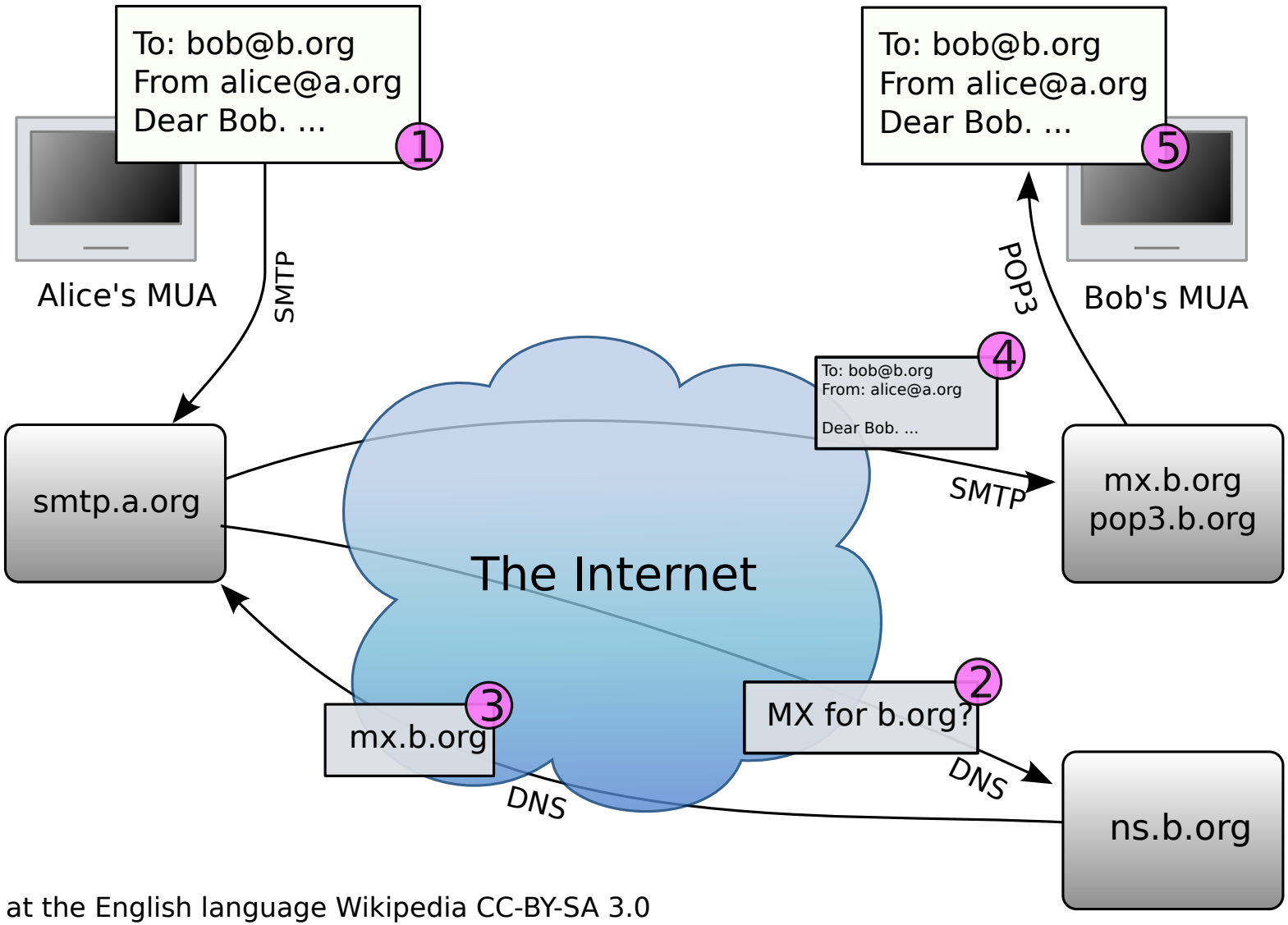
A measurement of SMTP over TLS

Ondřej Caletka

November 2015

The principle SMTP



Yzmo at the English language Wikipedia CC-BY-SA 3.0

Who’s possibly reading?

- sender’s server
- recipient’s server
- **anybody taping the wire**

Best Current Practice #188

Internet Engineering Task Force (IETF) — S. Farrell
Request for Comments: 7258 — Trinity College Dublin
BCP: 188 — H. Tschofenig
Category: Best Current Practice — ARM Ltd.
ISSN: 2070-1721 — May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Oportunistic encryption

- server announces support for STARTTLS
- client opens anonymous TLS
  - no identity check
  - old and broken ciphers are allowed
- if TLS fails **plain-text is used**
- only against passive taping

Opt-in for security

- server certificate fingerprint stored in secure DNS
- already standardised in RFC 7672
- presence of TLSA record states:
  Hey, don’t you ever try to deliver via plaintext to me! I do offer modest security!

