Real World DANE
Inter-domain email transport

Viktor Dukhovni
<ietf-dane@dukhovni.org>

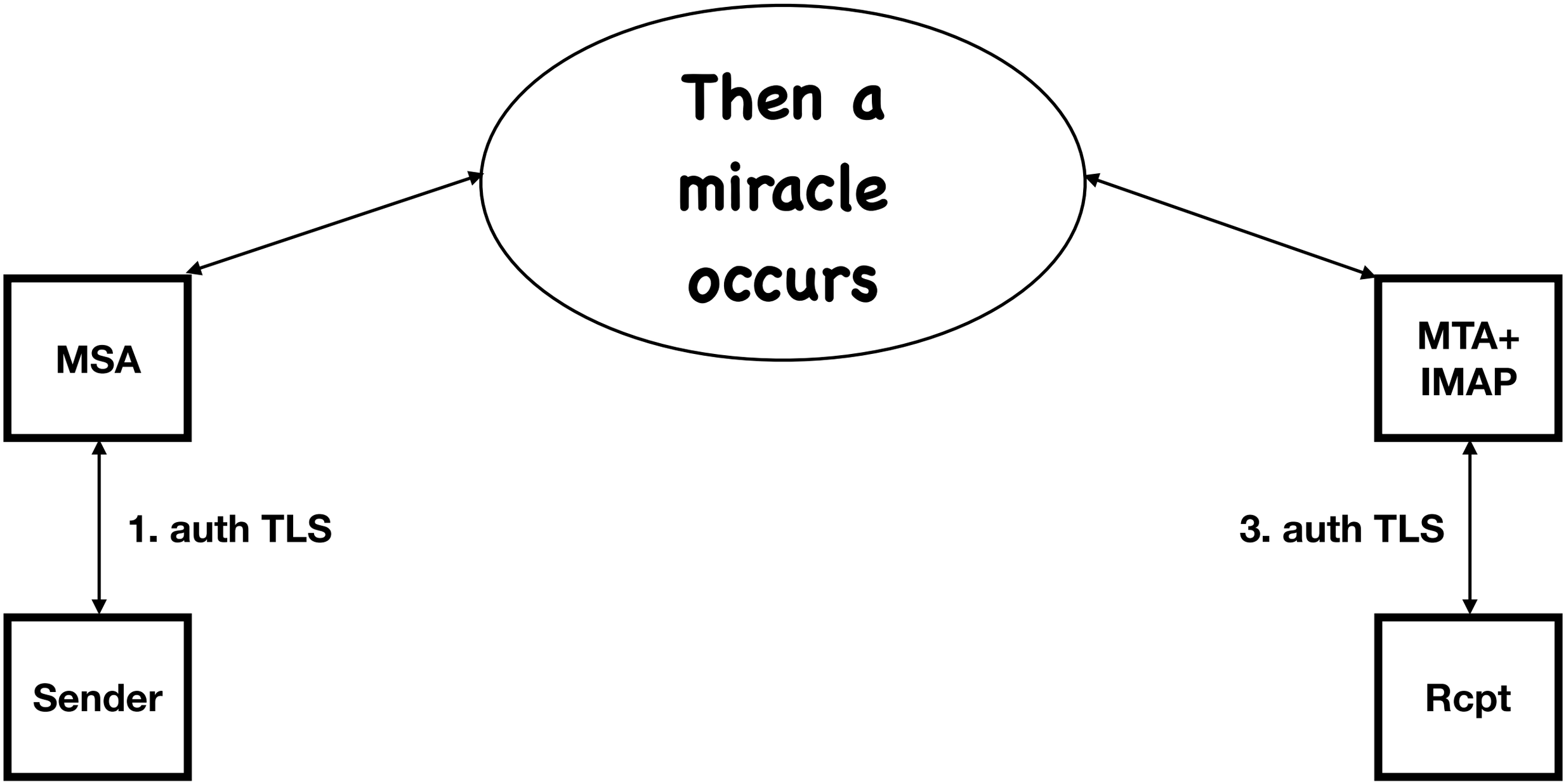
ICANN61 | San Juan, Puerto Rico | March 2018

Overview

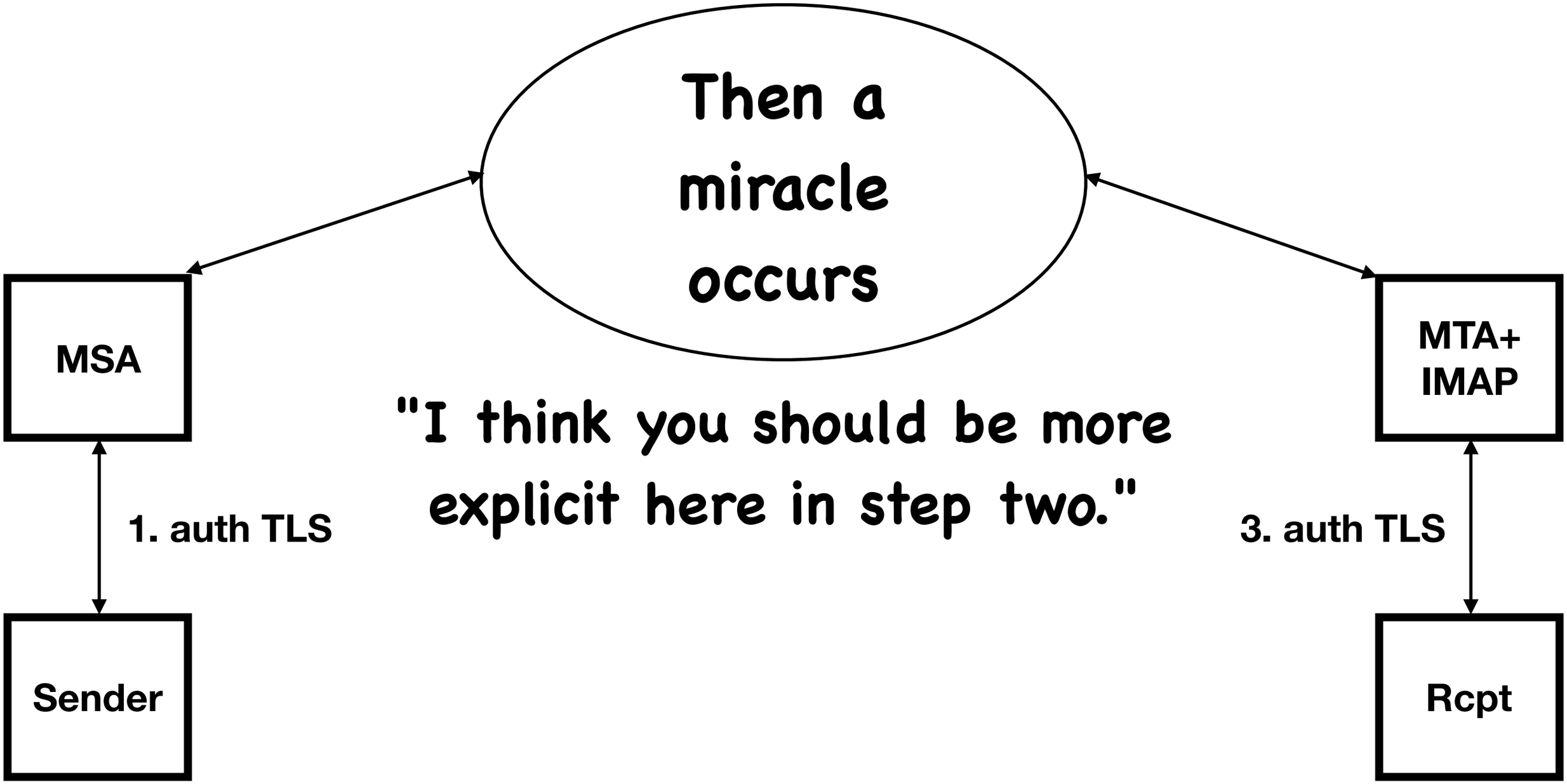
1. Background
2. DANE if you don't (DNSSEC hygiene)
3. DANE if you do (plan, automate, monitor)
4. DANE survey
5. Appendix

