DANE deployments past and present

Utrecht, July 2023

Who am I?

Sidsel Jensen

- Architecht of Deliverability and Abuse @ Open-Xchange
- Postmistress of OX Cloud
- Earlier: Team Manager for the Mail and Abuse Systems Engineering team in the hosting company one.com (now Group.one)
- MSc in Computer Science from the University of Copenhagen

In my spare time:

- Chair(wo)man of IDA IT - The IT section of The Danish Society of Engineers
- Boardmember of The Danish Council for Digital Security (RfDS)
- Active in M3AAWG as time permits
- Been planning open source conferences since 2001 (LinuxForum and Open Source Days - and since 2014 DrivingIT)

Twitter: @Purple0x

Mastodon: @purplehex@infosec.exchange

LinkedIn: https://www.linkedin.com/in/sidseljensen/

Stay Open. OX

DANE SMTP - RFC 7672

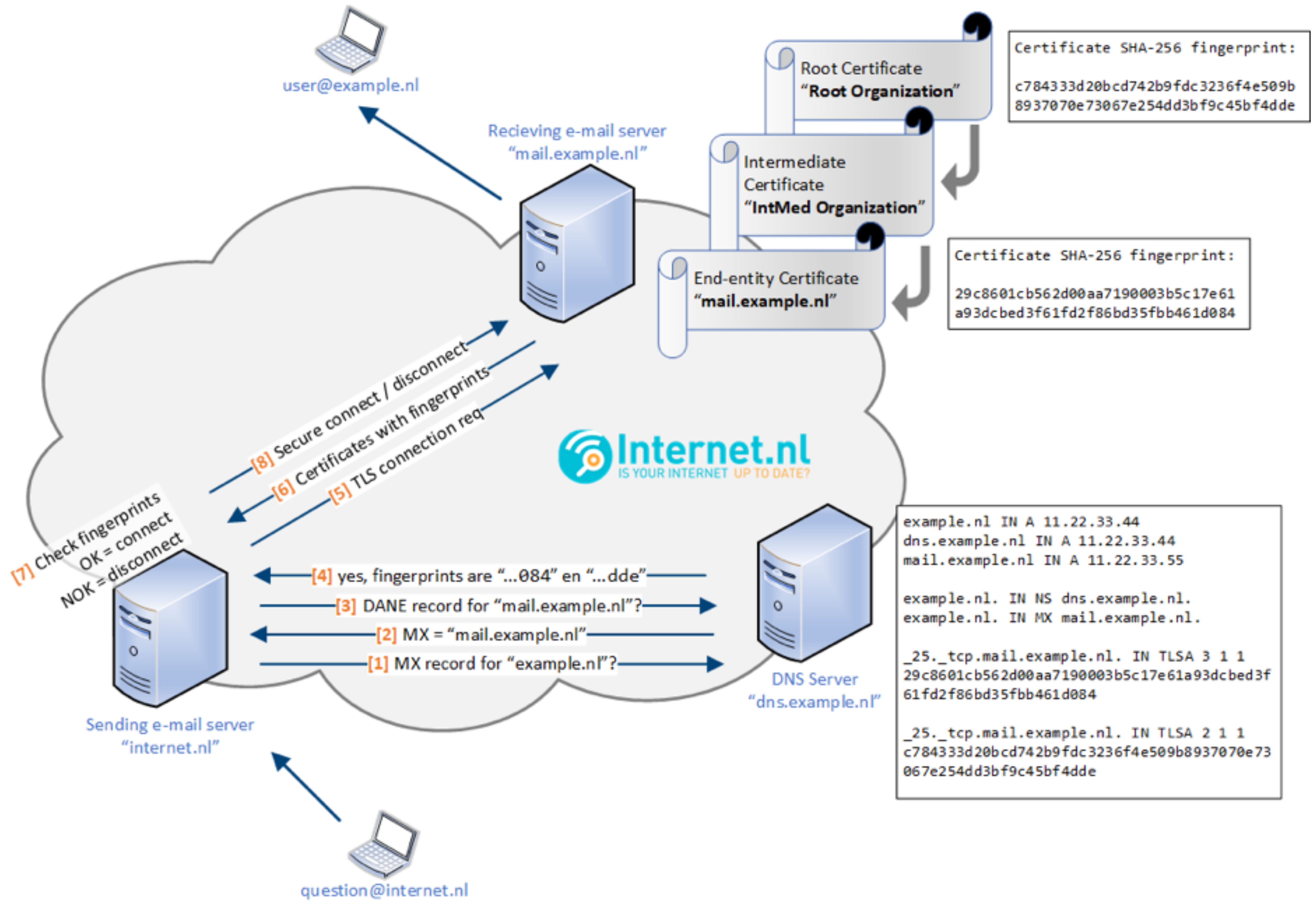
The Ultra Short Recap - DANE SMTP is the “Poster Girl” for DNSSEC

DNS-based **A**uthentication of **N**amed **E**ntities (DANE) for SMTP provides a more secure method for mail transport. It is is resistant to downgrade and man-in-the-middle (MITM) attacks.

By requiring DNSSEC, the client can authenticate the TLSA record itself, to build a chain-of-trust which functions as a replacement for the Public Key Infrastructure (PKI).

It uses the presence of the DANE TLSA records to securely signal TLS support and to publish the means by which SMTP clients can successfully authenticate legitimate SMTP servers.

