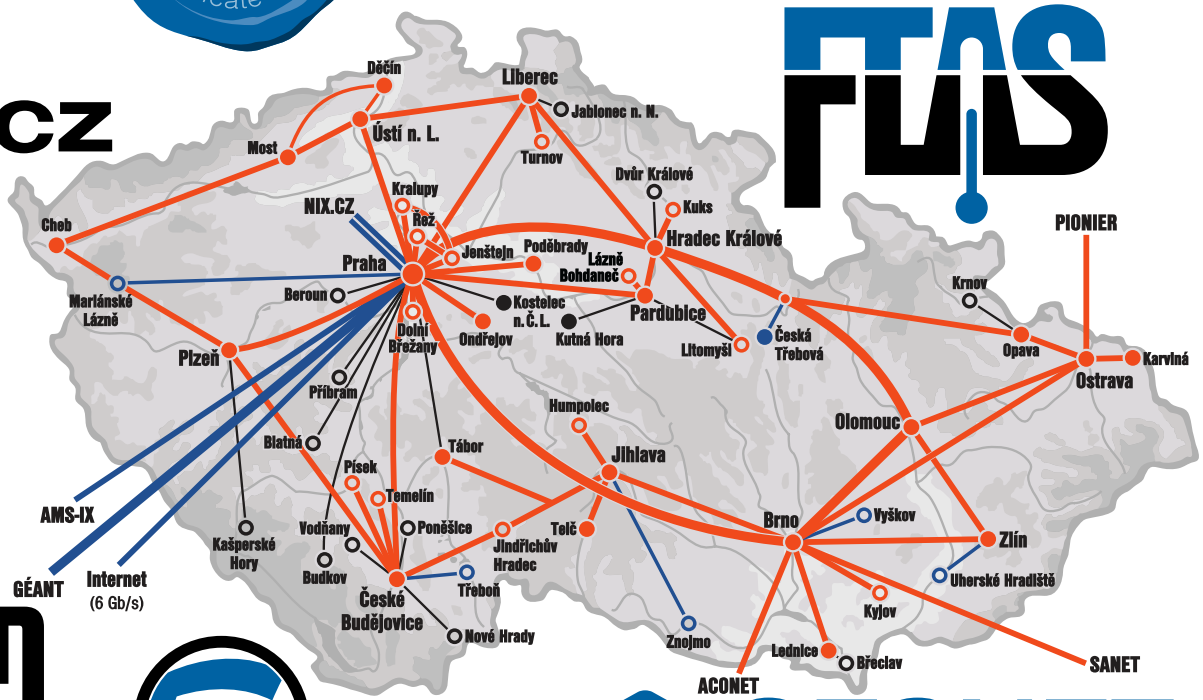
Bezpečnější e-mail
bezpečnější díky DANE