Email Security

Email Security

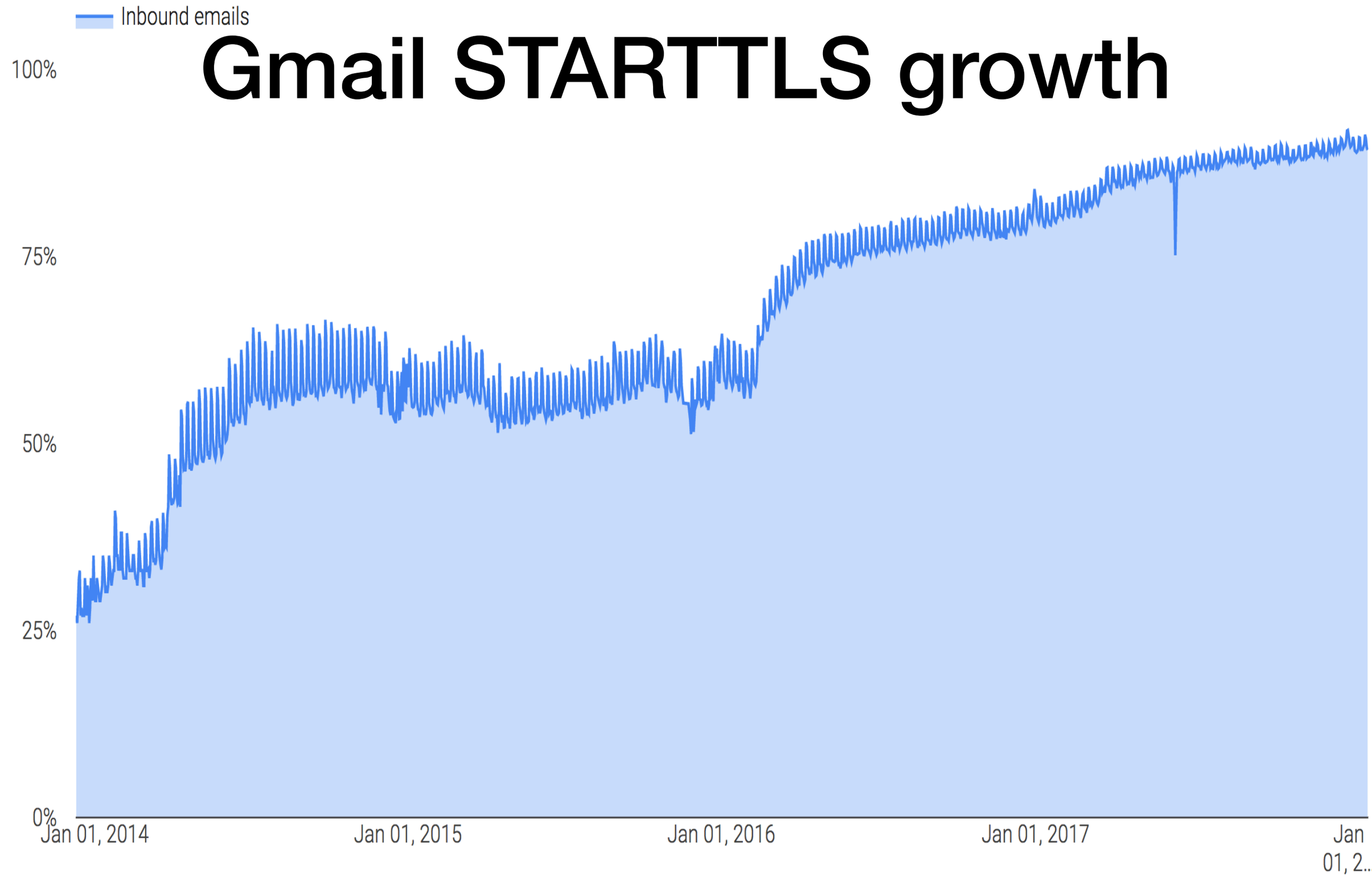


Email Security



Email Security

Gmail STARTTLS growth



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

Improving SMTP Security

- 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 for authentic MX hosts
- Web 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:

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

- Supported parameters (e.g. "3 1 1") are a contract to present a matching certificate chain for authentication

- Authenticates domain control via DNSSEC, no extraneous trusted third parties

- DNSSEC ensures downgrade protection

Coexisting with DANE

- DANE senders skip MX hosts that ***fail*** TLSA lookups
- When all MX hosts are skipped, delivery is deferred
- For DNSSEC-signed domains **without** TLSA records:
  - TLSA Denial of Existence (DoE) must function correctly
- DANE is first application protocol to need reliable DoE

DNSSEC Hygiene

- EDNS(0) support, NSEC3 support, for all nameservers
- Don't block IP fragments
- Reply NODATA or NXDomain, not NOTIMP, REFUSED, ...
- Test correct DoE for each edge case
- Monitor nameservers for correct DoE handling

Avoid DNS query filtering

- Some firewalls offer misguided filtering features, blocking TLSA, CAA, CDS, ... lookups
- These break more than DANE
- 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
```

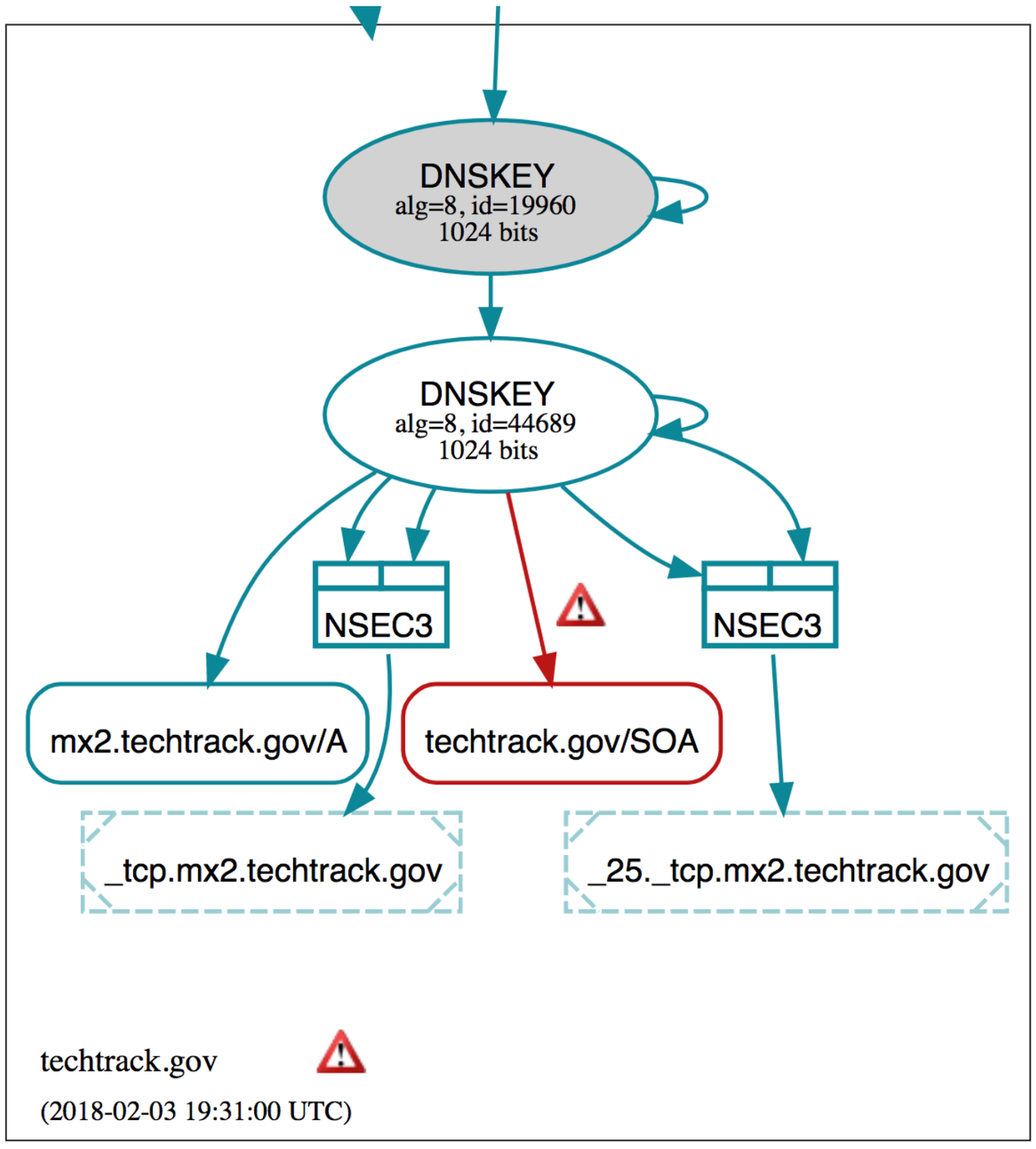
https://tools.ietf.org/html/draft-ietf-dnsop-no-response-issue

DNSSEC checklist

- Keep name-server software up to date
- Test zones with apex wildcard A or wildcard CNAMEs
- Test zones with empty non-terminals
- Avoid SOA serial number changes after signing
- 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/

Adopting DANE

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

Outbound DANE

- Need DNSSEC validating resolver, **local** to the MTA
- DANE-enabled MTA (Postfix, Exim, Cloudmark, ...)
- Enable DANE as documented
- Make a few policy exceptions:

`https://github.com/danefail/list`

Inbound DANE

- Need STARTTLS-capable SMTP server
- DNSSEC-signed MX records
- DNSSEC-signed TLSA records for each MX host
  - Provider's responsibility if MX hosts outsourced!
  - Including management of key and certificate rotation

TLSA records

- **3 1 1: certificate usage DANE-EE(3):**
  - Publishes end-entity (server) public key SHA256 hash
- **2 1 1: certificate usage DANE-TA(2):**
  - Publishes trust-anchor (CA) public key SHA256 hash
  - 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 0C72....D3D6
```