When opportunistic DANE TLS is determined to be unavailable, clients should fall back to pre-DANE opportunistic TLS.



```
Certificate SHA-256 fingerprint:

c784333d20bcd742b9fdc3236f4e509b
8937070e73067e254dd3bf9c45bf4dde
```

```
Certificate SHA-256 fingerprint:

29c8601cb562d00aa7190003b5c17e61
a93dcbed3f61fd2f86bd35fbb461d084
```

```
example.nl IN A 11.22.33.44
dns.example.nl IN A 11.22.33.44
mail.example.nl IN A 11.22.33.55

example.nl. IN NS dns.example.nl.
example.nl. IN MX mail.example.nl.

_25._tcp.mail.example.nl. IN TLSA 3 1 1
29c8601cb562d00aa7190003b5c17e61a93dcbed3f
61fd2f86bd35fbb461d084

_25._tcp.mail.example.nl. IN TLSA 2 1 1
c784333d20bcd742b9fdc3236f4e509b8937070e73
067e254dd3bf9c45bf4dde
```

Press Rewind to 2018

Notes on a small vertical line on a graph

We (one.com) really wanted to provide email security to our customers transparently - the typical segment was prosumers, which weren't fluent in security measures and definately NOT in mail standards - here customers didn't need to do anything.

We preferred the technical capabilities of DANE SMTP over MTA-STS, which was being marketed by big tech as a non-DNSSEC alternative.

The push for "secure-by-design" solutions in the aftermath of GDPR + The monetary incentive offered was a key parameter for shifting the priority from "nice-to-have" to "need-to-have" for management.

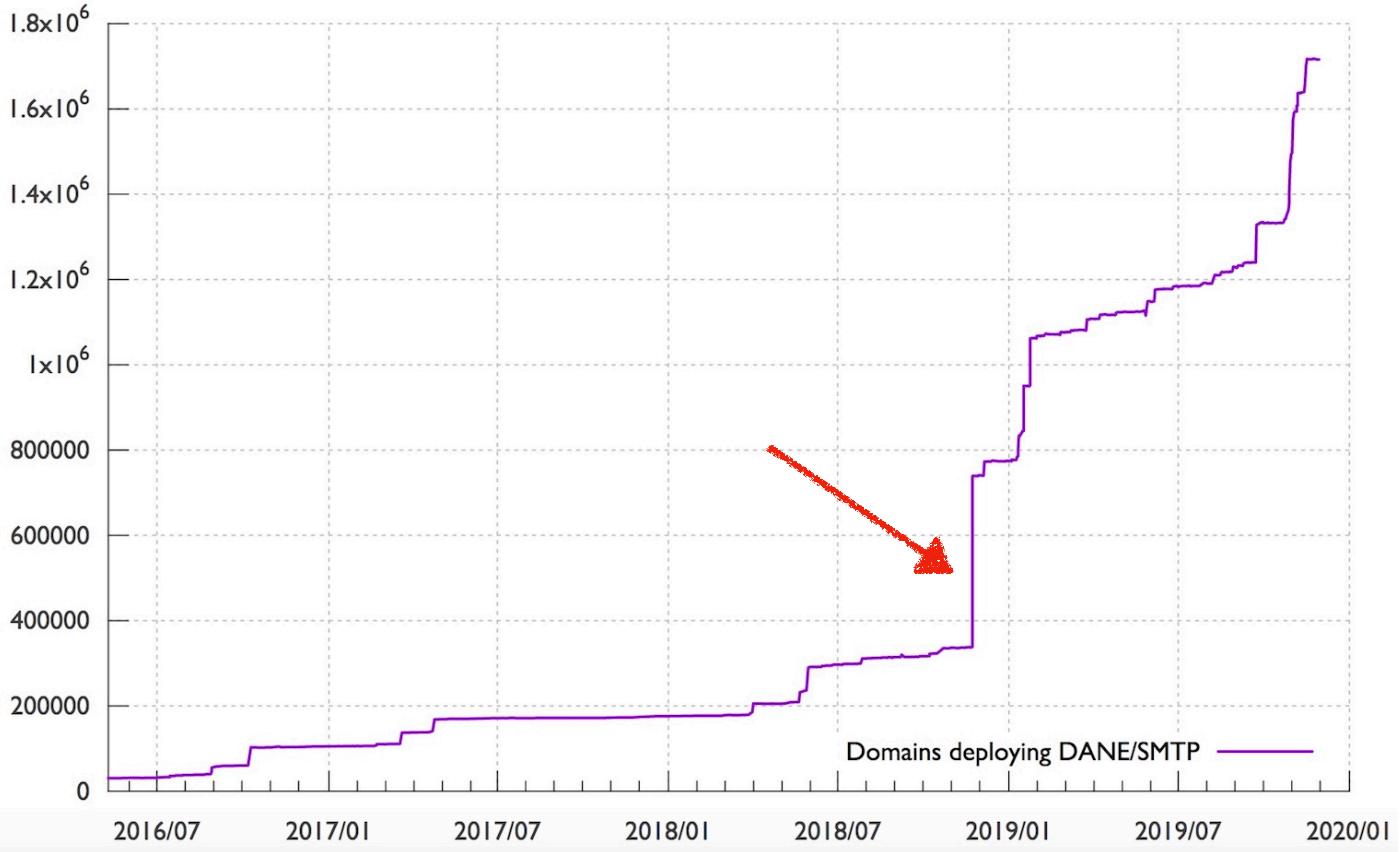
As you can see from the graph the curve was pretty flat from 2016 - 2018 — adoption was slow and there was a wish to show that it was possible to do DANE at a mass scale - it was a technically fun challenge which could push the adoption into a new gear.