Ondřej Caletka

8. listopadu 2015

Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O sdružení CESNET



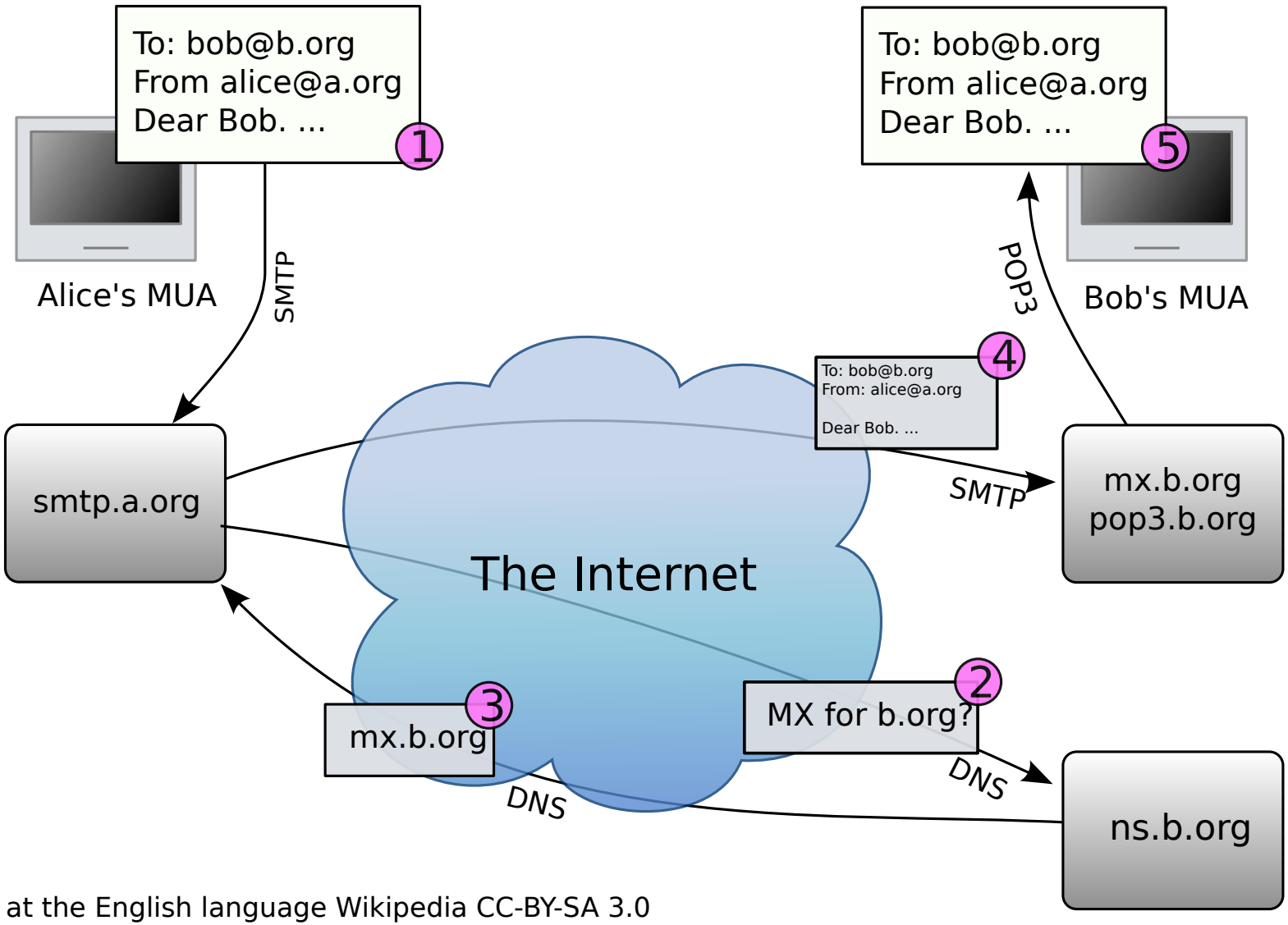
Elektronická pošta

- starší než Internet
- přepojování zpráv *hop-by-hop*
- na internetu používá protokol SMTP

E-mailová etiketa

E-mail není důvěrný: Do e-mailu nepište nic, co byste nenapsali na zadní stranu pohlednice. Vaše e-mailová korespondence se kdykoli může dostat do nepovolaných rukou… *zdroj*

Princip SMTP



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

Kdo poslouchá?

- server odesílatele
- server příjemce
- **kdokoli s odbočkou na kabelu**

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.

Bezpečnější e-mail

End-to-end

- S/MIME – CMS
- PGP
- ✓ vysoká úroveň bezpečnosti
- ✗ obtížné použití

Hop-by-hop

- DKIM
- **SMTP over TLS**
- ✓ bez přímé účasti uživatele
- ✗ jen proti třetím stranám

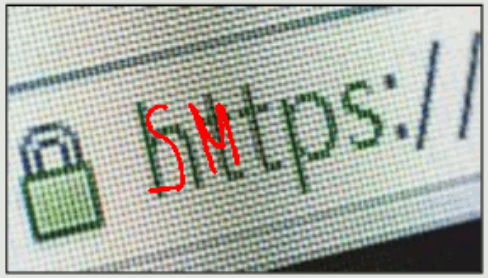
Oportunistické šifrování

- server signalizuje podporu STARTTLS
- klient naváže anonymní TLS spojení
  - ověření identity se neprovádí
  - vyhoví i slabé a nebezpečné šifry
- při selhání TLS spojení je **doručeno bez šifrování**
- odolné pouze proti pasivnímu odposlechu
- lze definovat cíle s vynuceným šifrováním
  - např. Gmail, Seznam,...
  - jak takový seznam získat a udržovat?

