DANE/SMTP Usage Report

Viktor Dukhovni
Two Sigma
<ietf-dane@dukhovni.org>

Wes Hardaker
USC/ISI
<hardaker@isi.edu>

ICANN63 | Barcellona, Spain | October 2018

Overview

1. Background
2. E-Mail Security without DANE
3. E-Mail Security with DANE
4. DNSSEC and DANE deployment statistics
5. Appendix

Email Security

Sending
Mail Server

1. User sends mail
to their outgoing
mail server

**Authenticated SMTP
over authenticated TLS**

Receiving
Mail Server

3. User receives mail
from their incoming
mail server

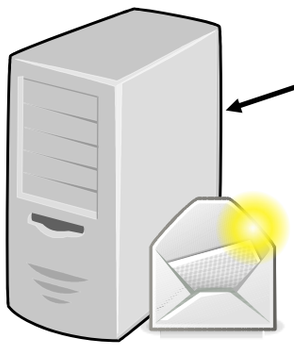
**Authenticated IMAP
over authenticated TLS**

Email Security

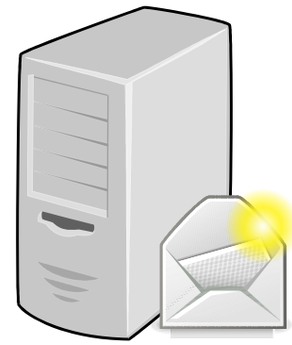
2. MTA-to-MTA SMTP

Then a miracle occurs

Sending Mail Server



Receiving Mail Server



1. User sends mail to their outgoing mail server

Authenticated SMTP over authenticated TLS

3. User receives mail from their incoming mail server

Authenticated IMAP over authenticated TLS

Email Security

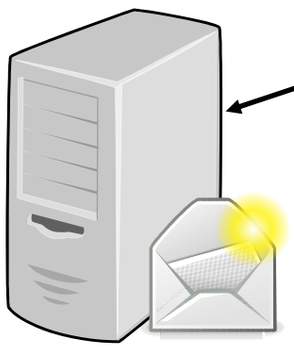
F
6/10

"I think you should be more explicit here in step two."

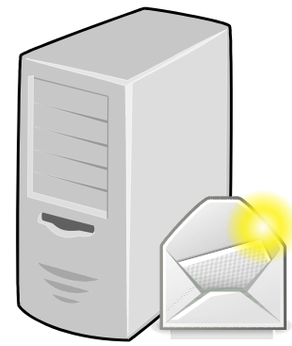
2. MTA-to-MTA SMTP

Then a miracle occurs

Sending Mail Server



Receiving Mail Server



1. User sends mail to their outgoing mail server

Authenticated SMTP over authenticated TLS

3. User receives mail from their incoming mail server

Authenticated IMAP over authenticated TLS

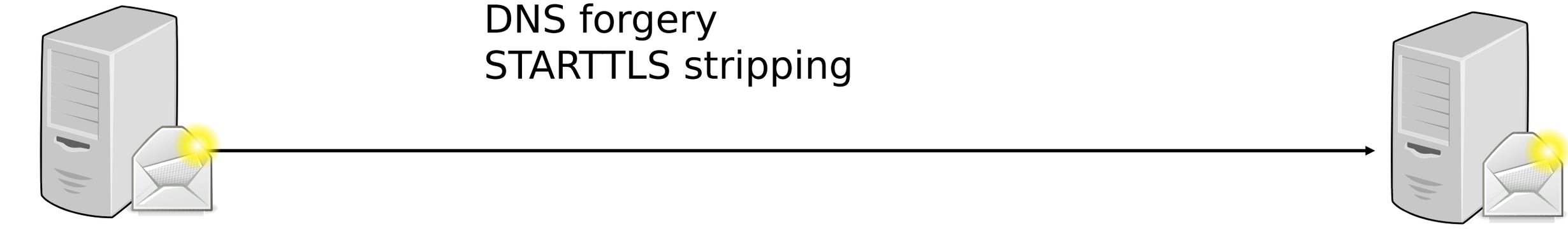
Email Security
One Solution

Choice 1: Opportunistic (START)TLS

Resists Passive monitoring
Still vulnerable to active attacks:
- BGP hijacking
- DNS forgery
- STARTTLS stripping

Sending Mail Server

Receiving Mail Server



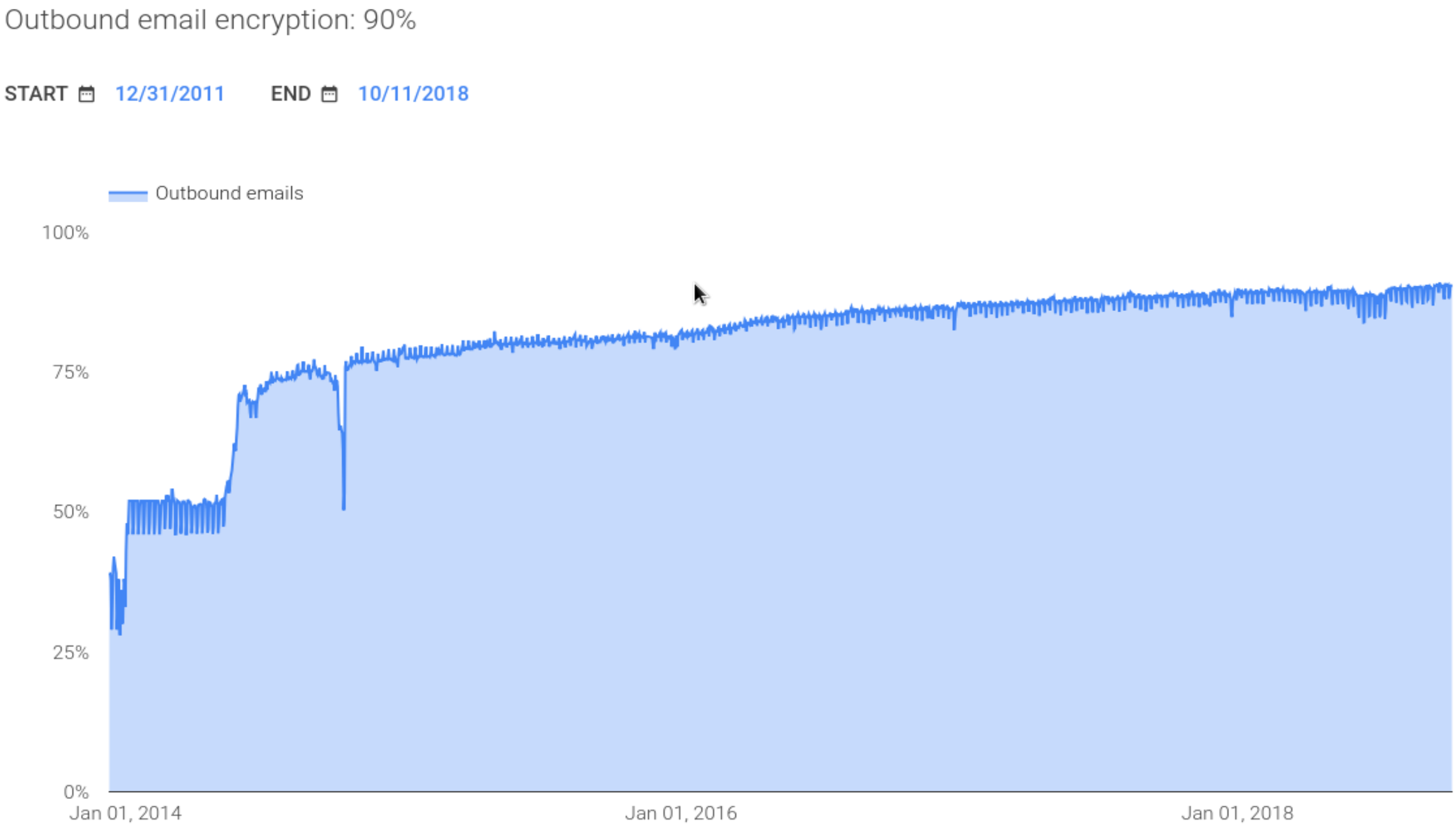
1. User sends mail to their outgoing mail server

Authenticated SMTP over authenticated TLS

3. User receives mail from their incoming mail server

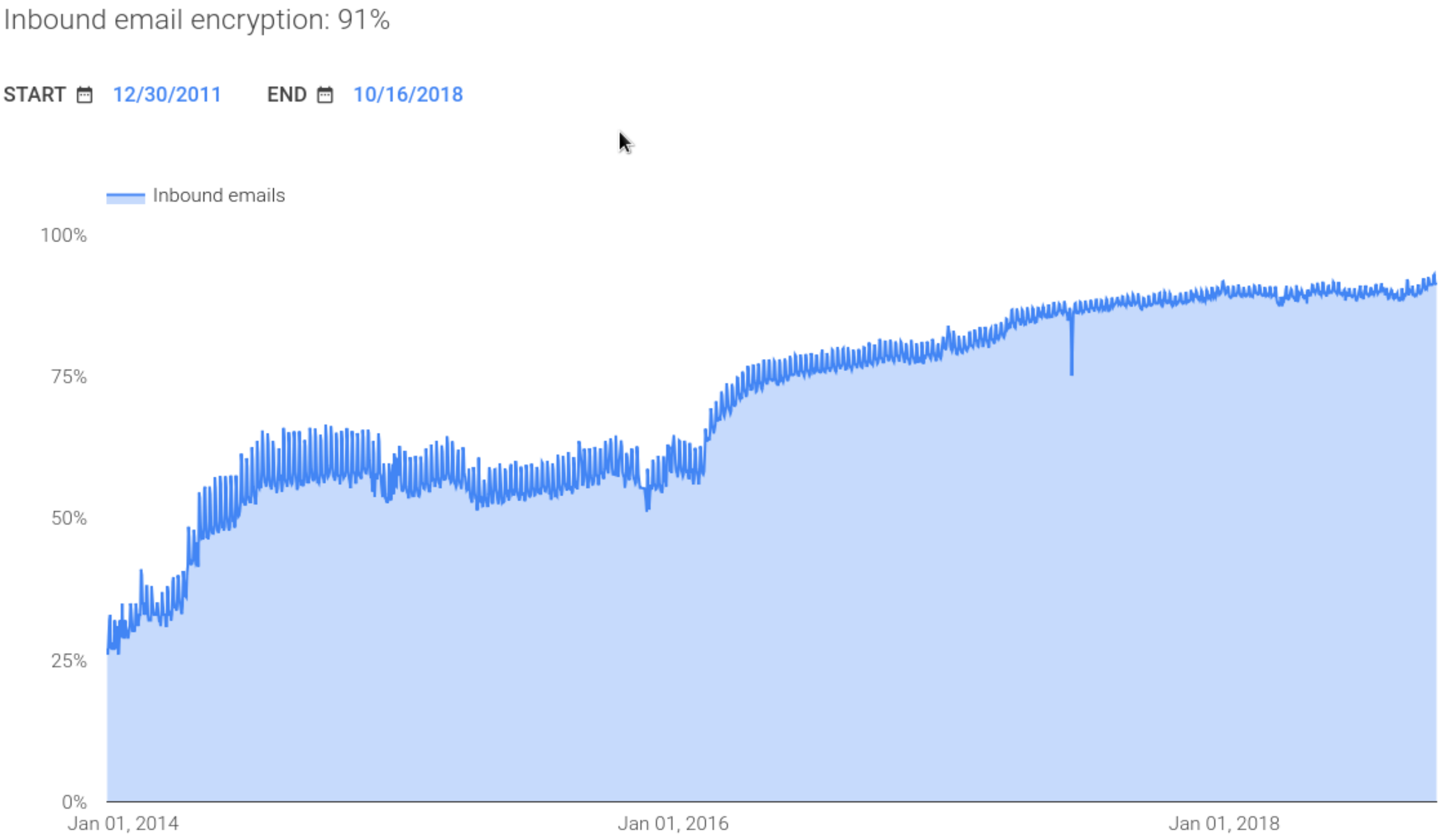
Authenticated IMAP over authenticated TLS