The rollout more than doubled the active DANE domains and **pushed the count to >1 mio.**

one.com supported DNSSEC as a registrar for 17 TLDs at that time: se, .de, .nu,

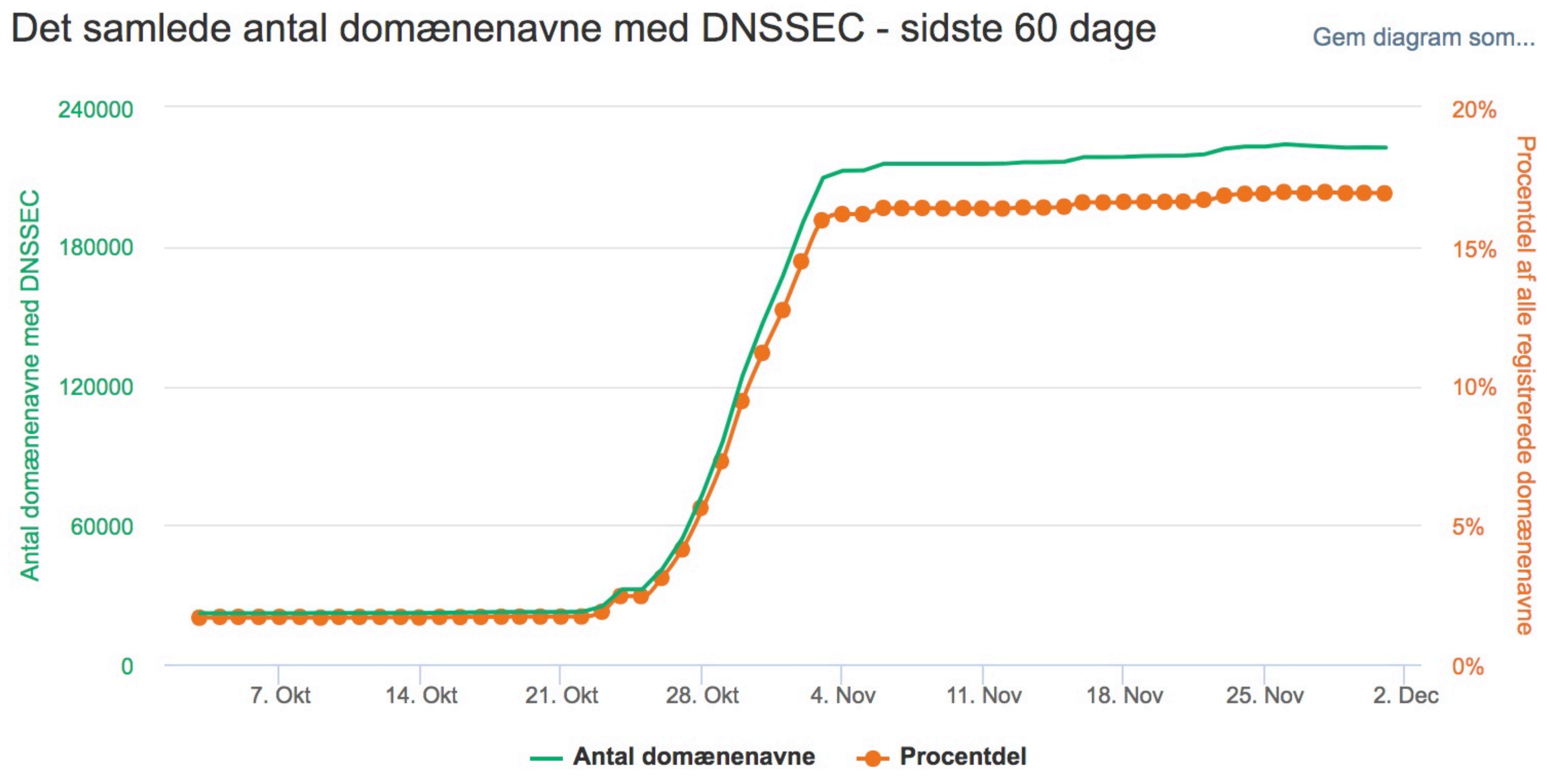
.nl, .be, .net, .com, .no, .eu, .fr, .one, .priv.no, .pm, .re, .yt, .tr, .wf

