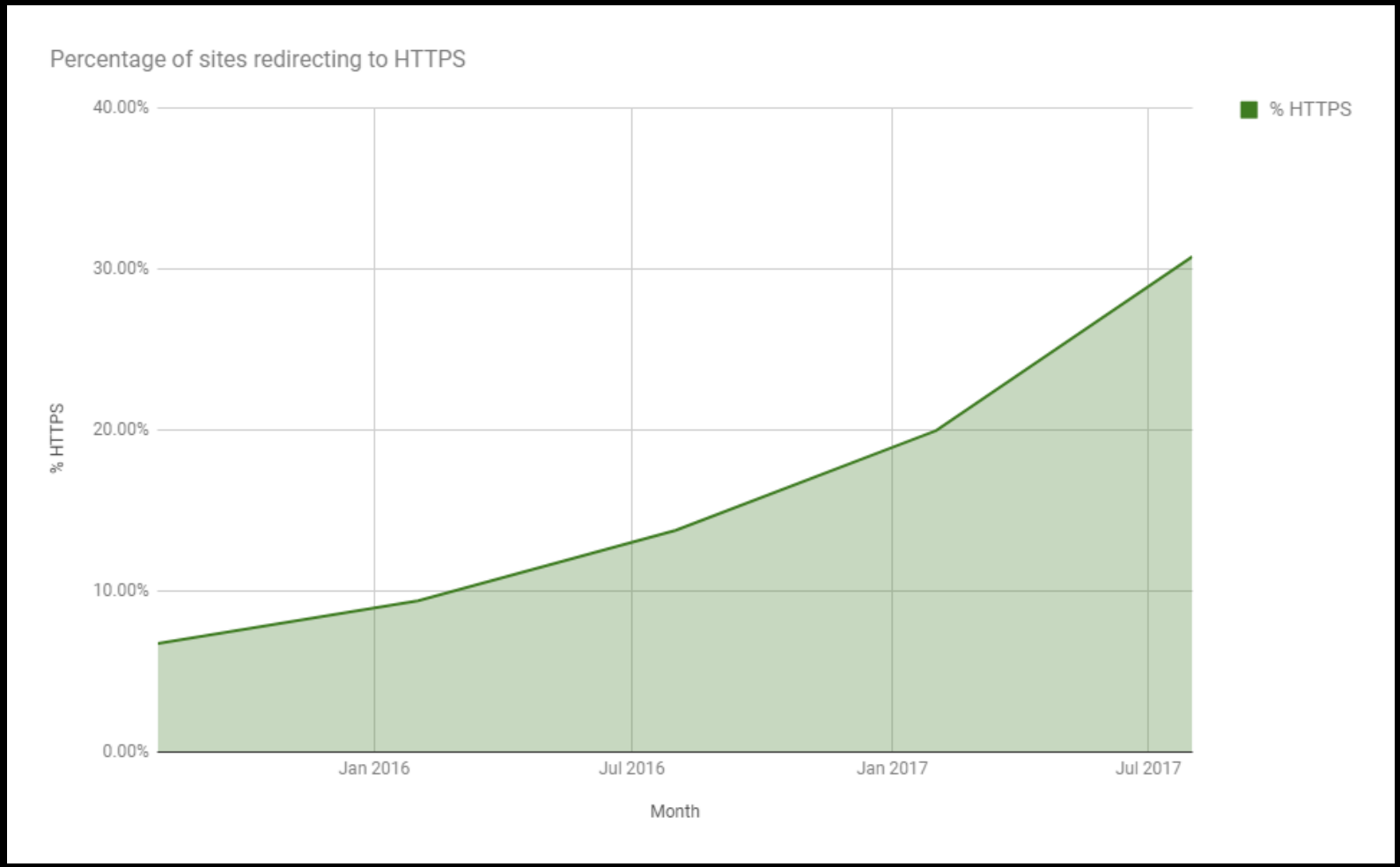
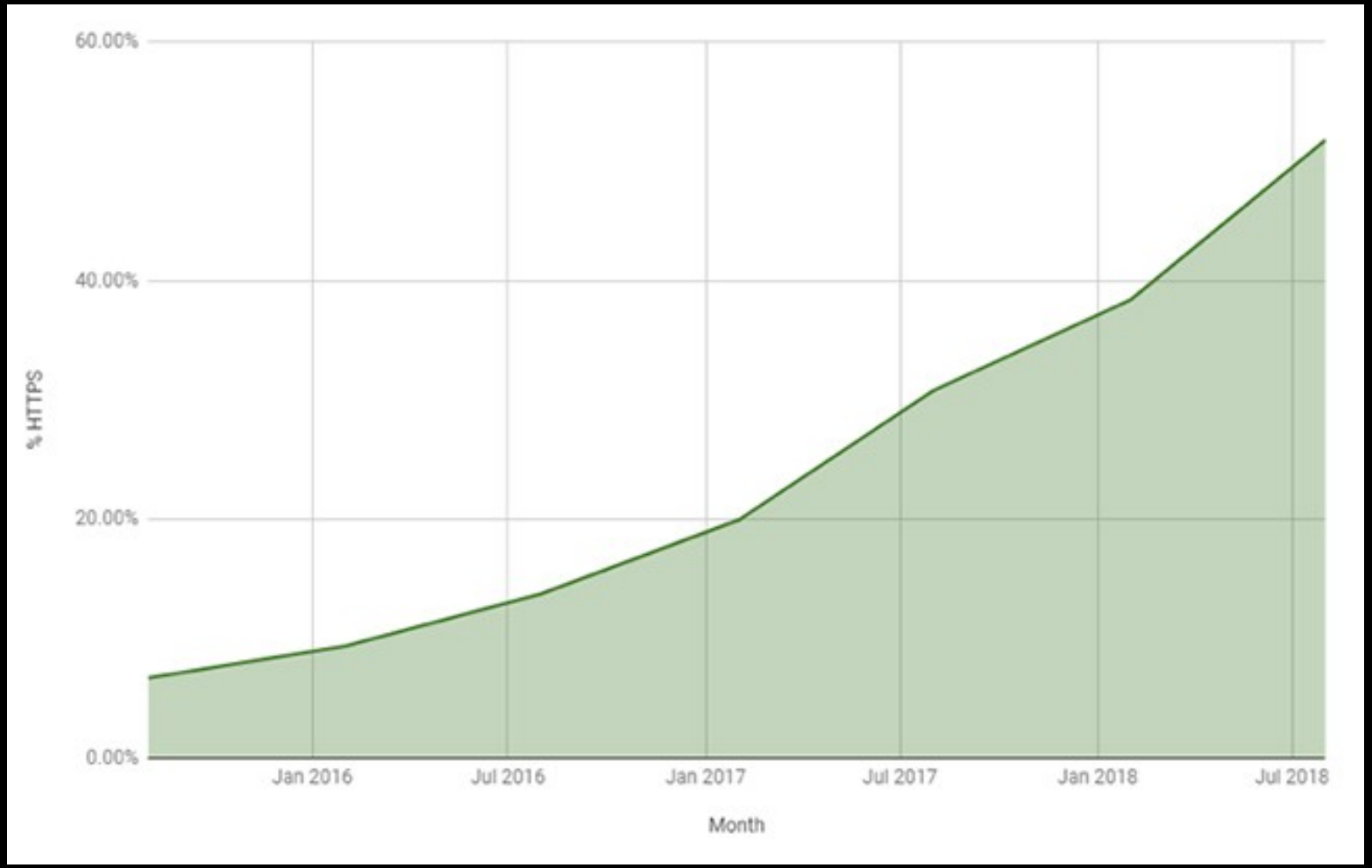
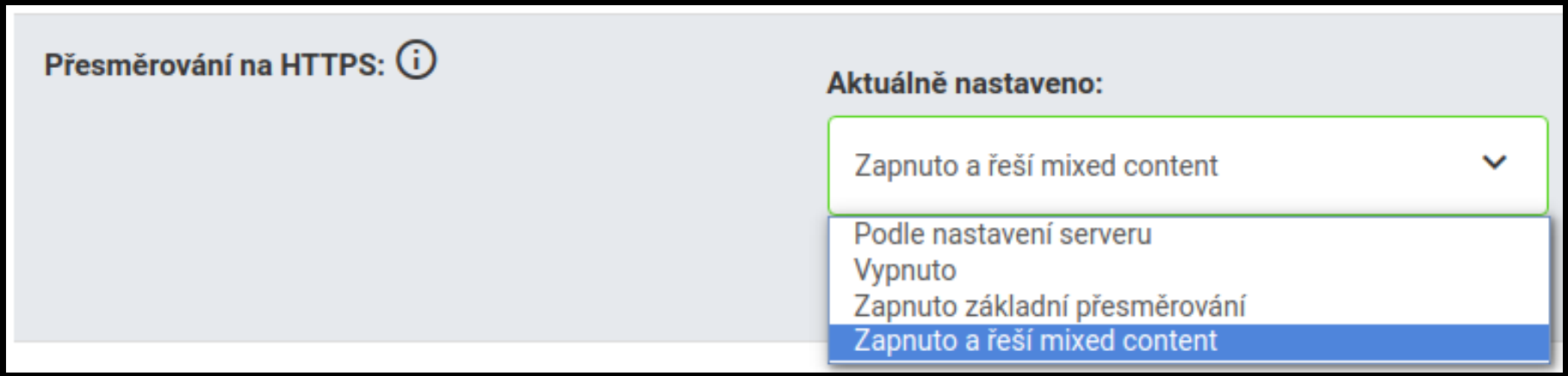
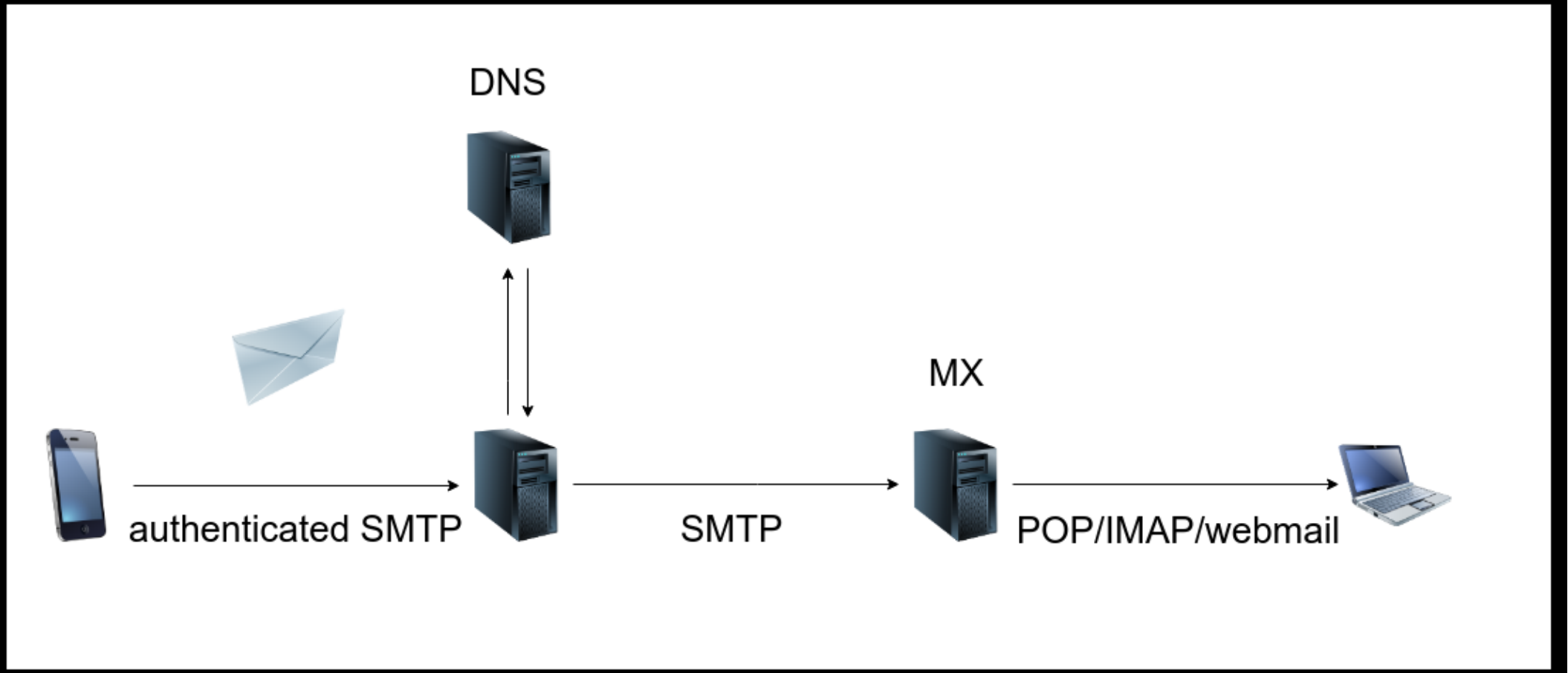
SMTP bezpečně aneb nezapomněli jsme na poštu?