Example

```
_25._tcp.mx.example.com. IN TLSA 3 1 1 AA793DA…
```

Testing with `posttls-finger`

Without TLSA record – Untrusted

```
$ /usr/sbin/posttls-finger -c gmail.com
posttls-finger: gmail-smtp-in.l.google.com[2a00:1450:4013:c01::1a]:25:
                Matched subjectAltName: gmail-smtp-in.l.google.com
posttls-finger: mx1.seznam.cz:25: Matched subjectAltName: mx1.seznam.cz
posttls-finger: certificate verification failed for gmail-smtp-in.l.google.
                com[2a00:1450:4013:c01::1a]:25: untrusted issuer
                /C=US/O=Equifax/OU=Equifax Secure Certificate Authority
posttls-finger: Untrusted TLS connection established to gmail-smtp-in.l.
                google.com[2a00:1450:4013:c01::1a]:25: TLSv1.2 with cipher
                ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits)
```

With TLSA record – Verified

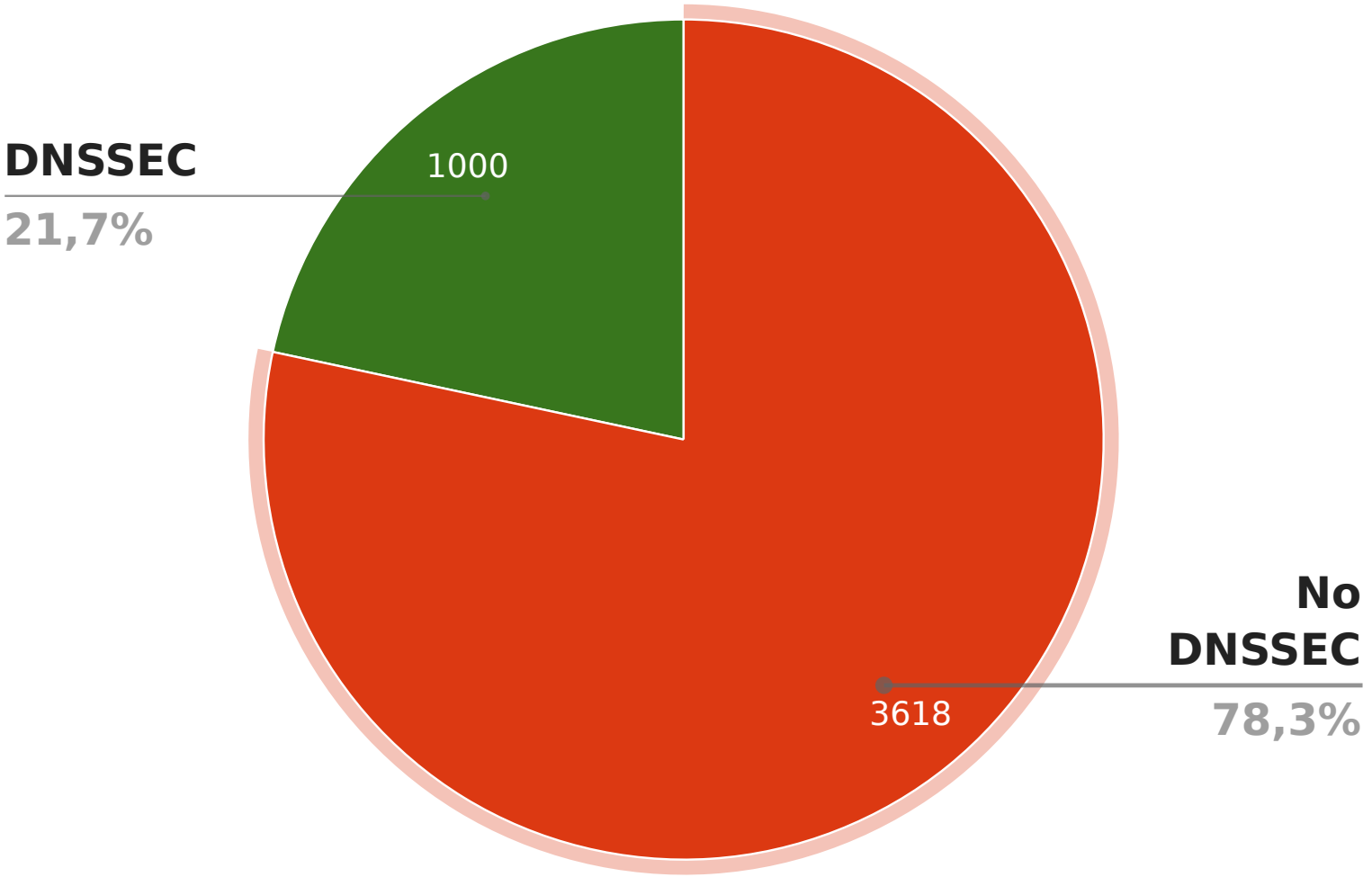
```
$ /usr/sbin/posttls-finger -c cesnet.cz
posttls-finger: using DANE RR: _25._tcp.… IN TLSA 2 0 1 5C:42:8B:01:3B:2E:3F:0D:30…
posttls-finger: postino.cesnet.cz:25: depth=1 matched trust anchor certificate
                sha256 digest 5C:42:8B:01:3B:2E:3F:0D:30…
posttls-finger: Verified TLS connection established to postino.cesnet.cz:25:
                TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits)
```