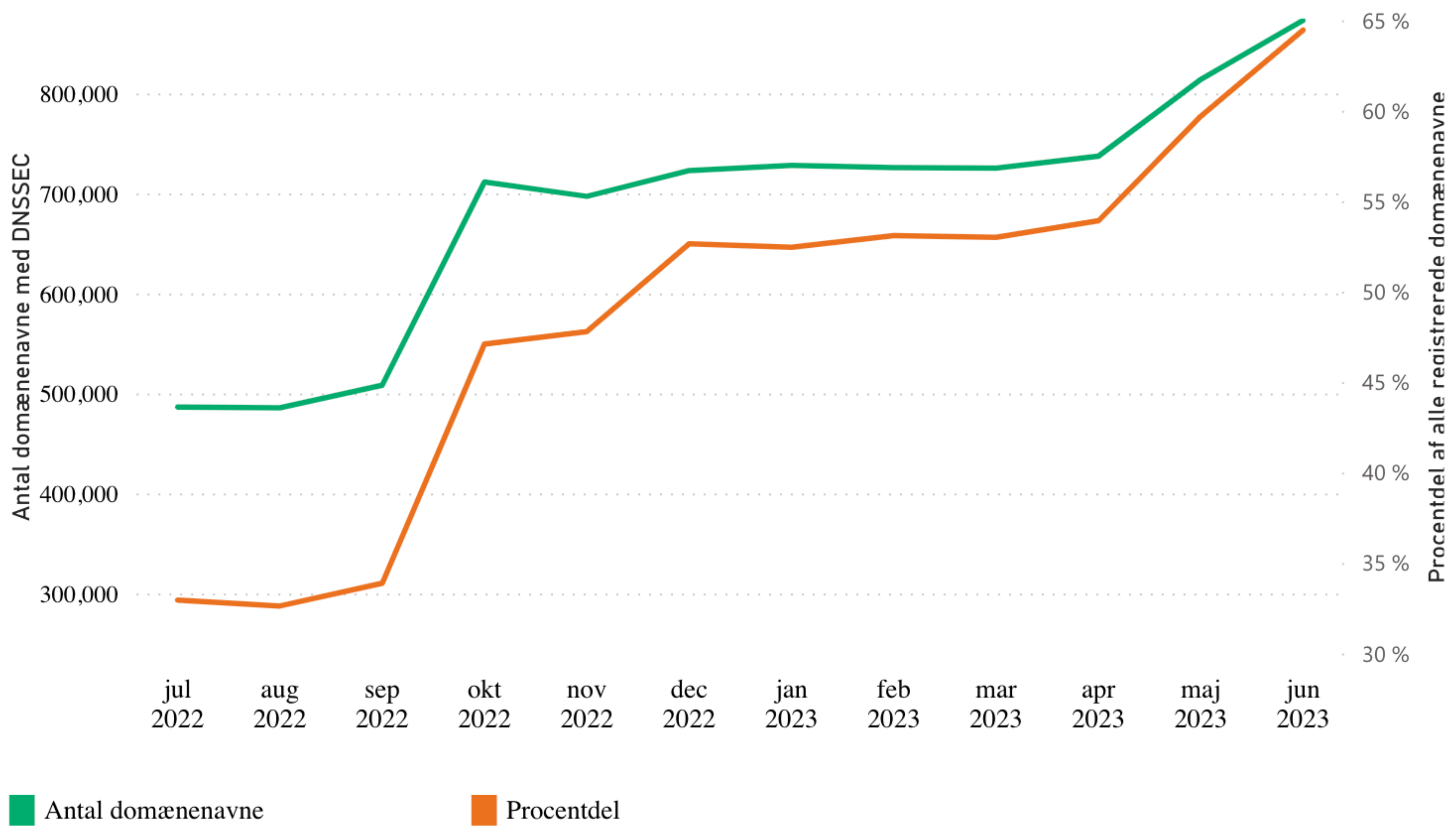
- more were added later like .dk



Driving up the DNSSEC adoption in Denmark

From ~2% to 17% in 2018 to ~64% today





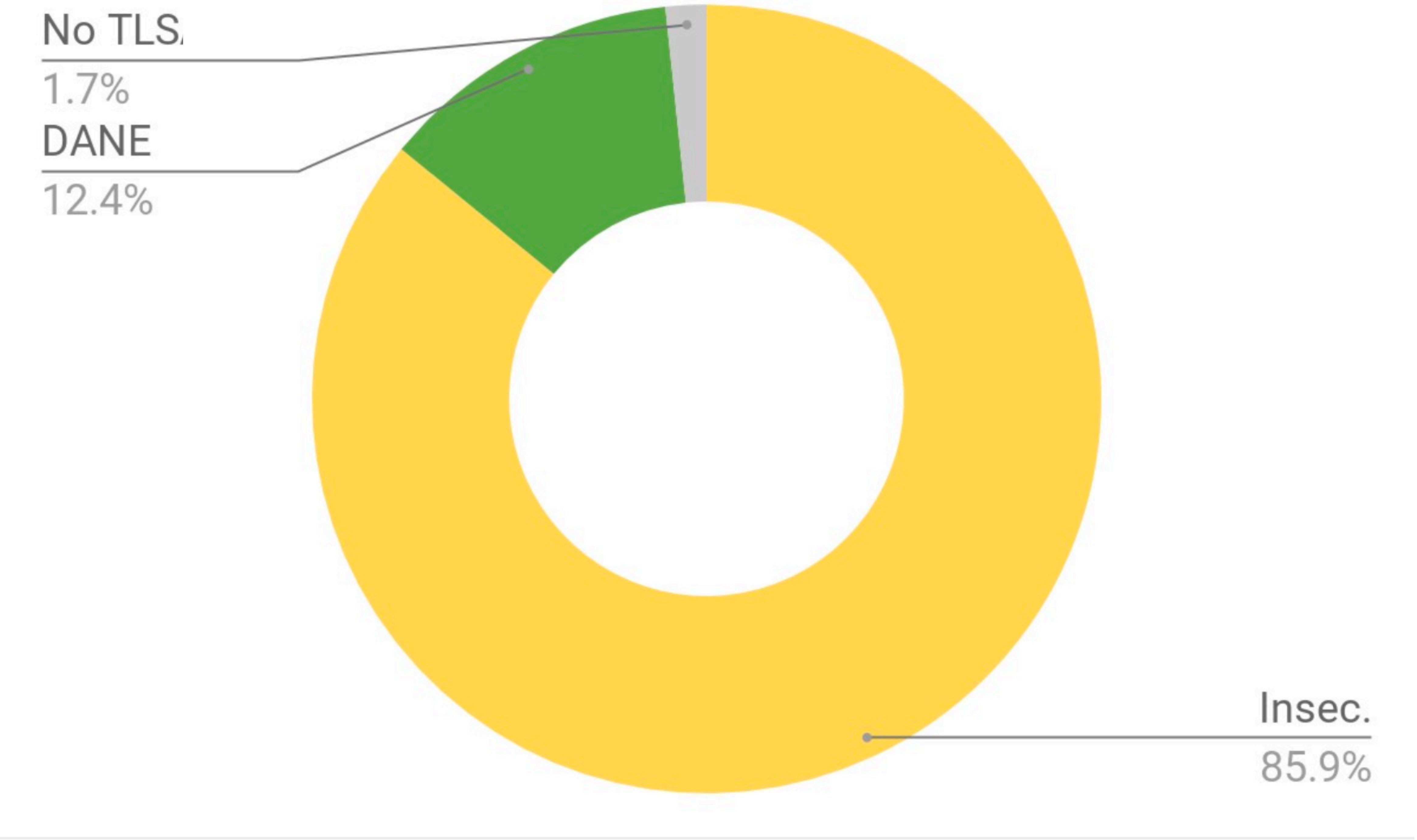
Stats can be found here: https://stats.punktum.dk/domains/dnssec_domains/

This means that .dk have finally caught up with some of the countries we normally compare ourselves to:
.nl which is at 59.32%, .no which is at 61% and .se which is at 61.44%

Lessons Learned from the one.com deployment

What did we learn?