Ing. Tomáš Hála
IT Security & Operations manager
ACTIVE 24, s.r.o.
@tomashala


Percentage of sites redirecting to HTTPS
% HTTPS
40.00%
30.00%
20.00%
10.00%
0.00%
% HTTPS
Jan 2016
Jul 2016
Jan 2017
Jul 2017
Month


60.00%
40.00%
20.00%
0.00%
% HTTPS
Jan 2016
Jul 2016
Jan 2017
Jul 2017
Jan 2018
Jul 2018
Month


Přesměrování na HTTPS:
Aktuálně nastaveno:
Zapnuto a řeší mixed content
Podle nastavení serveru
Vypnuto
Zapnuto základní přesměrování
Zapnuto a řeší mixed content


DNS
MX
authenticated SMTP
SMTP
POP/IMAP/webmail

Od Petr Beneš <petr.benes@obchod.wuestenrot.cz>

Odpovědět | Přeposlat

Předmět **RE: bydliště**

Komu [redacted]

Dobrý večer, máme hodně zabezpečené emaily, můžete do skenu + prosím o PSČ + rodné čísla dětí.
Změním všechny 4 smlouvy.
Děkuji,
PB

-----Original Message-----
From: Tomáš Hála [redacted]
Sent: Thursday, January 11, 2018 8:47 AM
To: Petr Beneš <petr.benes@obchod.wuestenrot.cz>
Subject: Re: bydliště

Dobrý den,
dnes jsem si vyzvedl novou občanku. Stačí vám číslo nebo chcete ten scan? A jestli scan, je možné ho uploadovat nějakou bezpečnou cestou nebo to chcete jen takto do emailu?
S pozdravem Tomáš Hála

Dne 2.1.2018 v 09:13 Petr Beneš napsal(a):

> Dobrý den, pane Hálo, jsem tento týden mimo Prahu, máte nový OP?
>
> Můžete poslat sken?
>
> Budu 8.1.
>
> Děkuji za pochopení,
>
> Petr Beneš

```
$ dig +short MX obchod.wuestenrot.cz
20 antispam2.wia.cz.
10 antispam1.wia.cz.
```

Nezabezpečeno | wia.cz

Tento web používá soubory cookie. Setrváním na těchto stránkách souhlasíte s jejich používáním. Ochrana osobních údajů

WIA | komplexní telekomunikační řešení

GOOGLE APPS AUTHORIZED RESELLER Google

bezdrátové připojení
AirMAX

bezdrátové připojení
WiFi

bezdrátové připojení
5G

pevné připojení
DSL

pevná linka
SIPY

optické připojení
FIBER

WIA DSL

Ještě rychlejší DSL internet

od **339** Kč/měs.

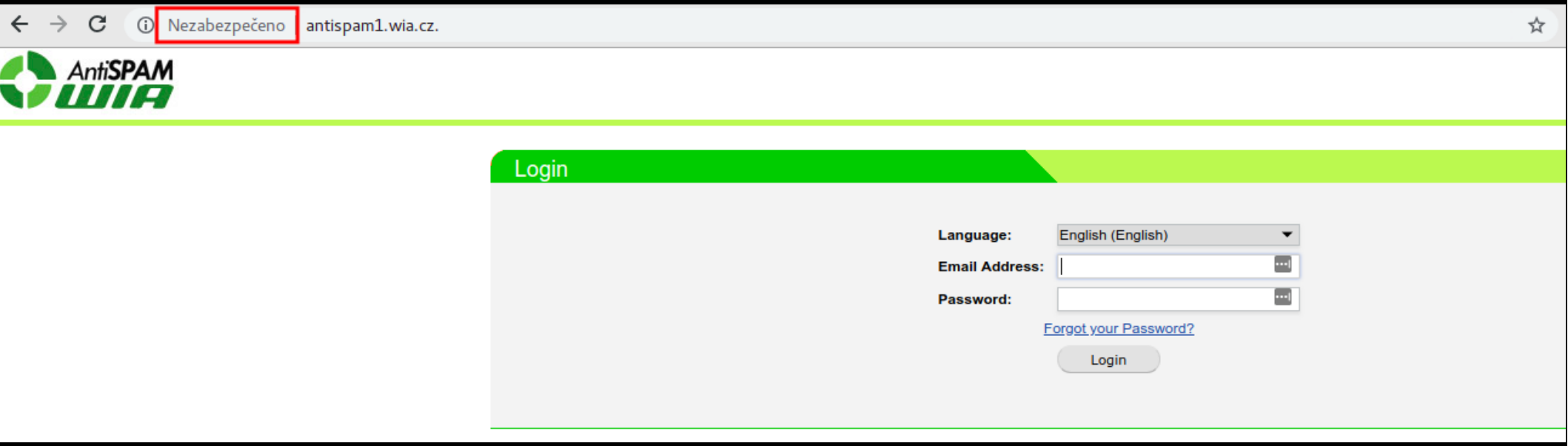
- **Platte rychle a spolehlivě** – kartou nebo online převody. payu
- **Žádné smlouvy ani závazky.**
- **Instalace zdarma.**

Objednávejte na
211 151 211

Více informací

myWIA úvodní stránka profil zákaznický program akce aktuality dokumenty pracovní příležitosti kontakt zjištění IP adresy

WIA WIA FIRMA WIA WiFi WIA 5G WIA AirMAX WIA DSL WIA FIX WIA Fiber WIA BusinessDSL SIPY WIA SafeLAN WIA AntiSPAM


Nezabezpečeno
antispam1.wia.cz.
AntiSPAM WIA
Login
Language:
English (English)
Email Address:
Password:
Forgot your Password?
Login

SSL check results of obchod.wuestenrot.cz

Discover if the mail servers for **obchod.wuestenrot.cz** can be reached through a secure connection.

@ example.com Test mail servers

NEW You can also bulk check multiple servers.

To establish a secure connection a mail server has to offer **STARTTLS** (SSL), a trustworthy **SSL certificate**, support for the Diffie-Hellman-Algorithm to guarantee **Perfect Forward Secrecy** and must not be vulnerable against the **Heartbleed** attack. Futhermore we recommend using end-to-end encryption with GnuPG.

Summary

Report created **Sat, 06 Oct 2018 11:17:18 +0000**

JSON Refresh

Certificates	Protocol	DANE
Problems found	Problems found	Missing

The mailservers of obchod.wuestenrot.cz can be reached through an encrypted connection.

However, we found problems that may affect the security.

Servers

Incoming Mails

These servers are responsible for incoming mails to **@obchod.wuestenrot.cz** addresses.

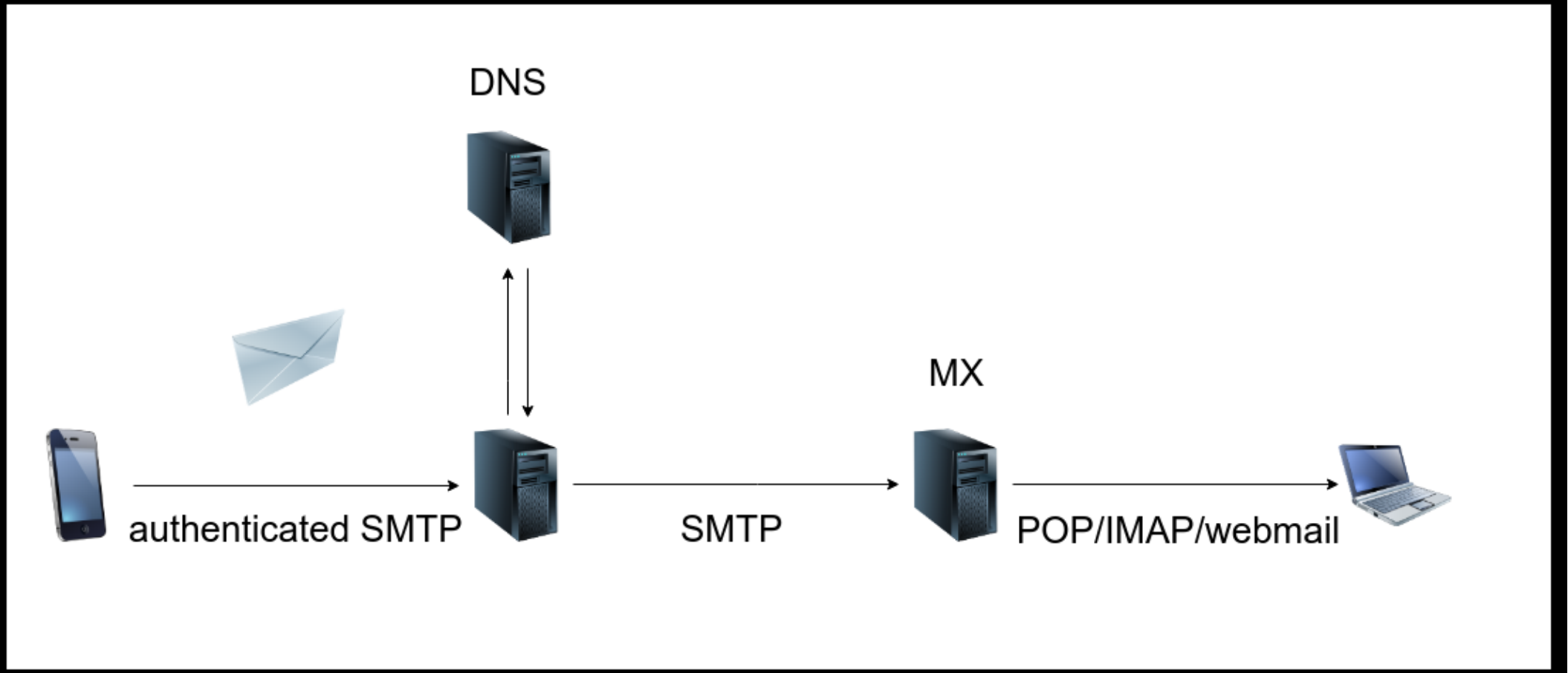
Hostname / IP address	Priority	STARTTLS	Certificates	Protocol			
antispam1.wia.cz 80.250.3.18	10	supported ✔	*.wia.cz ✔	**DANE** **PFS** **Heartbleed** **Weak ciphers**	? missing ✔ supported ✔ not vulnerable ⚠ supported • ECDHE_RSA_WITH_RC4_128_SHA • SSL_RSA_WITH_RC4_128_SHA	TLSv1.2 TLSv1.1 TLSv1.0 SSLv3 ⚠	2 minutes ago 12.0 s
antispam2.wia.cz 31.7.247.78	20	supported ✔	smtp.bpv-bp.com ⚠	**DANE** **PFS** **Heartbleed** **Weak ciphers**	? missing ✔ supported ✔ not vulnerable ⚠ supported • SSL_RSA_EXPORT_WITH_RC4_40_MD5 • SSL_RSA_WITH_RC4_128_SHA	TLSv1.2 TLSv1.1 TLSv1.0 SSLv3 ⚠	2 minutes ago 12.0 s

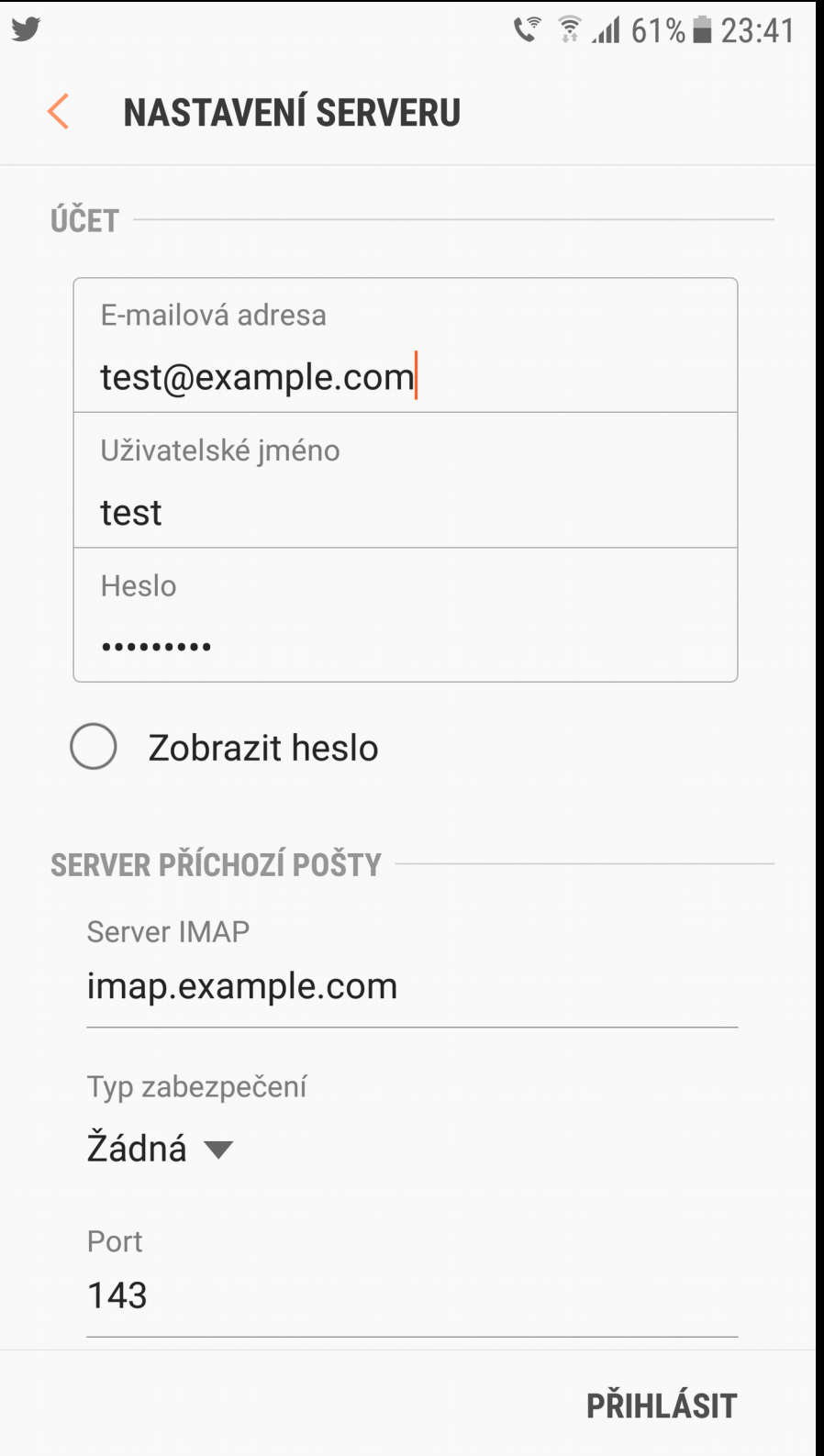
```
host pop3.wia.cz
pop3.wia.cz is an alias for mail2.wia.cz.
mail2.wia.cz has address 80.250.3.10
mail2.wia.cz has IPv6 address 2a01:6400:2:22::2

$ host imap.wia.cz
imap.wia.cz is an alias for mail2.wia.cz.
mail2.wia.cz has address 80.250.3.10
mail2.wia.cz has IPv6 address 2a01:6400:2:22::2
```