GMail STARTTLS growth: out



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

GMail STARTTLS growth: in



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

Better SMTP Security Goals

- Resist active attacks:
  - Must be downgrade-resistant
    - (even on first contact)
  - Must support mixed environment
  - Must signal which peers to encrypt
  - Must indicate how to authenticate each peer

SMTP is not like HTTPS

https://tools.ietf.org/html/rfc7672#section-1.3

- Must trust DNS to obtain authoritative MX hosts
- Web-like CA trust would be problematic
  - Too many CAs to trust, but no user to "click OK"
  - Can't avoid trusting them all

DNS-Based Authentication of Named Entities (DANE)

- In SMTP, presence of DANE TLSA records is:
  - A contract to support STARTTLS
  - Parameters needed to contact (“3 1 1”)
  - Which certificates and/or signers to trust

```
_25._tcp.mx1.example.com. TLSA 3 1 1 curr-pubkey-sha256
_25._tcp.mx1.example.com. TLSA 3 1 1 next-pubkey-sha256
```

- Records authenticated via DNSSEC
  - no trusted third parties required
  - ensures downgrade protection

DANE Usage and Operational Practice

ICANN63 | Barcellona, Spain | October 2018

Coexisting with DANE

- For DNSSEC-signed domains **without DANE**:
  - TLSA Denial of Existence (DoE) must function correctly
    - *(DANE is first protocol requiring reliable DoE)*
  - Proven lack of a TLSA record means no security
  - Send over unencrypted SMTP, as you used to

- What happens when DANE DNSSEC lookup **fails**?
  - DANE senders skip those MX hosts
  - When all MX hosts are skipped, delivery is deferred

Adopting DANE

- Deploying DNSSEC is the main barrier
- Coordinating TLSA records and cert chain may look hard
- We'll make it easy

Outbound SMTP/DANE

- DANE-enabled MTA (Postfix, Exim, Cloudmark, ...)
- Need DNSSEC validating resolver
  - (see your MTA docs)
- Enable DANE as documented
- Make a few policy exceptions:

https://github.com/danefail/list

Inbound SMTP/DANE

- Need STARTTLS-capable SMTP server
- DNSSEC-signed MX records
- DNSSEC-signed TLSA records for each MX host
  - If MX hosts are outsourced, they must be signed!
  - Properly managed key and certificate rotation

DANE tools

- https://dane.sys4.de/ and list dane-users@sys4.de
- https://github.com/letoams/hash-slinger
- https://github.com/PennockTech/smtpdane
- https://github.com/vdukhovni/danecheck
- Bare knuckles† with `openssl s_client`

† see last two slides of Appendix.

DANE SMTP Survey

ICANN63 | Barcellona, Spain | October 2018

Introducing stats.dnssec-tools.org

- https://stats.dnssec-tools.org/
  - Created by Viktor Dukhovni and Wes Hardaker
  - (Eventually) a continually updating web-page
  - “Just ramping up” (aka still under development)

- Reporting deployment statistics for:
  - DNSSEC generally
  - DANE specifically

- The data from the following slides are on this site

Introducing stats.dnssec-tools.org

Overview

The following DNSSEC deployment statics come from the work of Viktor Dukhovni (Two Sigma), published by Wes Hardaker (USC/ISI) as part of the DNSSEC-Tools project.

Summary Statistics

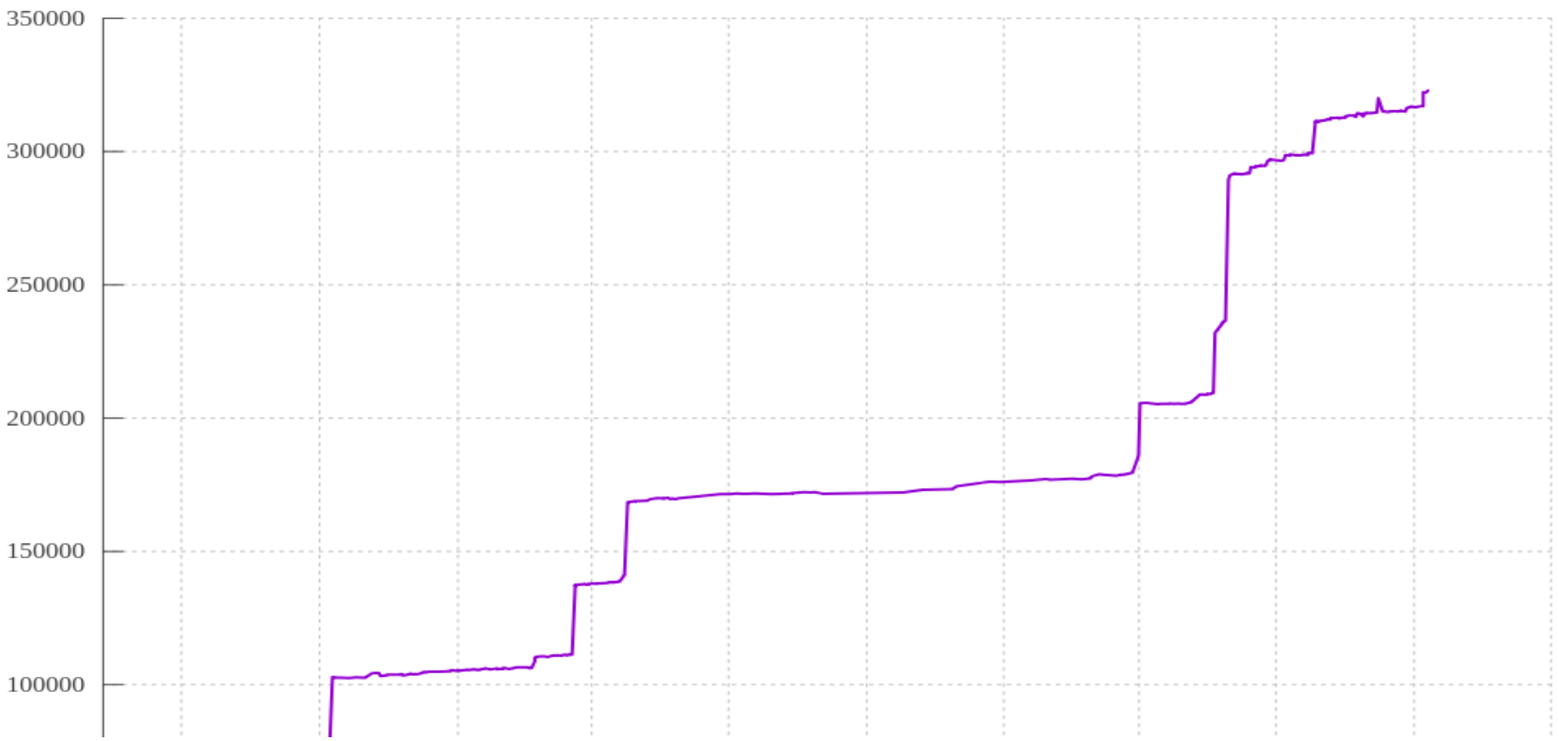
The September 2018 numbers from the DANE/DNSSEC survey are:

```
Total DS RRsets:                8,913,611
Validatable apex DNSKEY RRsets: 8,766,973
```

DANE Trend graphs

Domains with signed MX and DANE records

The following graph depicts the number of domains that have deployed DANE/SMTP. Specifically, their zone is signed, their MX records all point to hosts that have DANE TLSA records.



ICANN63 | Barcellona, Spain | October 2018

DNSSEC / DANE Survey

(all work by Viktor Dukhovni)

- Monitors domains delegated from public suffixes
- Notifies operators of botched key/cert rotation
- Sourced from ICANN CZDS, Verisign, https://scans.io/, open access for .se, .nu, .fr, .nl, ... (more ccTLD data wanted), FarSight Security
- Covers ~200 million candidate domain names
- Captures DS, DNSKEY, MX, A, AAAA, TLSA records
- Captures certificate chains of MX hosts

Survey Stats

(as of 2018-10-11)

- 8.95 million domains with DNSSEC-validated MX
- 323 thousand domains with DANE SMTP
- Millions of users (gmx.de, web.de, comcast.net)
- 5538 DANE MX hosts in 3641 zones
- ~500 domains with TLSA record lookup problems
- ~258 domains with wrong TLSA records or no STARTTLS

Top TLDs

DANE domains x1000		TLD
3,089		NL
935		COM
820		SE
597		CZ
507		BR
503		EU
472		PL
411		FR
377		NO
145		BE
130		NET
129		NU
119		HU
97		ORG
85		DE
500		other