CESNET

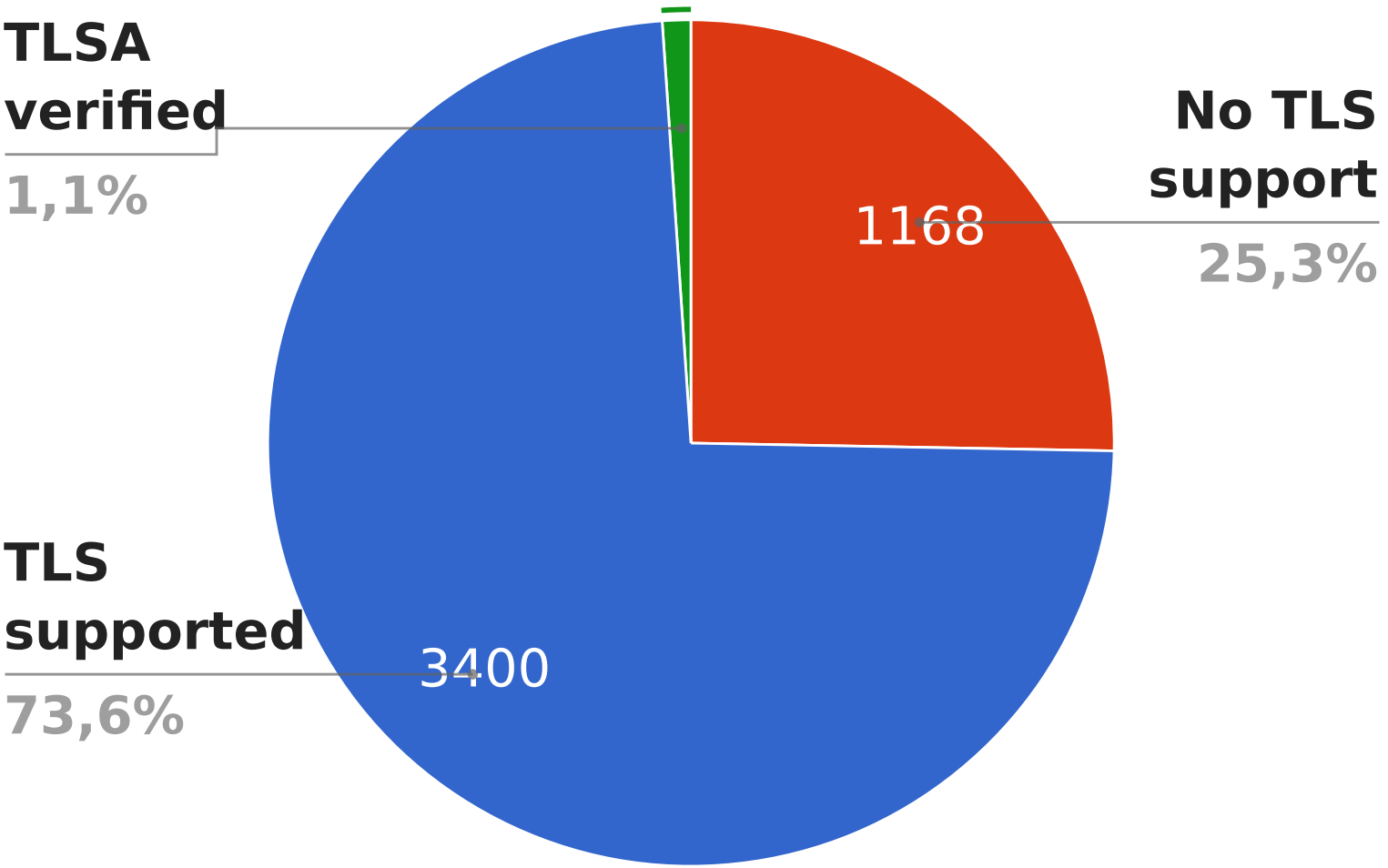
SMTP-over-TLS measurement

on 4618 e-mail domain names collected from our server

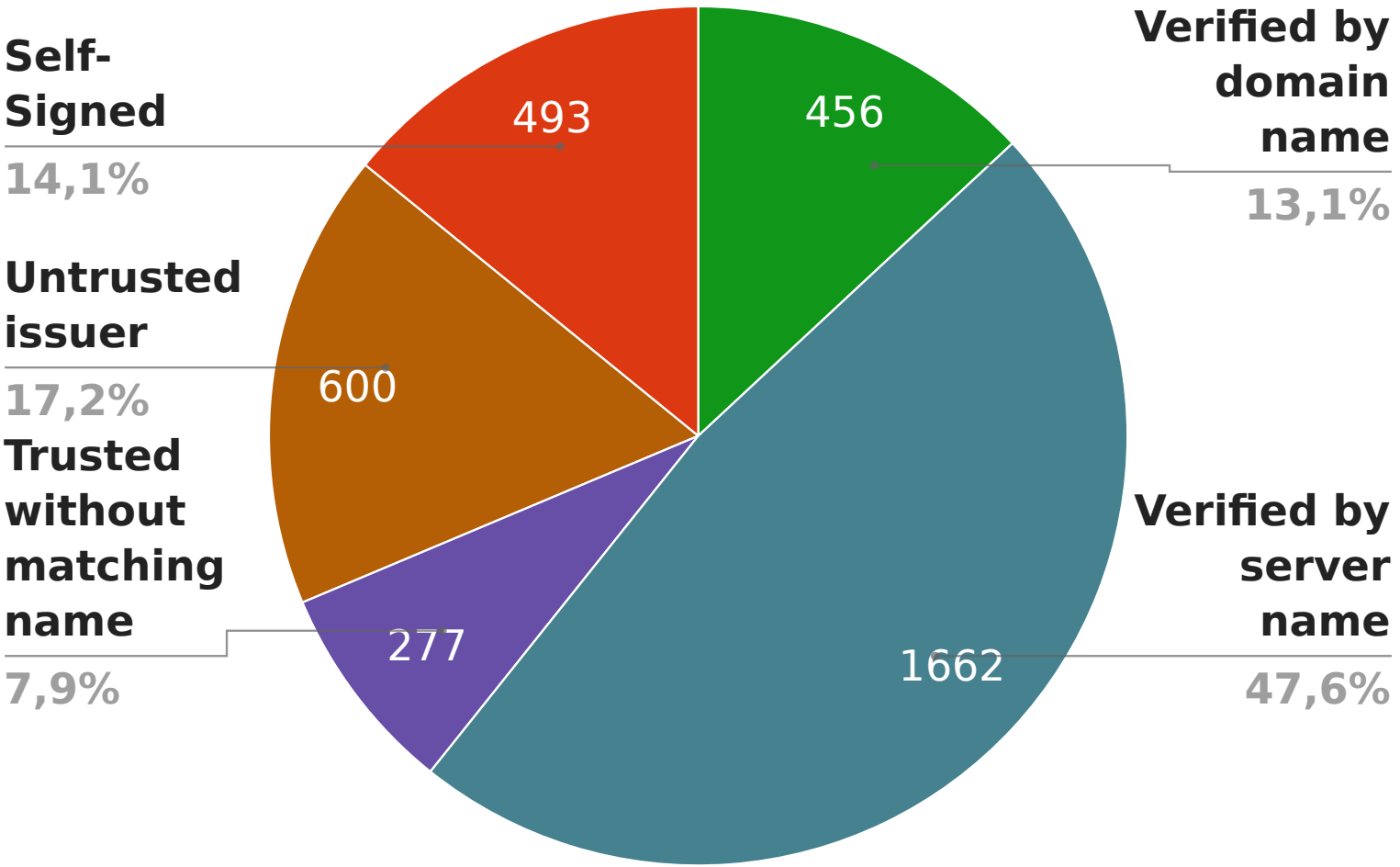
DNSSEC for MX record



STARTTLS support on servers



SMTP certificate types



TLSA Hall of Fame

Conclusion

- enable STARTTLS support on your MX servers
  - virtually no cost
  - self-signed certificate is OK
- there’s no secure e-mail without DNSSEC
- once DNSSEC is deployed, TLSA records cost nothing
- check your domain at `https://dane.sys4.de`
- it is safe to validate TLSA records
  - but better check the logs for errors like `Server certificate not trusted`

Thank You!

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz