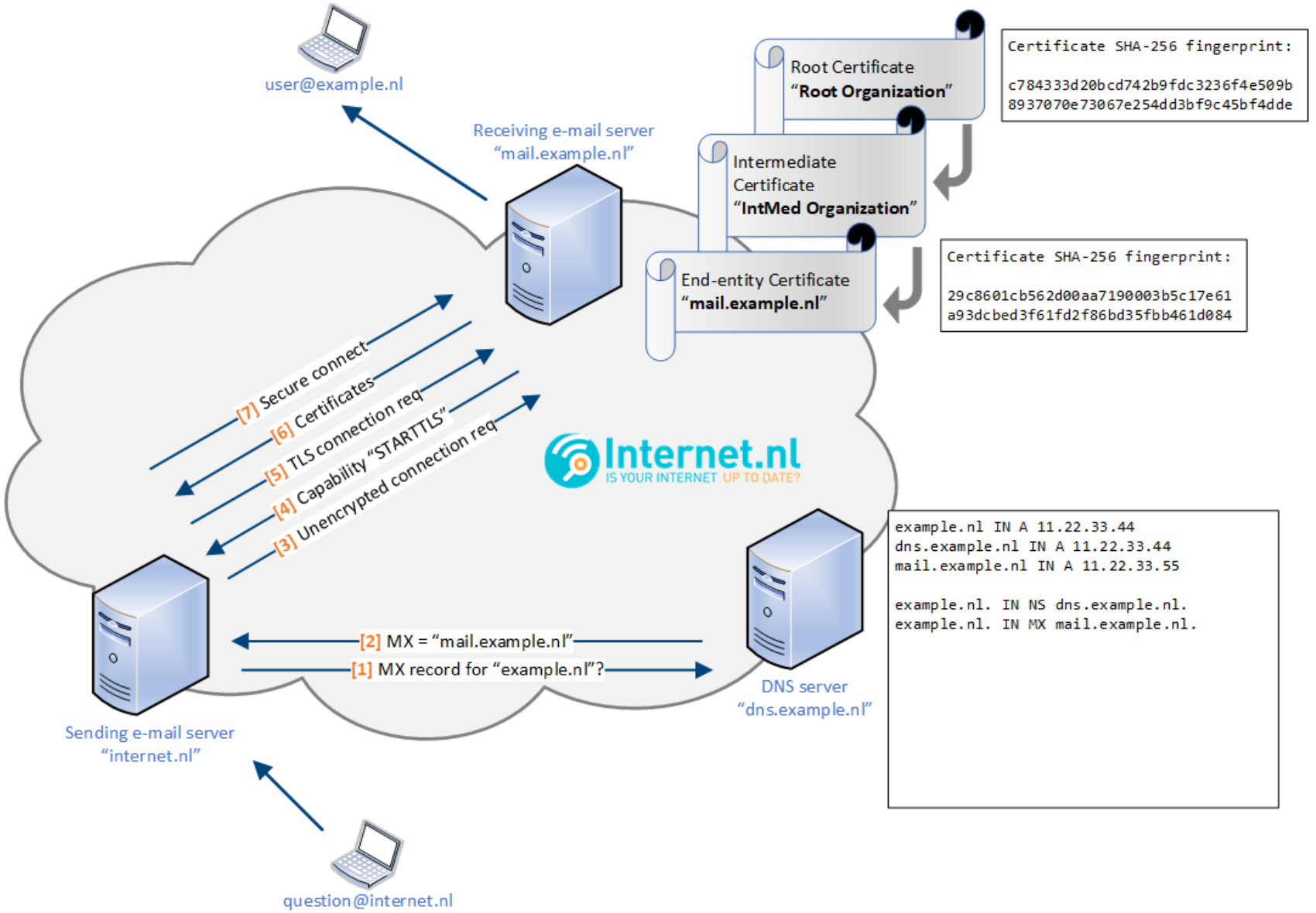
RFC7672 to the rescue

DANE: DNS-based Authentication of Named Entities

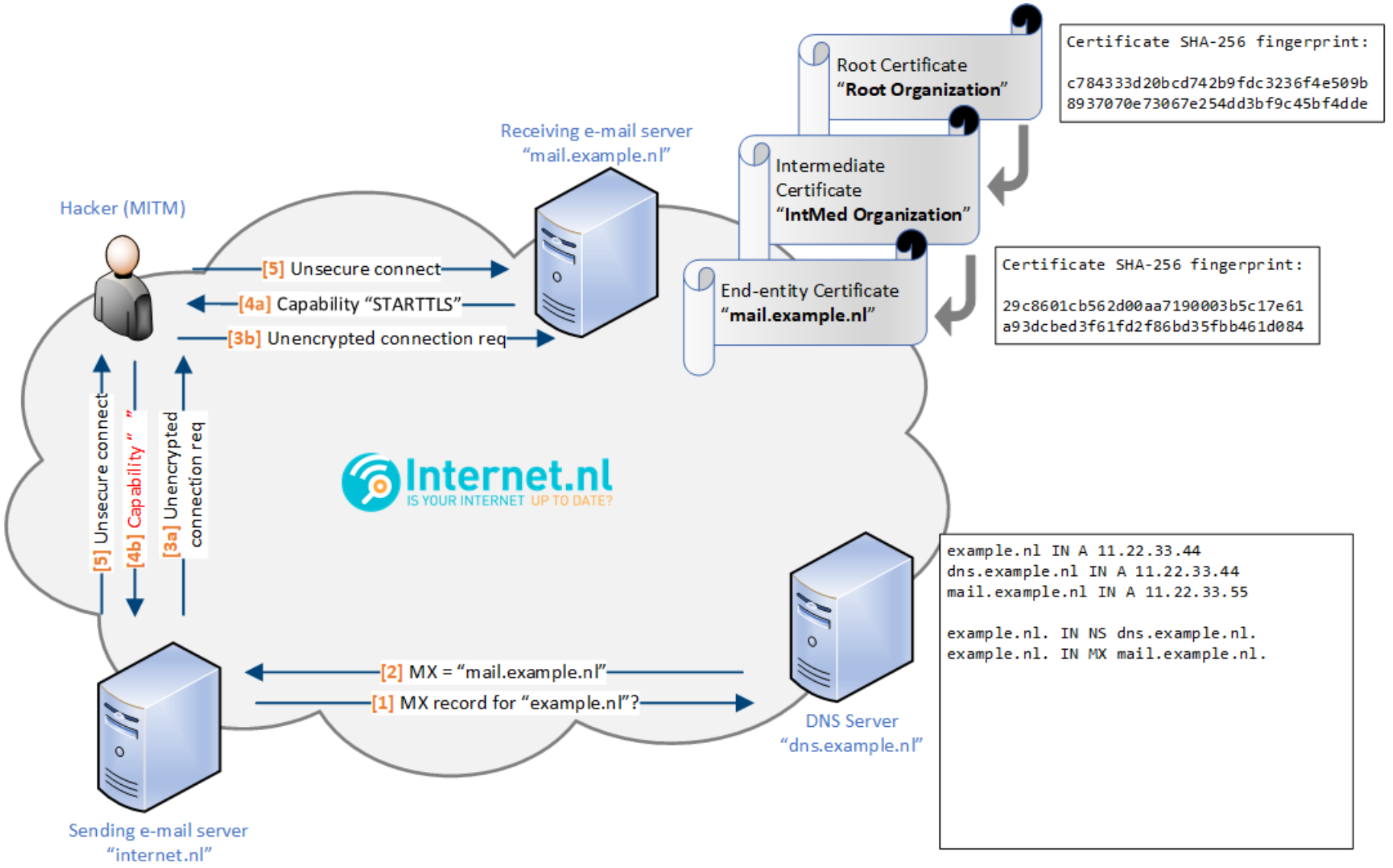
- Je zet een zogenaamd TLSA record (gesigned) in DNS
- Dit is een afspiegeling van het gebruikte TLS-certificaat
  - Kan ook iets meer meta zijn, dus bijvoorbeeld de gebruikte CA

Prima uitleg op: https://github.com/internetstandards/toolbox-wiki/blob/main/DANE-for-SMTP-how-to.md