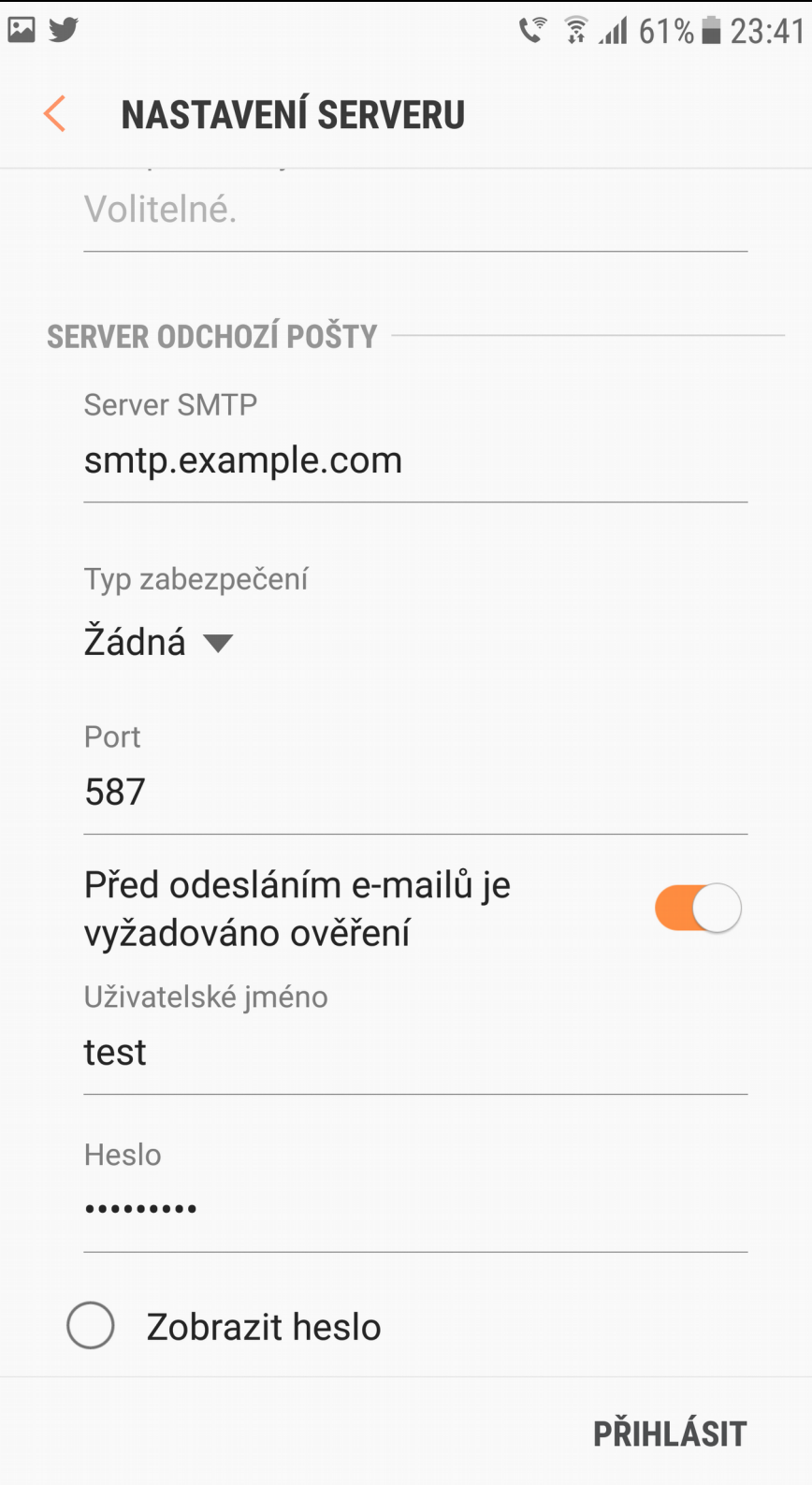
```
$ telnet pop3.wia.cz 110
Trying 2a01:6400:2:22::2...
Connected to mail2.wia.cz.
Escape character is '^]'.
+OK Hello there.
USER test
+OK Password required.
PASS test
-ERR Login failed.
```

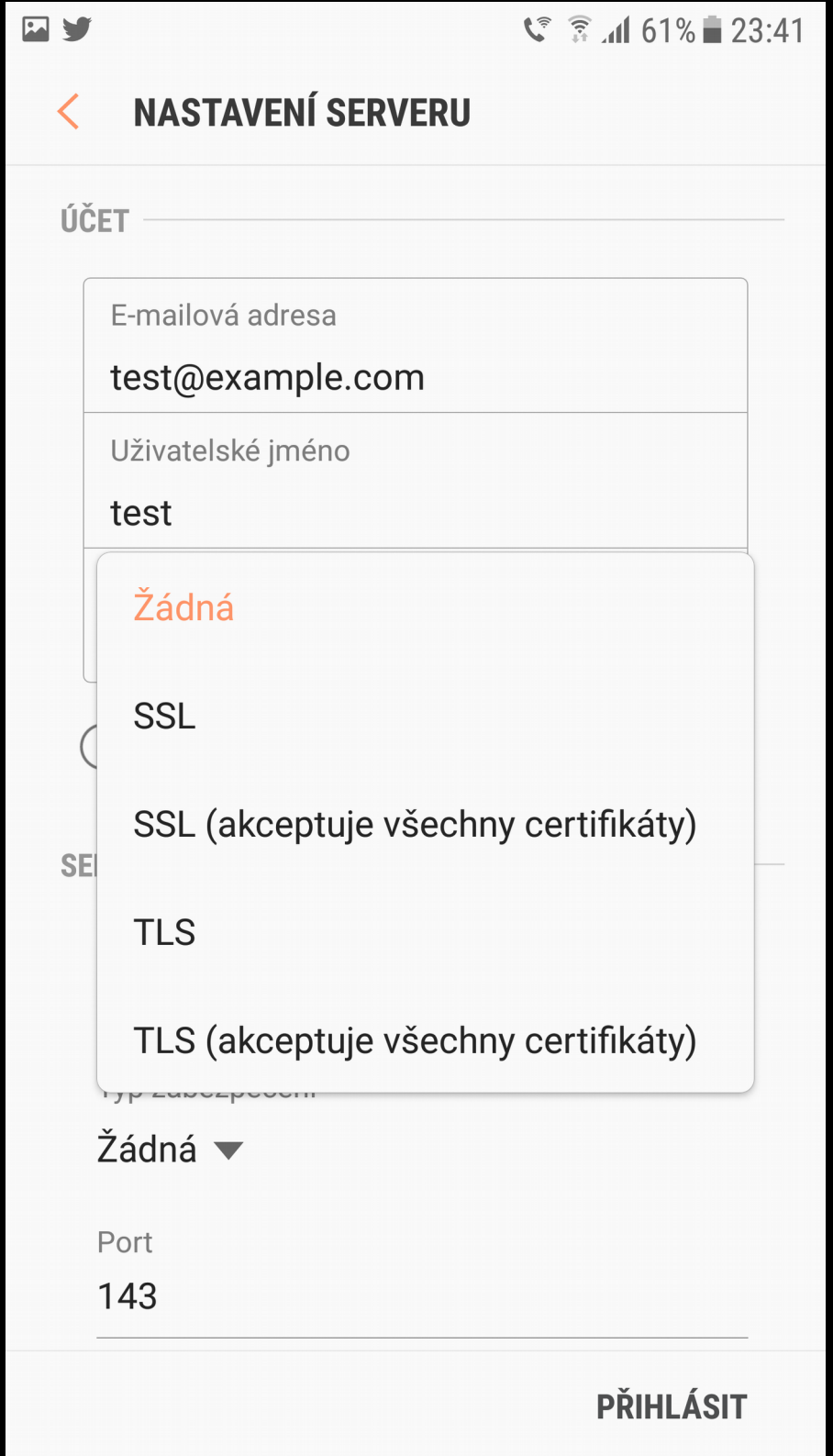
```
$ nmap antispam1.wia.cz

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-06 13:25 CEST
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.85% done; ETC: 13:26 (0:00:54 remaining)
Interesting ports on antispam.wia.cz (80.250.3.18):
Not shown: 1691 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
199/tcp  open  smux
443/tcp  open  https
5432/tcp open  postgres
```

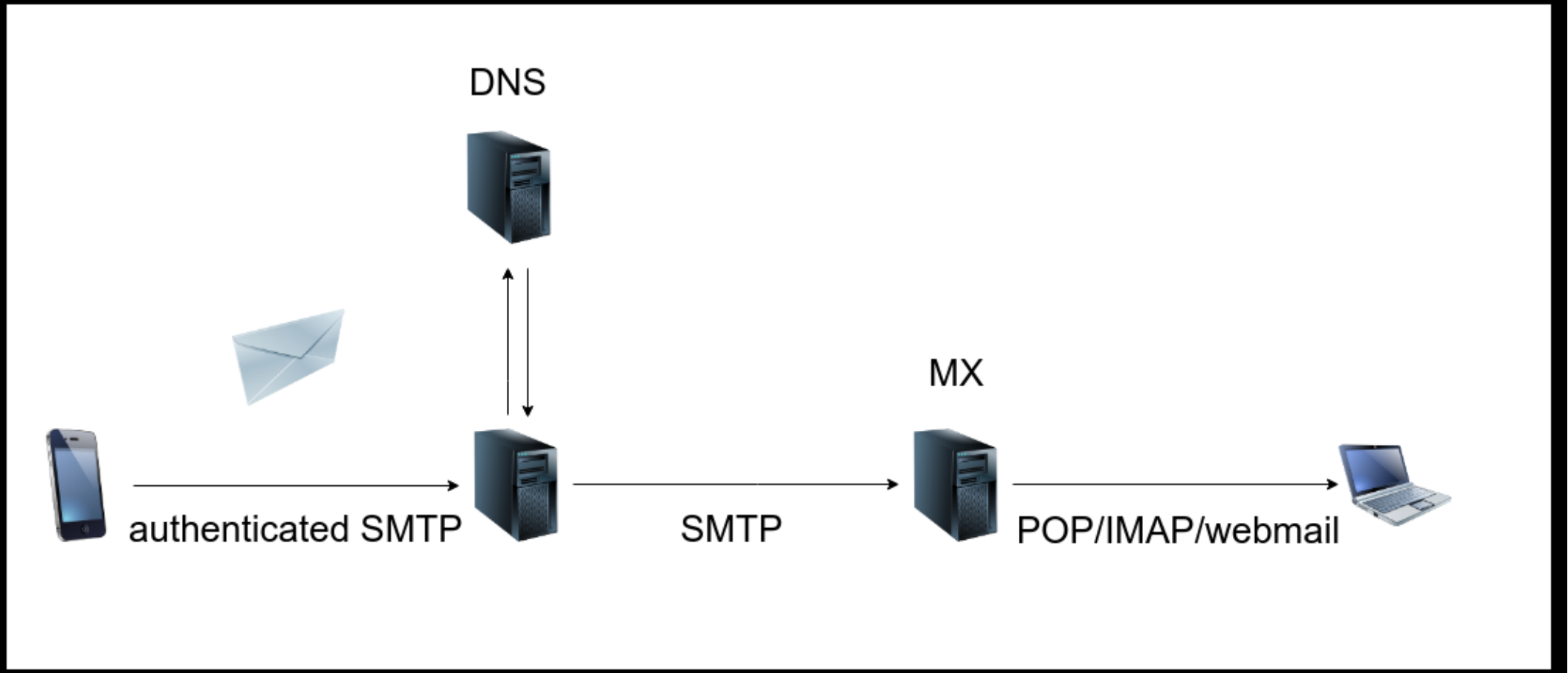
PGP?


