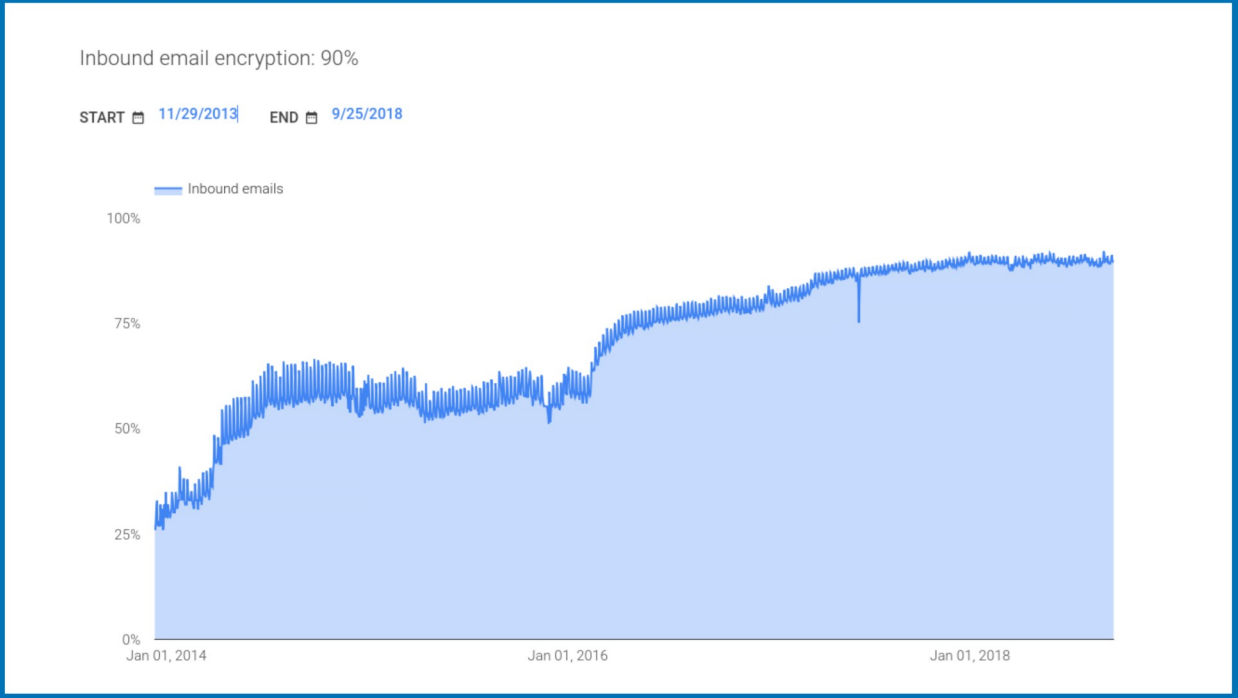
Five Years of DANE

Modern, Secure and Stress-free SMTP

90% encryption! Why bother?



https://transparencyreport.google.com/safer-email/overview

Most of the time
we send email encrypted
to destinations
we probably know.

Most of the time?
We probably know?

Clients don’t know
a server can encrypt
before the server offers it
during the session.

Clients can’t tell
by themselves
they are talking
to the right server.

Opportunistic TLS Security Flaws

- CA model
- MITM attack
- Downgrade attack
- Incomplete automation for certification rollover

BrOken CA Model

- Any CA may issue certificates for any domain
- CAs have been compromised in the past
- CAs have issued wrong or unauthorized certificates

MITM Attack

- What's in a name?
- Attackers impersonate using matching certificates
- Everyone accepts self signed certificates anyway...