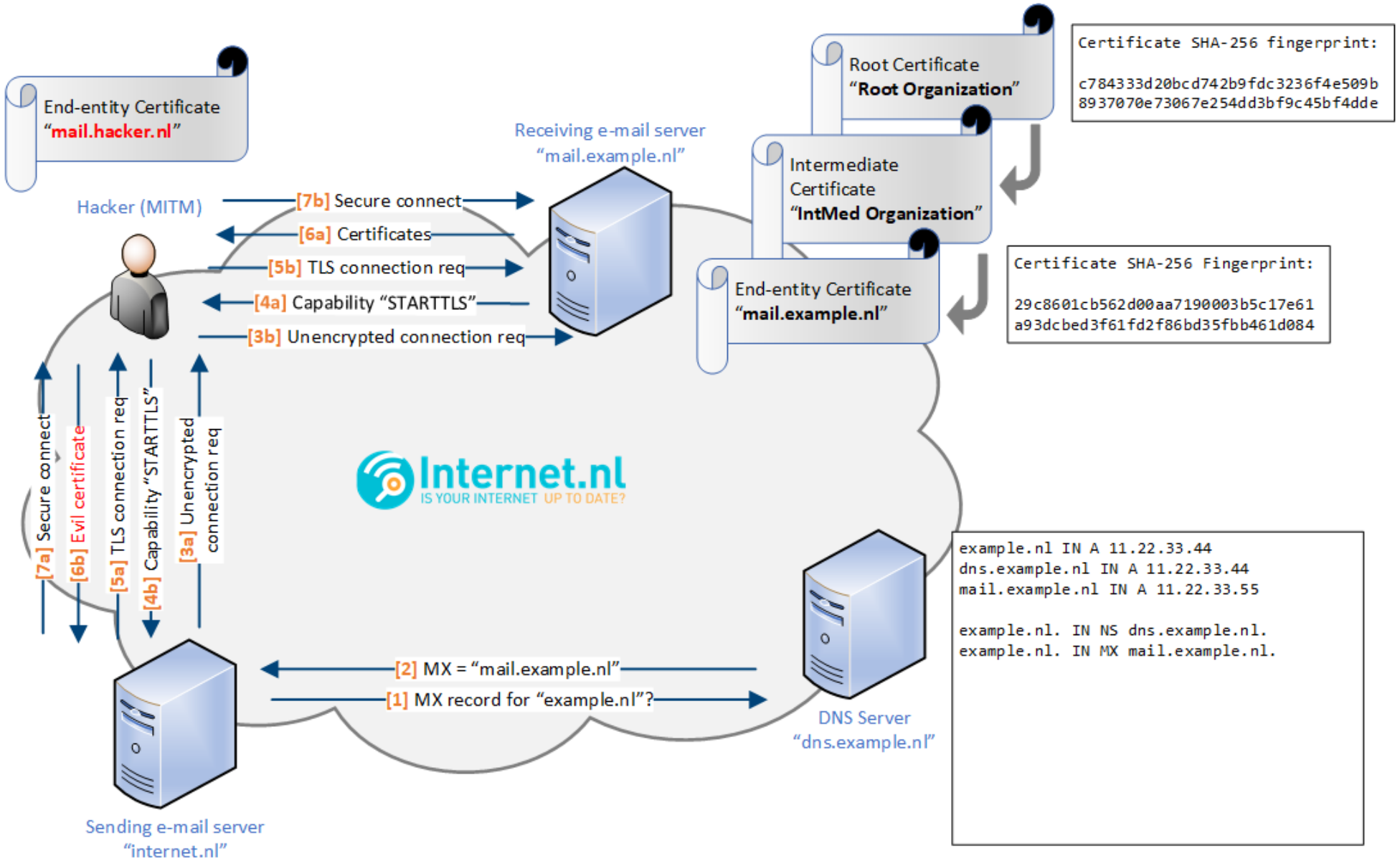
Werking zonder DANE



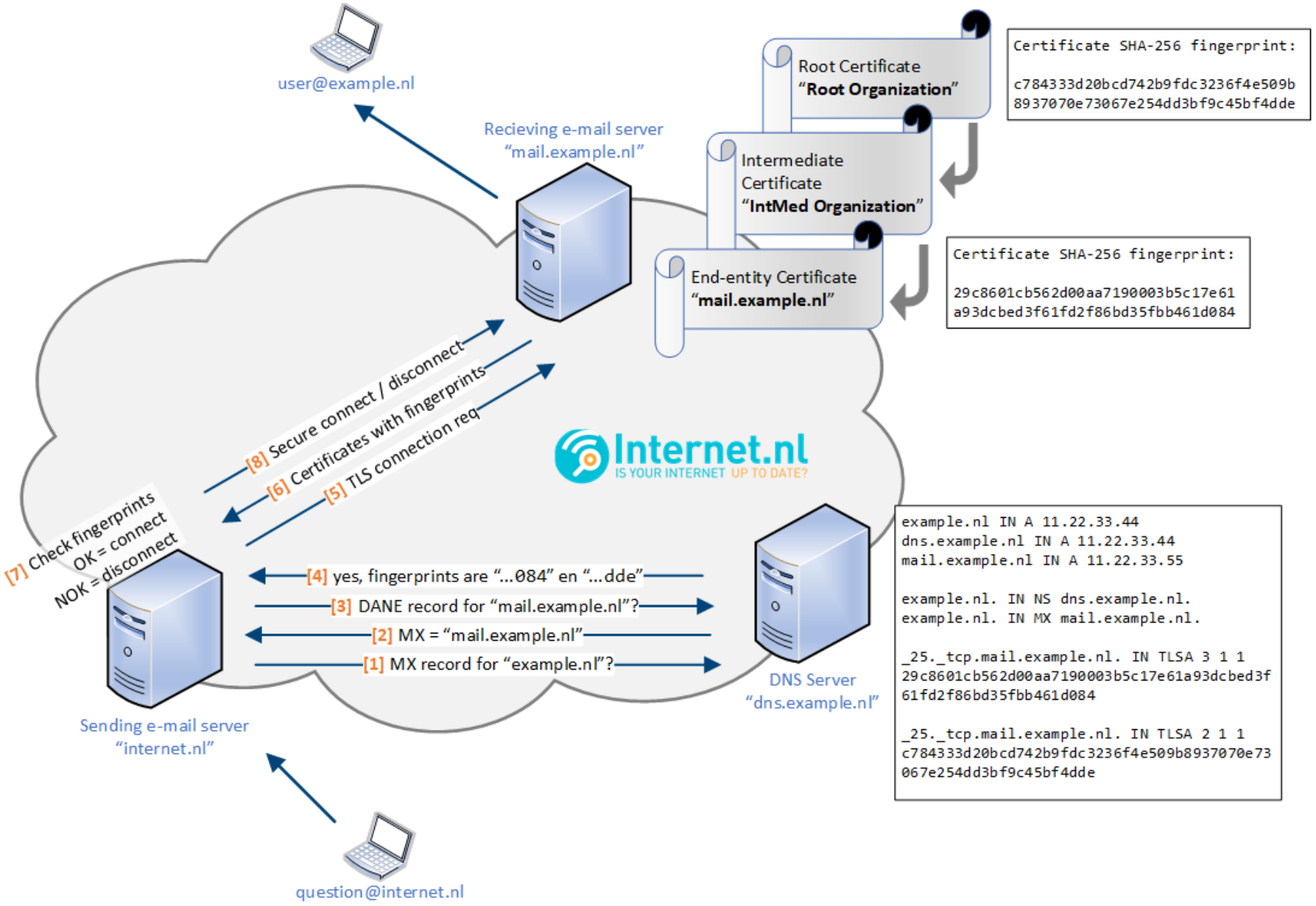
Stripping TLS door MITM



Vals certificaat