Predicting the future

- Need matching TLSA in place when chain is updated
- TLSA records can include present and future values
- Publish **keys** well in advance of obtaining certificates
- Two models:
  - EE Key + Next EE Key: (3 1 1 + 3 1 1)
  - EE Key + TA Key: (3 1 1 + 2 1 1)

Current + Next

- Generate next key when deploying current key and cert
- 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
```

- Weeks later, obtain certificate for pre-generated *next* key†
  - But first, make sure TLSA record is already in place
- Repeat!

† With Let's Encrypt, use `certbot "--csr"` option

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
```

- Deploy certificates from same CA, if EE key changes:
  - Promptly update **3 1 1** hash to match new EE key
- If CA key changes, keep same EE 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
    - Cert chain acquisition and deployment
- Have working contacts in WHOIS, SOA, postmaster

Monitor

- DNSSEC DS and DNSKEY records
- DNSSEC signatures (avoid near expiration)
- Slave nameserver synchronization
- TLSA records matching of 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 hosts
- Stagger certificate rotation for separate MX hosts
- 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

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.

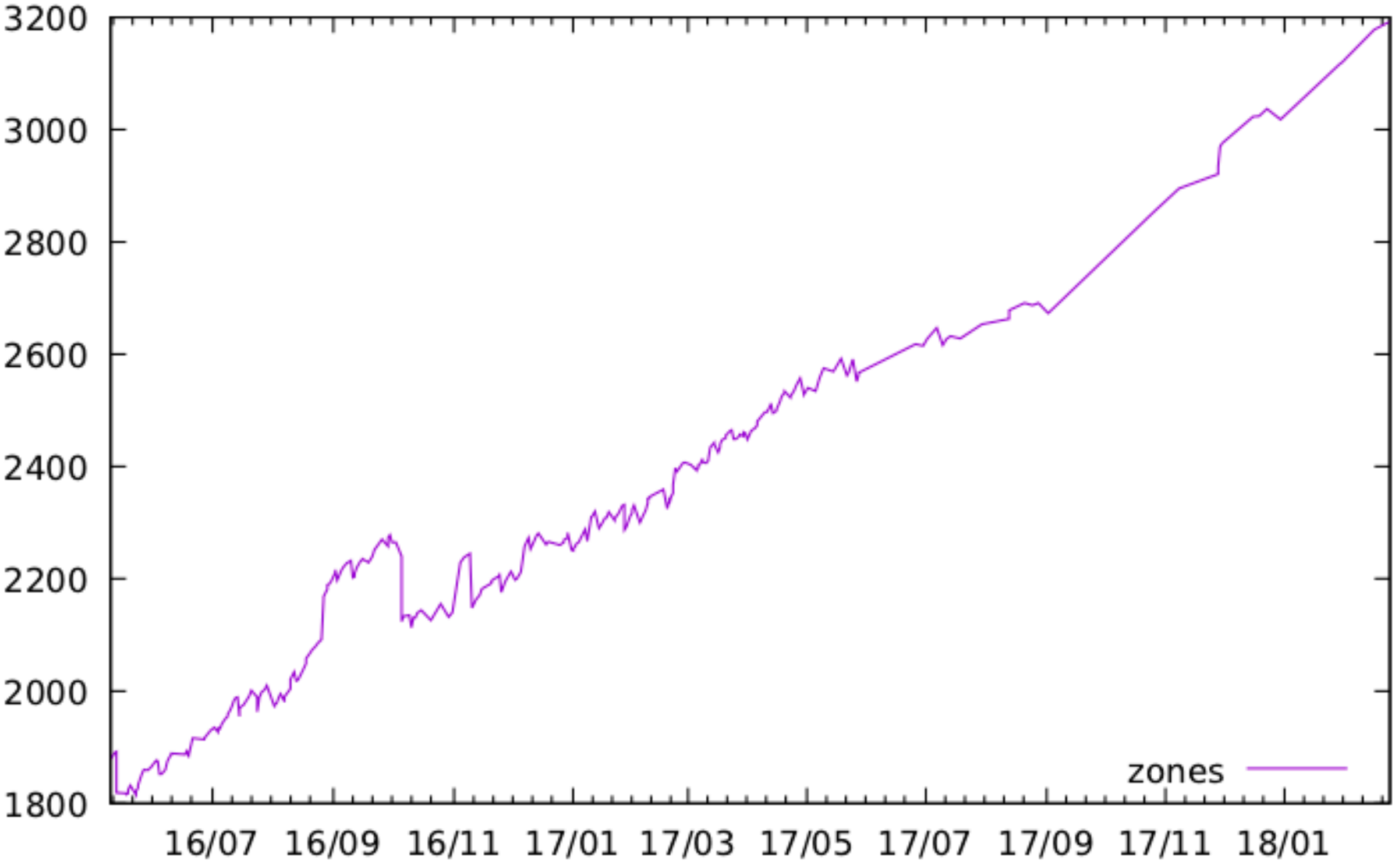
DANE SMTP Survey

- Monitors domains directly 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, ... (more ccTLD data wanted)
- Covers ~200 million candidate domain names
- Captures DS, DNSKEY, MX, A, AAAA, TLSA records
- Captures certificate chains of MX hosts

Survey Stats

- 5.2 million domains with DNSSEC-validated MX
- 178 thousand domains with DANE SMTP
- Millions of users (gmx.de, web.de, comcast.net)
- 5253 DANE MX hosts in 3585 zones
- ~100 domains with TLSA record lookup problems
- ~150 domains with wrong TLSA records or no STARTTLS

#Zones of DANE MX hosts



Well known DANE domains

gmx.at
registro.br
gmx.ch
open.ch
gmx.com
isavedialogue.com
mail.com
solvinity.com
trashmail.com
xfinity.com
xfinityhomesecurity.com
bund.de
freenet.de

gmx.de
jpberlin.de
lrz.de
mail.de
posteo.de
ruhr-uni-bochum.de
unitymedia.de
web.de
octopuce.fr
comcast.net
dd24.net
gmx.net
hr-manager.net

t-2.net
xs4all.net
ouderportaal.nl
overheid.nl
xs4all.nl
domeneshop.no
debian.org
freebsd.org
gentoo.org
ietf.org
netbsd.org
samba.org
torproject.org

Almost-DANE domains

Thousands 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
- Please remediate denial of existence issues
- Please enable DANE ***outbound*** even if own domain unsigned
- Please enable DNSSEC and DANE on hosting MX servers
  - Especially when hosting thousands signed domains
    - ovh.net, googlemail.com, ...
  - Or, more than 10^7 as yet unsigned domains (secureserver.net)