Reliability

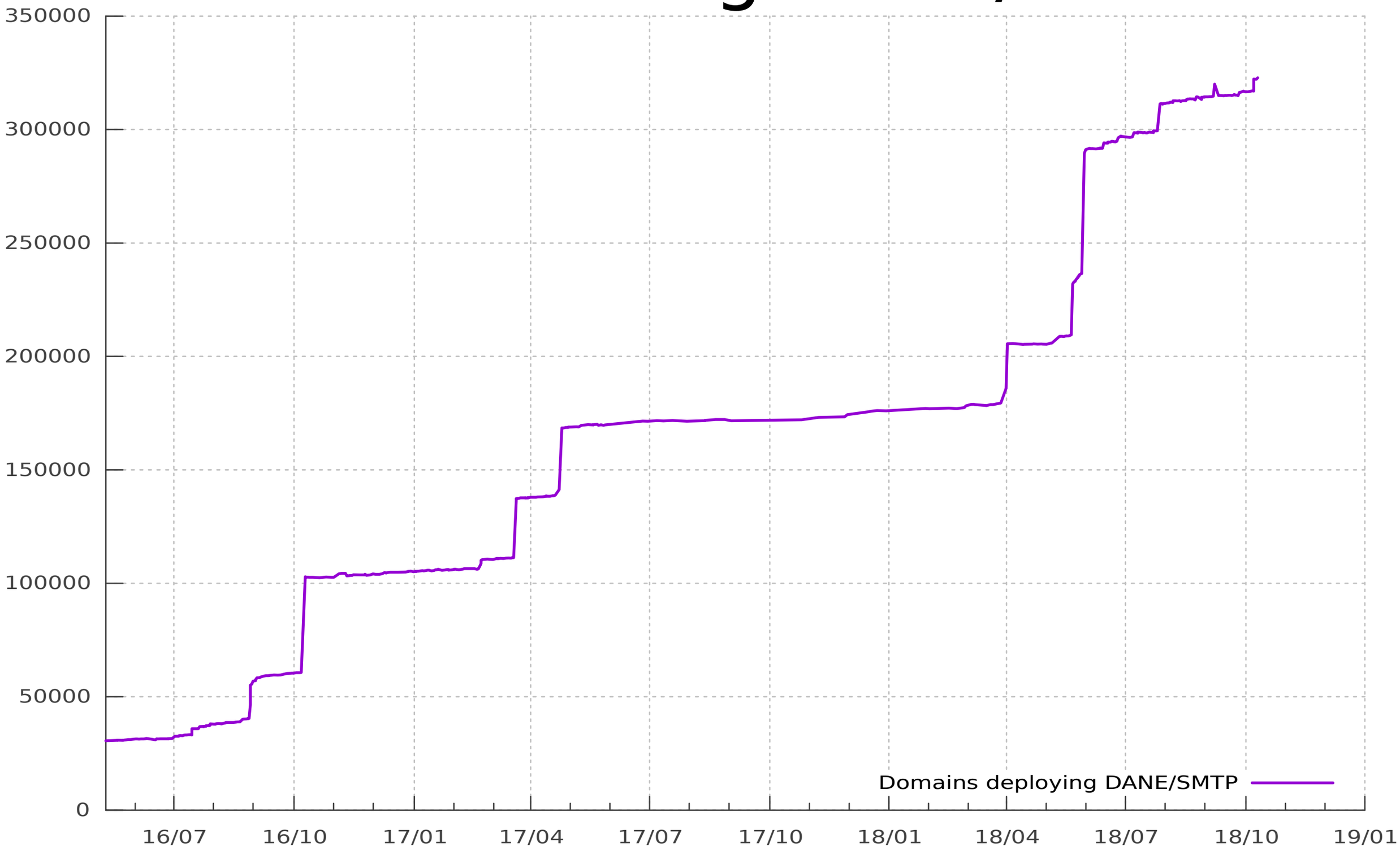
- Breakage largely at parked domains
  - Many just lame delegations
  - (ordinary DNS outage).

- Denial of existence problem only at ~500 domains

- Low breakage % TLDs:
  - . 香港 (0.00), .BR (0.04), .HK (0.06)

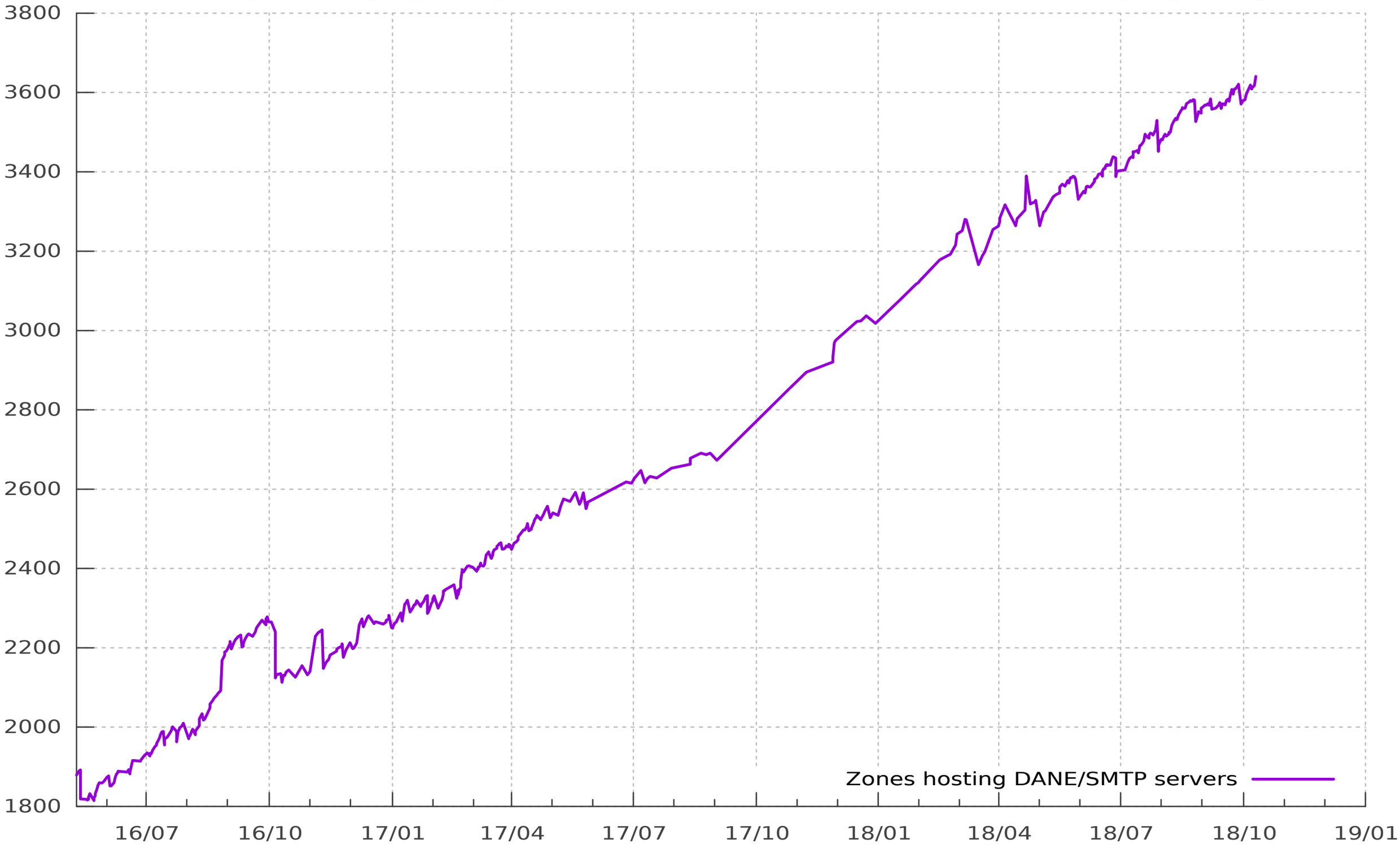
- High breakage TLDs:
  - .BANK (41.9), .NRW (11.5), .RU (9.6)

#Domains using SMTP/DANE



ICANN63 | Barcellona, Spain | October 2018

#Zones of DANE MX hosts



ICANN63 | Barcellona, Spain | October 2018

Well known DANE domains

gmx.at
transip.be
travelbirdbelgique.be
nic.br
registro.br
gmx.ch
open.ch
anubisnetworks.com
geektimes.com
gmx.com
habr.com
mail.com
societe.com
solvinity.com
t-2.com
trashmail.com
xfinity.com
xfinitymobile.com
active24.cz
clubcard.cz
cuni.cz
cvc.cz
destroystores.cz
itesco.cz
klubpevnehozdravi.cz
knizni-magazin.cz
localssrcapp.cz
nic.cz
optimail.cz
smtp.cz
bayern.de
bund.de
elster.de
fau.de
freenet.de
gmx.de
jpberlin.de
kabelmail.de
lrz.de
mail.de
posteo.de
ruhr-uni-bochum.de
tum.de
uni-erlangen.de
unitybox.de
unitymedia.de
web.de
dk-hostmaster.dk
egmontpublishing.dk
netic.dk
tilburguniversity.edu
transip.eu
insee.fr
octopuce.fr
comcast.net
dd24.net
dns-oarc.net
gmx.net
habramail.net
hr-manager.net
inexio.net
mpssec.net
mylobu.net
t-2.net
transip.net
xs4all.net
xworks.net
ardanta.nl
bhosted.nl
bit.nl
boozyshop.nl
deltion.nl
hierinloggen.nl
hr.nl
hro.nl
interconnect.nl
intermax.nl
markteffectmail.nl
ouderportaal.nl
overheid.nl
pathe.nl
politie.nl
previder.nl
rotterdam.nl
transip.nl
truetickets.nl
uvt.nl
verschoore.nl
xs4all.nl
domeneshop.no
handelsbanken.no
rushtrondheim.no
webcruitermail.no
aegee.org
debian.org
freebsd.org
gentoo.org
ietf.org
isc.org
lazarus-ide.org
netbsd.org
openssl.org
samba.org
torproject.org
asf.com.pt
handelsbanken.se
iis.se
minmyndighetspost.se
skatteverket.se
t-2.si
mail.co.uk
govtrack.us

Almost-DANE domains

(hosting mail servers for DNSSEC signed MX records)

1000s of DNSSEC MX RRs		Provider yet to deploy DANE TLSA
1,427		ovh.net
875		one.com
651		google.com
335		googlemail.com
307		firstfind.nl
168		mijndomain.nl
104		outlook.com
80		pcextreme.nl
73		argewebhosting.nl
56		wedos.net

Help wanted

- More ccTLD lists of signed delegations
- Fix any DNSSEC issues
  - Including ones centered on Denial of Existence!
- Please enable DANE ***outbound***
  - (even if your own domain is unsigned)
- Please enable DNSSEC and DANE on hosting MX servers
  - Especially when hosting thousands signed domains
    - e.g. ovh.net, googlemail.com, ...

Questions?

https://stats.dnssec-tools.org/

Hint: There are a

LOT of extra slides

beyond this one

Viktor Dukhovni
<ietf-dane@dukhovni.org>

Wes Hardaker
<hardaker@isi.edu>

TLSA record types

- **3 1 1: certificate usage DANE-EE(3):**
  - Publishes server's public key SHA256 hash
- **2 1 1: certificate usage DANE-TA(2):**
  - Publishes CA's public key SHA256 hash
  - Can use this if you the CA is secure enough
- Rest of record is hash value:

```
$ dig +nosplit +short -t tlsa _25._tcp.mail.ietf.org
3 1 1 0C72AC70B745AC19998...E7CB23E5B514B56664C5D3D6
```

Rolling Your TLS Keys

- Use multiple TLSA records to publish current and future keys
  - Publish **keys** well in advance of using them!
  - Required by DNS caching

- Two models:
  - EE Key + Next EE Key: (3 1 1 + 3 1 1)
  - EE Key + TA Key: (3 1 1 + 2 1 1)

- Deploy new chain, and publish new TLSA records:

```
_25._tcp.mx.example.com. IN TLSA 3 1 1 curr-pubkey-sha256
_25._tcp.mx.example.com. IN TLSA 3 1 1 next-pubkey-sha256
```

Current + Issuer CA

- Publish TLSA RRs for server key & issuer CA key

```
_25._tcp.mx.example.com. IN TLSA 3 1 1 ee-pubkey-sha256
_25._tcp.mx.example.com. IN TLSA 2 1 1 ta-pubkey-sha256
```

- To change your end-certificate:
  - Deploy certificates from same CA
  - Promptly update **3 1 1** hash to match new EE key

- If the CA’s key changes:
  - Keep using your same certificate key
  - Obtain cert from new CA
  - Promptly update **2 1 1** hash to match new CA key

Automate

- Automate:
  - TLSA record updates and zone re-signing
  - Key rollover
  - Acquiring any certs ...
  - ... and converting to TLSA records

- Have working contacts in WHOIS, SOA, postmaster

Appendix

- Gmail TLS status
- SMTP-STS
- DNSViz samples
- Survey metrics
- DANE tools

DNSSEC Hygiene

- All nameservers need:
  - EDNS(0) support
  - NSEC3 support

- Don't block IP fragments

- Reply NODATA or NXDomain
  - (not NOTIMP, REFUSED, ...)