DNS
MX
authenticated SMTP
SMTP
POP/IMAP/webmail


61% 23:41
NASTAVENÍ SERVERU
ÚČET
E-mailová adresa
test@example.com
Uživatelské jméno
test
Heslo
•••••••••
Zobrazit heslo
SERVER PŘÍCHOZÍ POŠTY
Server IMAP
imap.example.com
Typ zabezpečení
Žádná
Port
143
PŘIHLÁSIT


61% 23:41
NASTAVENÍ SERVERU
Volitelné.
SERVER ODCHOZÍ POŠTY
Server SMTP
smtp.example.com
Typ zabezpečení
Žádná
Port
587
Před odesláním e-mailů je vyžadováno ověření
Uživatelské jméno
test
Heslo
Zobrazit heslo
PŘIHLÁSIT


61% 23:41
NASTAVENÍ SERVERU
ÚČET
E-mailová adresa
test@example.com
Uživatelské jméno
test
Žádná
SSL
SSL (akceptuje všechny certifikáty)
TLS
TLS (akceptuje všechny certifikáty)
Žádná
Port
143
PŘIHLÁSIT


DNS
MX
authenticated SMTP
SMTP
POP/IMAP/webmail

Root.cz - 2015

Root.cz » Bezpečnost » Bezpečnější předávání pošty s TLSA záznamy

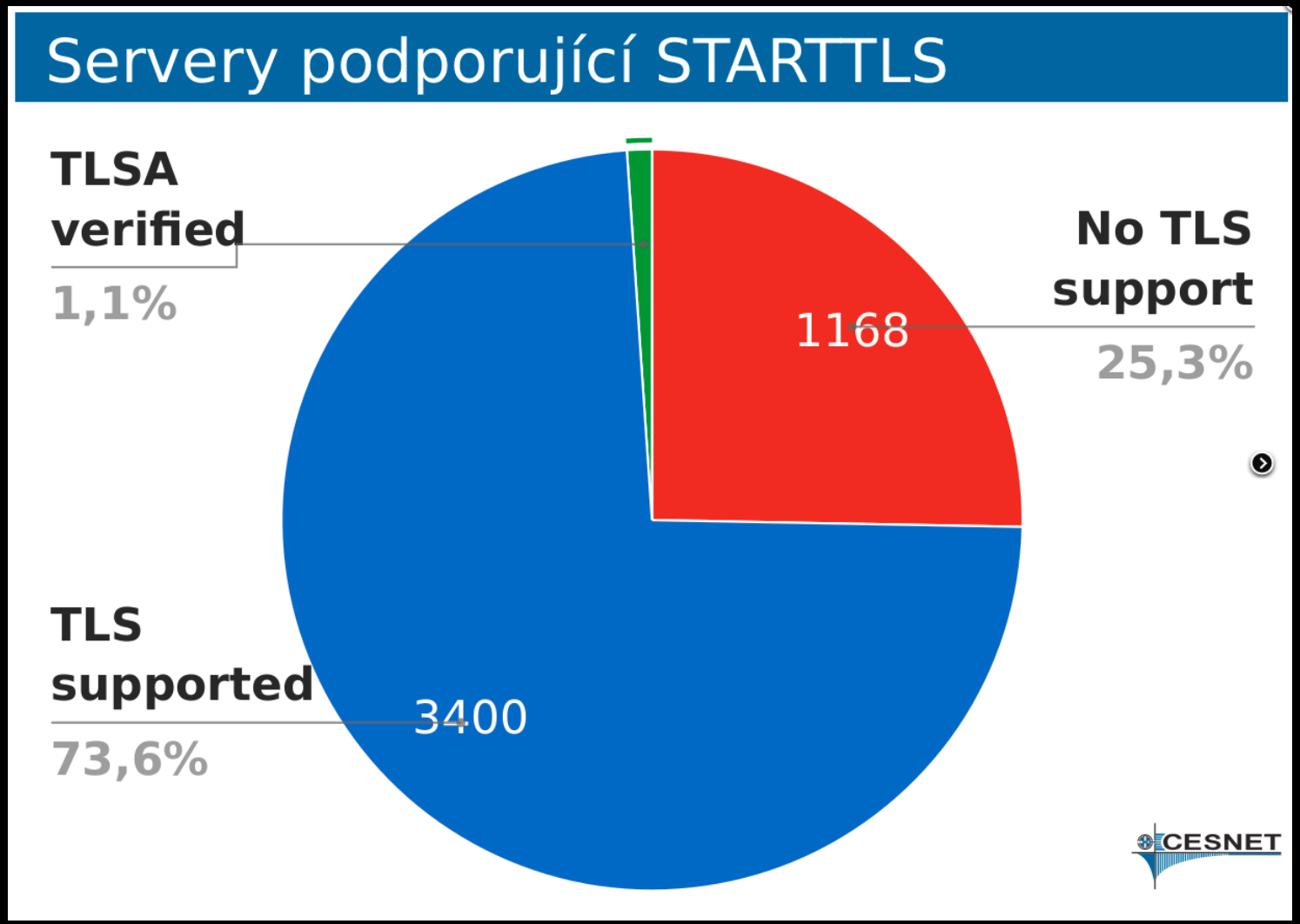
Bezpečnější předávání pošty s TLSA záznamy

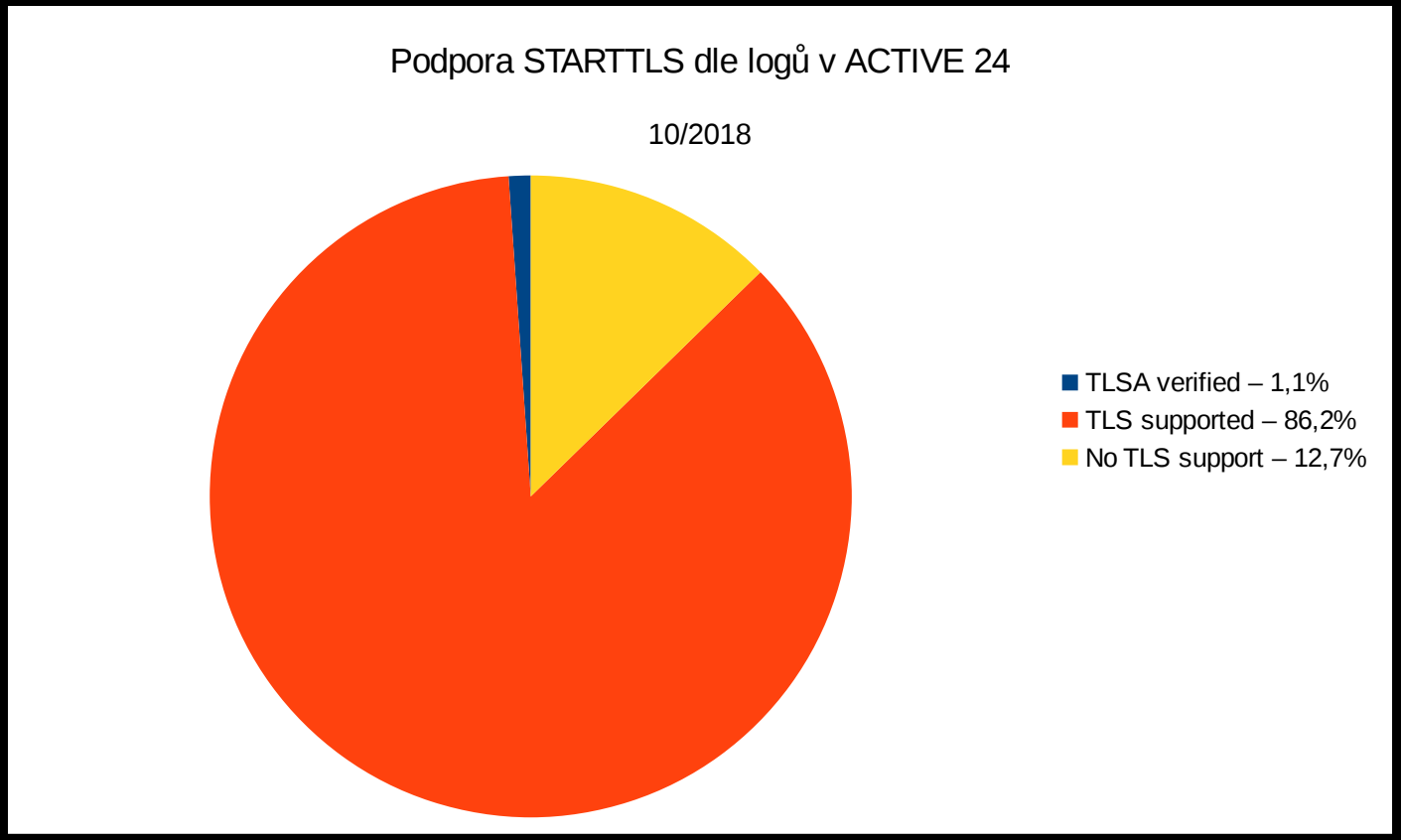
20. 11. 2015

DNS záznam typu TLSA má za úkol zlepšit práci s TLS certifikáty a nabídnout alternativní kanál k jejich dalšímu ověření. Přestože se zatím v HTTPS neprosadil, můžeme jej velmi úspěšně nasadit ve spojení se SMTP. Zabezpečíme tím přenosový kanál pro svou poštu, která tak už nebude snadno odposlechnutelná.

Doba čtení: **6 minut**

Root.cz - 2015


Servery podporující STARTTLS
TLSA verified
1,1%
No TLS support
25,3%
1168
TLS supported
73,6%
3400
CESNET


Podpora STARTTLS dle logů v ACTIVE 24
10/2018
TLSA verified – 1,1%
TLS supported – 86,2%
No TLS support – 12,7%

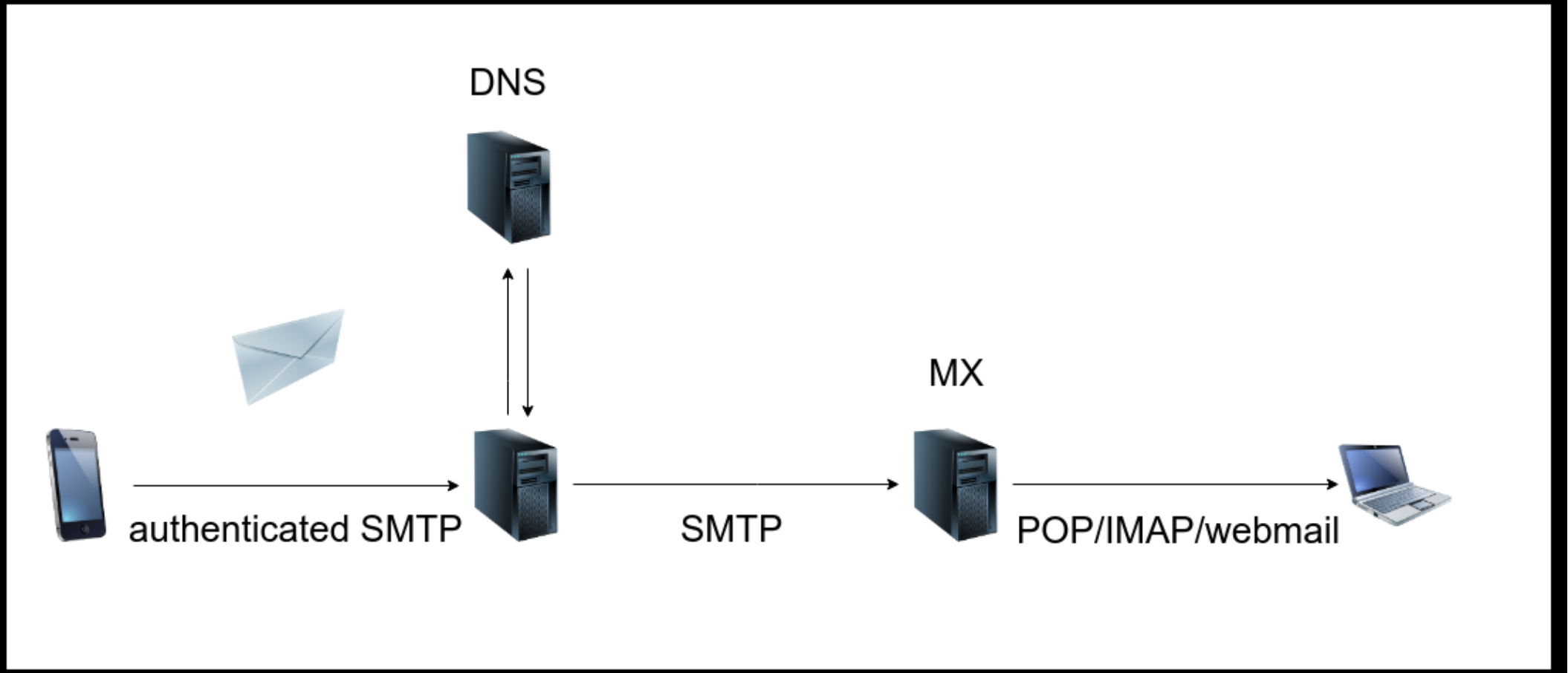
Vaše připojení není soukromé

Útočníci se mohou pokusit odcizit vaše údaje na webu **self-signed.badssl.com** (například hesla, zprávy nebo informace o platebních kartách). Další informace