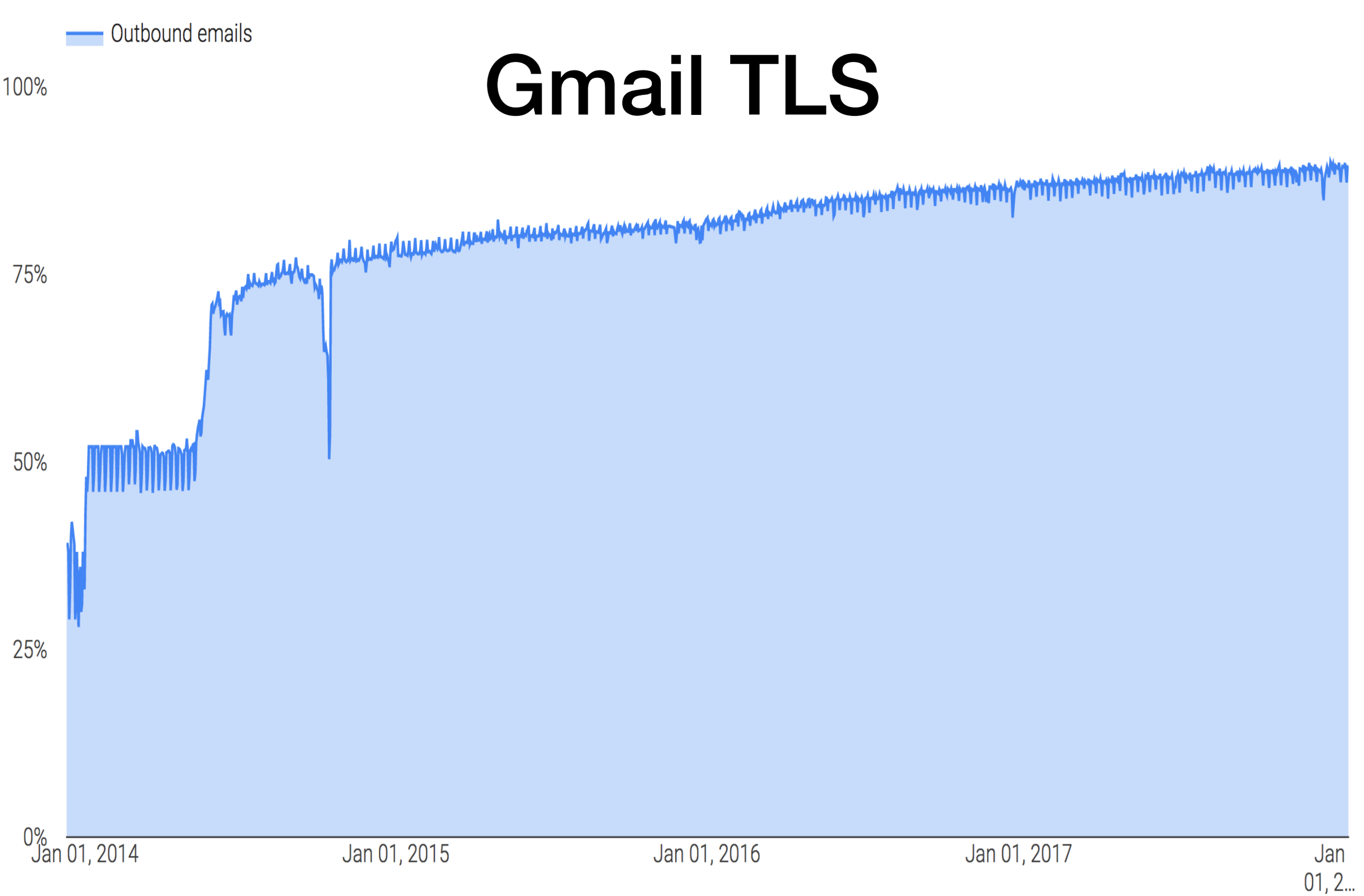
Appendix

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

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

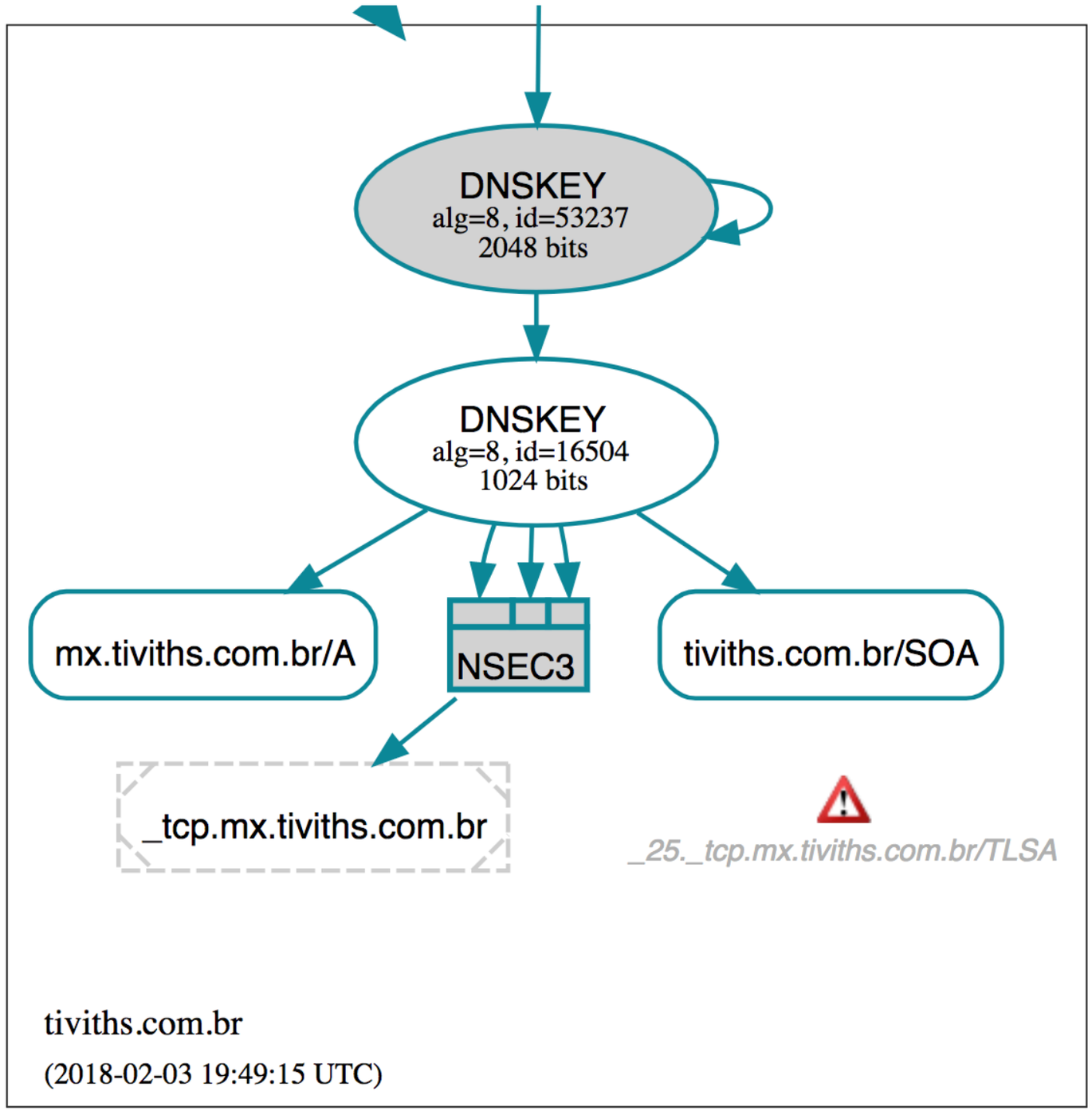
SMTP-STS

- 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