- Test correct denial-of-existence for each edge case

- Monitor nameservers for correct DNSSEC handling

Avoid DNS query filtering

- Some firewalls offer misguided filtering features
  - blocking TLSA, CAA, CDS, ... lookups
  - These break more than DANE
  - Please turn off filters that block queries for some record types!!
- Monitor correct responses for unexpected types:

```
$ dig -t TYPE12345 example.com.          -> NODATA
$ dig -t TYPE12345 n.x.example.com.      -> NXDomain
```

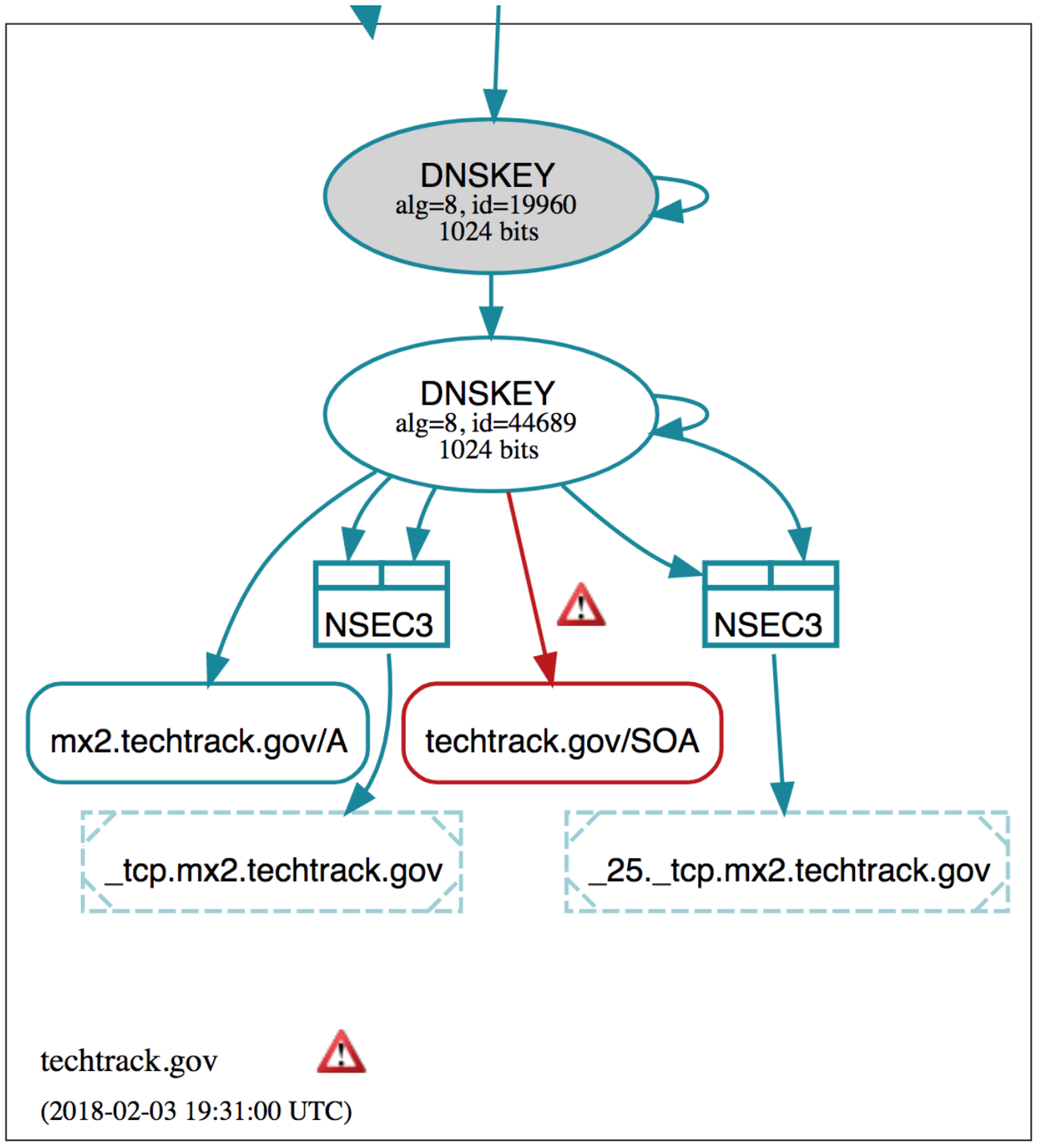
https://tools.ietf.org/html/draft-ietf-dnsop-no-response-issue

DNSSEC checklist

- Keep name-server software up to date
- Test zones with apex wildcard A or CNAMEs
- Test zones with empty non-terminals
- Always sign after changing SOA serial numbers
- Avoid NSEC3 opt-out in most zones
- Avoid high NSEC3 (extra) iteration counts
  - (0 is BCP!)

https://lists.dns-oarc.net/pipermail/dns-operations/2017-December/017127.html
https://lists.dns-oarc.net/pipermail/dns-operations/2018-January/017173.html

Check DNSViz



http://dnsviz.net/d/_25._tcp.mx2.techtrack.gov/WnYN-A/dnssec/

Monitor

- DNSSEC DS and DNSKEY records
- DNSSEC signatures (avoid near expiration)
- Slave nameserver synchronization
- TLSA records match your live cert chain

Operational BCP

- Publish the current and next TLSA record
- Don't offer STARTTLS selectively to just some clients
- Use a separate certificate for each MX host
  - Stagger certificate rotation between them
- Publish TLSA RRs for each each deployed certificate type: RSA, ECDSA, ...

DANE software

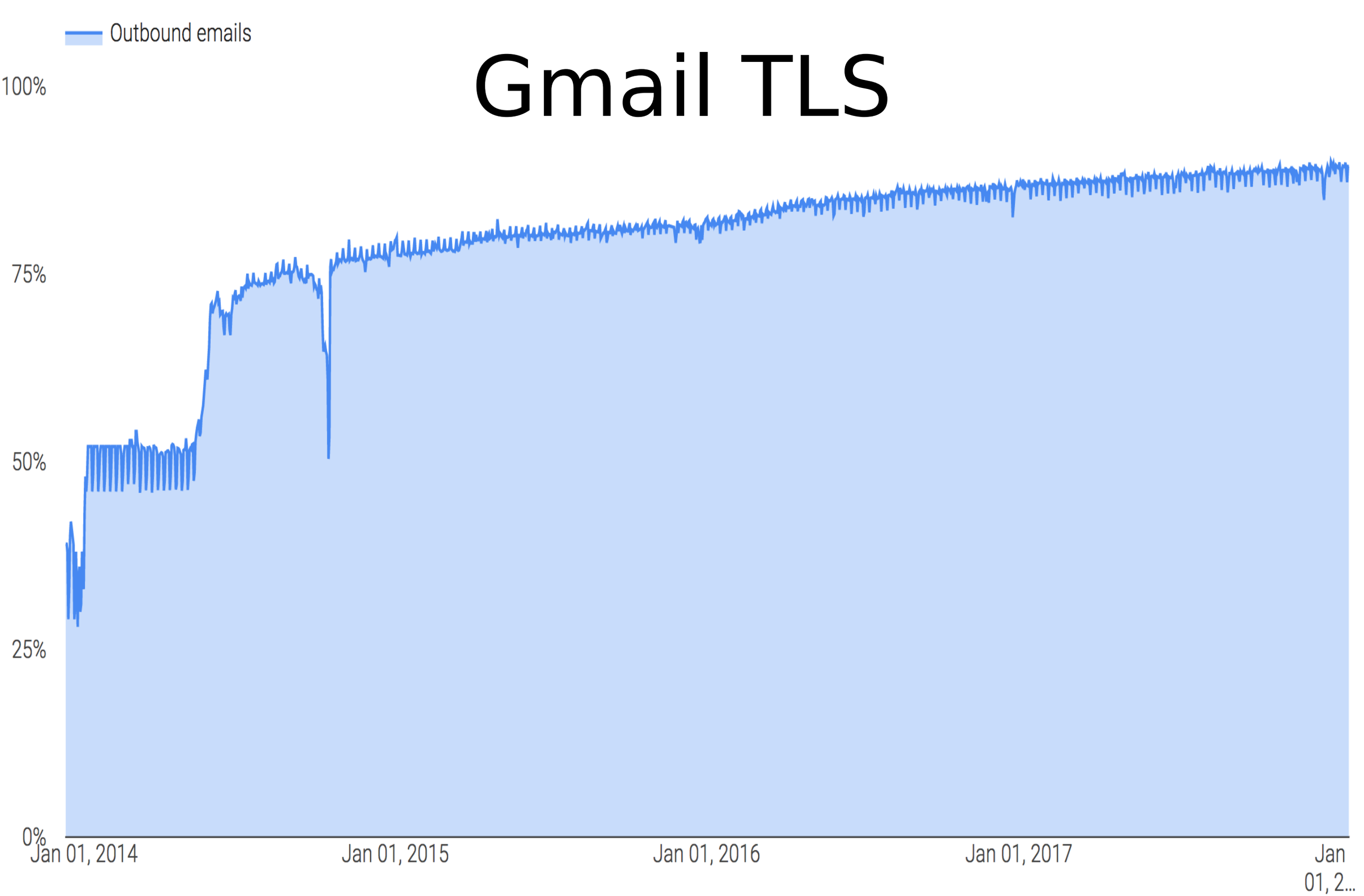
- Postfix, Exim, Cloudmark, https://mailinabox.email, ...
- OpenSSL ≥ 1.1.0 DANE verification API

  https://www.openssl.org/docs/man1.1.0/ssl/SSL_CTX_dane_enable.html
- GnuTLS (somewhat incomplete)
- Maintainers of DANE S/W please get in touch

Gmail TLS status

- Outbound TLS much like inbound presently at ~90%
- Remaining 10% mostly bulk marketing
- Some user-mailbox domains yet to adopt STARTTLS!