example.com

example.com

Session downgrade

- STARTTLS without policy channel
- STARTTLS support unknown before SMTP session
- Attacker may downgrade session to „Non-TLS“

```
220 mail.example.com ESMTP
EHLO client.example.com
250-mail.example.com
250-PIPELINING
250-SIZE 40960000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

No Automation

- Manual verification
- Verification requires knowledge
- Verification requires presence
- Need to monitor certificate change

DANE

DANE (RFC 7672)

- Adds a policy channel
  → DNS
- Adds a trust layer
  → DNSSEC
- Indicates encryption
  → TLSA Resource Record
- Identifies identity
  → TLSA Resource Record

How it works (in one slide)

Federal Office for Information Security

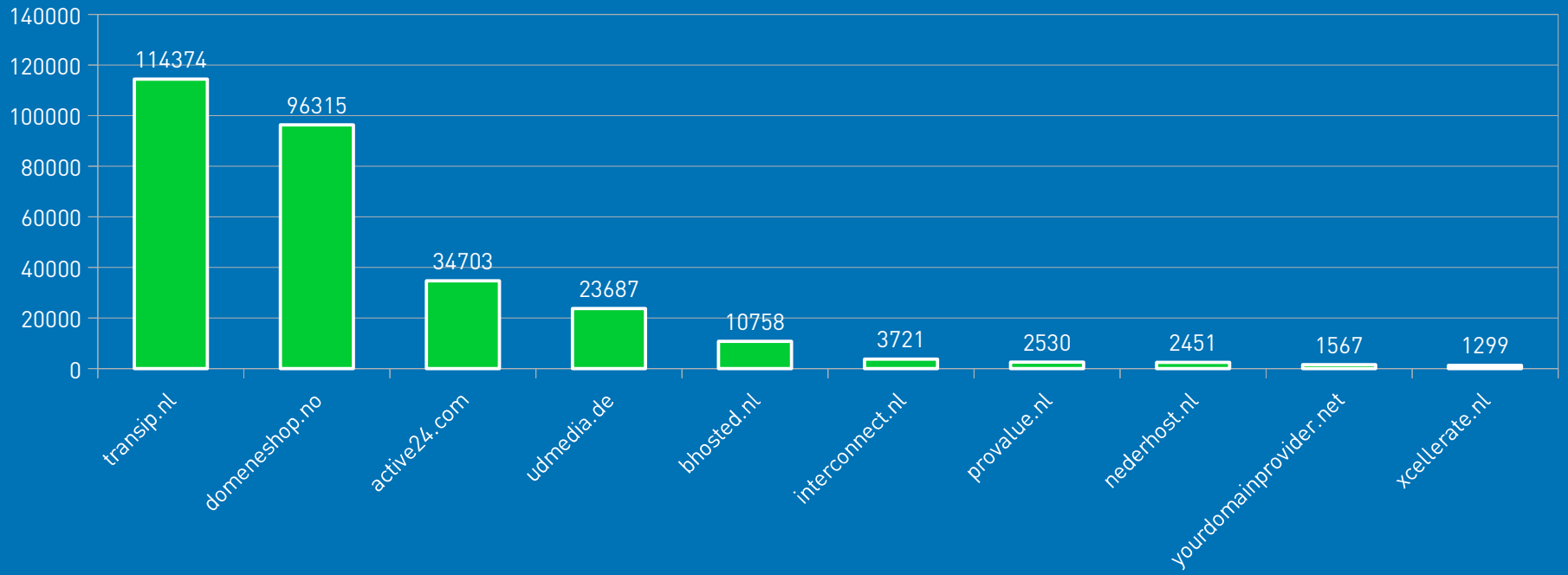
- Technical guideline BSI TR-03108, “Sicherer E-Mail-Transport”
- Requirements for ESPs about secure message transport
- Essential component: “automate secure transport … via DANE/TLSA using DNSSEC”