CESNET

V ideálním světě...

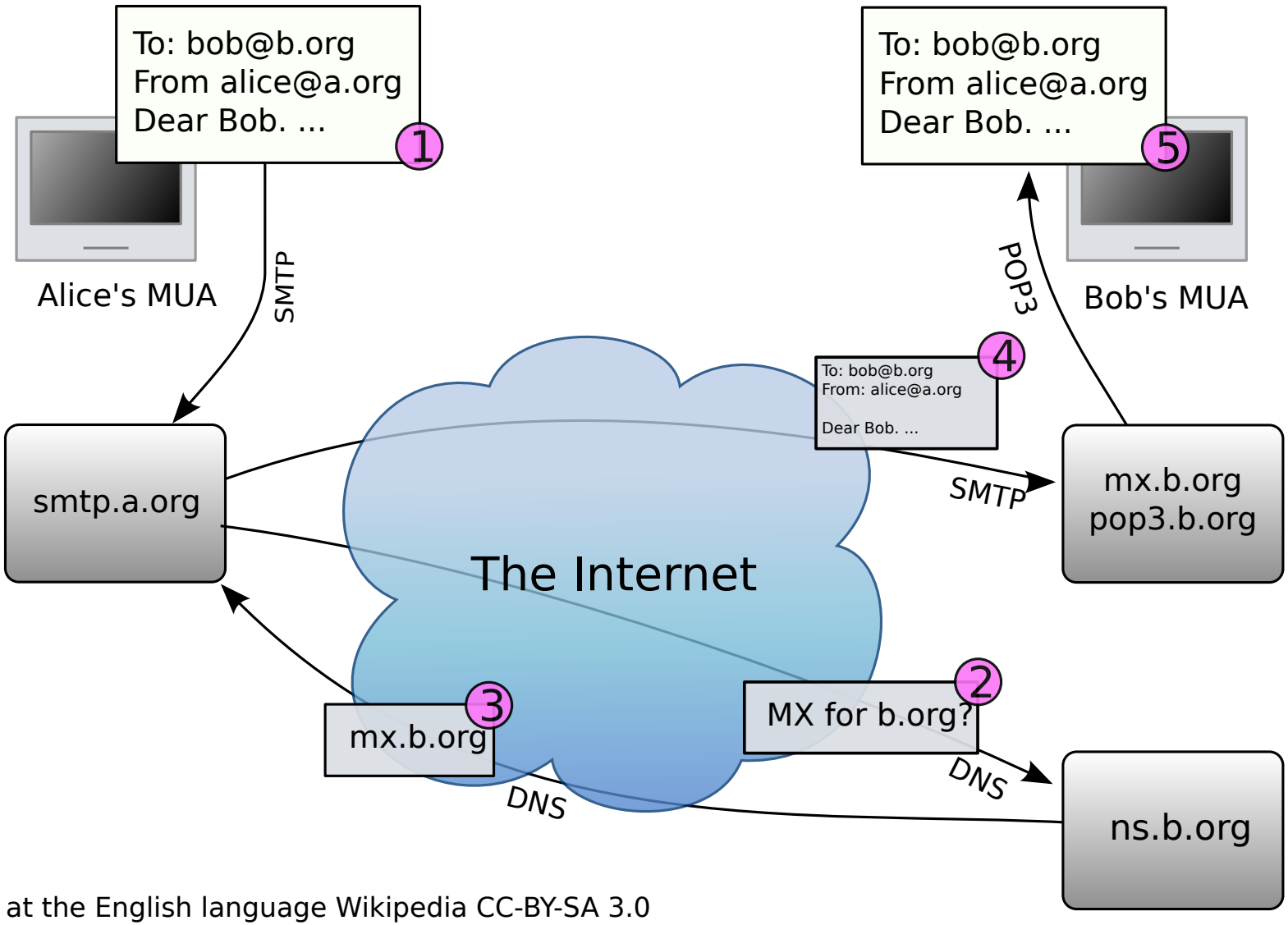
~~H~~SMTPS BY MĚLO BÝT VŠUDE



Celý internet směřuje k šifrování. Bezpečnostních kauz přibývá a s nimi se násobí úsilí rozšířit i šifrování mezi uživatelem a službami. ~~H~~SMTPS by se mělo stát standardem, který bude nejen očekáván, ale i vyžadován na mnoha úrovních: od prohlížečů až po uživatele. Výsledkem bude lepší ~~web~~ E-MAIL pro všechny.