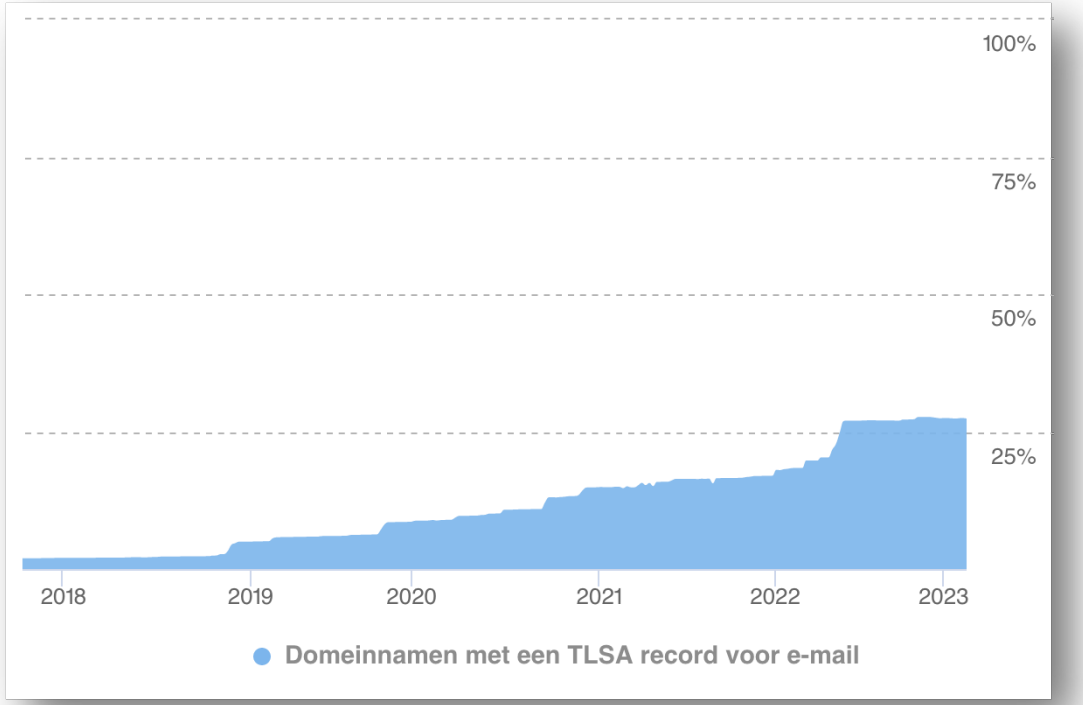
Met DANE



SIDN LABS

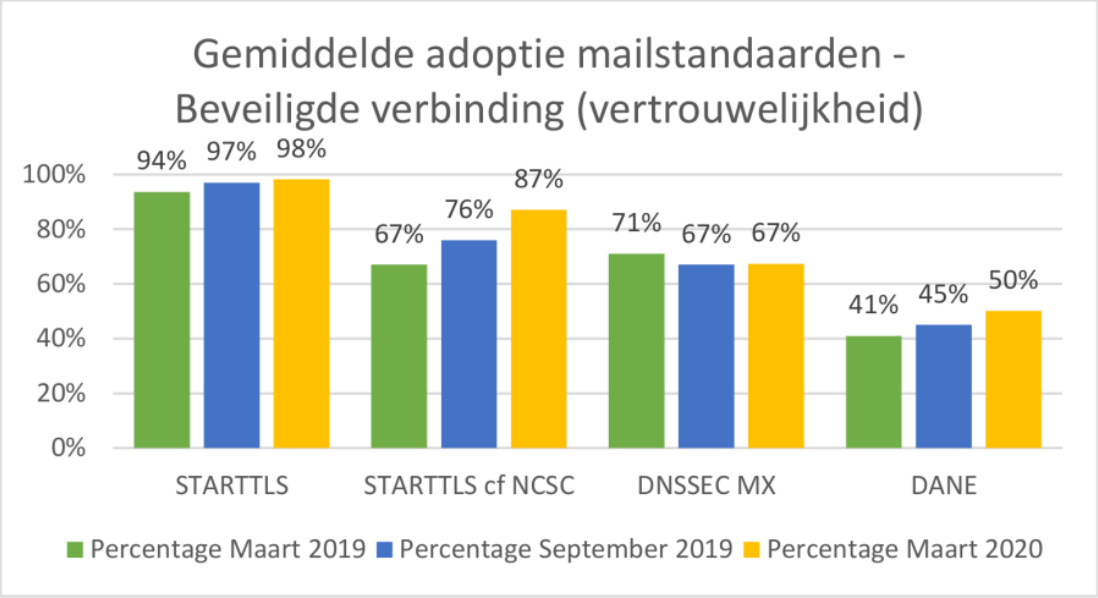
Adoptie behoorlijk goed

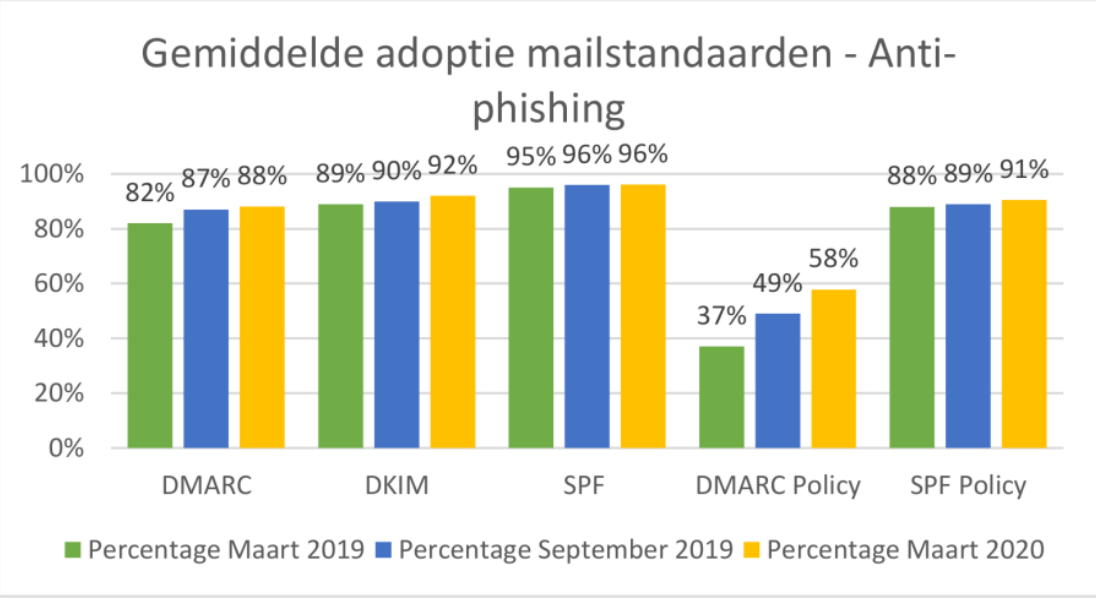