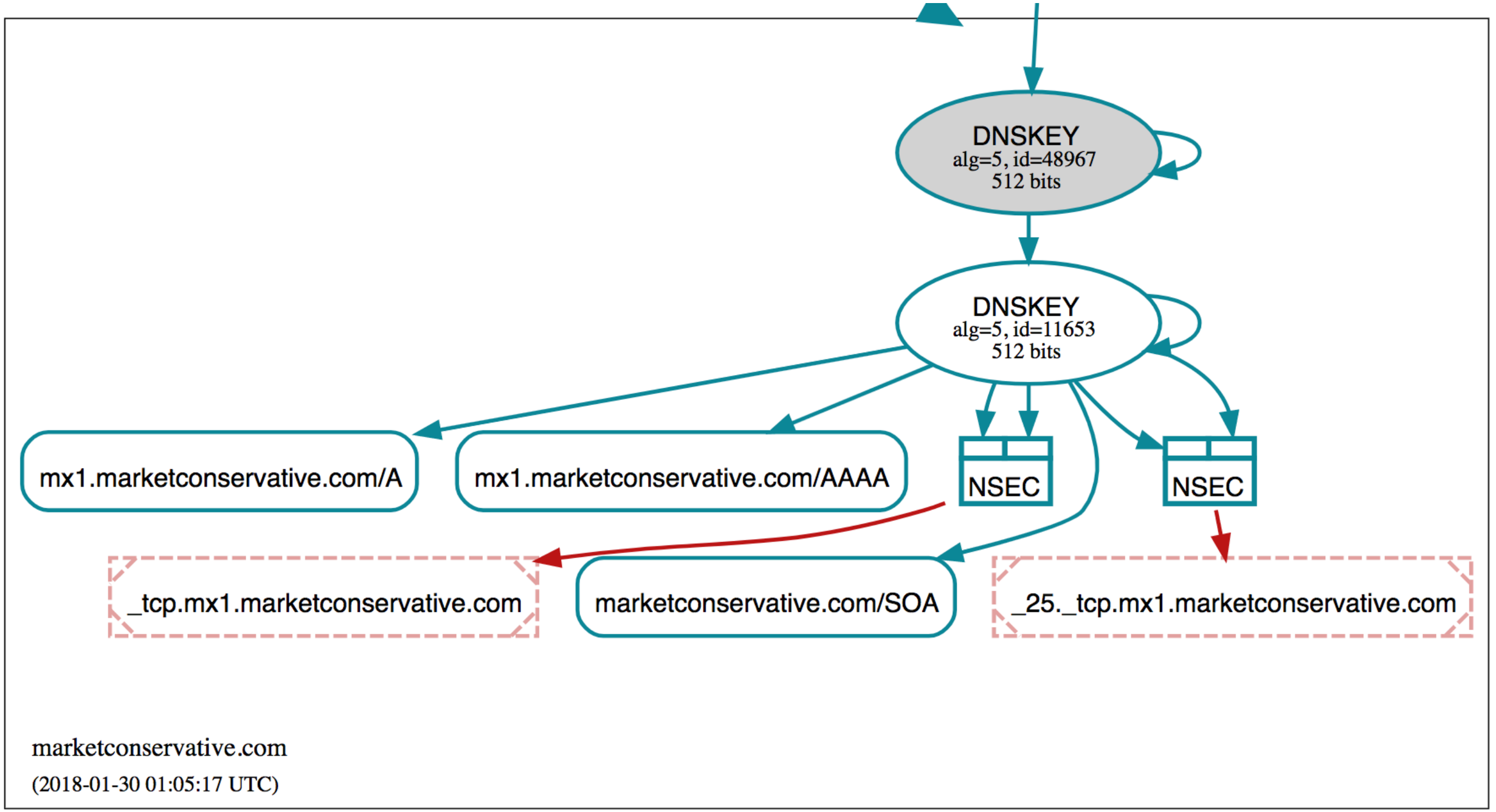
- Examples of various name-server edge-cases
- Follow links to live DNSViz site
- Mouse-over "red" elements provides more detail

TLSA queries blocked (resolved)



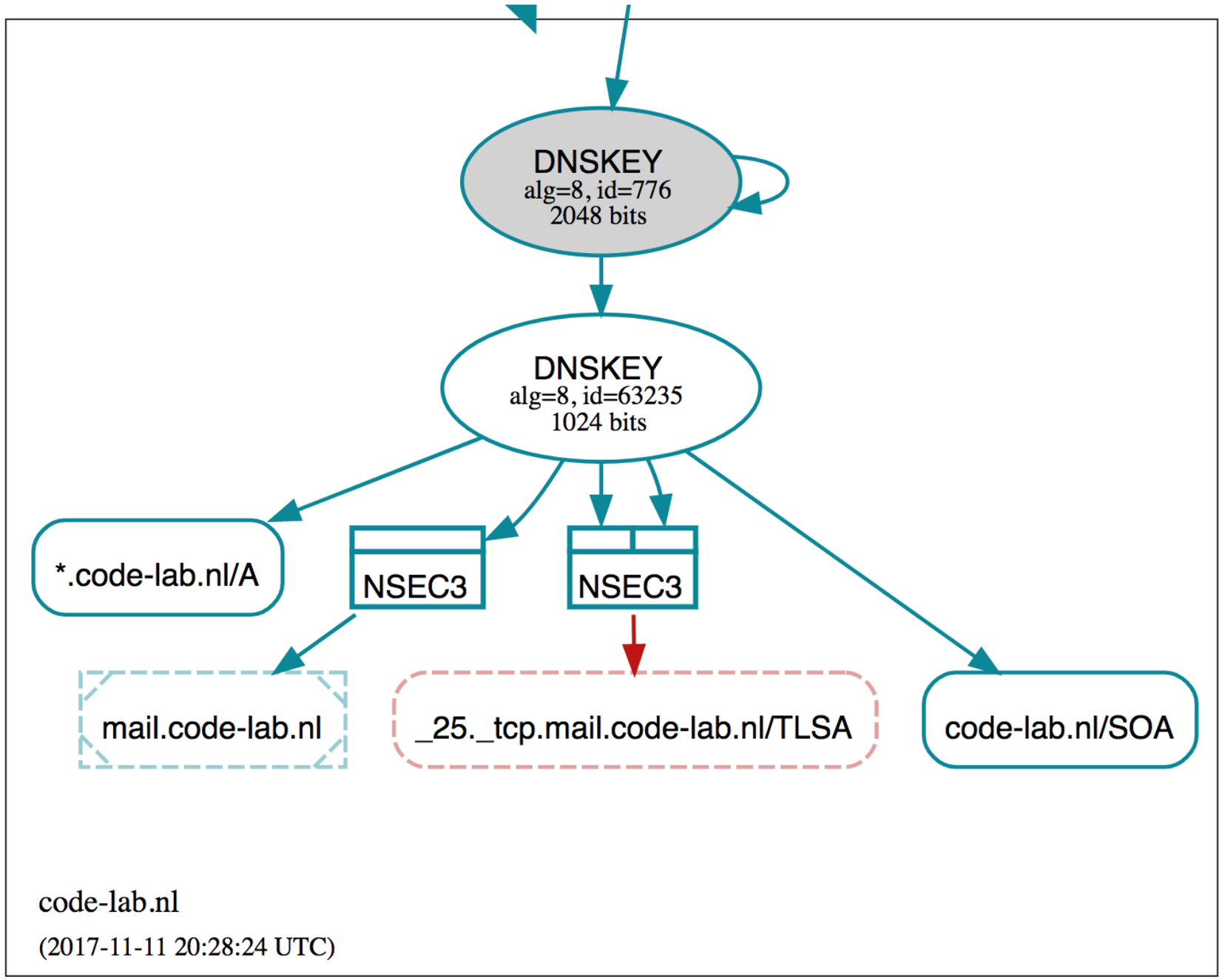
http://dnsviz.net/d/_25._tcp.mx.tiviths.com.br/WnYSUg/dnssec/