- všechny SMTP servery přijímají poštu šifrovaně
- každý SMTP server používá validní TLS certifikát od důvěryhodné autority
- předávání e-mailů je pak naprosto bezpečné
  ...nebo snad ne?

Princip SMTP



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

Ten DNSSEC bude asi fakt potřeba...

- bez bezpečného DNS není možné věřit směrování MX záznamů
- certifikáty serverů by musely být vystaveny na jméno domény, pro kterou přijímají poštu
  - což je stejně špatné, jako u dnešního webu
  - pro e-maily velmi nepraktické
- bezpečné DNS může nést informaci o vynucení šifrování předávané pošty

TLSA záznam pro vynucení šifrování

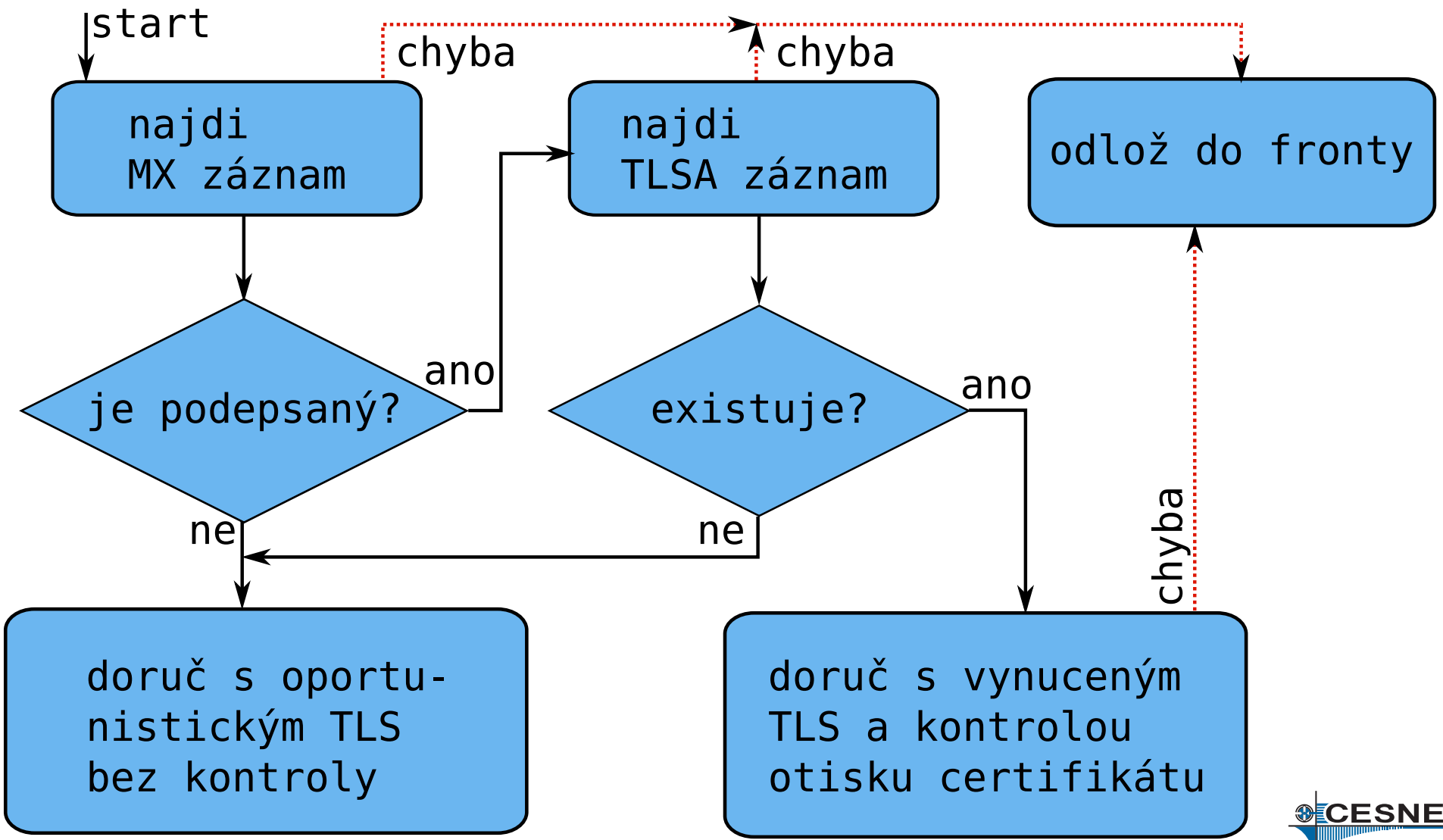
- umístění otisku serverového certifikátu v DNS
- použití pro SMTPS standardizováno v RFC 7672
- několik různých způsobů použití:
  0. ~~připíchnutí CA~~
  1. ~~připíchnutí koncového certifikátu~~
  2. vložení nové CA
  3. vložení koncového certifikátu bez ohledu na PKI