NET::ERR_CERT_AUTHORITY_INVALID

ROZŠÍŘENÁ NASTAVENÍ

Zpět na bezpečnější stránku


DNS
MX
authenticated SMTP
SMTP
POP/IMAP/webmail

ISPs Removing Their Customers' Email Encryption

TECHNICAL ANALYSIS BY **JACOB HOFFMAN-ANDREWS** | NOVEMBER 11, 2014

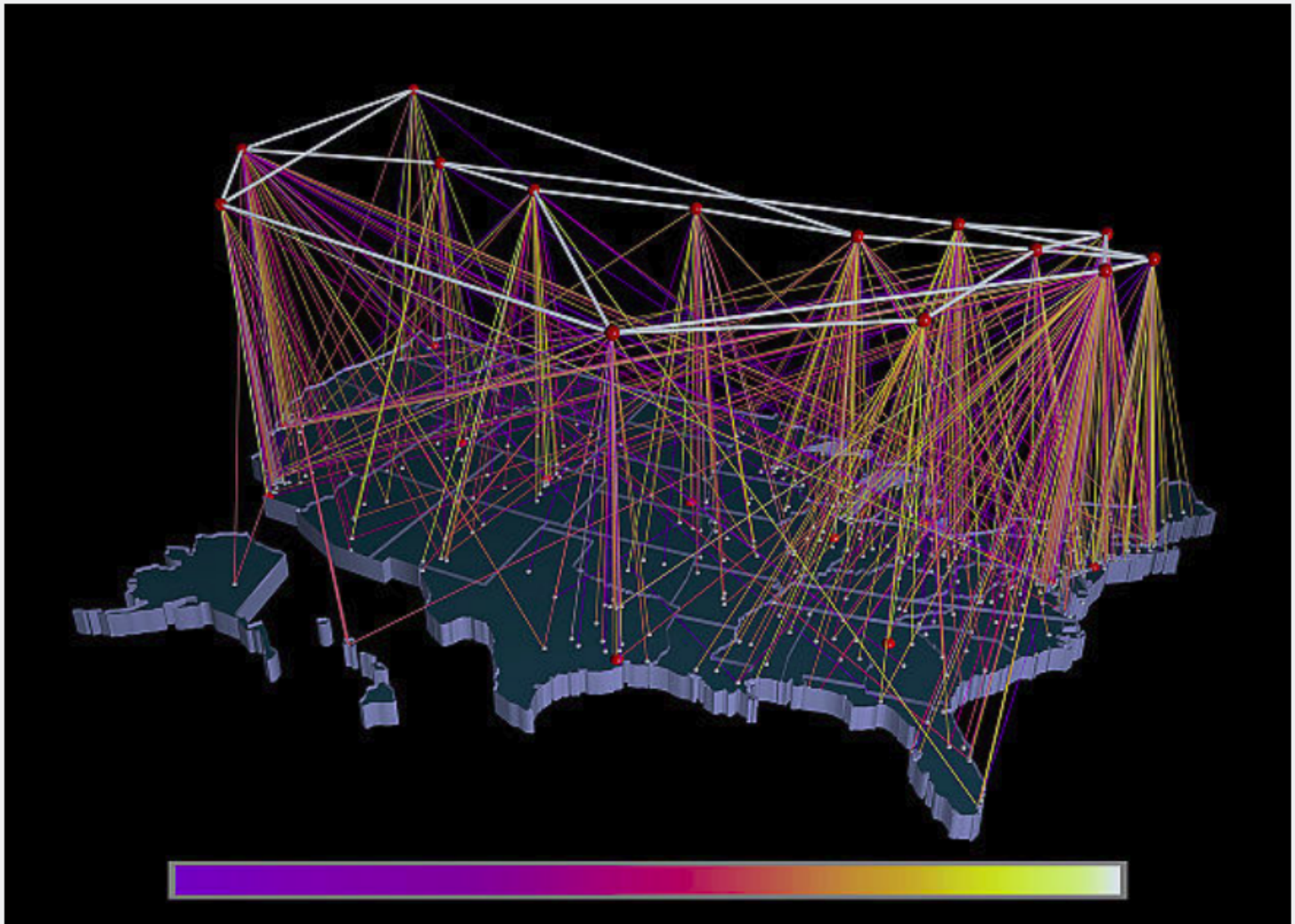
Recently, Verizon was caught tampering with its customer's web requests to inject a tracking super-cookie. Another network-tampering threat to user safety has come to light from other providers: email encryption downgrade attacks. In recent months, researchers have reported ISPs in the US and Thailand intercepting their customers' data to strip a security flag—called STARTTLS—from email traffic. The STARTTLS flag is an essential security and privacy protection used by an email server to request encryption when talking to another server or client.[1]

BIZ & IT —

Repeated attacks hijack huge chunks of Internet traffic, researchers warn

Man-in-the-middle attacks divert data on scale never before seen in the wild.

DAN GOODIN - 11/20/2013, 1:00 PM



kipedia

BGPMON

HOME | AUTONOMOUS SYSTEMS | PREFIXES | ALERTS | PEERMON

My Alerts

Alerts Details

Tools

On Friday October 21st 2016 at 12:08 UTC we detected an announcement for 81.95.96.0/20 (*CZ-ACTIVE24-NET1*) that failed ROA validation.
Validation details: ROA validation failed: Invalid Prefix-Length + Invalid Origin ASN, expected 25234

Alert description: ROA validation failure
Detected Prefix: 81.95.96.0/20
Validation details: ROA validation failed: Invalid Prefix-Length + Invalid Origin ASN, expected 25234

This alert was detected by 1 unique probes in 1 unique countries
Russian Federation: 1 Peers

ROA VALIDATION FAILURE	**AS25234** - 81.95.96.0/20	81.95.96.153/32	AS3267	AS3267	2016-10-21 12:08:23
ROA VALIDATION FAILURE	**AS25234** - 31.15.8.0/21	31.15.12.141/32	AS3267	AS3267	2016-10-21 12:08:23
ROA VALIDATION FAILURE	**AS25234** - 31.15.8.0/21	31.15.12.22/32	AS3267	AS3267	2016-10-21 12:08:23

BGPMON

HOME | AUTONOMOUS SYSTEMS | PREFIXES | ALERTS | PEERMON

My Alerts

Alerts Details

Tools

On Thursday December 24th 2015 at 13:11 UTC we detected an announcement for 81.95.96.0/20 (*CZ-ACTIVE24-NET1*) that failed ROA validation.
Validation details: ROA validation failed: Invalid Prefix-Length + Invalid Origin ASN, expected 25234

Alert description: ROA validation failure
Detected Prefix: 81.95.96.0/20
Validation details: ROA validation failed: Invalid Prefix-Length + Invalid Origin ASN, expected 25234

This alert was detected by 1 unique probes in 1 unique countries
Russian Federation: 1 Peers

Internet Engineering Task Force (IETF)
Request for Comments: 6698
Category: Standards Track
ISSN: 2070-1721

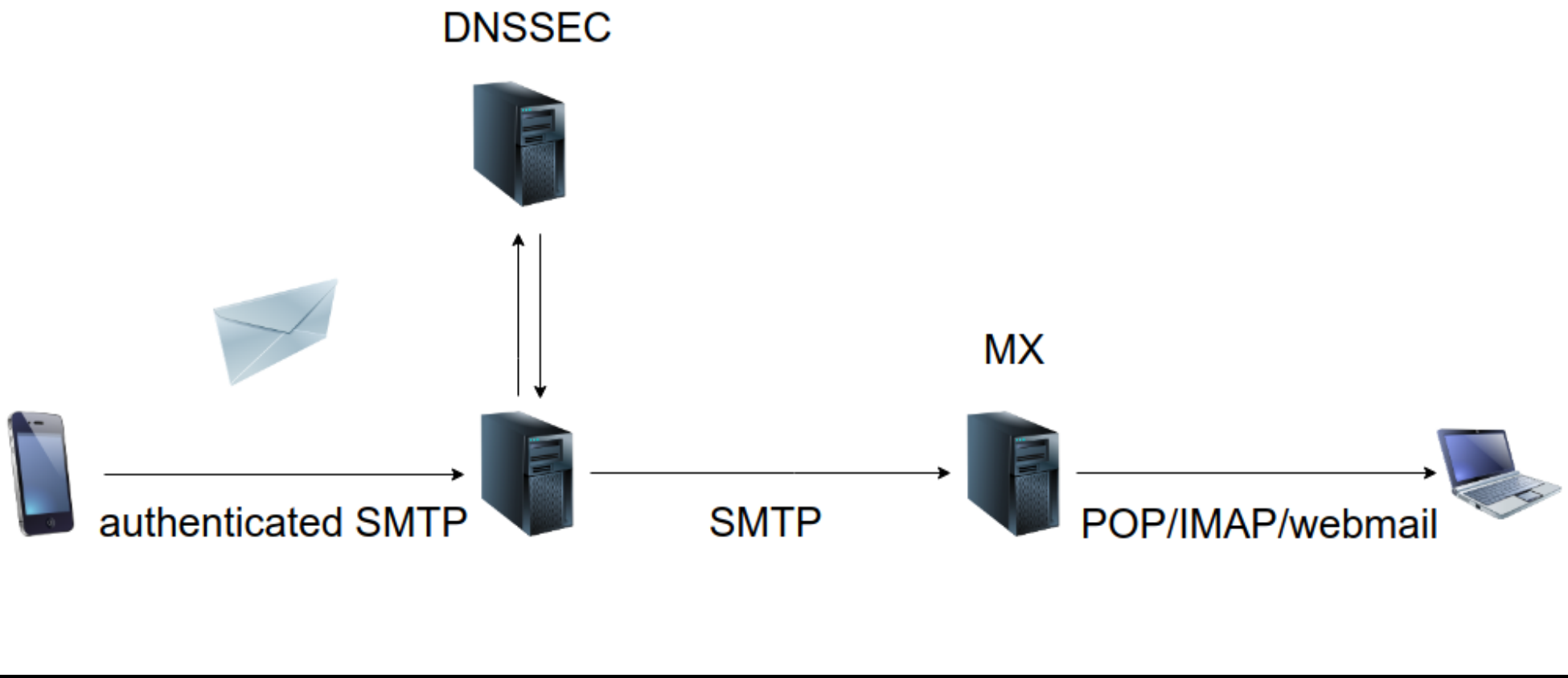
P. Hoffman
VPN Consortium
J. Schlyter
Kirei AB

August 2012

The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA

Abstract

Encrypted communication on the Internet often uses Transport Layer Security (TLS), which depends on third parties to certify the keys used. This document improves on that situation by enabling the administrators of domain names to specify the keys used in that domain's TLS servers. This requires matching improvements in TLS client software, but no change in TLS server software.


DNSSEC
MX
authenticated SMTP
SMTP
POP/IMAP/webmail

Jak nasadit DANE?

Jak nasadit DANE?