- DANE required for “recertification”
- Major German players web.de and GMX adopt DANE

Status Quo DANE

DANE

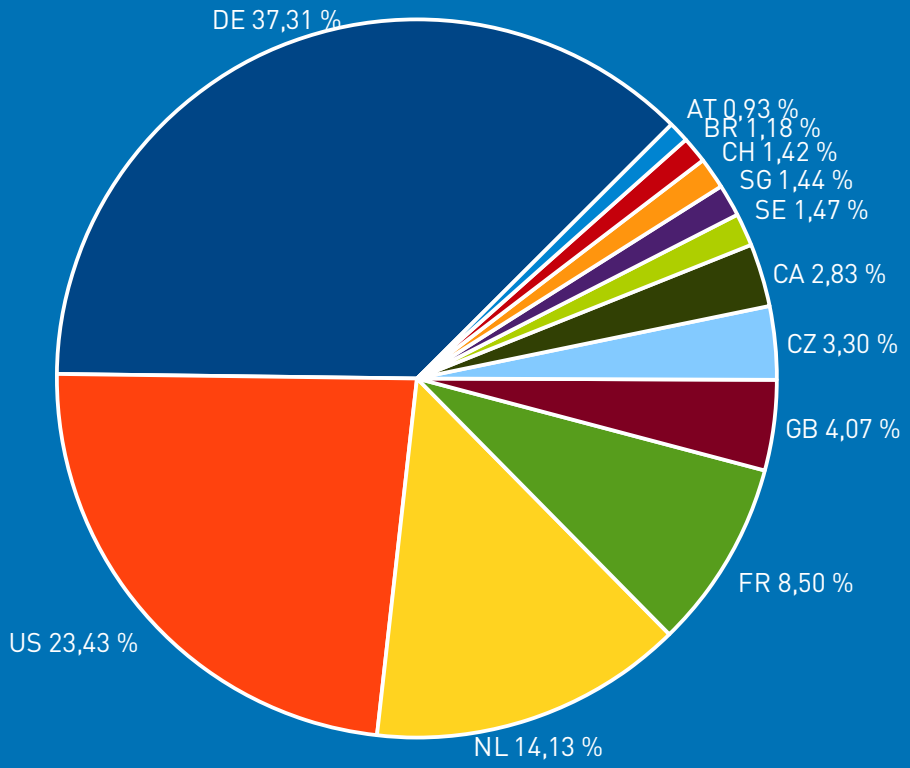
- 8.99 million domains with DNSSEC-validated MX answers
- ~316 thousand domains fully DANE TLSA covered
- ~ 1.000 domains partially DANE TLSA covered
- 5.443 MX hosts in ~3620 organizations (DNS zones)
- ~530 domains with TLSA lookup problems
- ~250 domains with wrong TLSA or no STARTTLS (despite TLSA)

Top 10 DANE MX Host Providers



Source: Viktor Dukhovni, DANE Survey 2018/09

Top 12 DANE MX Hosts



Source: Viktor Dukhovni, DANE Survey 2018/09, IPv4 GeoIP

Significant Domains

active24.cz aegee.org anubisnetworks.com asf.com.pt **bayern.de** bhosted.nl boozyshop.nl **bund.de** **comcast.net** cuni.cz debian.org deltion.nl destroystores.cz dk-hostmaster.dk domeneshop.no egmontpublishing.dk **elster.de** fau.de freebsd.org **freenet.de** gentoo.org **gmx.at gmx.ch gmx.com