- Enable DANE outbound first if possible - and monitor closely
- It was a split team-effort between mail and DNS engineers - and aligning on priorities can be hard if the organisation is silo'ed. Communication is key.
- For a long time we were blocked on not being able to DNSSEC sign one.com. I believe this is a typical problem.
- We had to build the automation and wrapper scripts around the key-rollover handling ourselves - nothing existed at the time. Automate it from the start - do the key-roll often and do it well (with Lets Encrypt it's every 90 days).
- If you are a Hoster, you can add ccTLDs one at a time and slowly buildup - to minimise risk
- Using the DANE fail list eased the maintenance task, but it was a manual daily task to check and handle



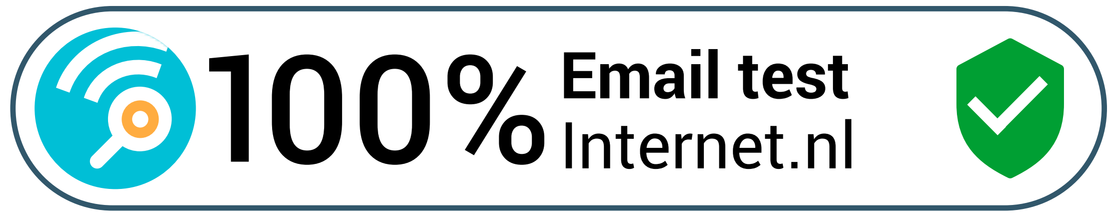
Mijndomein DANE deployment in June 2022

Getting to the famed 100%

- We (OX) rolled out inbound DANE support for Mijndomein in June 2022. Outbound DANE was unfortunately not a possibility since the Vade MTA Builder didn't support it at the time.
- We also rolled out inbound IPv6 support so they could reach a 100% in the internet.nl e-mail test.

How did it go?

- It was the most boring rollout ever! (Yes - you may quote me on that!)
- It just worked right away - no weird errors
- We had a 2 year cert, so we never got around to doing the key-roll over
- No DANE fail list needed - it's not actively maintained any more
- We had zero 2. Lvl Support tickets relating to DANE SMTP or IPv6
- We ran this setup for almost a year (until mid April 2023)



~10% of the inbound traffic was running IPv6

Fastforward to 2023

DANE statistics as of July 1st 2023 by Viktor Dukhovni

As of today, I count ~3.88 million domains with correct SMTP DANE TLSA records at every primary MX host that accepts connections[1].

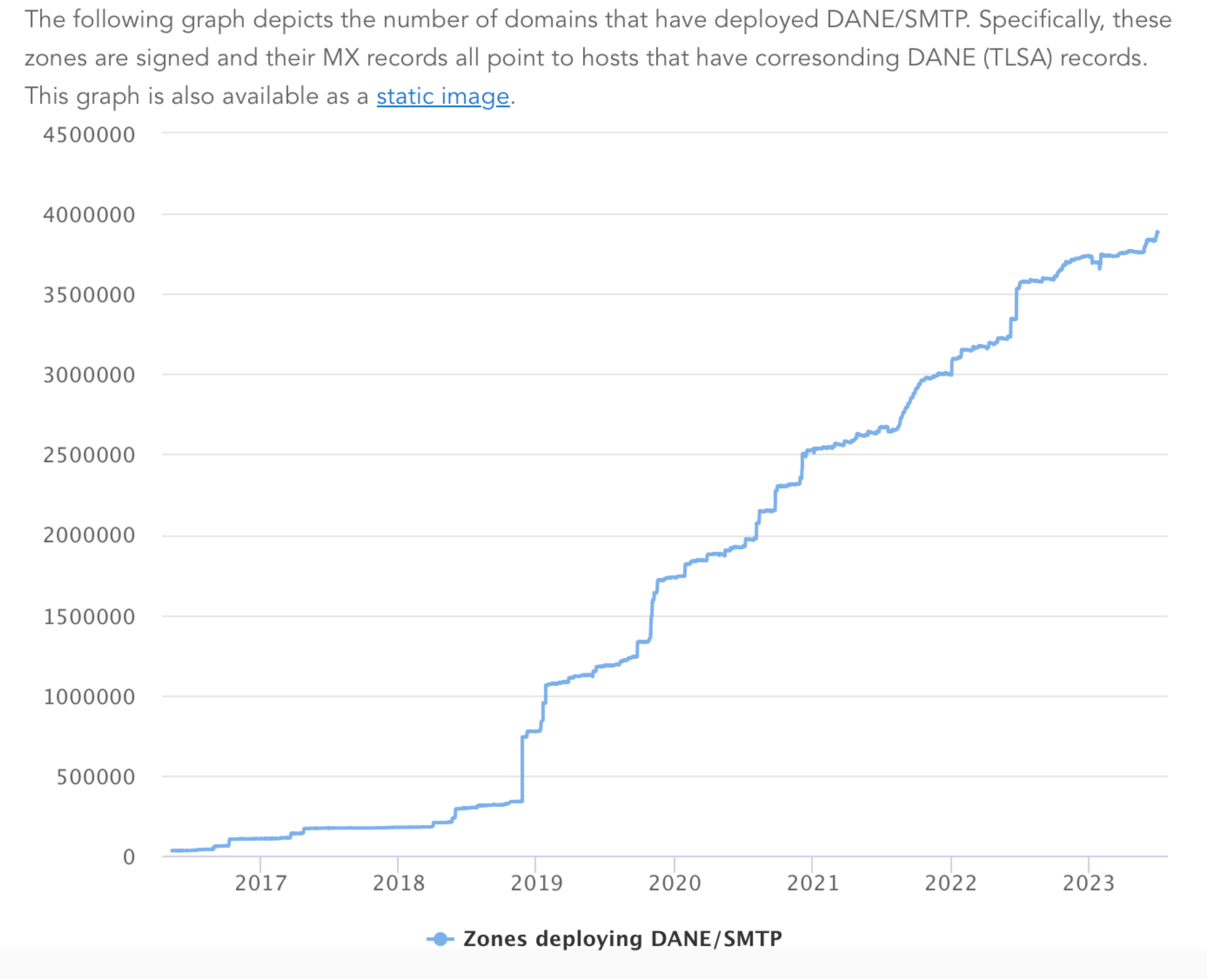
As expected, the bulk of the DANE domains are hosted by the DNS/email hosting providers who've enabled DANE support for the customer domains they host.