- Voor het web is het niet van de grond gekomen
- Voor e-mail best wel aardig!



https://stats.sidnlabs.nl/nl/mail.html#dane

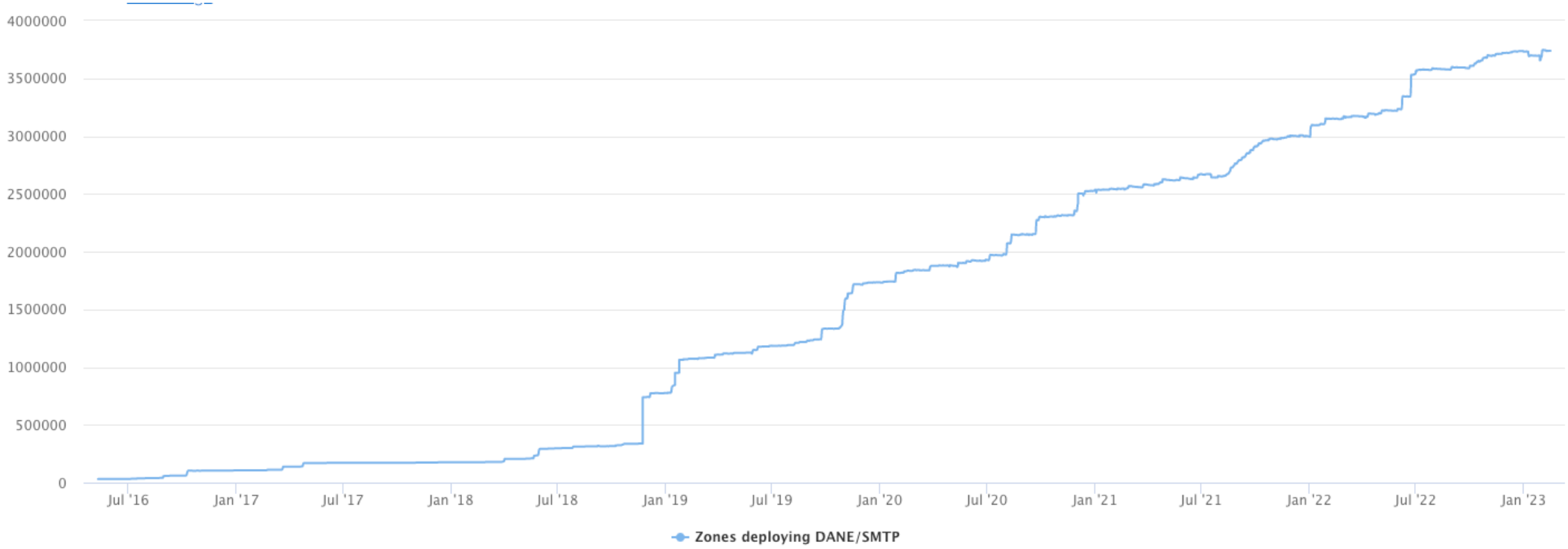
Adoptie behoorlijk goed





https://www.sidn.nl/nieuws-en-blogs/internetbeveiligingsstandaarden-moeten-opboksen-tegen-zakelijke-belangen-van-internetleveranciers