Gmail TLS



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

Non-TLS domains

Top domains by region: Inbound

RED YELLOW GREEN

Domain	%
From: cmail19.com via createsend.com	93%
From: cmail20.com via createsend.com	93%
From: cuenote.jp	73%
From: ed10.net via ed10.com	22%
From: emergencyemail.org	0%
From: prohirespowerhouse.com	0%
From: secureserver.net	62%
From: timesjobs.com via tbsl.in	0%
From: wattpadmail.com	10%
From: wayfair.com	5%

Mon, Feb 5, 2018

Top domains by region: Outbound

Domain	%
To: alice.it via aliceposta.it	0%
To: amazon.{...}	51%
To: bigpond.com	0%
To: btinternet.com via cpcloud.co.uk	0%
To: cox.net	2%
To: docomo.ne.jp	0%
To: ezweb.ne.jp	0%
To: nauta.cu via etecsa.net	0%
To: uol.com.br	0%
To: yahoo.co.jp	0%

Mon, Feb 5, 2018

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

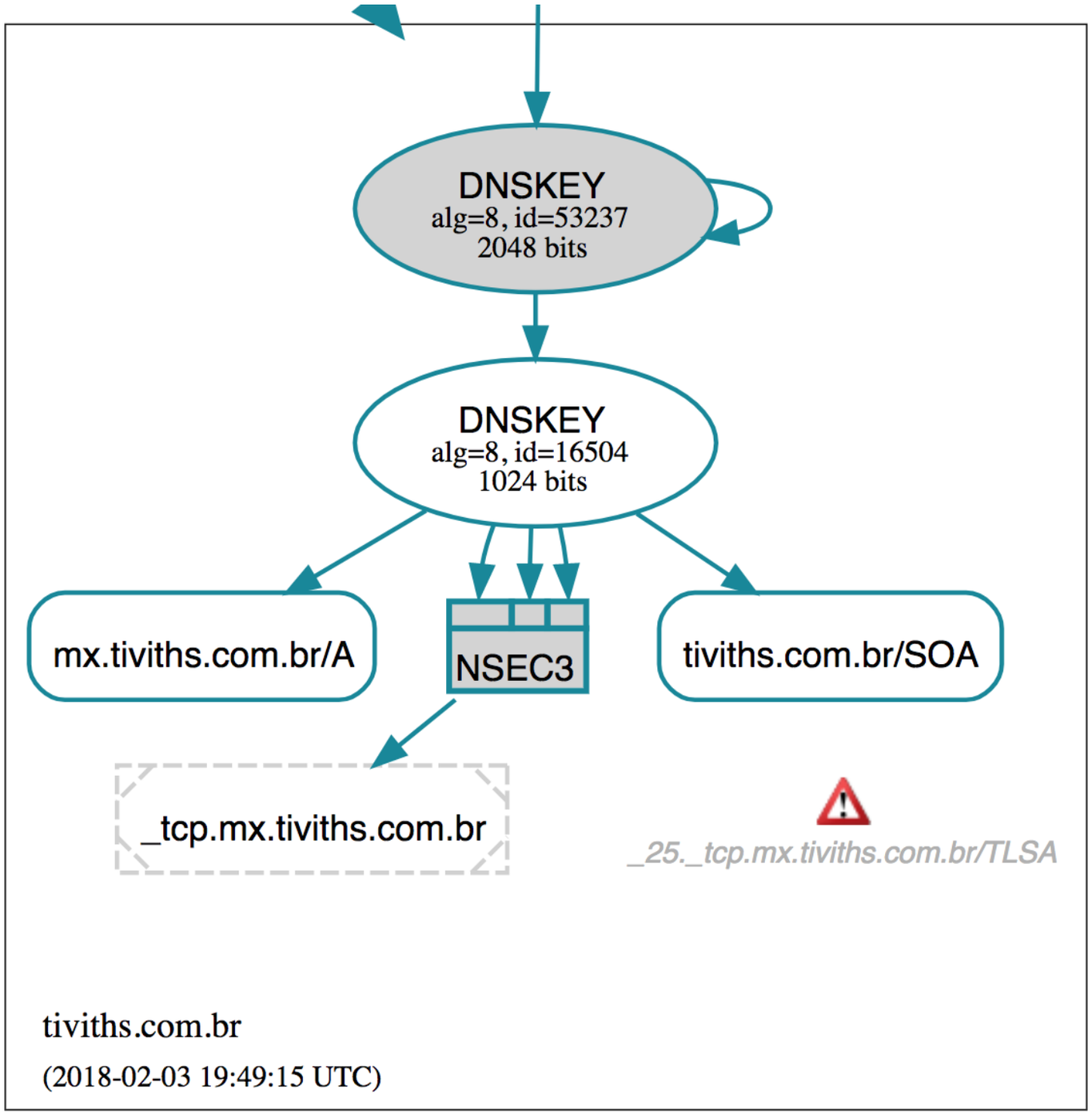
SMTP-STS

- SMTP-STS: compromise for the DNSSEC-challenged
  - Still can and **should** prefer DANE ***outbound***
  - Authenticates domain control via CA leap of faith!
    - Vulnerable to MiTM at cert bootstrap
    - Vulnerable to weakest root CA, and unauthorized certs
    - Open to downgrade on first (or irregular) contact
    - Complex mix of HTTPS, unsigned DNS and SMTP

DNSViz samples

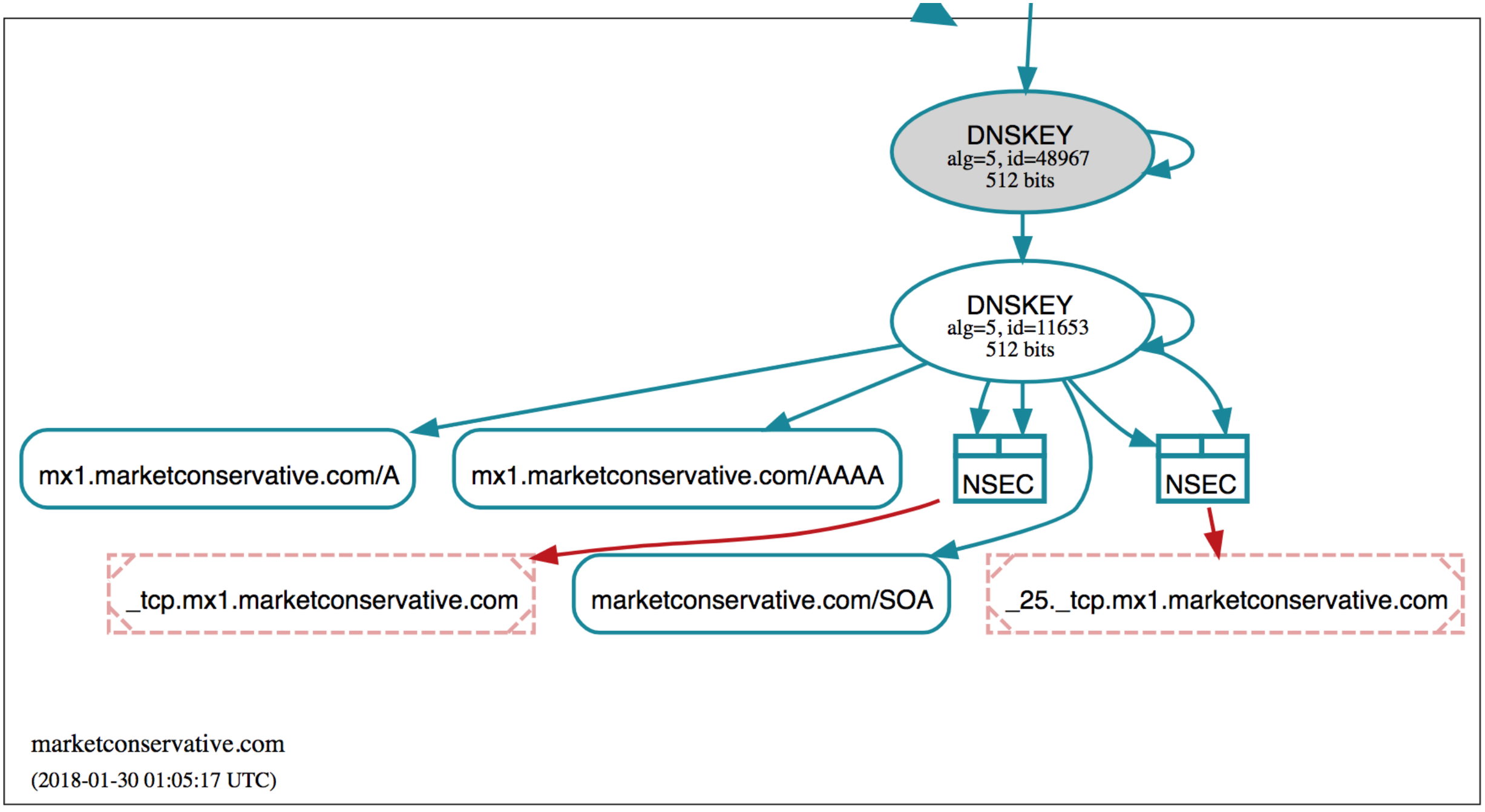
- Examples of various name-server edge-cases
- Follow links to live DNSViz site
- Mouse-over "red" elements provides more detail

TLSA queries blocked (resolved)