NSEC covers wrong wildcard



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

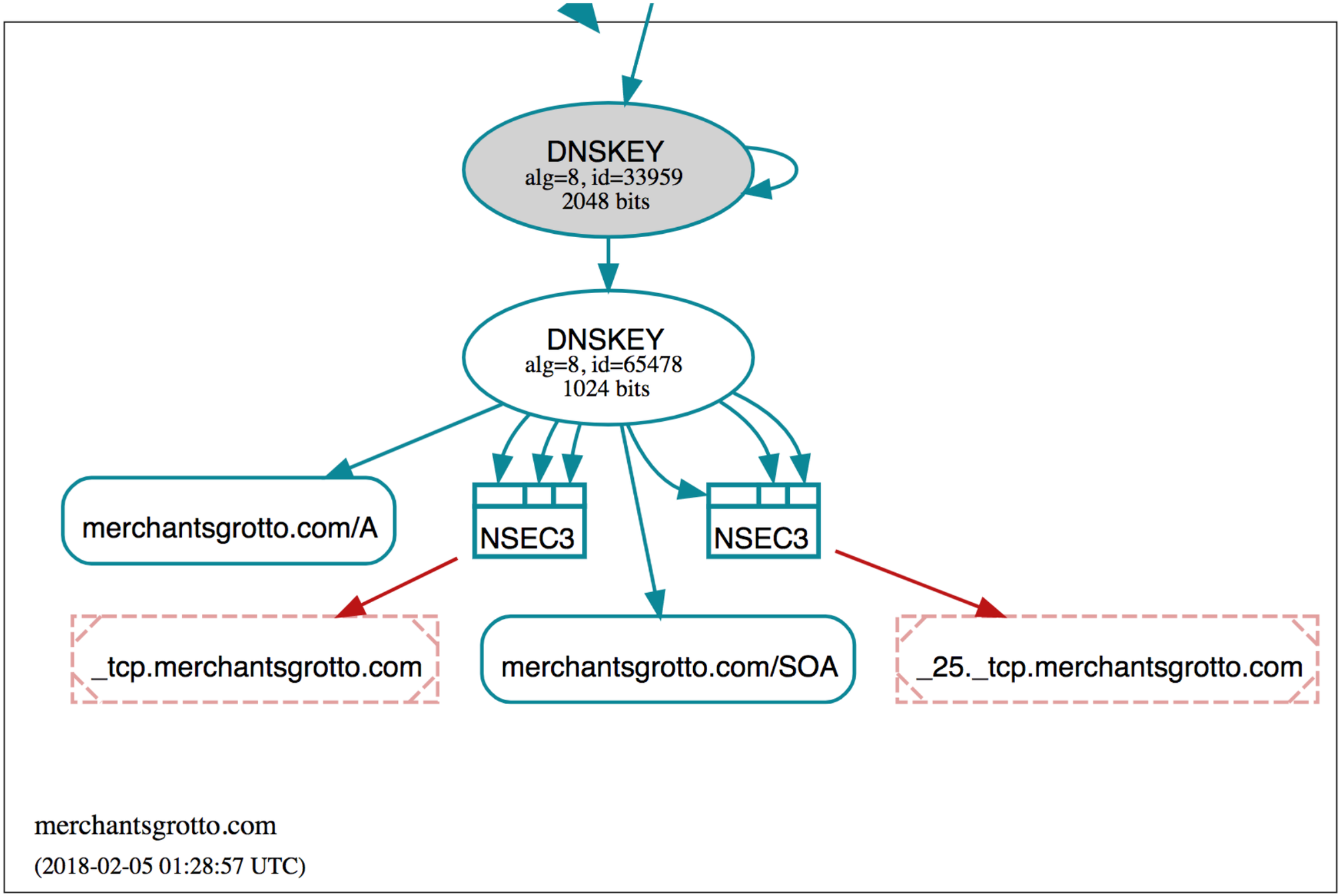
Misused zone apex wildcard



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

primary nameserver: `ns3.firstfind.nl`

Wildcard ENT NODATA (resolved)



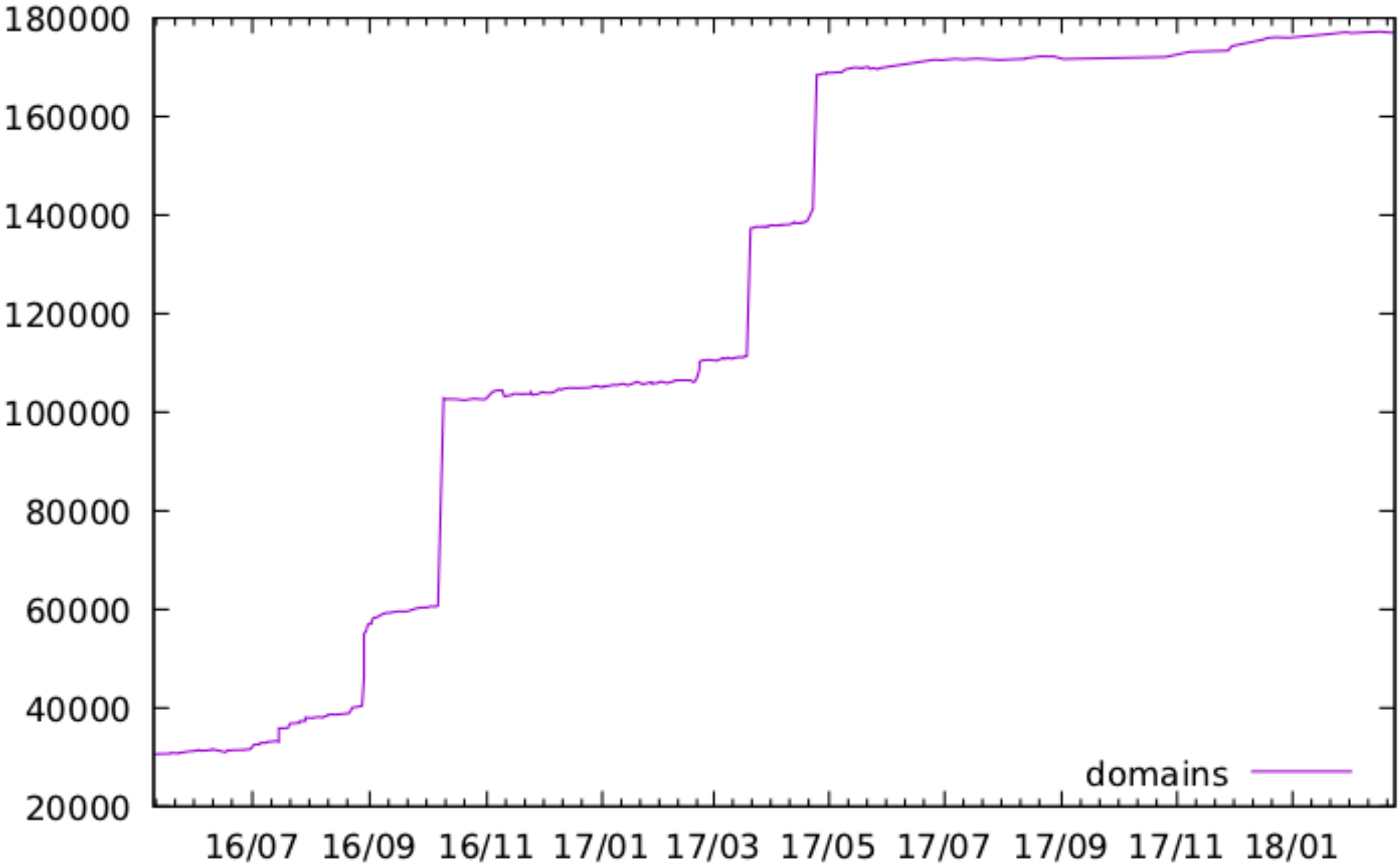
http://dnsviz.net/d/_25._tcp.merchantsgrotto.com/WnezZQ/dnssec/

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, ...

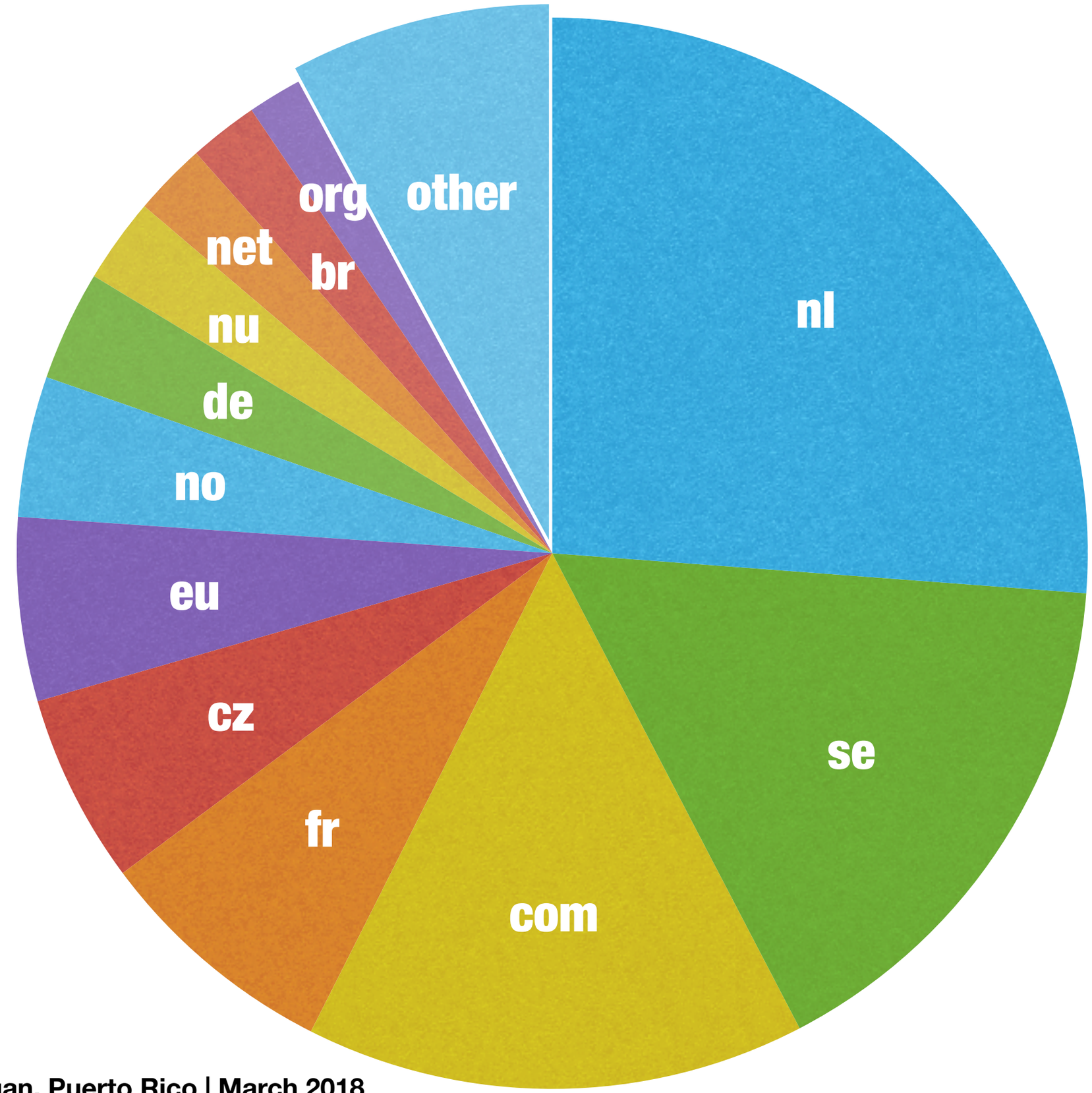
#DANE SMTP domains



DNSSEC by TLD

DNSSEC domains x1000	TLD
1,357	NL
837	SE
781	COM
382	FR
297	CZ
287	EU
220	NO
172	DE
133	NU
114	NET
108	BR
407	other