1) DNSSEC

2) Certifikát (klidně self-signed) a zapnuté TLS

3) Vygenerovat a zveřejnit TLSA záznam z certifikátu

4) Rotace certfikátu – při změně aktualizovat i TLSA záznam

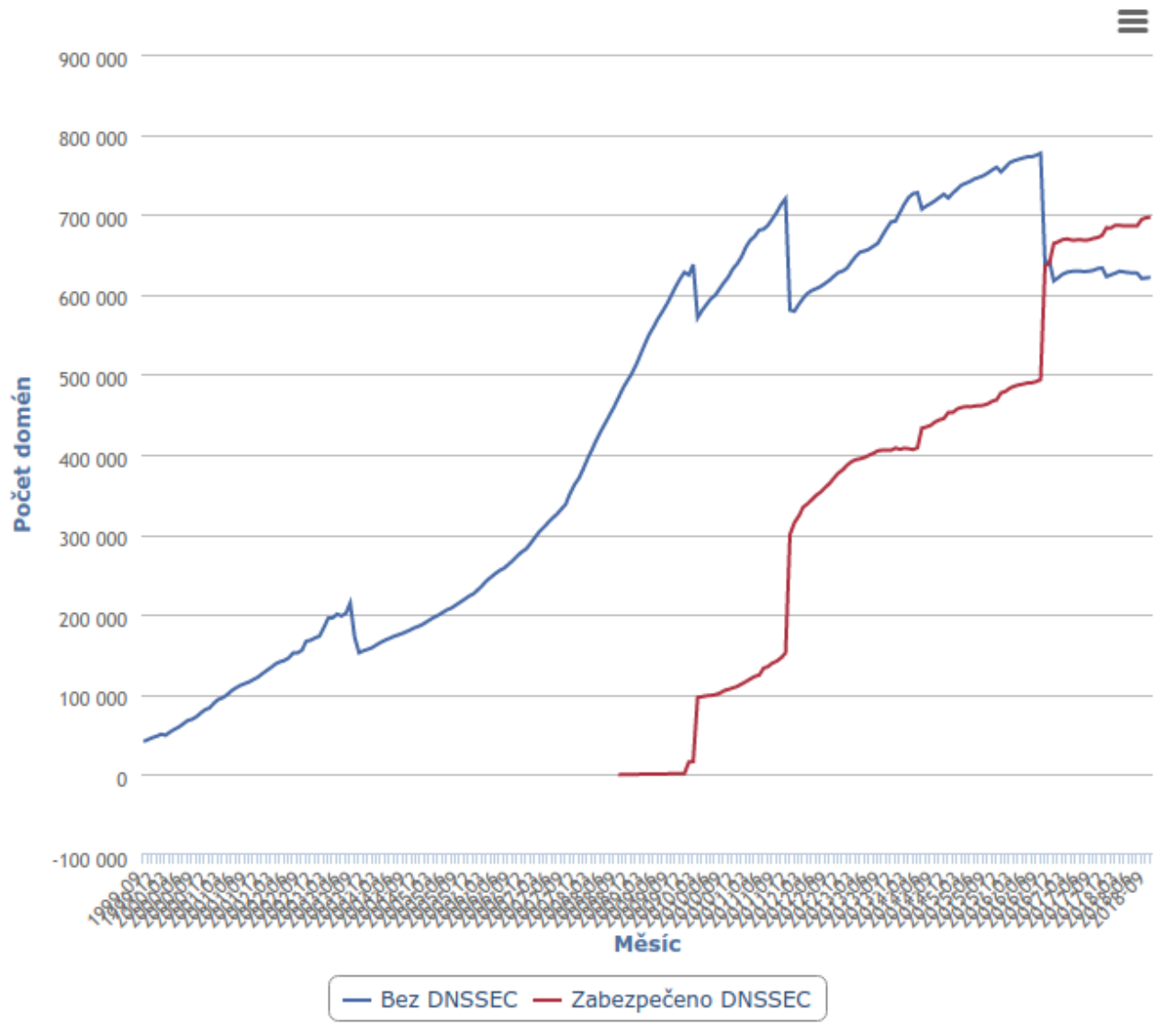
DOMÉNY PODLE DNSSEC

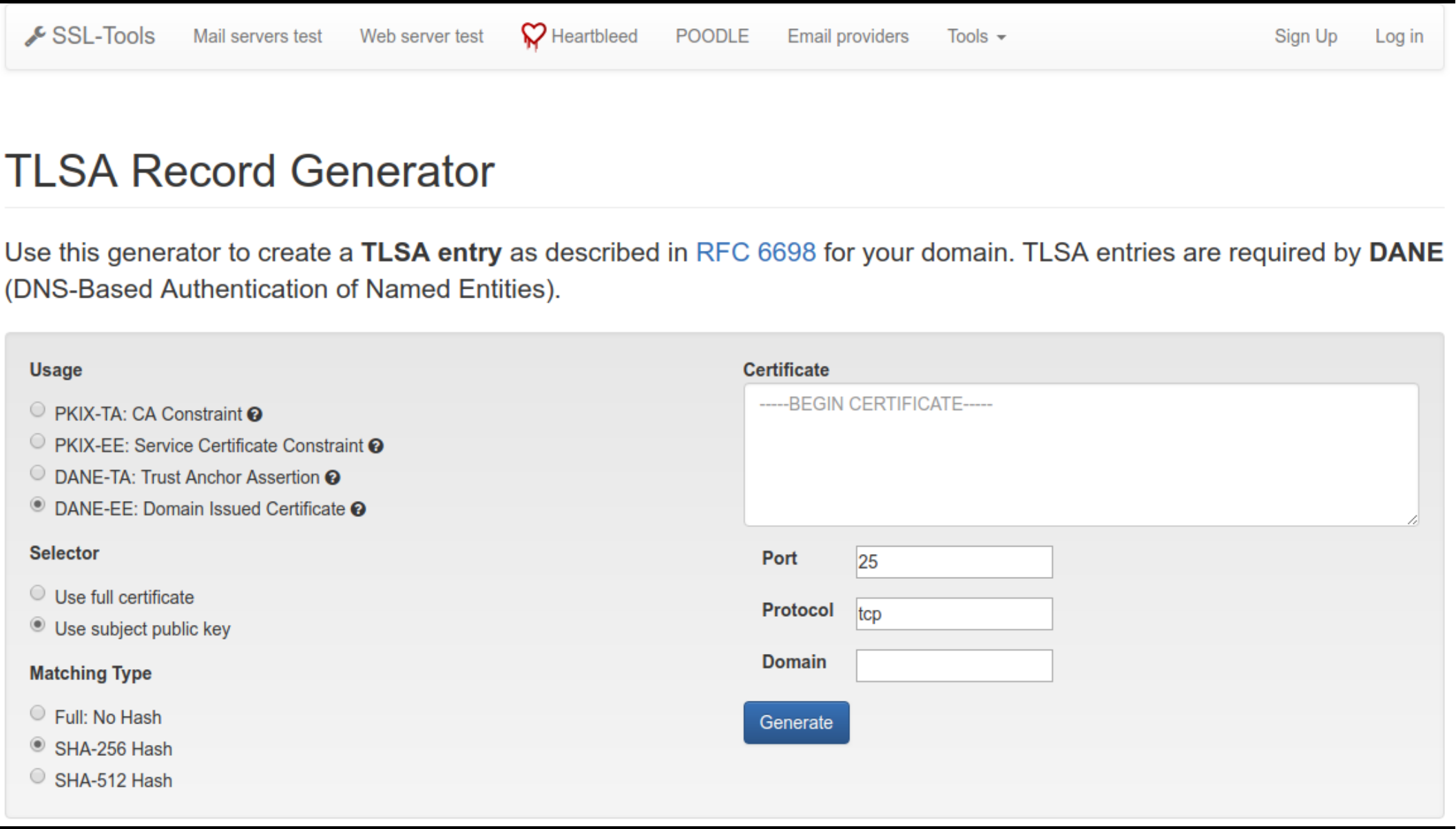
Od 2018-10-04 zpět maximum Zobraz jednotlivé měsíce

Série Vše Škála normální Zobrazit jako graf

Stáhnout CSV Obnovit Odkaz na tuto stránku

OD 1999-09 DO 2018-10

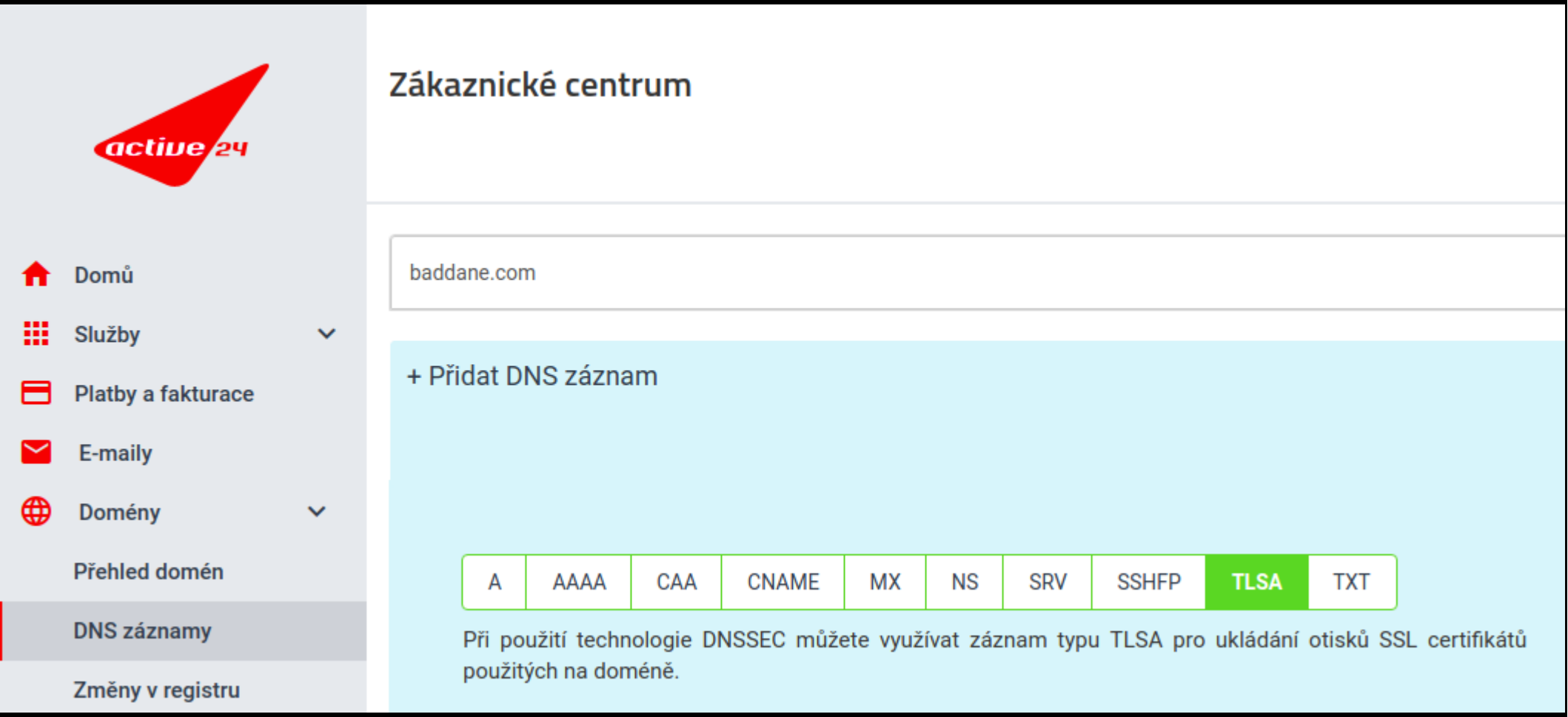




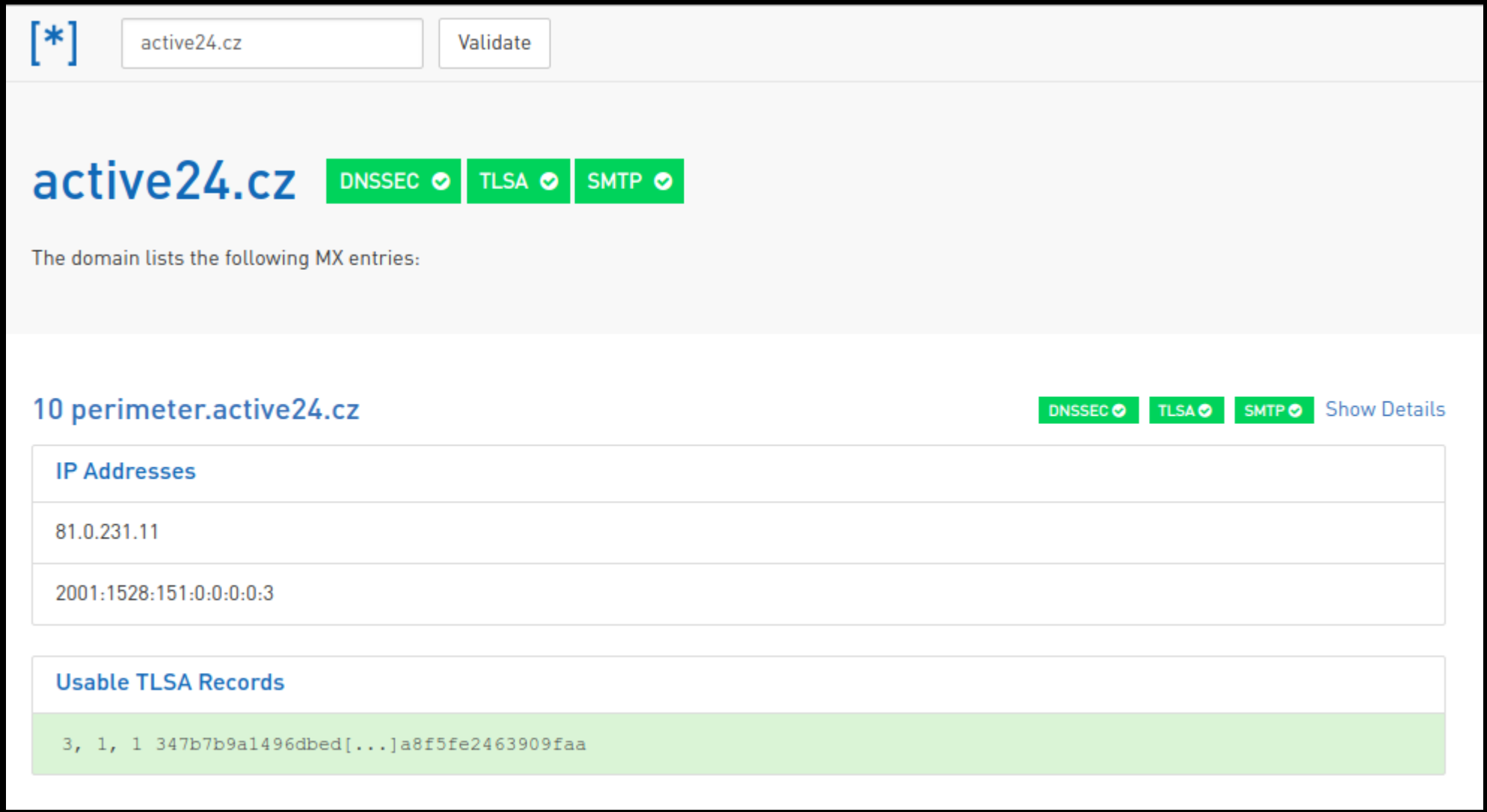
https://ssl-tools.net/tlsa-generator

```
swede create --port 25 --protocol tcp --output rfc --usage 3
--selector 1 --mtype 1 --certificate cert.pem mx1.example.com
```

_25._tcp.mx1.example.com. IN TLSA 3 1 1
510d20e5c47f63cf666b20f61af62bc099a42ac824ffa443a2da7c90b1808a91


Zákaznické centrum
Domů
Služby
Platby a fakturace
E-maily
Domény
Přehled domén
DNS záznamy
Změny v registru
baddane.com
+ Přidat DNS záznam
A
AAAA
CAA
CNAME
MX
NS
SRV
SSHFP
TLSA
TXT
Při použití technologie DNSSEC můžete využívat záznam typu TLSA pro ukládání otisků SSL certifikátů použitých na doméně.

Typ záznamu	Název	TTL	Hodnota
A	**mx1**	3600	IP adresa: 81.95.97.116
A	**mx2**	3600	IP adresa: 81.0.238.28
AAAA	**mx1**	3600	IP adresa: 2a02:4a8:ac24:101::97:116
TLSA	**_25._tcp.mx1**	3600	Certificate usage: 3 Selector: 1 Matching type: 1 Hash: acae1b3b3d2749f4db89d869d014e794404b31864c535bd95fa9255cd599a08d
TLSA	**_25._tcp.mx2**	3600	Certificate usage: 3 Selector: 1 Matching type: 1 Hash: acae1b3b3d2749f4db89d869d014e794404b31864c535bd95fa9255cd599a08d



https://dane.sys4.de/

[*] baddane.com Validate

baddane.com DNSSEC TLSA SMTP

The domain lists the following MX entries:

10 mx1.baddane.com

DNSSEC TLSA SMTP Show Details

All TLSA RRs failed. (See details.)

IP Addresses

81.95.97.116

2a02:4a8:ac24:101:0:0:97:116

Usable TLSA Records

`3, 1, 1 acae1b3b3d2749f4[...]5fa9255cd599a08d` - Hostname mismatch: (62) - Hostname mismatch: (62)

20 mx2.baddane.com

DNSSEC TLSA SMTP Show Details

452 mx2.cesnet.cz
337 mx01.emig.gmx.net
213 mx1.comcast.net
87 mx-ha03.web.de
85 mx1.xs4all.nl
79 mx-ha02.web.de
45 mx00.mail.com
32 mx.transip.email
28 syms.mzv.cz
15 titan.bonicom.cz

[*] mzv.cz Validate

mzv.cz DNSSEC TLSA SMTP

The domain lists the following MX entries:

10 syms.mzv.cz

DNSSEC TLSA SMTP Show Details

IP Addresses

31.130.168.90

Usable TLSA Records

```
3, 0, 1 c3f458316dab3b82[...]0d4e8f8df4ad667d
```

50 syms2.mzv.cz

DNSSEC TLSA SMTP Show Details

IP Addresses

213.175.34.248

2001:4de8:fa43:1:fe01:0:0:95

Usable TLSA Records

```
3, 0, 1 c3f458316dab3b82[...]0d4e8f8df4ad667d
```

Validace DANE

Validace DANE

Postfix:

smtp_tls_security_level = dane

smtp_dns_support_level = dnssec

Validace DANE

Exim:

```
dnssec_request_domains = *
hosts_try_dane  = *
```

2018-10-05_17:44:11 ahop postfix/smtp[30547]: **Verified TLS connection established** to perimeter.active24.cz[2001:1528:151::3]:25: TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)

2018-10-05_17:46:07 perimeter postfix/smtp[12700]: 2A6A142E3D: to=<test@baddane.com>, relay=mx2.baddane.com[81.0.238.28]:25, delay=0.56, delays=0.02/0/0.55/0, dsn=4.7.5, **status=deferred (Server certificate not trusted)**

Vaše připojení není soukromé

Útočníci se mohou pokusit odcizit vaše údaje na webu **subdomain.preloaded-hsts.badssl.com** (například hesla, zprávy nebo informace o platebních kartách). Další informace

NET::ERR_CERT_COMMON_NAME_INVALID

SKRÝT ROZŠÍŘENÉ

Načíst znovu

Web subdomain.preloaded-hsts.badssl.com vaše informace běžně chrání šifrováním. Když se prohlížeč Chrome k webu subdomain.preloaded-hsts.badssl.com pokusil připojit tentokrát, web vrátil neobvyklé a nesprávné identifikační údaje. K tomuto problému může dojít, pokud se za web subdomain.preloaded-hsts.badssl.com pokouší vydávat nějaký útočník nebo pokud bylo připojení přerušeno přihlašovací obrazovkou sítě Wi-Fi. Vaše informace jsou i nadále v bezpečí, protože prohlížeč Google Chrome připojení přerušil dříve, než došlo k odeslání jakýchkoliv dat.