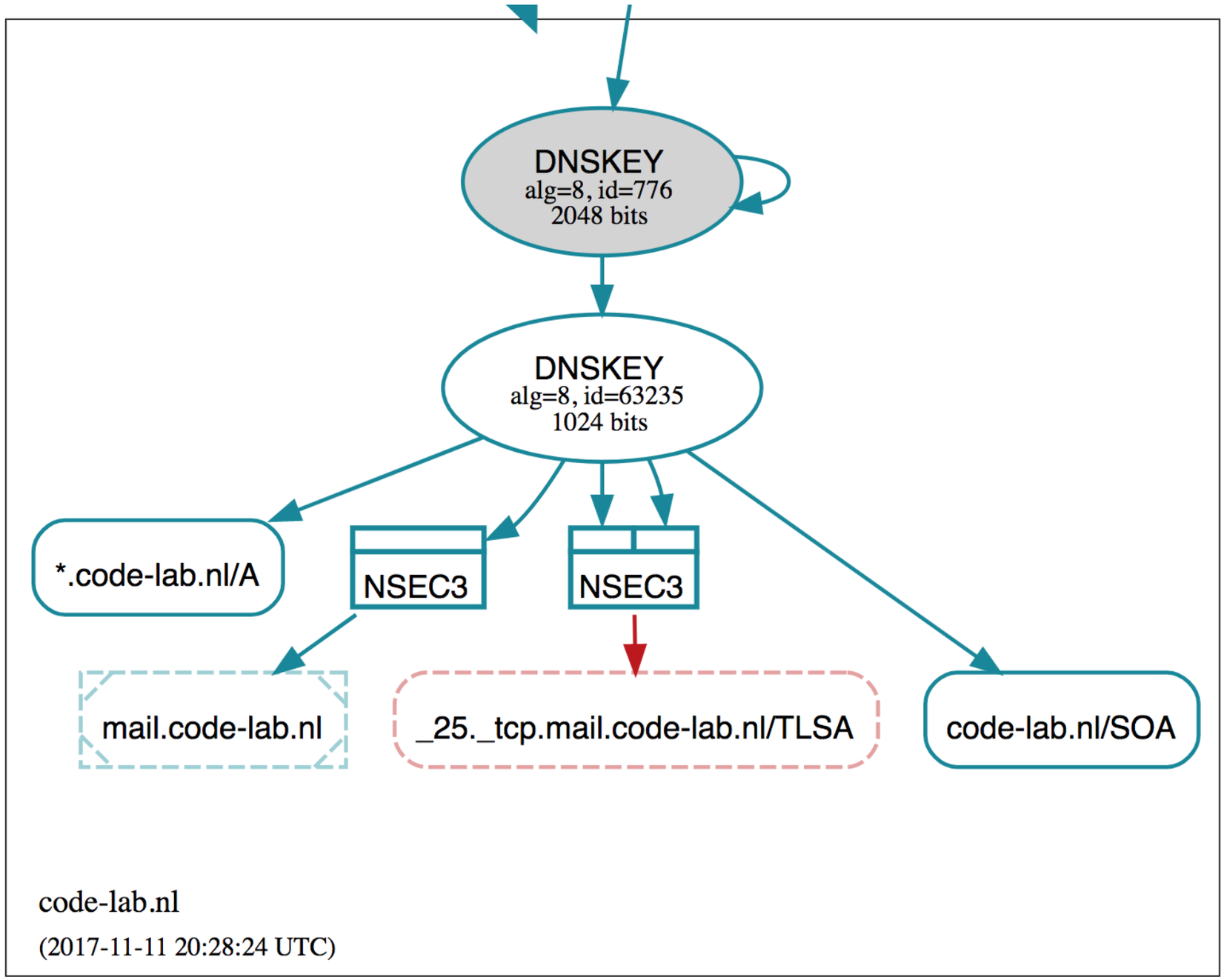
http://dnsviz.net/d/_25._tcp.mx.tiviths.com.br/WnYSUg/dnssec/

NSEC covers wrong wildcard



http://dnsviz.net/d/_25._tcp.mx1.marketconservative.com/Wm_E1w/dnssec/

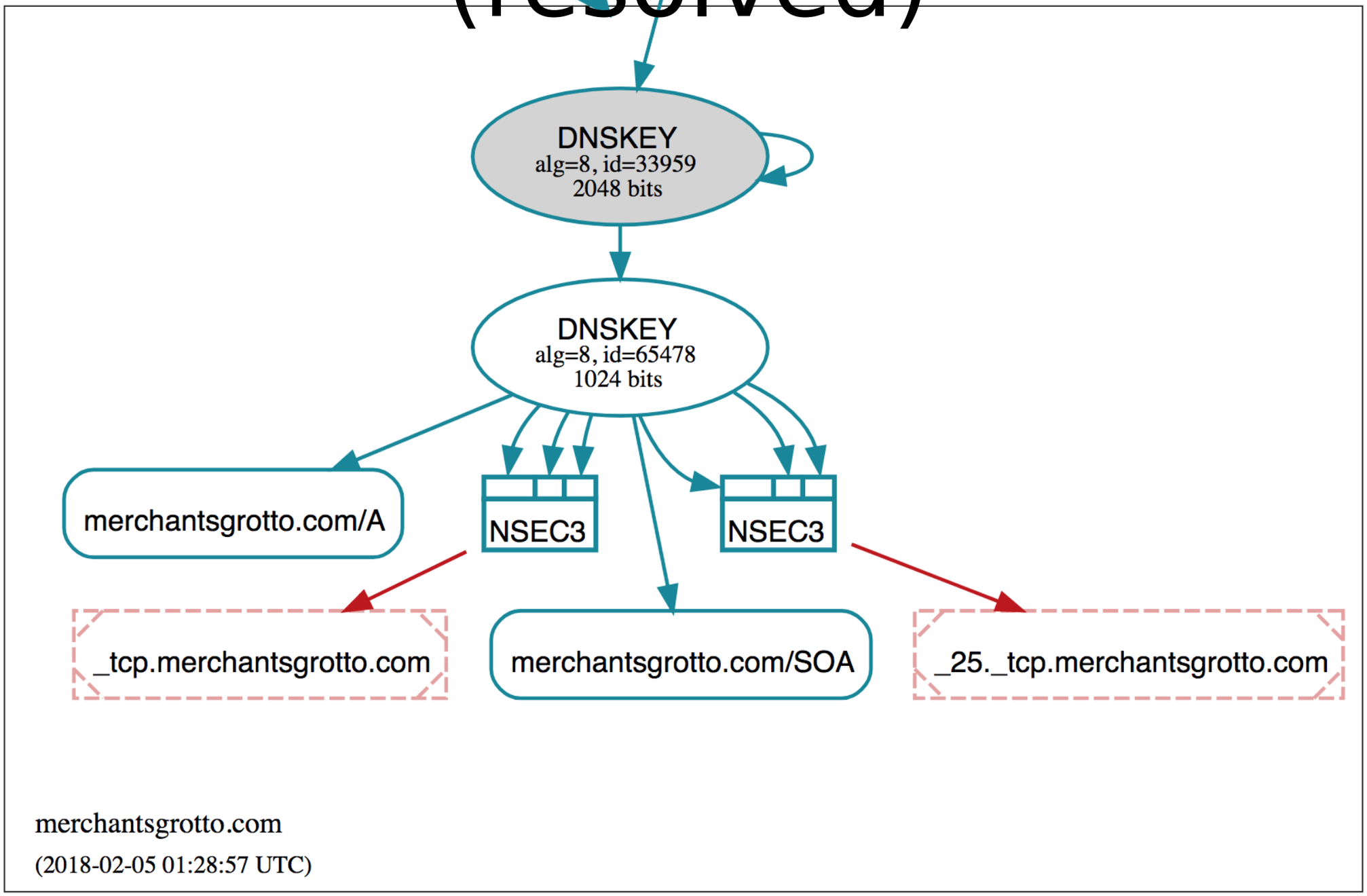
Misused zone apex wildcard



http://dnsviz.net/d/_25._tcp.mail.code-lab.nl/WgddbA/dnssec/

primary nameserver: `ns3.firstfind.nl`

Wildcard ENT NODATA (resolved)



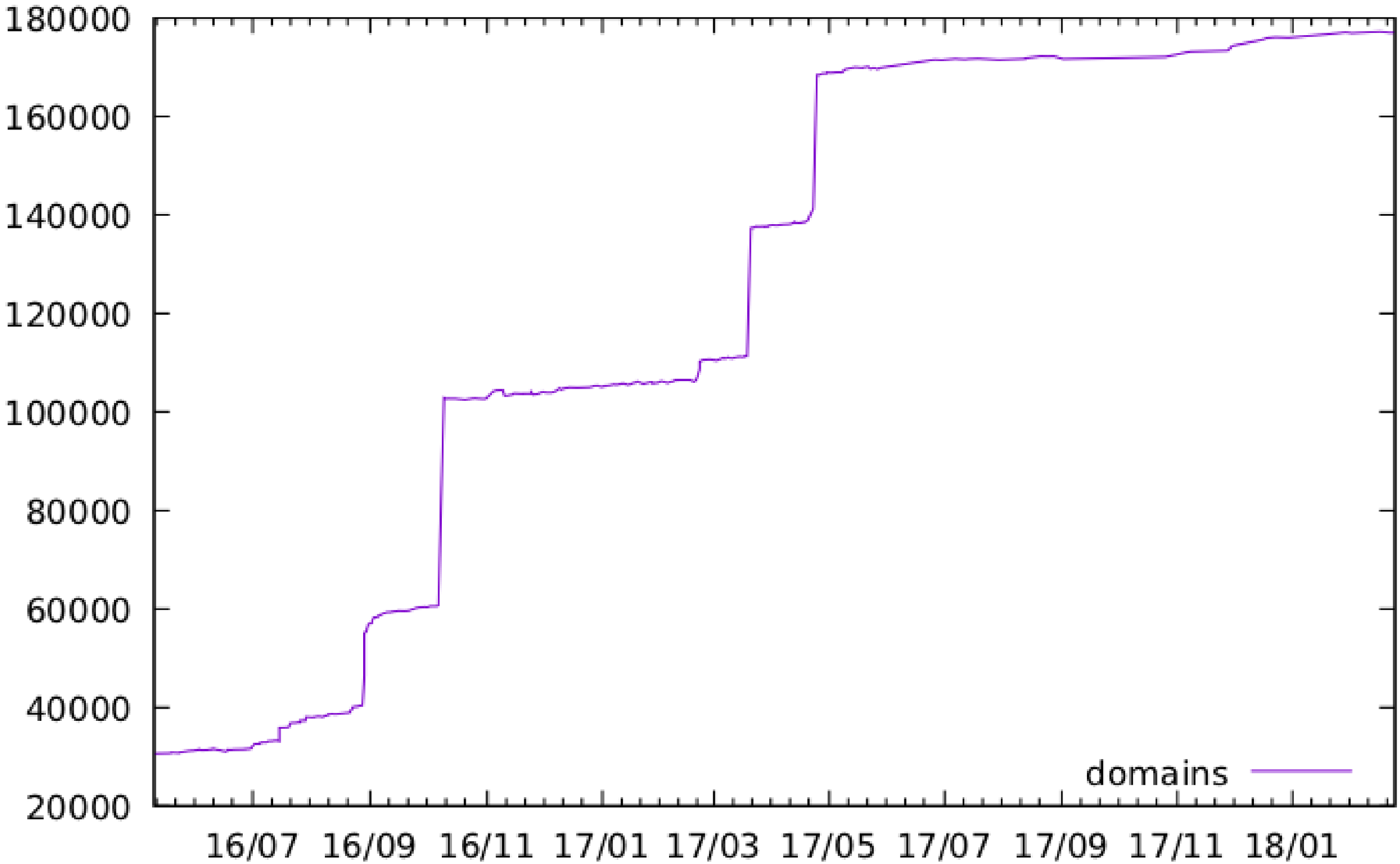
http://dnsviz.net/d/_25._tcp.merchantsgrotto.com/WnezZQ/dnssec/

primary nameserver: `ns-cloud-e1.googledomains.com`

Survey metrics

- Adoption primarily in Northern Europe and USA
- Steady growth in MX count driven by adopting organizations
- Domain count jumps driven by hosting provider adoption
- But also smaller scale in Indonesia, Tanzania, ...