The top 10 MX host providers by domain count are listed on the right. Dutch hosters taking up 5 of the spots.

Place	This month	Last month	Diff	Domain
#1	1.324.503	1.248.752	75.751	one.com
#2	296.480	294.782	1.698	hostpoint.ch
#3	201.194	200.314	880	infomaniak.ch
#4	170.591	170.011	580	transip.nl
#5	169.148	169.976	-828	mijndomein.nl
#6	145.940	147.502	-1.562	argewebhosting.nl
#7	142.604	139.123	3.481	jouwweb.nl
#8	133.765	135.347	-1.582	simply.com
#9	111.038	110.750	288	hostnet.nl
#10	109.875	109.742	133	domeneshop.no

Fastforward to 2023

DANE statistics as of July 1st 2023 by Viktor Dukhovni



The following graph depicts the number of domains that have deployed DANE/SMTP. Specifically, these zones are signed and their MX records all point to hosts that have corresonding DANE (TLSA) records. This graph is also available as a static image.

The latest numbers from one.com

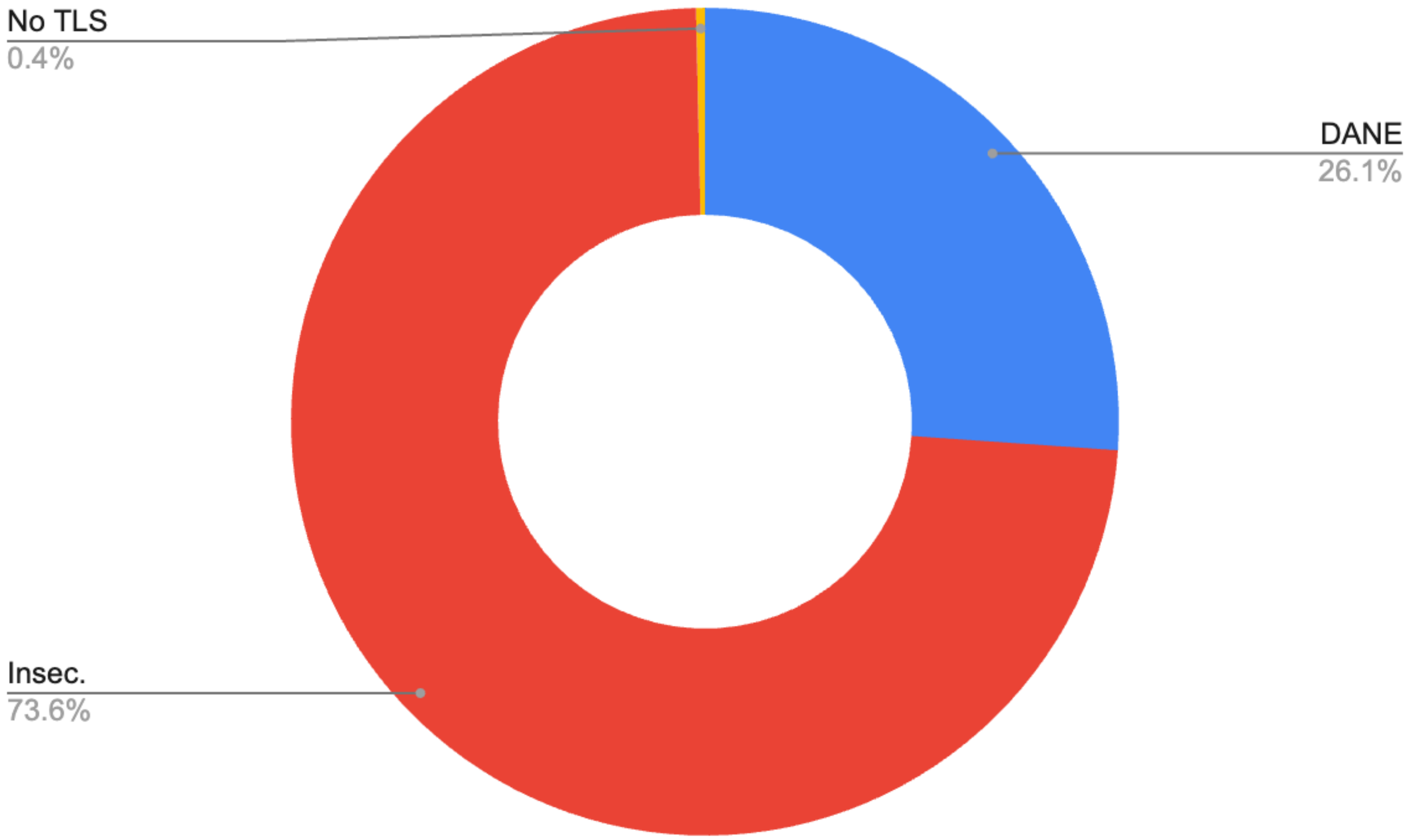
Heavy on internal traffic

Based on data gathered in the period **June 16th - 26th 2023** and based on mails sent from send.one.com - which are regular mails from user to user. Mails from websites, newsletters, webforms, etc are all sent from mailout.one.com and hence not included.