Adoptie behoorlijk goed



https://stats.dnssec-tools.org/#/?top=dane&trend_tab=1

Aandachtspunten

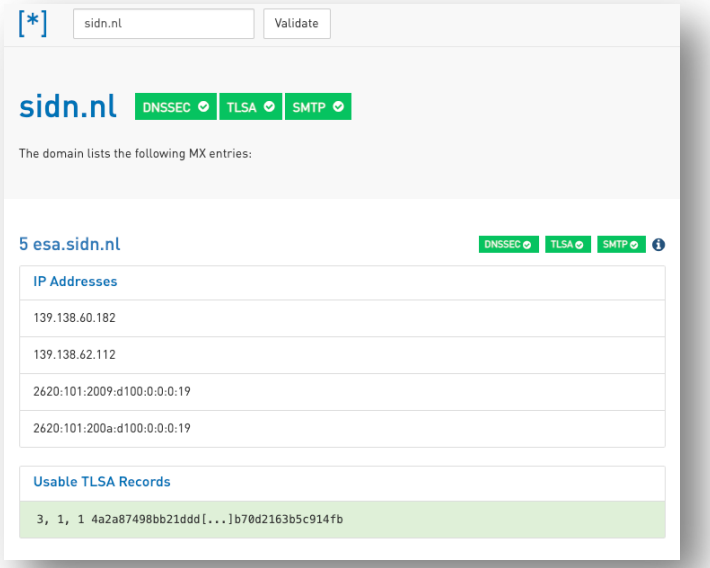
- Vereist DNSSEC, goed werkende ‘Denial of Existence’ vereist!
- Als je certificaat veranderd, dan moet je niet vergeten het TLSA record in DNS aan te passen.
- Dit is soms een operationele uitdaging, dus goed borgen in procedures.
- Een certificaat moet netjes ‘gerold’ worden, dit vereist begrip van de materie.
- Aanzetten en controleren zijn twee verschillende dingen.
- Je kan het dus wel gefaseerd aanzetten.

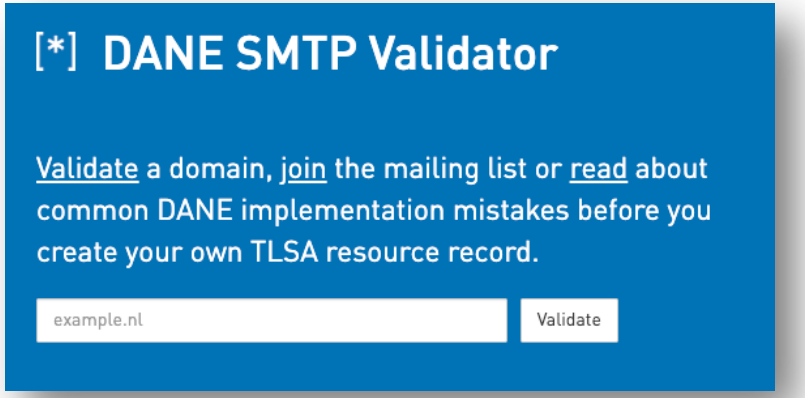
Goed om te weten

- De DANE standaard staat op de ‘pas-toe-of-leg-uit’-lijst van de overheid.
- En het is onderdeel van onze ‘incentive-regeling’.
- Werkt desgewenst ook met ‘self signed’-certificaten.