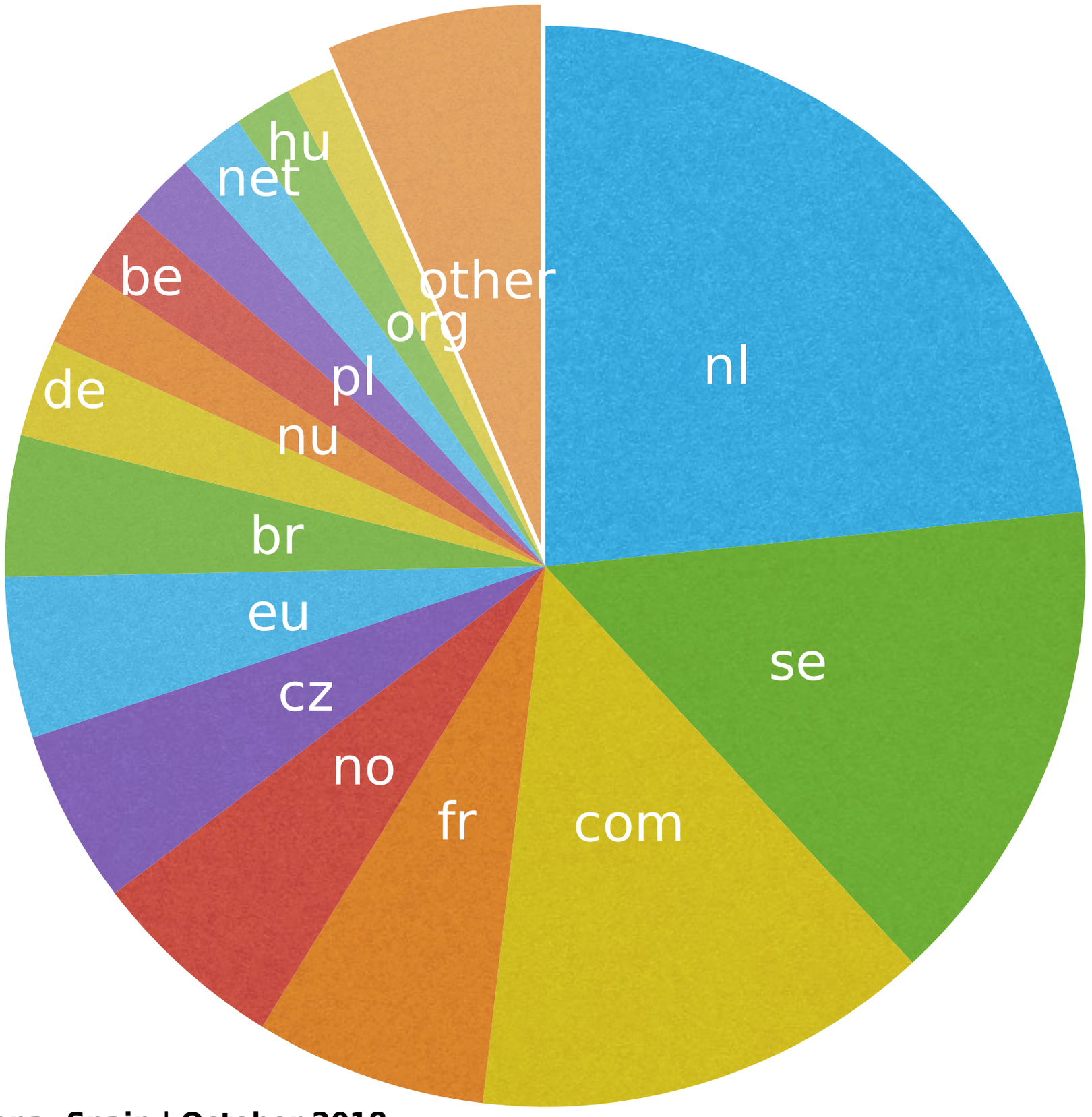
#DANE SMTP domains



ICANN63 | Barcellona, Spain | October 2018

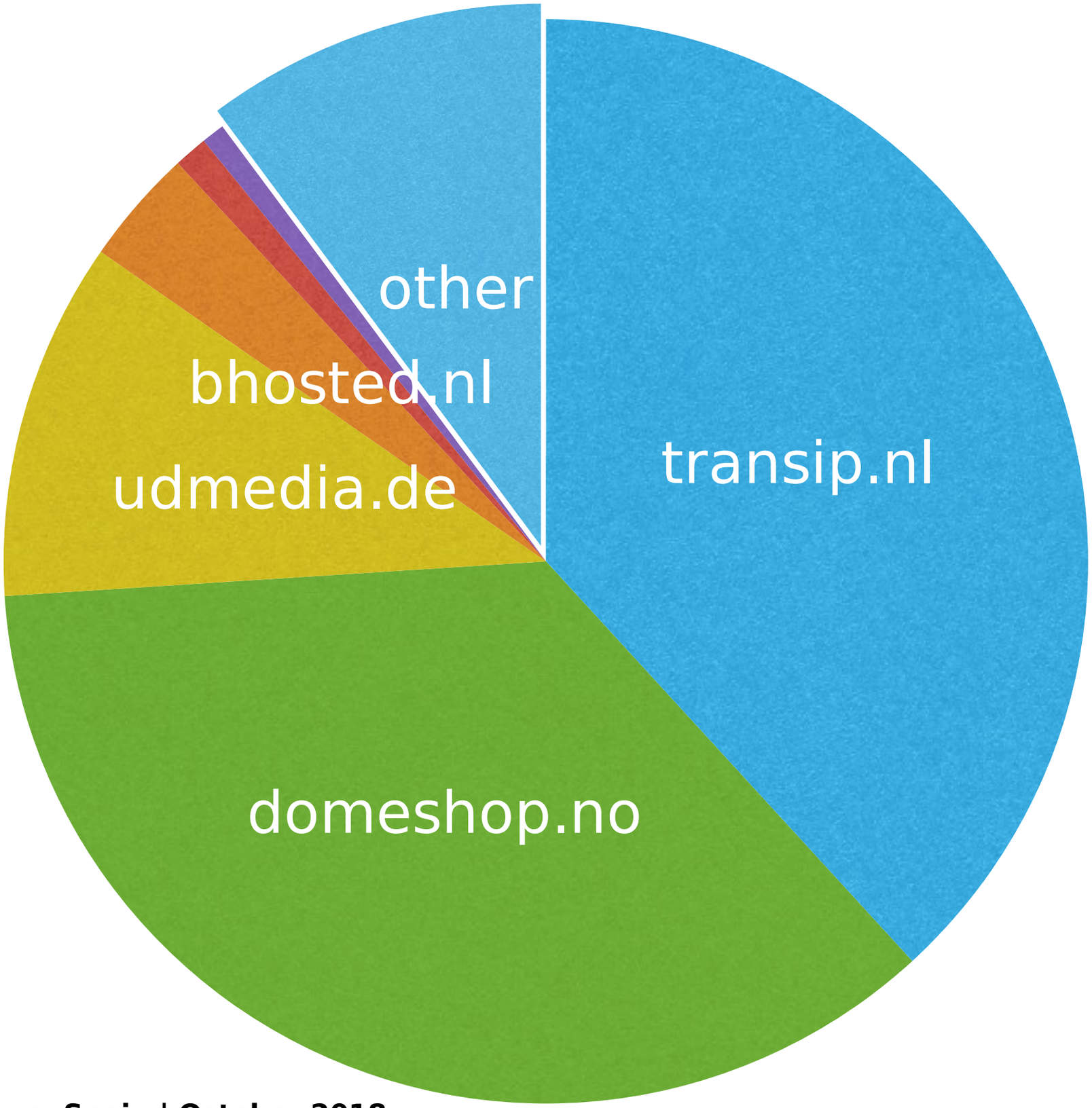
DNSSEC by TLD

DNSSEC domains x1000		TLD
1,367		NL
861		SE
803		COM
405		FR
345		NO
304		CZ
282		EU
247		BR
171		DE
135		NU
130		BE
120		PL
116		NET
101		HU
86		ORG
375		other


nl
se
com
fr
no
cz
eu
br
nu
pl
de
be
net
hu
other
org

Top 10 DANE providers

#domains		Provider
68,318		domeneshop.no
64,011		transip.nl
19,137		udmedia.de
6,183		bhosted.nl
1,792		nederhost.nl
1,230		yourdomainprovider.net
760		ec-elements.com
564		surfmailfilter.nl
537		core-networks.de
437		omc-mail.com
15,909		other