Excluding internal traffic: 4.15% DANE

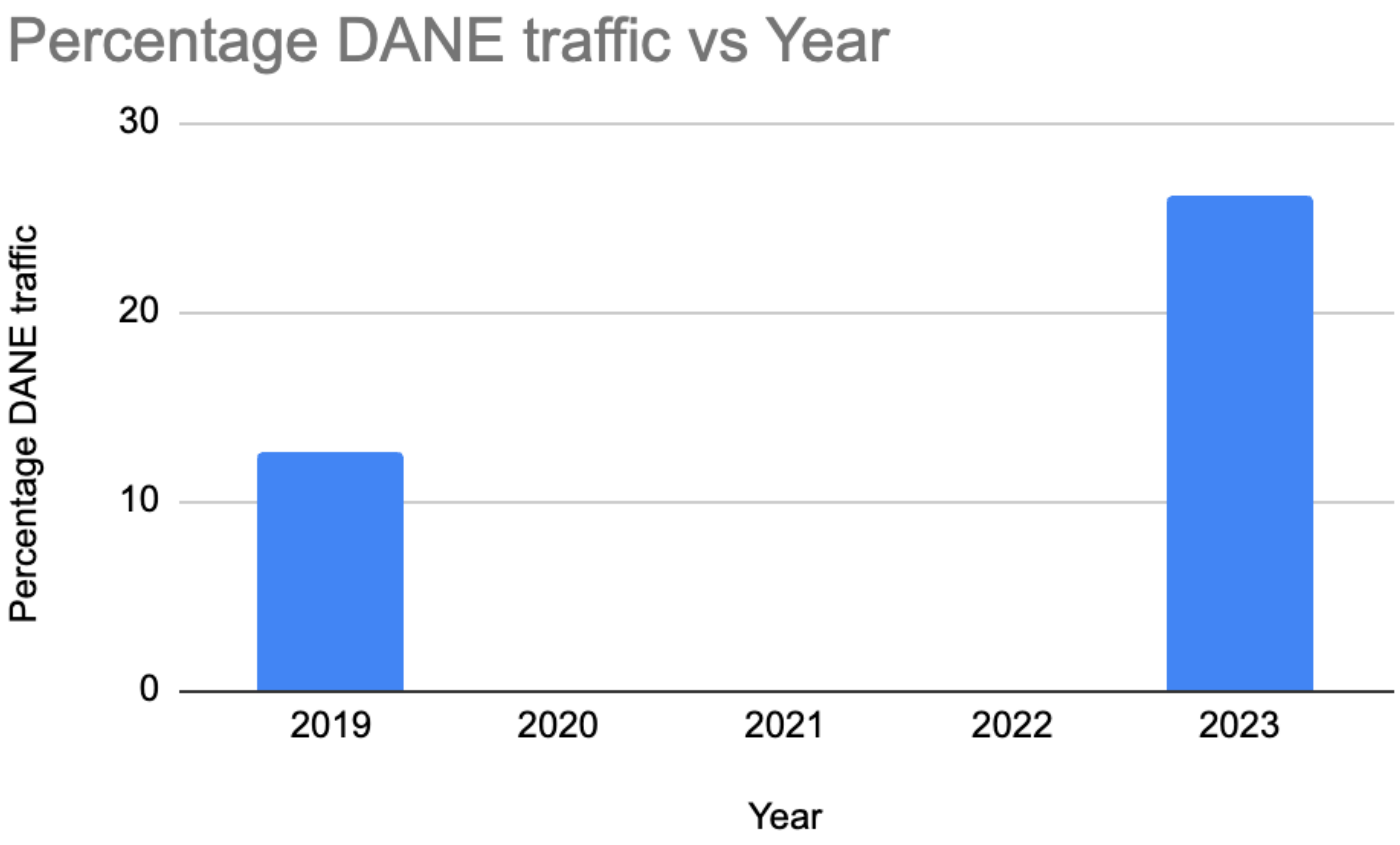
Including internal traffic: 26.1% DANE

non-TLS is 0.35%



The latest numbers from one.com

DANE traffic doubled in 5 years



Hot of the press in Denmark

New updated technical minimal requirements for state/government entities

By the end of June a new set of technical requirements to state entities was made public. The requirements are non-negotiable and must ensure a common high level of security in the Danish state entities. **The requirements must be met no later than by July 1st 2024.**

The 20 technical minimal requirements for state entities can be found here (unfortunately currently only in Danish):

https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/tekniske-minimumskrav-2024

From the section **on requirements for domain security**:

17. Internet facing services belonging to the entity MUST be registered under a .dk domain
18. DNSSEC MUST be associated to all domain names belonging to the entity
19. It MUST be guaranteed that inbound mail gateways are operating on DNSSEC signed domains
20. **DANE MUST be used for all inbound mail gateways**
21. DNSSEC validation MUST be performed for all DNS queries
22. The entity MUST use a secure DNS service OR implement another solution to provide security against known harmful domains.
23. A DMARC reject policy MUST be implemented on all domains belonging to the entity

Where are the challenges for further adoption?

Improvement Ideas

We still see hard dependencies between mail and DNS engineers in a deployment. Perhaps it could be possible to further improve the **DNS management REST APIs** - to loosen the dependencies? It would most likely help combat the “silofication”. Companies moving to the Cloud typically get access to provider APIs.

The amount of **DNS providers that now support DNSSEC** have increased compared to earlier - but push the ones that still don’t - make DNSSEC support a requirement for choosing them. Your capabilities are impacted by their capabilities.