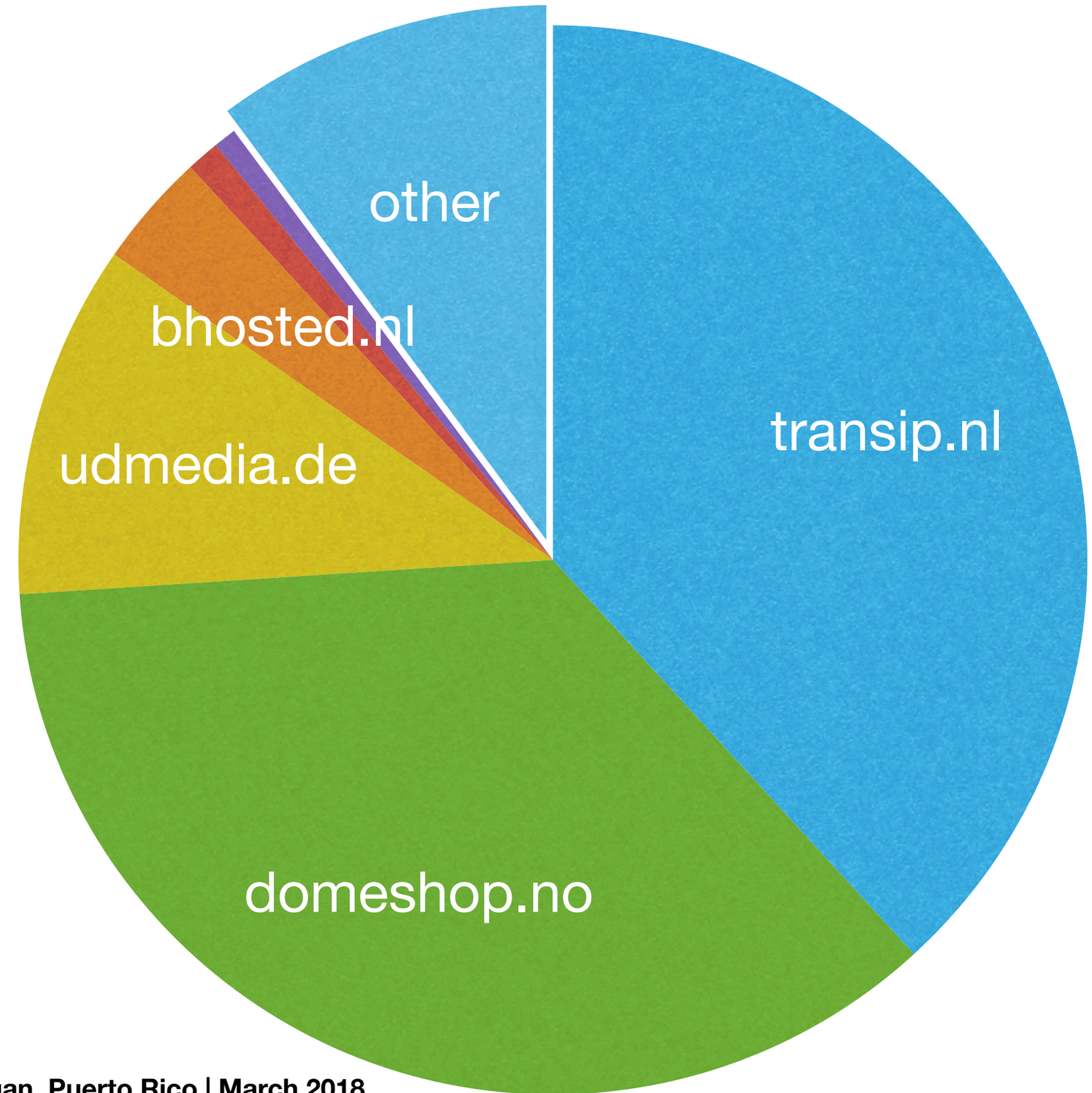
DNSSEC by TLD



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

DANE Domains by provider



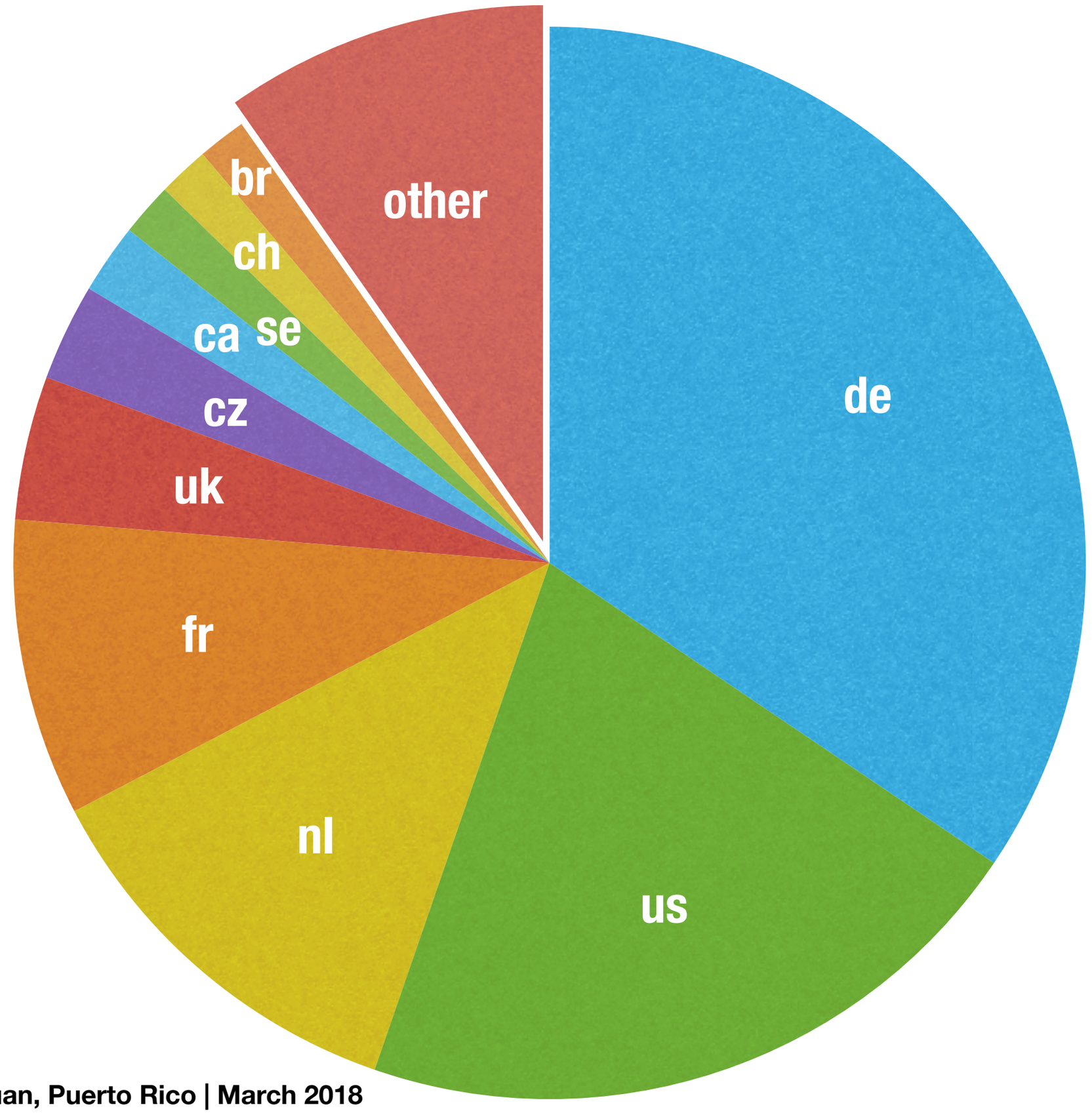
DANE MX host IPv4 GeoIP

#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

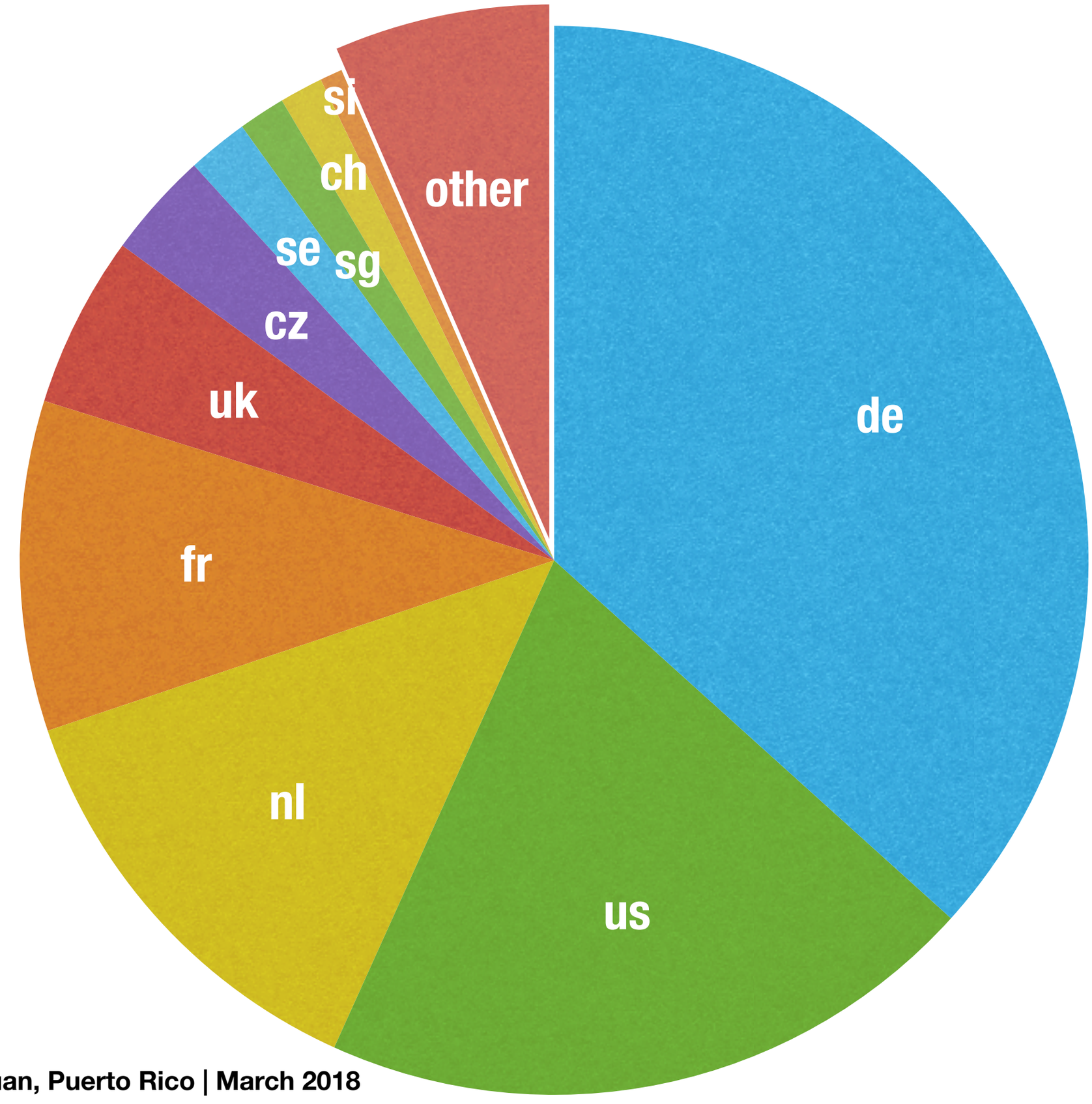