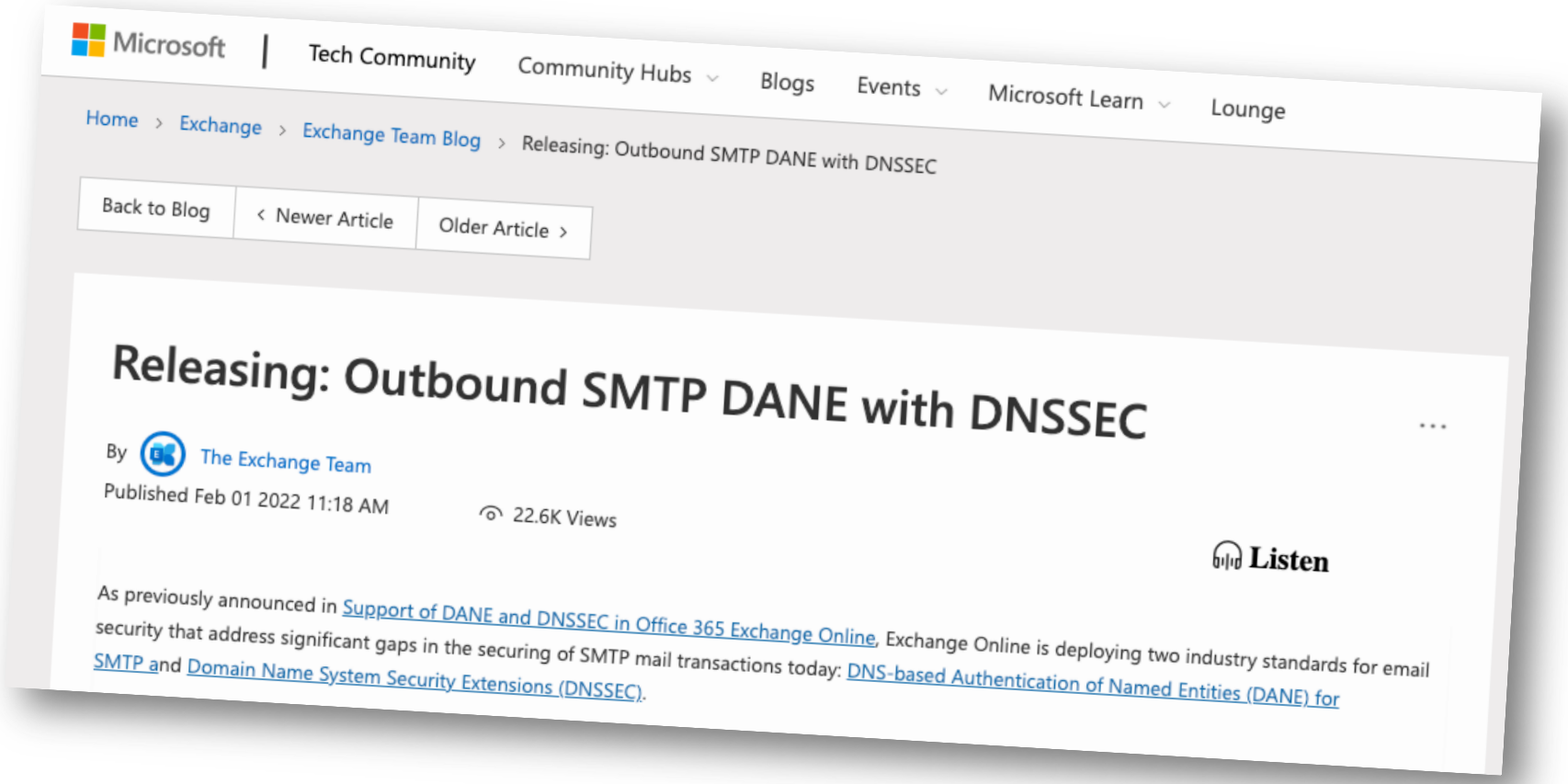
Zelf aan de slag

- https://www.sidn.nl/moderne-internetstandaarden/e-mailbeveiliging
- Uitgebreide FAQ.
- Hands-on voor Postfix en Exim.
- Controleer het op: https://internet.nl of https://dane.sys4.de/
- of op https://www.mailhardener.com/tools/dane-validator





Of via je leverancier



https://techcommunity.microsoft.com/t5/exchange-team-blog/releasing-outbound-smtp-dane-with-dnssec/ba-p/3100920

https://www.sidn.nl/nieuws-en-blogs/exchange-online-ondersteunt-uitgaande-dane-validatie

Bedankt!

https://www.sidn.nl/zoeken?s=DANE

SIDN LABS