KSK rollovers are complex, but not if you're both a DNS operator and a registrar, in that case automating KSK rollovers can also be routine. The difficulty arises largely because it can be tricky to coordinate MTA public key/certificate rollovers with DNS TLSA RRset updates. This is where https://github.com/tlsaware/danebot can come in handy.

Start nudging those in the long tail of slow adopters. Check out the list at https://dnssec-stats.ant.isi.edu/~viktor/hosters.html - if you have someone there in your professional network contact them and offer to help.

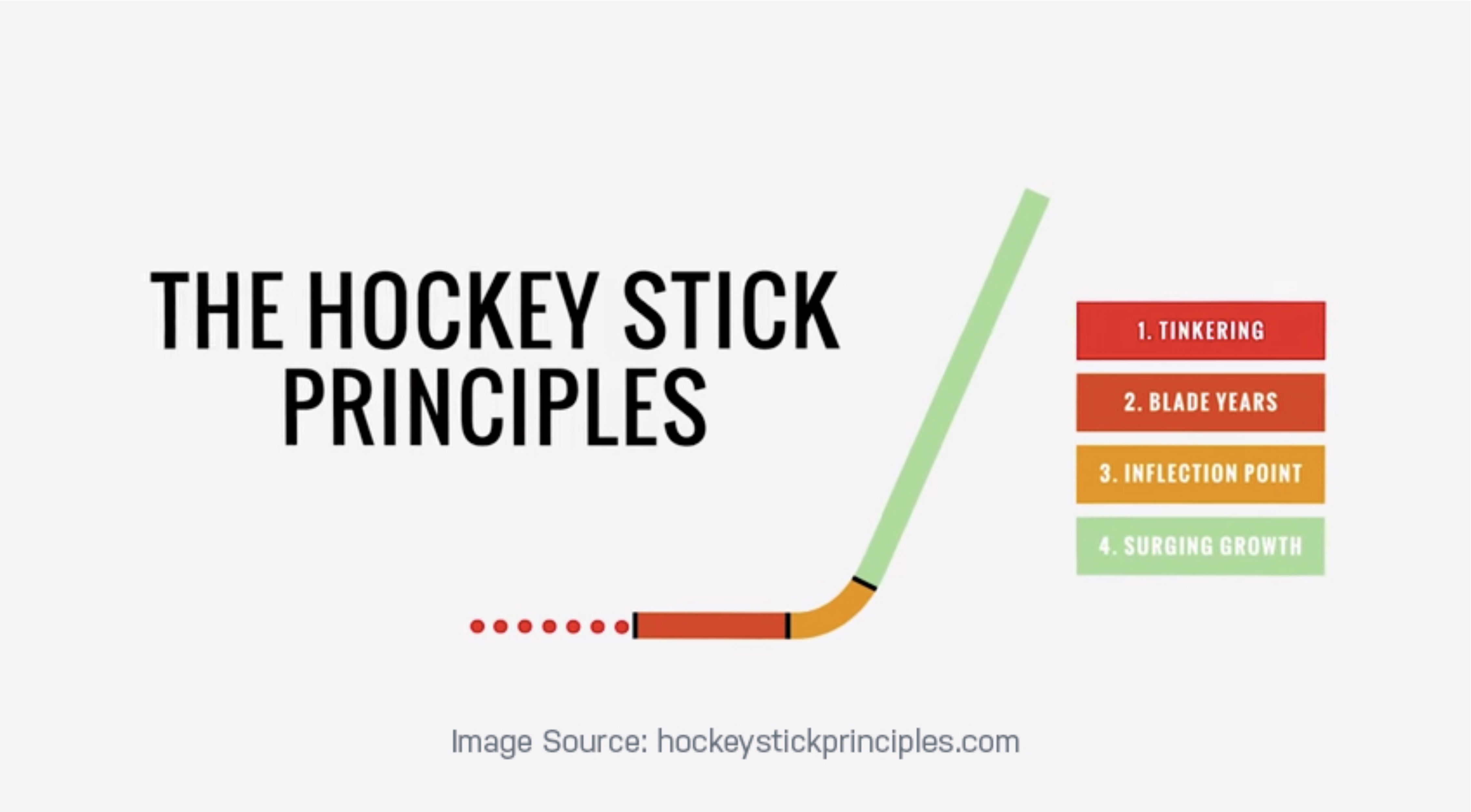


Image Source: hockeystickprinciples.com

How can you help?

We need to focus the effort

- We need even **better tooling**: Viktor would appreciate some help improving https://github.com/tlsaware/danebot . Danebot is a certbot wrapper that helps to avoid SMTP outages due to mismatched TLSA records resulting from a Let's Encrypt automated certificate renewal. It should be quite usable already, but could use some polish. The main missing piece is support for modifying the list of supported domains. There will be an improvement list under the GitHub project, so it’s going to be easier to pitch in.

- We need **better documentation**: Write a blog in your local language describing how to set up DANE SMTP or how to do the key rotation right without impacting mail deliveries or simply spread the knowledge about danebot for instance. https://github.com/internetstandards/toolbox-wiki/blob/main/DANE-for-SMTP-how-to.md is an excellent example to be followed.

- We need **further common incentives** in more European countries or on EU level for management to prioritise implementation of DANE SMTP among the multitude of other IT/security projects. NIS2 work is coming up soon, which will take a lot of focus like we saw during the GDPR implementation. The “comply or explain” legislation is working - we just need it in more countries.

- We also need to **bridge the gap** between EU and US. US still seems to be either focused on MTA-STS or on the negative effects of DNSSEC breakage. DANE SMTP is on Cloudflare’s current Roadmap - more pressure on Cloudflare would be helpful. A good US based Hoster implementation story would also be great for awareness.

Questions?