Příklad

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

CESNET

Chování SMTP klienta



Opt-in for security

- umístěním TLSA záznamu deklarujeme, že poštu přijímáme pouze šifrovaně
- validující klienti případný *downgrade* útok odhalí a zprávu nedoručí
  - Postfix od 2.11
  - Exim – ve vývoji
  - OpenSMTPd – ve vývoji
- na rozdíl od webu na SMTP serverech není problém s funkčností DNSSEC validace
- bezpečené spojení s validujícím DNS serverem **je nutné** (ideálně Unbound na localhost)
- doručování na adresy bez DNSSECu nebo bez TLSA záznamu funguje jako doposud
  …nebo ne?

Problémy se zapnutou TLSA validací

Chybná údržba TLSA záznamů

- správu TLSA záznamů je nutné přidat do workflow výměny certifikátů
- nejprve publikovat nový, pak změnit certifikát

Rozbité autoritativní DNSSEC servery

- vrací nevalidní data pro neexistující záznamy
- chybu DNSSEC validace vyhodnotí SMTP klient jako podvrh a zprávu odloží

Testujeme nástrojem `posttls-finger`

Bez TLSA záznamu – Untrusted

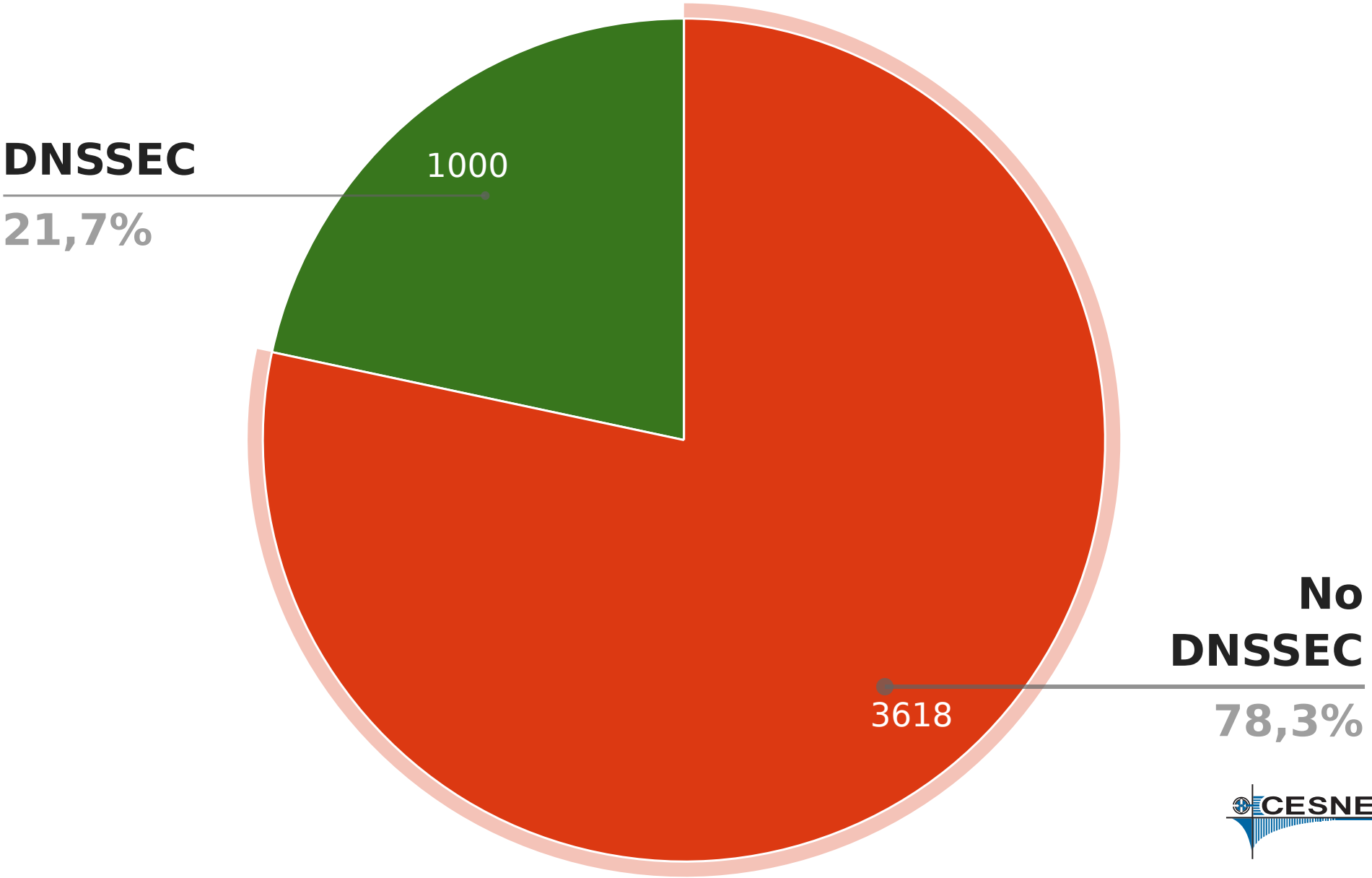
```
$ /usr/sbin/posttls-finger -c seznam.cz
posttls-finger: mx1.seznam.cz:25: Matched subjectAltName: mx1.seznam.cz
posttls-finger: certificate verification failed for mx1.seznam.cz:25:
                untrusted issuer /C=US/O=thawte, Inc./OU=Certification
                Services Division/OU=(c) 2006 thawte, Inc. - For
                authorized use only/CN=thawte Primary Root CA
posttls-finger: Untrusted TLS connection established to mx1.seznam.cz:25:
                TLSv1.2 with cipher AES128-SHA (128/128 bits)
```