Web subdomain.preloaded-hsts.badssl.com teď nemůžete navštívit, protože používá zabezpečení HSTS. Síťové chyby a útoky jsou obvykle dočasné, tato stránka pravděpodobně později bude fungovat.

Obnova/revokace certifikátu

[*] linuxdays.cz Validate

linuxdays.cz DNSSEC TLSA SMTP Revalidate*

* This is a cached result.

The domain lists the following MX entries:

10 mx.cesnet.cz

DNSSEC TLSA SMTP Show Details

IP Addresses

195.113.161.46

2001:718:1:a100:0:0:161:46

Usable TLSA Records

2, 0, 1 beb8efe9b1a73c84[...]dd7b938d6fe8c5d8

2, 0, 1 be6a0d9e1d115f22[...]a503597993e77a25 - certificate not trusted: (27) - certificate not trusted: (27)

10 mx2.cesnet.cz

DNSSEC TLSA SMTP Show Details

IP Addresses

195.113.144.198

2001:718:1:1:0:0:144:198

Usable TLSA Records

2, 0, 1 beb8efe9b1a73c84[...]dd7b938d6fe8c5d8

2, 0, 1 be6a0d9e1d115f22[...]a503597993e77a25 - certificate not trusted: (27) - certificate not trusted: (27)


BAKALÁŘI

Od Bakaláři - uživatelská podpora <technicka.podpora@bakalari.cz>

Předmět **certifikát**

Komu [redacted]

Dobrý den,

omlouvám se za vzniklé potíže.
Informaci o nedůvěryhodném certifikátu zobrazuje pouze prohlížeč Chrome v.66.
Přikládám nový certifikát, který stačí vyměnit v IIS.
http://napoveda.bakalari.cz/wa_instal_certifikat_w2008.htm?zoom_highlightsub=certi

Případně zavolejte na podporu a pomůžeme Vám certifikát vyměnit.

Přiložený certifikát je zaheslován a heslo je platné s přihlášením do https://skola.bakalari.cz

S pozdravem,
Kamil Kohoutek

BAKALÁŘI

Kamil Kohoutek
oddělení uživatelské podpory

BAKALÁŘI software s.r.o.
tel.: 466 566 981-3
e-mail: podpora@bakalari.cz
www.bakalari.cz

Nápovědu k systému Bakaláři najdete na napoveda.bakalari.cz

1 příloha: bakalari_wildcard_3899.pfx 5,6 KB

Od Bakaláři - uživatelská podpora <technicka.podpora@bakalari.cz>

Předmět **certifikát**

Komu [redacted]

Dobrý den,

omlouvám se za vzniklé potíže.
Informaci o nedůvěryhodném certifikátu zobrazuje pouze prohlížeč Chrome v.66.
Přikládám nový certifikát, který stačí vyměnit v IIS.
http://napoveda.bakalari.cz/wa_instal_certifikat_w2008.htm?zoom_highlightsub=certi

Případně zavolejte na podporu a pomůžeme Vám certifikát vyměnit.

Přiložený certifikát je zaheslován a heslo je platné s přihlášením do https://skola.bakalari.cz

S pozdravem,
Kamil Kohoutek

BAKALÁŘI

Kamil Kohoutek
oddělení uživatelské podpory

BAKALÁŘI software s.r.o.
tel.: 466 566 981-3
e-mail: podpora@bakalari.cz
www.bakalari.cz

Nápovědu k systému Bakaláři najdete na napoveda.bakalari.cz

1 příloha bakalari_wildcard_3899.pfx 5,6 KB


[*]
gmail.com
Validate
gmail.com
DNSSEC
TLSA
SMTP
DNSSEC: Insecure Domain.

Internet Engineering Task Force (IETF)
Request for Comments: 8461
Category: Standards Track
ISSN: 2070-1721

D. Margolis
M. Risher
Google, Inc.
B. Ramakrishnan
Oath, Inc.
A. Brotman
Comcast, Inc.
J. Jones
Microsoft, Inc.

September 2018

SMTP MTA Strict Transport Security (MTA-STS)

Abstract

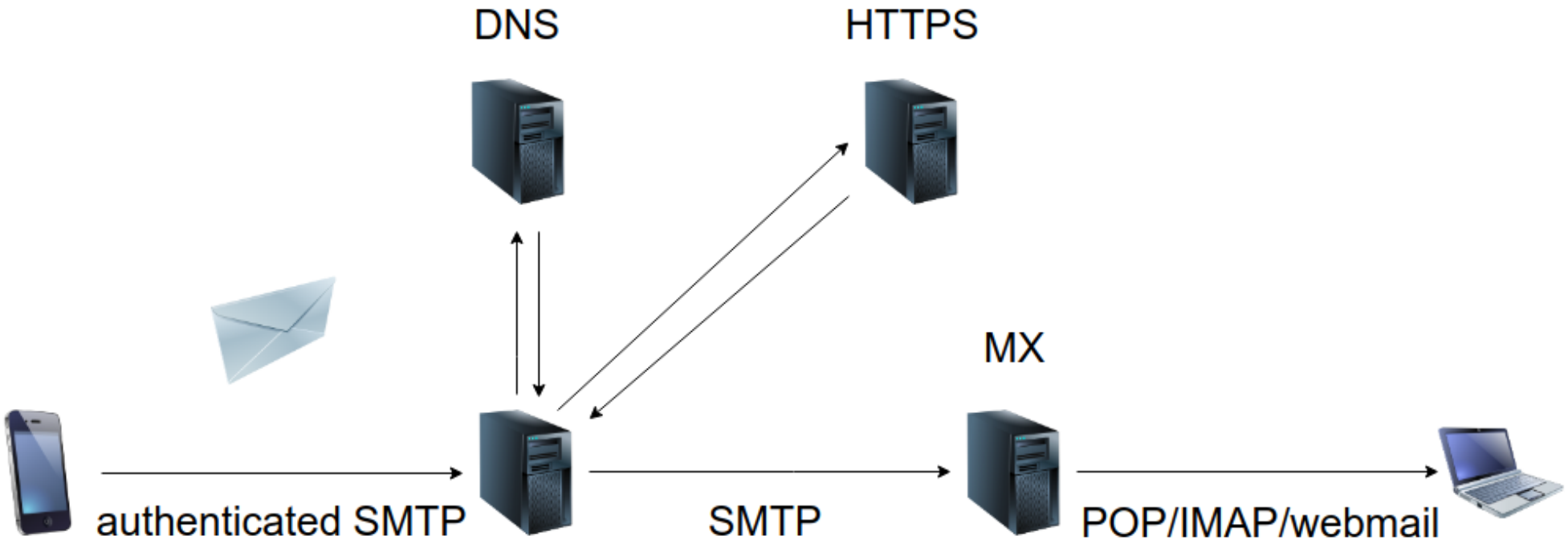
SMTP MTA Strict Transport Security (MTA-STS) is a mechanism enabling mail service providers (SPs) to declare their ability to receive Transport Layer Security (TLS) secure SMTP connections and to specify whether sending SMTP servers should refuse to deliver to MX hosts that do not offer TLS with a trusted server certificate.

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. However, MTA-STS is designed not to interfere with DANE deployments when the two overlap; in particular, senders who implement MTA-STS validation MUST NOT allow MTA-STS Policy validation to override a failing DANE validation.


Our e-mails can be forged due to lack of trust in the DNS! Any ideas how to fix it?
Deploy policy file on some HTTPS URL, make everybody cache and refresh it regularly and then filter DNS results by that!
Add another DNS record to signal that DNS cannot be trusted!
Fix the trust in the DNS by deploying DNSSEC?
imgflip.com

MTA-STS - princip

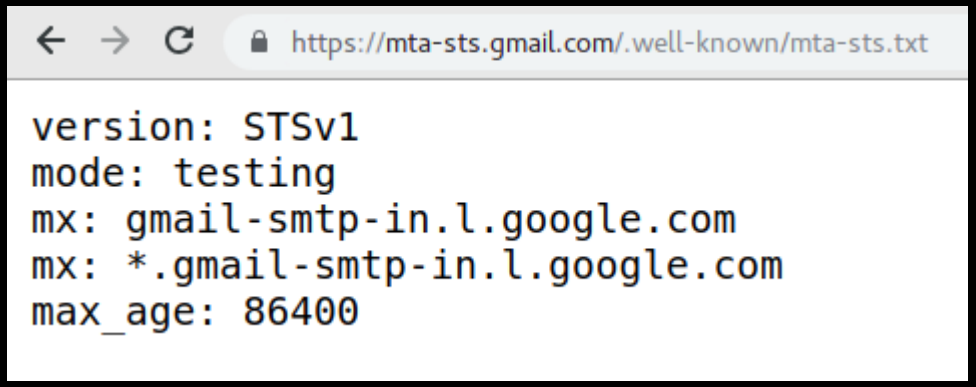
1) Signalizuje politiku přes nespolehlivé DNS a HTTPS
2) Spojení pak ověřuje přes PKI.
3) Získanou policy cacheuje

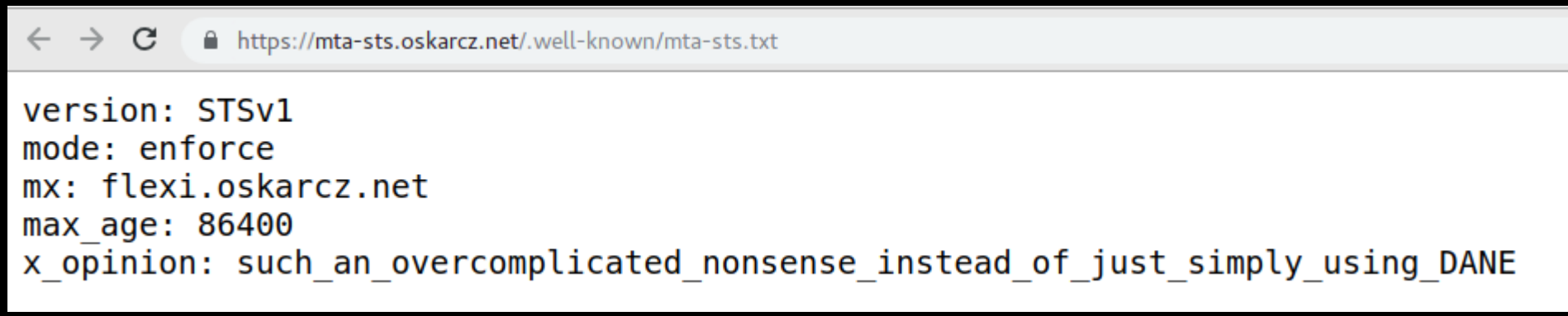

DNS
HTTPS
MX
authenticated SMTP
SMTP
POP/IMAP/webmail

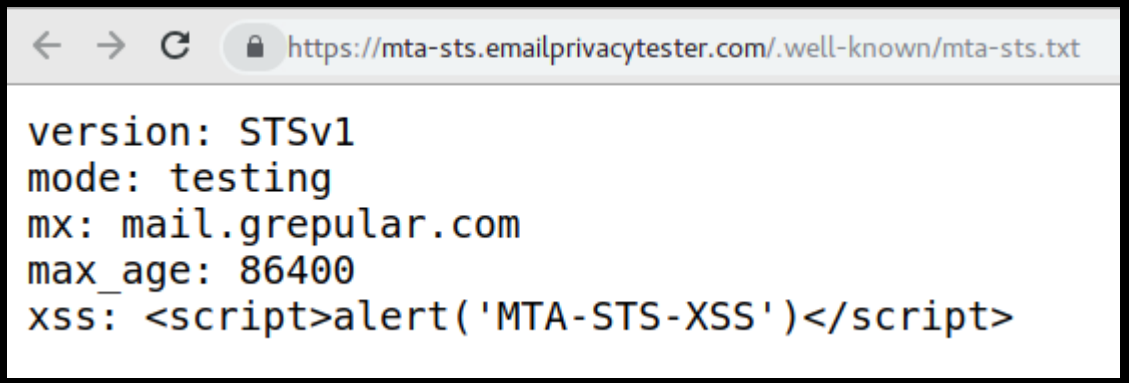
Jak nasadit MTA-STS

1) Spustit HTTPS server na mta-sts.example.com
2) Publikovat policy pod URL /.well-known/mta-sts.txt
3) Publikovat TXT DNS záznam

```
version: STSv1
mode: testing
mx: mx1.example.com
mx: mx2.example.com
mx: mx.backup-example.com
max_age: 1296000
```


https://mta-sts.gmail.com/.well-known/mta-sts.txt
version: STSv1
mode: testing
mx: gmail-smtp-in.l.google.com
mx: *.gmail-smtp-in.l.google.com
max_age: 86400


https://mta-sts.oskarcz.net/.well-known/mta-sts.txt
version: STSv1
mode: enforce
mx: flexi.oskarcz.net
max_age: 86400
x_opinion: such_an_overcomplicated_nonsense_instead_of_just_simply_using_DANE


https://mta-sts.emailprivacytester.com/.well-known/mta-sts.txt
version: STSv1
mode: testing
mx: mail.grepular.com
max_age: 86400
xss: <script>alert('MTA-STS-XSS')</script>

```
_mta-sts.example.com.  IN TXT "v=STSv1; id=20160831085700Z;"
```

MTA-STS - validace

For example (mode: testing, means there's little security from this
at present):

```
$ curl https://mta-sts.gmail.com/.well-known/mta-sts.txt
version: STSv1
mode: testing
mx: gmail-smtp-in.l.google.com
mx: .gmail-smtp-in.l.google.com
max_age: 86400
```

would translate (via a suitable cron job to update the table) into:

```
tls-policy:
   gmail.com secure match=gmail-smtp-in.l.google.com:.gmail-smtp-in.l.google.com
```

assuming one also has something along the lines of:

```
main.cf:
  indexed = ${default_database_type}:${config_directory}/
  smtp_tls_policy_maps = ${indexed}tls-policy
  smtp_tls_CApath = ... c_rehash'ed directory with usual WebPKI roots ...
```

and provided one is bold enough to ignore "testing" and just require
working TLS authentication.