gmx.de gmx.net** govtrack.us handelsbanken.no handelsbanken.se hierinloggen.nl hr-manager.net **ietf.org** inexio.net insee.fr interconnect.nl intermax.nl isc.org jpberlin.de klubpevnehozdravi.cz lrz.de **mail.com mail.de** minmyndighetspost.se mpssec.net netbsd.org netic.dk nic.br octopuce.fr open.ch **openssl.org** optimail.cz ouderportaal.nl overheid.nl pathe.nl politie.nl **posteo.de** registro.br ruhr-uni-bochum.de rushtrondheim.no samba.org skatteverket.se smtp.cz societe.com solvinity.com t-2.com t-2.net t-2.si tilburguniversity.edu **torproject.org** transip.be transip.net transip.nl trashmail.com truetickets.nl tum.de uni-erlangen.de unitybox.de **unitymedia.de** uvt.nl **web.de** webcruitermail.no xfinity.com xfinityhomesecurity.com xfinitymobile.com **xs4all.net** **xs4all.nl**

Source: Gmail email transparency report

Lessons learned...

DANE for everyone

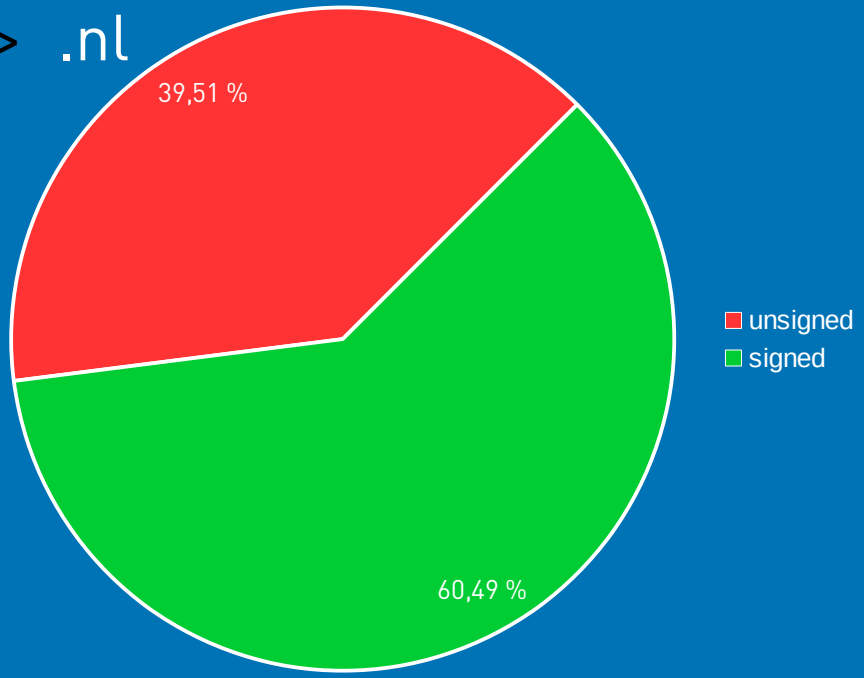
- Enable DNSSEC capable resolvers