S TLSA záznamem – Verified

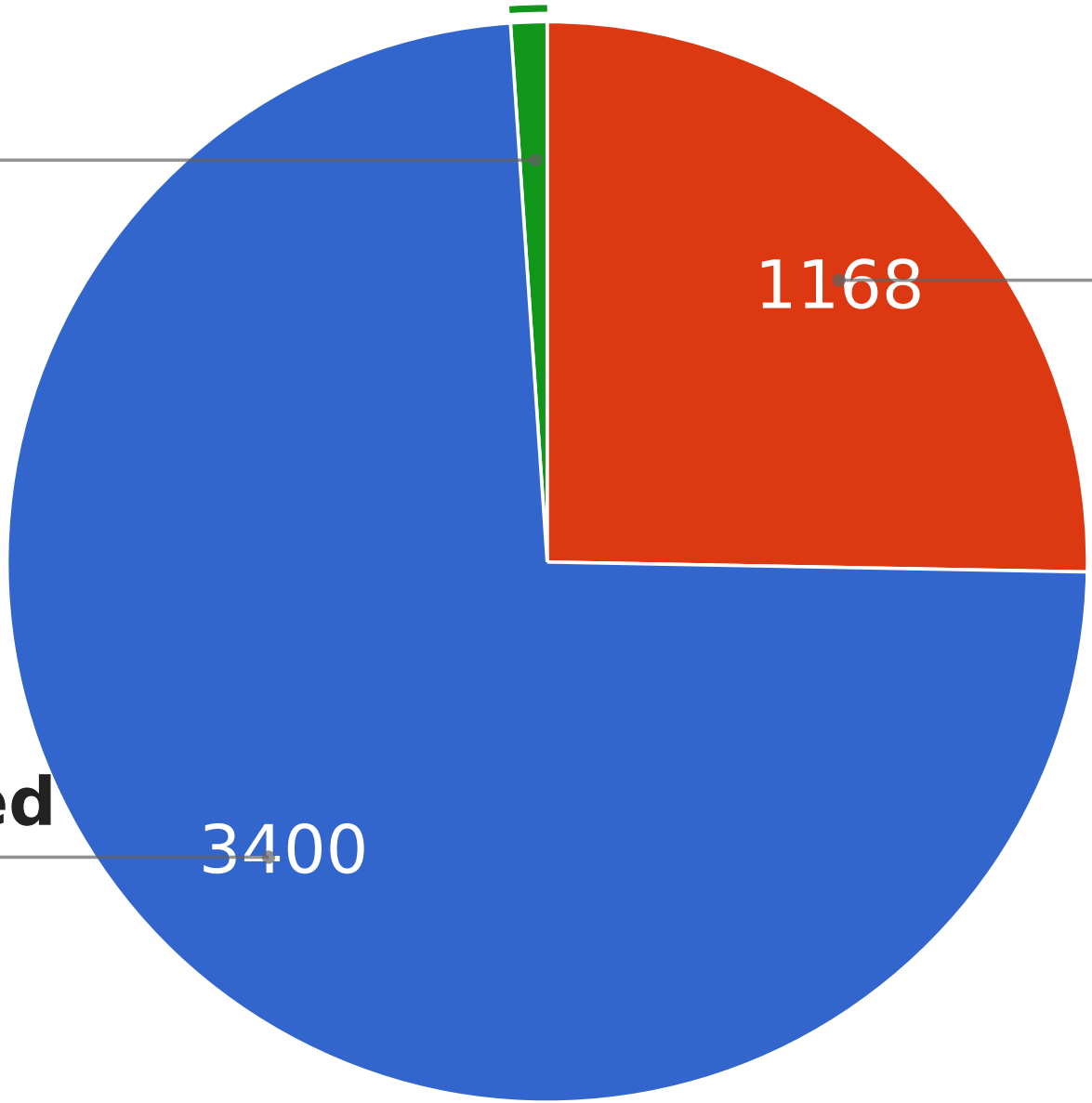
```
$ /usr/sbin/posttls-finger -c cesnet.cz
posttls-finger: using DANE RR: _25._tcp.… IN TLSA 2 0 1 5C:42:8B:01:3B:2E:3F:0D:30…
posttls-finger: postino.cesnet.cz:25: depth=1 matched trust anchor certificate
                sha256 digest 5C:42:8B:01:3B:2E:3F:0D:30…
posttls-finger: Verified TLS connection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

Měření SMTP-over-TLS

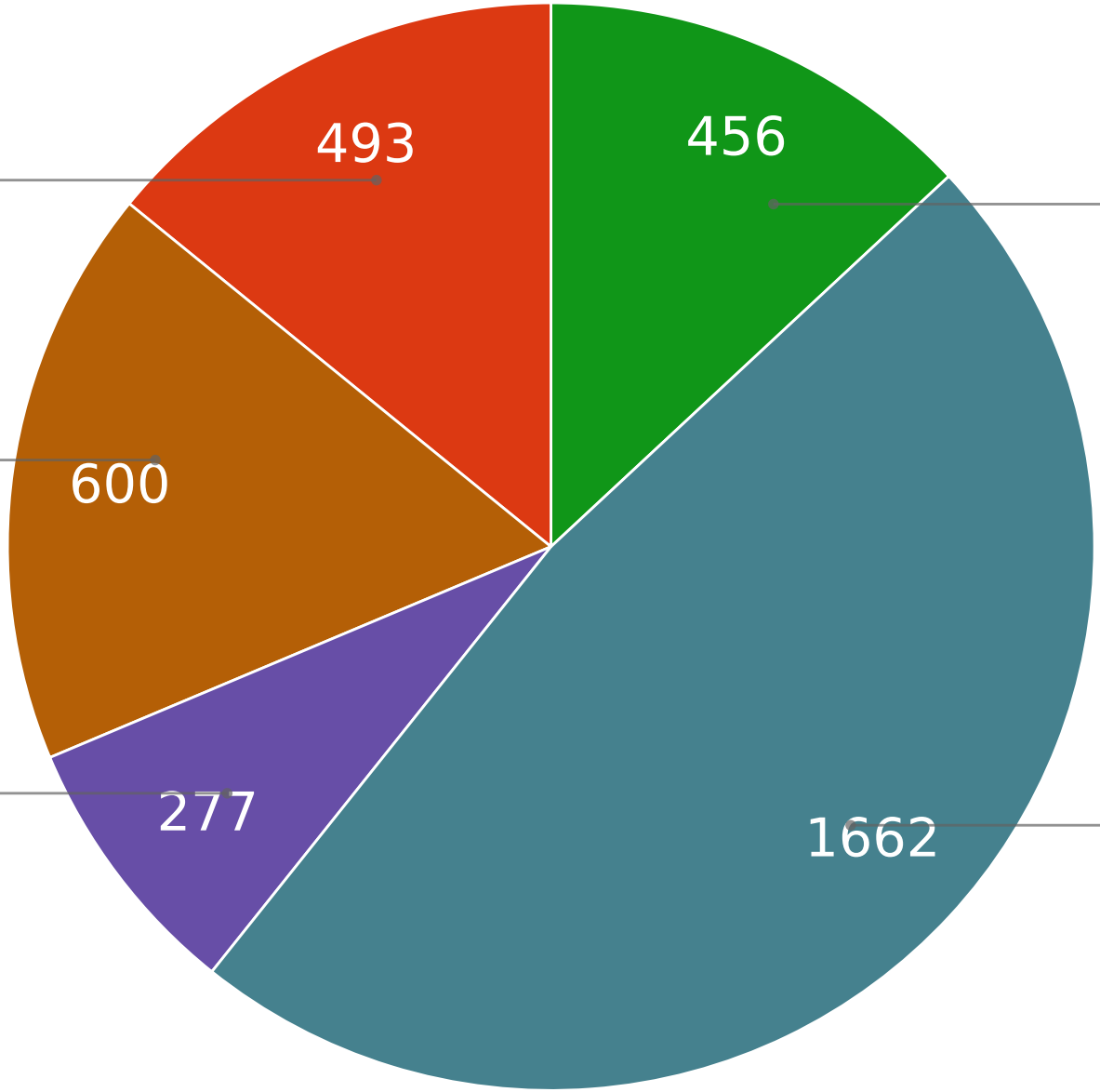
Stav DNSSEC pro MX záznamy



Servery podporující STARTTLS



Typy certifikátů na SMTP serverech



Self-Signed
14,1%

Verified by domain name
13,1%

Untrusted issuer
17,2%

Trusted without matching name
7,9%

Verified by server name
47,6%

CESNET

TLSA Hall of Fame

Závěrem

- povolte šifrování na svých SMTP serverech
  - nic to nestojí
  - na typu certifikátu vůbec nezáleží
- bez DNSSECu nelze dosáhnout bezpečnosti e-mailu
- když už máte DNSSEC, TLSA nic nestojí
- provozovat validaci je bezpečné
  - ale vyplatí se sledovat logy na výskyt chyby `Server certificate not trusted`

Kam dál?

OPENPGPKEY a SMIMEA záznamy

- uložení veřejných PGP a S/MIME klíčů
- vyřeší problém získání klíče pro šifrování
- možnost transparentně šifrovat zprávu na serveru

Autentizace klientského certifikátu

- použití např. v reputačních systémech

Závěr

Děkuji za pozornost

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