--
Viktor.

MTA-STS validator

emailprivacytester.com Check!

Summary

Result for: **emailprivacytester.com**

MTA-STS ⚠

Warning: make sure the MTA-STS DNS record, the policy file and the mail servers are all set up correctly.

SMTP-TLSRPT ✔

Everything is set up correctly! You should receive reports on tlsrpt@grepular.com, as soon as mail senders start sending them.

Details

✔ MTA-STS TXT record

Policy: `v=STSv1; id=2018062702; xss=<script>alert('MTA-STS-XSS')</script>;`

✔ SMTP-TLSRPT TXT record

Policy: `v=TLSRPTv1;rua=mailto:tlsrpt@grepular.com`

⚠ Policy file

Policy: https://mta-sts.emailprivacytester.com/.well-known/mta-sts.txt

```
version: STSv1
mode: testing
mx: mail.grepular.com
max_age: 86400
xss: <script>alert('MTA-STS-XSS')</script>
```

https://aykevl.nl/apps/mta-sts/

MTA-STS vs. DANE

MTA-STS

- nevyžaduje DNSSEC

- potřebujete webserver pro doručování pošty

- extra DNS záznam pro každou doménu

- extra validní certifikát pro každou doménu

- chrání vás až při opakovaném pokusu o doručení emailu

- vyžaduje pravidelné aktualizace CA certifikátů na mailserverech

- podporu implementují velcí hráči v čele s Google

DANE

- vyžaduje DNSSEC

- vystačí se self-signed certifikátem

- přidáním TLSA záznamu k MX zabezpečíte všechny domény, které tyto MX používají (a mají aktivní DNSSEC)

- nepotřebujete zasahovat do DNS zóny jednotlivých domén

- nepotřebujete webserver

- chrání vás už při prvním pokusu o doručení emailu

- pokrývá 50% DE trhu a začínají ho vyžadovat/doporučovat vlády úřadům

Active24.cz
@active24cz

Sleduji

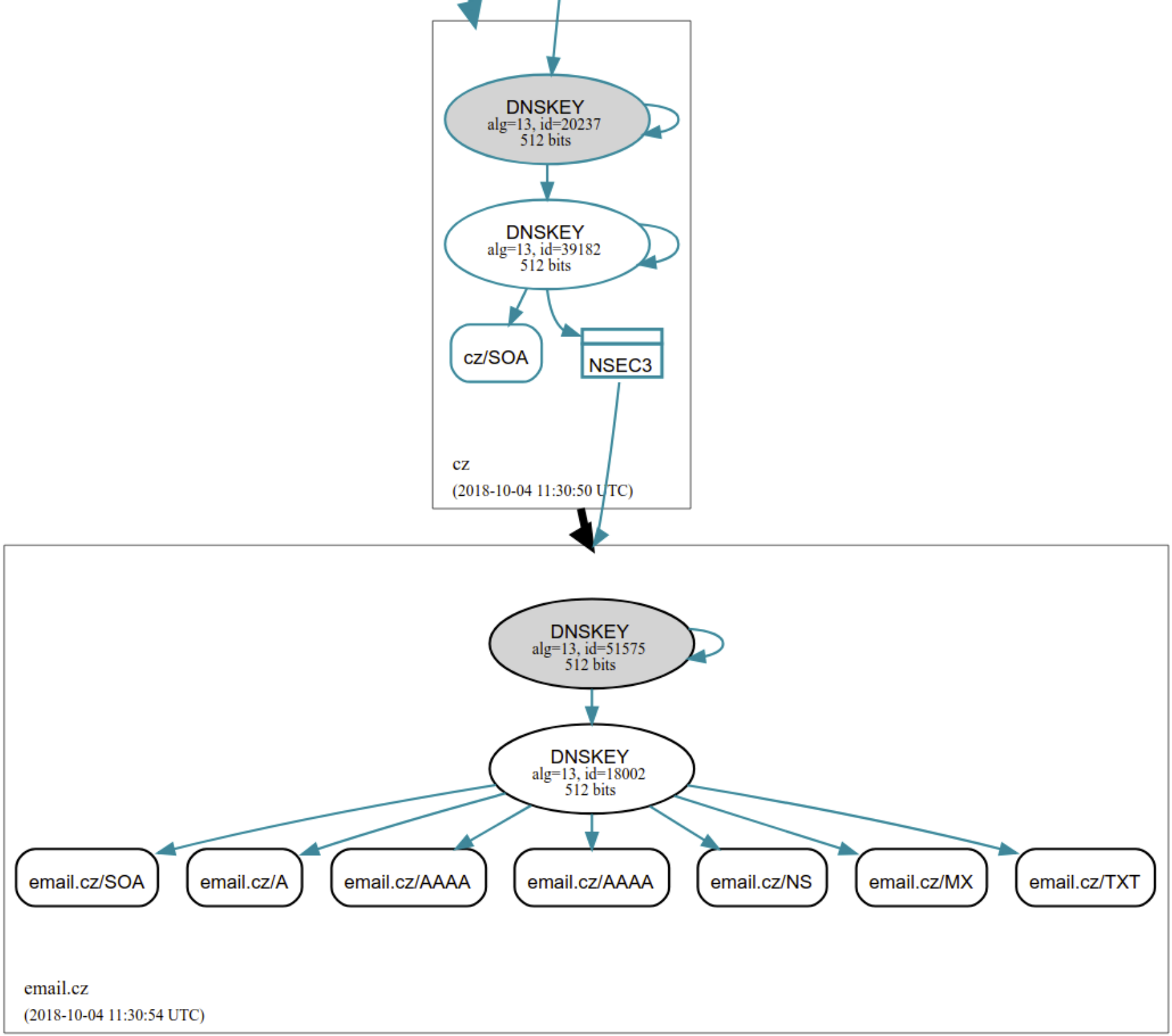
V České republice jsme s nasazením #DANE TLSA zatím osamoceni spolu s akademickým @CESNET_cz. Přitom #DNSSEC má více než polovina .CZ domén, tedy k nasazení je to už jen krůček. Kdo se přidá a pomůže zabezpečit transport pošty v ČR? A nechystá se to @CZ_NIC nějak postrčit? :-)

Internet.nl @internet_nl
Latest survey shows 316,920 domains with correct DANE TLSA records for secure mail transport. Do you DANE? mail.sys4.de/pipermail/dane… #DNSSEC #DANE #mailsecurity

13:01 - 4. 10. 2018

6 retweetů **10** lajků

3 6 10


DNSKEY
alg=13, id=20237
512 bits
DNSKEY
alg=13, id=39182
512 bits
cz/SOA
NSEC3
cz
(2018-10-04 11:30:50 UTC)
DNSKEY
alg=13, id=51575
512 bits
DNSKEY
alg=13, id=18002
512 bits
email.cz/SOA
email.cz/A
email.cz/AAAA
email.cz/AAAA
email.cz/NS
email.cz/MX
email.cz/TXT
email.cz
(2018-10-04 11:30:54 UTC)

protonmail.com

DNSSEC ✓ TLSA ! SMTP !

The domain lists the following MX entries:

5 mail.protonmail.ch

DNSSEC ✓ TLSA ! SMTP ! Show Details

No TLSA records.

Tomáš Hála @tomashala · 21. 5.

Hello @ProtonMail @ProtonMailHelp, I was surprised, that you do not use DANE to prevent interception of communication to your MX hosts. You already have DNSSEC in place, so are there any plans to publish TLSA records to DNS? dane.sys4.de/smtp/protonmai…

Přeložit Tweet

2 1 5

Bart Butler @BartCButler · 21. 5.

We do plan to, it just hasn't gotten to the front the queue yet.

Přeložit Tweet

2 2 3

Viktor Dukhovni @VDukhovni · 1. 9.

90 days have gone by, any change in the plans or the front of the queue?

Přeložit Tweet

1 2 5

Bart Butler
@BartCButler

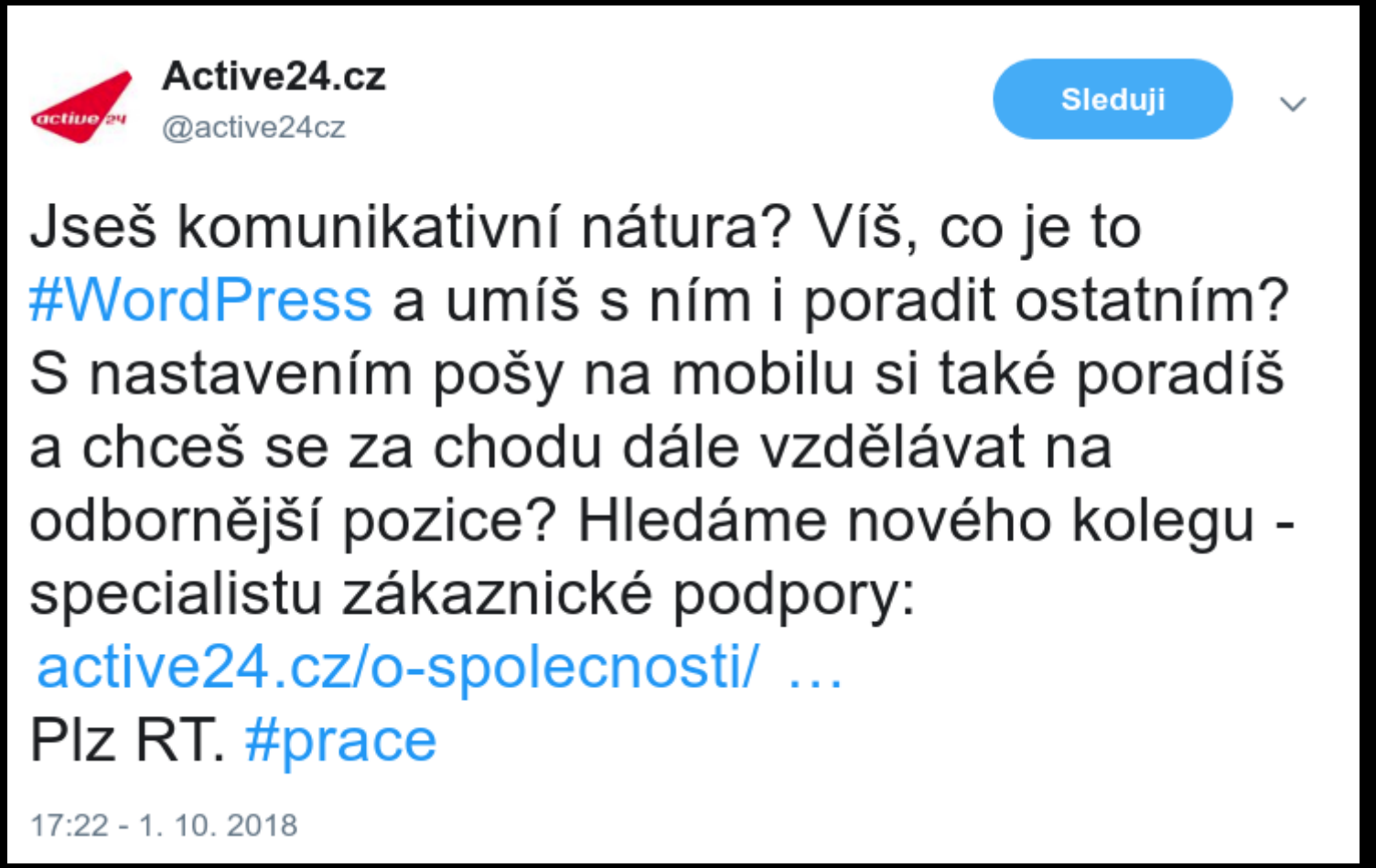
Sledovat

Odpověď uživatelům @VDukhovni @tomashala a 2 dalším uživatelům

Hi Victor, we are refactoring a bunch of our DKIM/DNS code now, once that is done the plan is to use the new system to implement DANE support.

Přeložit Tweet

21:37 - 7. 9. 2018


Active24.cz
@active24cz
Sleduji
Jseš komunikativní nátura? Víš, co je to #WordPress a umíš s ním i poradit ostatním? S nastavením pošy na mobilu si také poradíš a chceš se za chodu dále vzdělávat na odbornější pozice? Hledáme nového kolegu - specialistu zákaznické podpory: active24.cz/o-spolecnosti/ …
Plz RT. #prace
17:22 - 1. 10. 2018

16:00

Hakuna Matata - Account Lifecycle Management

Per Thorsheim

16:00 - 16:50

16:30

EN

Děkuji za pozornost!

www.active24.cz
blog.active24.cz
@active24cz
@tomashala