  You probably have them in place and don't know it
- Enable outbound DANE
  You don't need your domain to be DNSSEC enabled
- Use Postfix, Exim, Halon, Cisco ESP, Port 25, Cloudmark, ...

Deploying DNSSEC is the main barrier

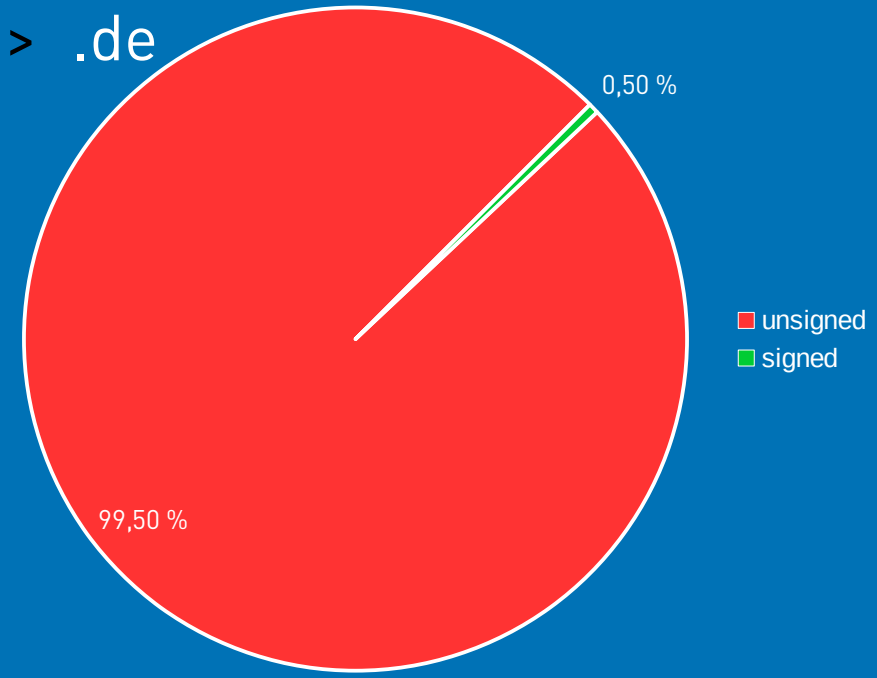
- „DNSSEC is a fail, because it does not encrypt!”
- „DNSSEC is fancy technology without a business case”
- „DNSSEC makes DNS mission critical“
- Registrars offer incomplete or no DNSSEC-support
- Missing know-how for automated certificate-management and DNSSEC signing
- Missing toolchain for automated management

Signed vs. Unsigned Domain Ratio

> .nl

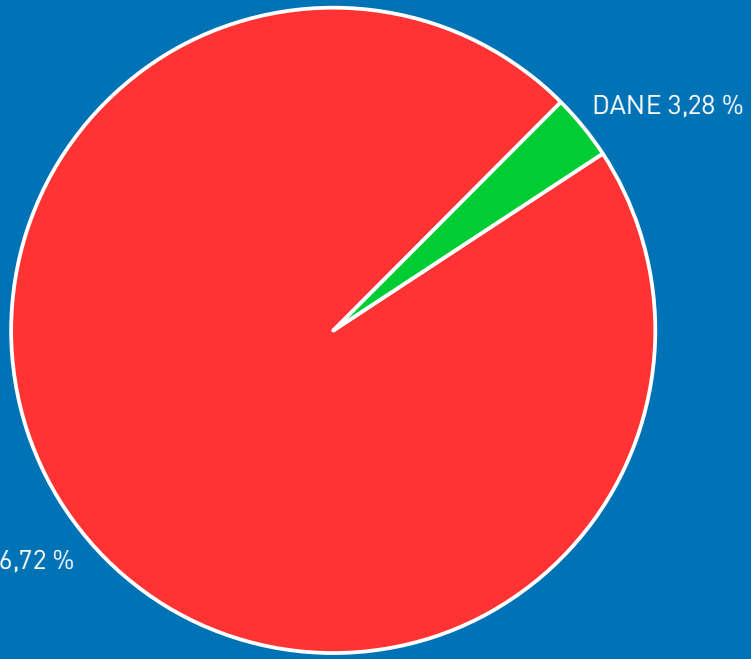


> .de

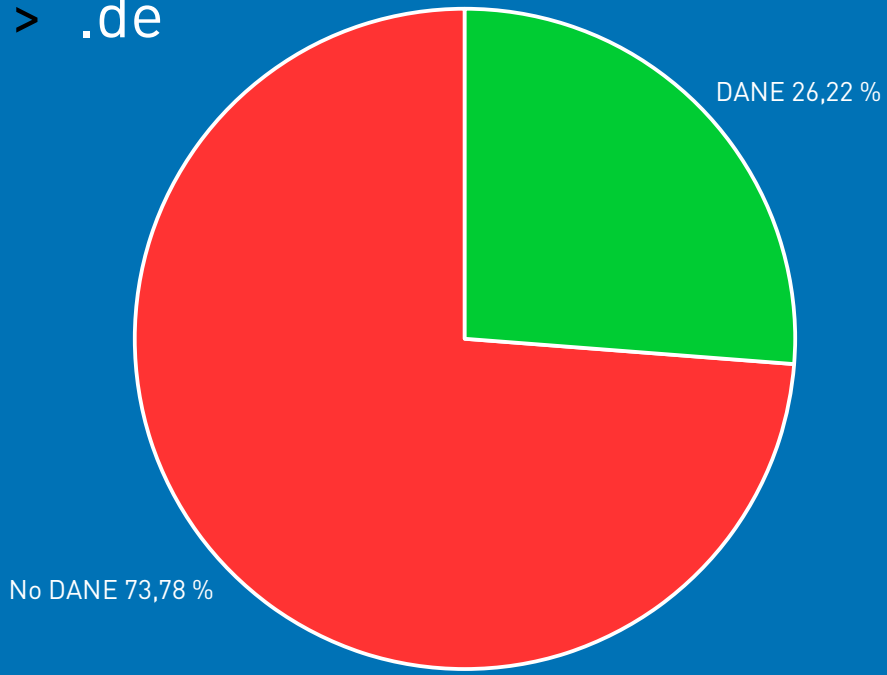


No DANE vs. DANE Ratio

> .nl



> .de



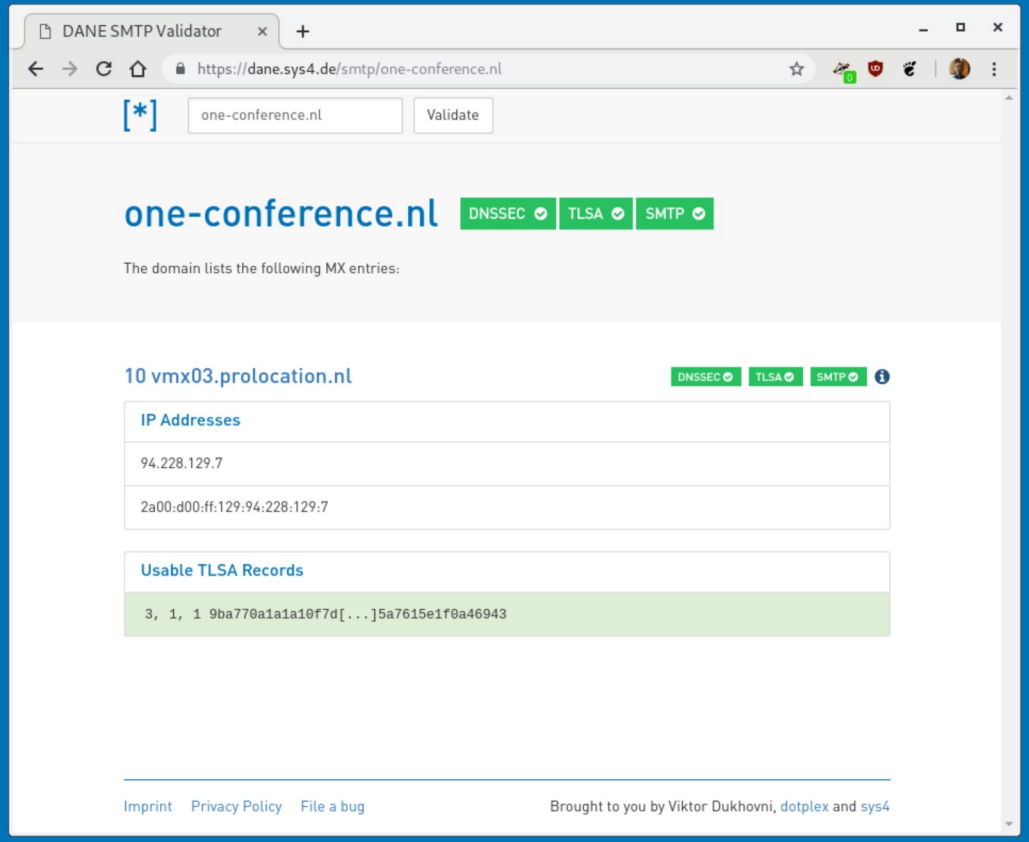
TLSA Best Practice

- Reuse Key
  No need to update TLSA Resource Record
- Automate key rotation
  Most failures stem from forgotten TLSA Resource Records
- Anticipate foreign cache issues
  Deploy new certificate on time (at least 2x $TTL)
- Prepare to fail
  Deploy two TLSA records with different expiry – one for production, one as fallback
- Measure, don't speculate
  Monitor TLSA correctness

SMTP TLS Reporting (RFC 8460)

- “(...) a reporting mechanism and format by which sending systems can share statistics and specific information about potential failures with recipient domains.”
- DANE-specific
  - tlsa-invalid
  - dnssec-invalid
  - dane-required

DANE Validator



We do ASCII

Patrick Ben Koetter, p@sys4.de

https://sys4.de/download/dane-one.pdf

MTA-STS (RFC 8461)

- "...the mechanism described here instead relies on certification authorities (CAs) and does not require DNSSEC, at a cost of risking malicious downgrades."
- "The primary motivation of MTA-STS is to provide a mechanism for domains to ensure transport security even when deploying DNSSEC is undesirable or impractical."