DANE MX host IPv6 GeoIP

#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

DANE MX IPv4 GeoIP



DANE MX IPv6 GeoIP

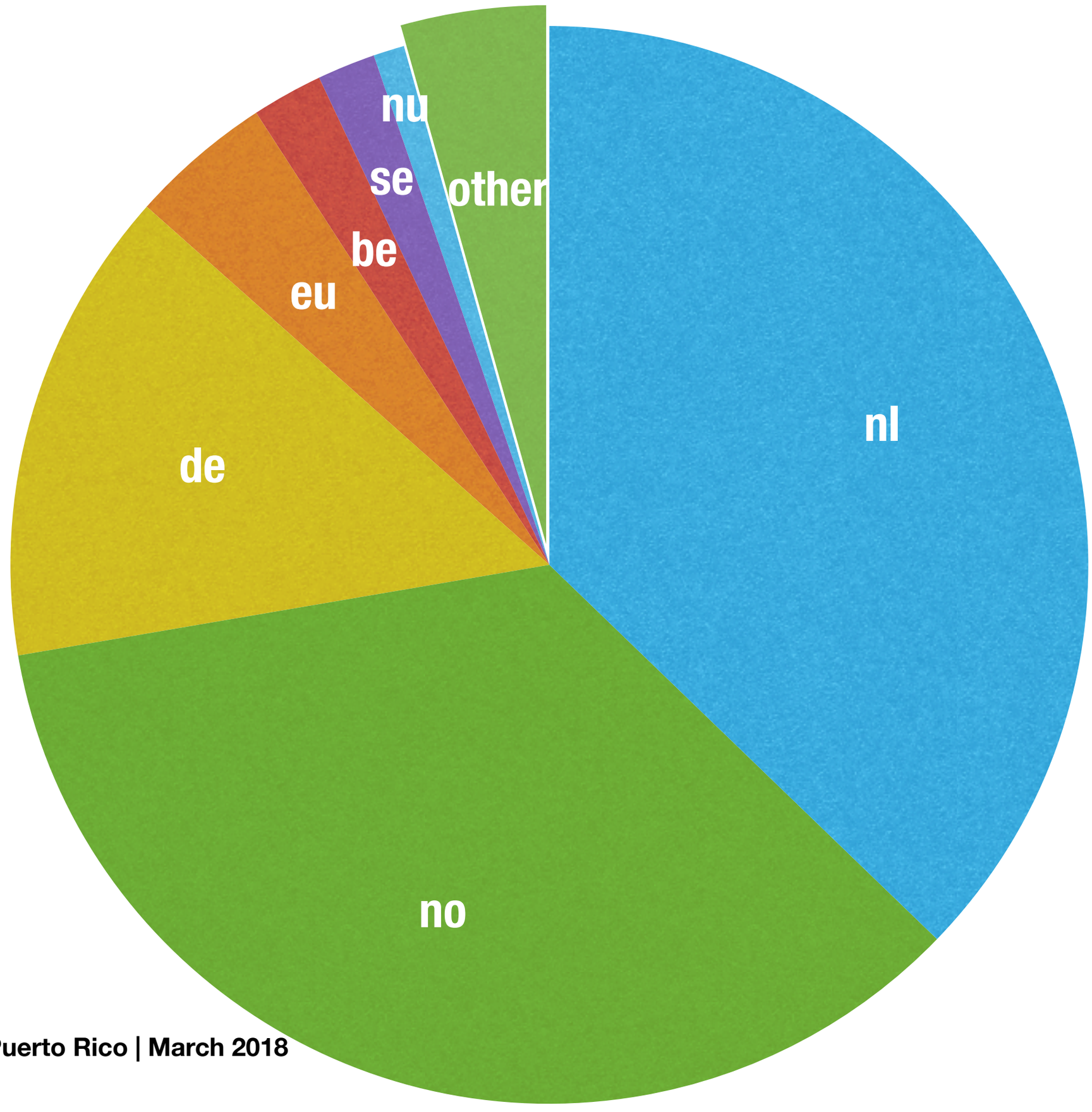


DANE in ccTLDs

- 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

DANE Domains by ccTLD



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
```