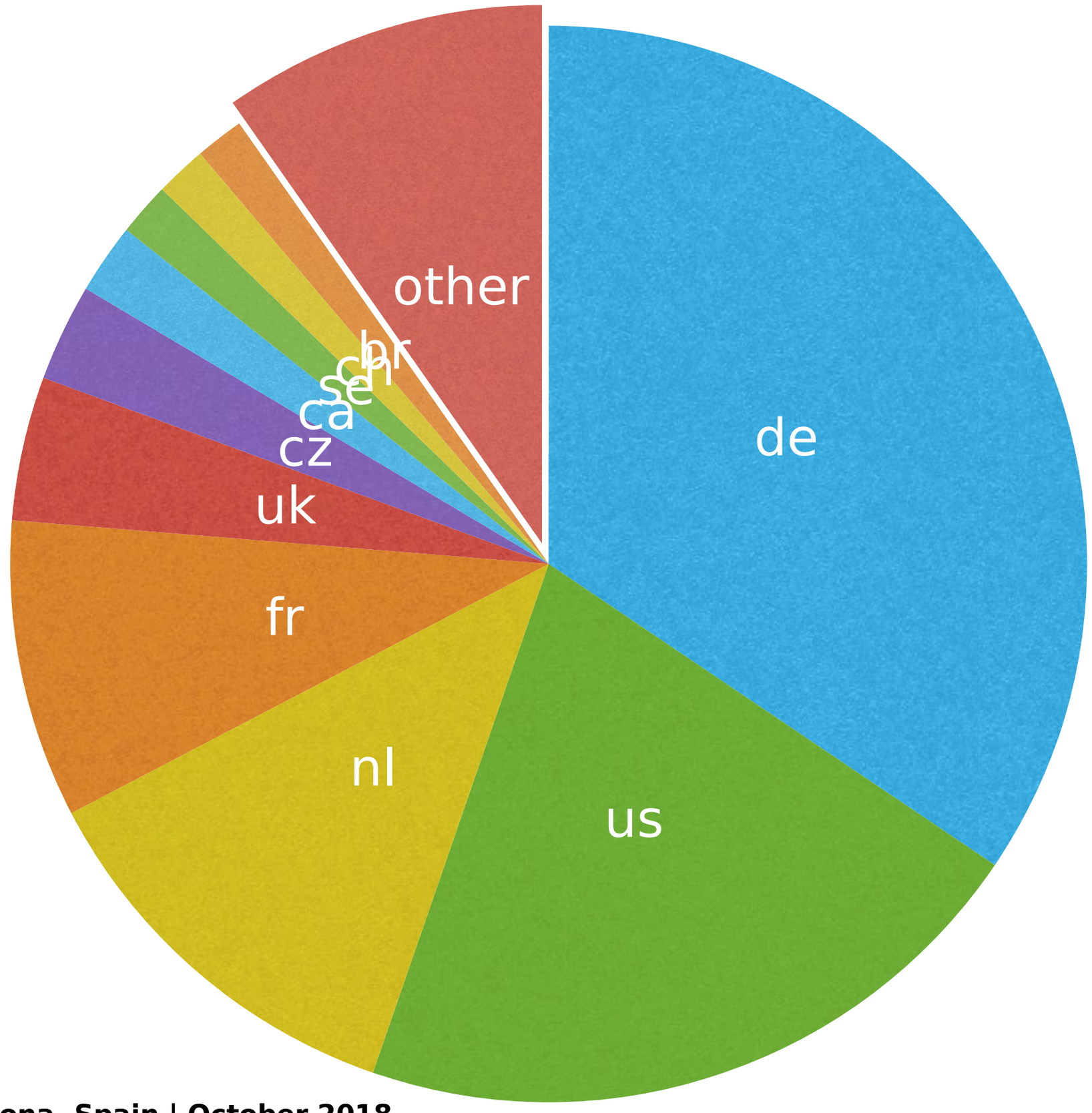

other
bhosted.nl
udmedia.de
transip.nl
domeshop.no

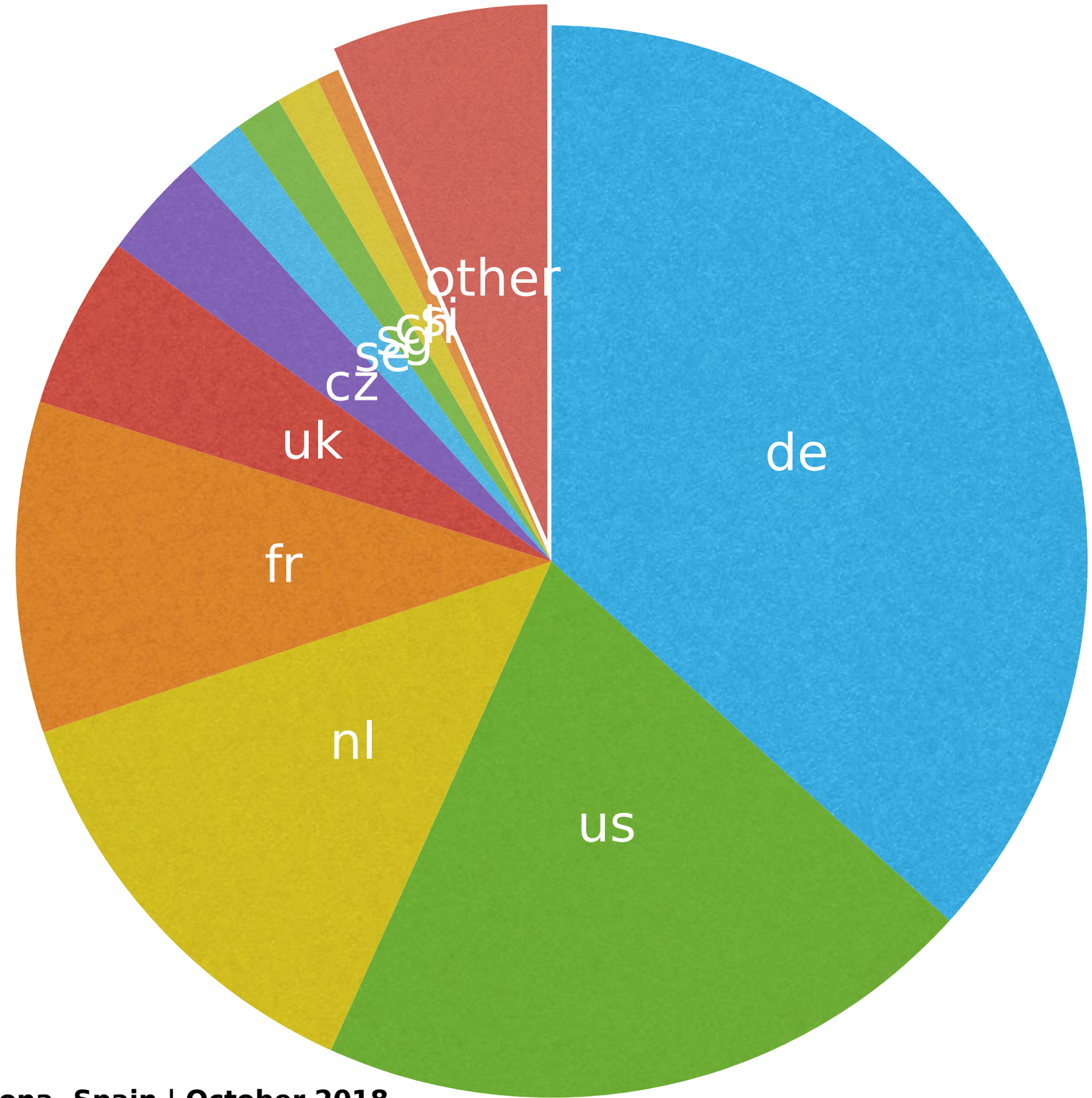
DANE MX host IPv4 GeoIP

#MX IP		Country
1,273		DE, Germany
770		US, United States
445		NL, Netherlands
331		FR, France
160		UK, United Kingdom
108		CZ, Czech Republic
78		CA, Canada
59		SE, Sweden
57		CH, Switzerland
54		BR, Brazil
360		other

DANE MX host IPv6 GeoIP

#MX IP		Country
698		DE, Germany
382		US, United States
249		NL, Netherlands
190		FR, France
99		UK, United Kingdom
61		CZ, Czech Republic
35		SE, Sweden
27		SG, Singapore
25		CH, Switzerland
13		SI, Slovenia
124		other

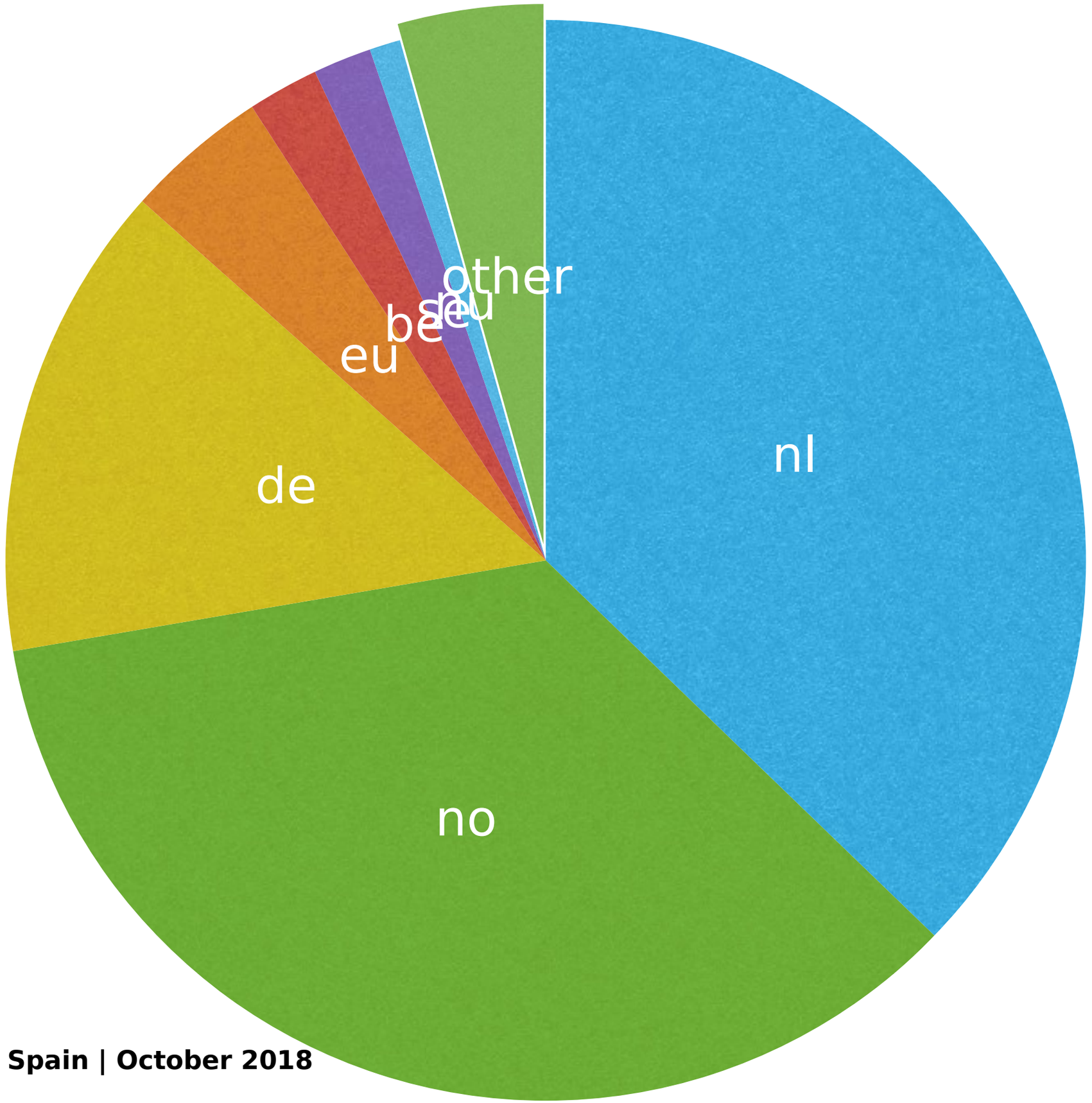

other
br
ch
se
ca
cz
uk
fr
nl
us
de


other
fi
se
cz
uk
fr
nl
us
de

DANE in ccTLDs

- 125 out of 247 ccTLDs have DNSSEC
- 114 have at least one DNSSEC delegated domain
- 73 have DANE-enabled domains, 19 have more than 100:

  10000+: nl, no, de
  1000+: eu, be, se, nu
  100+: uk, dk, cz, fr, at, ch, us, me, io, hu, tv, fi


nl
de
eu
be
se
other
no

OpenSSL DANE check

- Bash shell function to retrieve TLSA records
- Check SMTP server certificate chain vs. TLSA records
- Requires OpenSSL 1.1.0 or later

```
$ danesmtp() {
  local host=$1; shift
  local opts=(-starttls smtp -connect "$host:25" \
              -verify 9 -verify_return_error -brief \
              -dane_ee_no_namechecks -dane_tlsa_domain "$host")
  set -- $(dig +short +nosplit -t tlsa "_25._tcp.$host" |
           egrep -i '^[23] [01] [012] [0-9a-f]+$')
  while [ $# -ge 4 ]
  do
    opts=("${opts[@]}" "-dane_tlsa_rrdata" "$1 $2 $3 $4")
    shift 4
  done
  (sleep 1; printf "QUIT\r\n") | openssl s_client "${opts[@]}"
}
```

```
$ danesmtp mail.ietf.org
...
Protocol version: TLSv1.2
Ciphersuite: ECDHE-RSA-AES256-GCM-SHA384
Peer certificate: OU = Domain Control Validated, CN = *.ietf.org
Hash used: SHA512
Verification: OK
DANE TLSA 3 1 1 ...e7cb23e5b514b56664c5d3d6 matched EE certificate at depth 0
...

$ echo $?
0
```