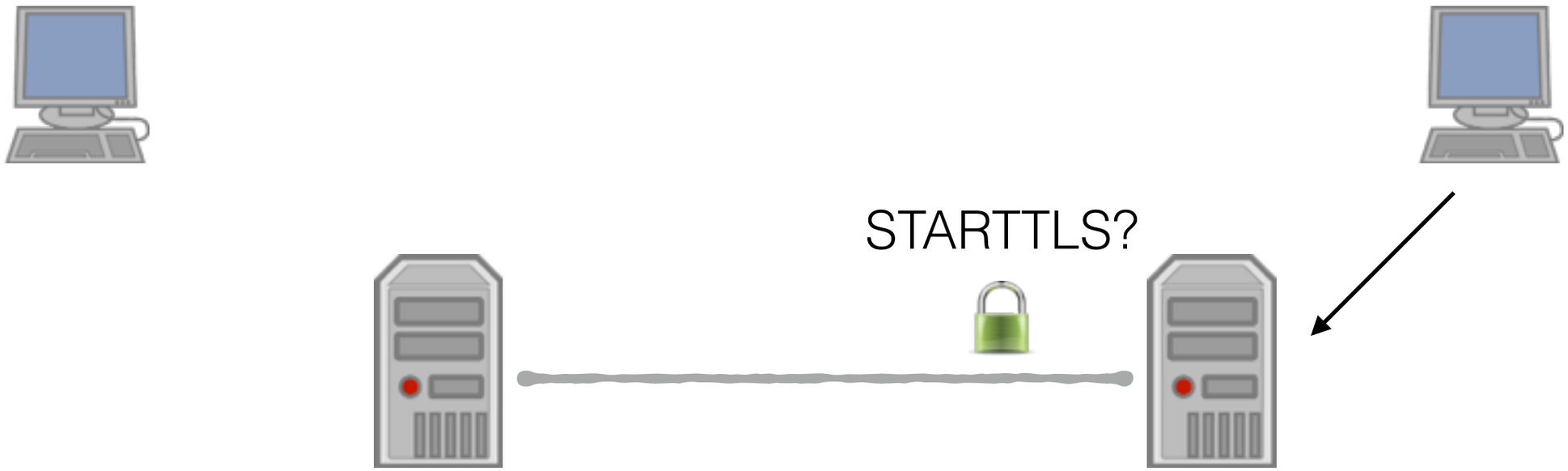
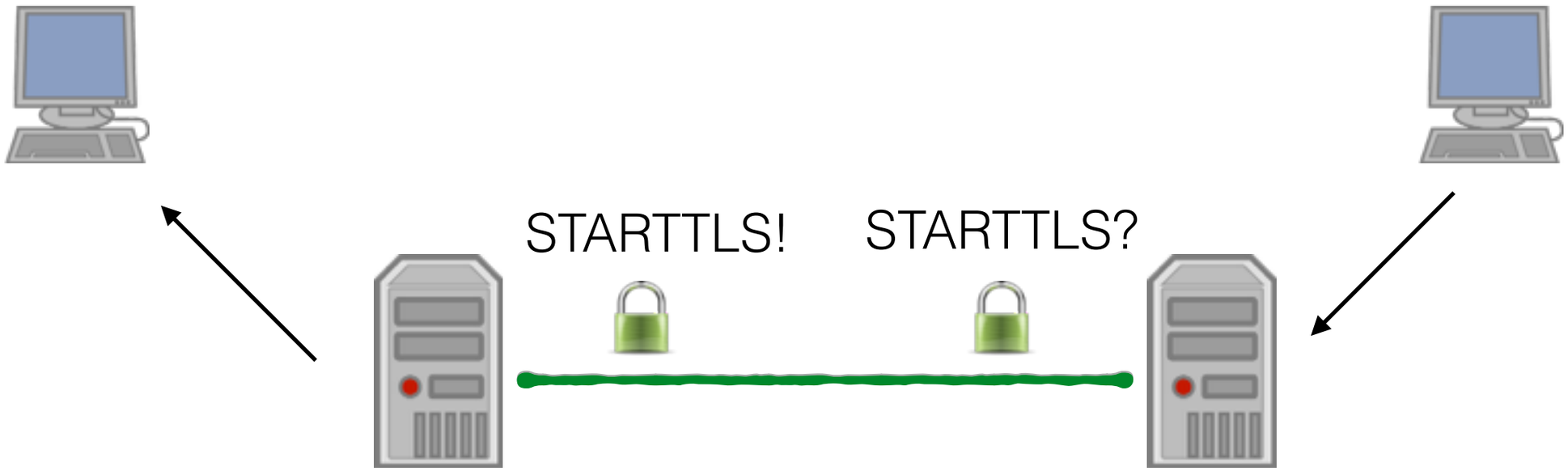
DANEs don't lie

Patrick Ben Koetter
Carsten Strotmann

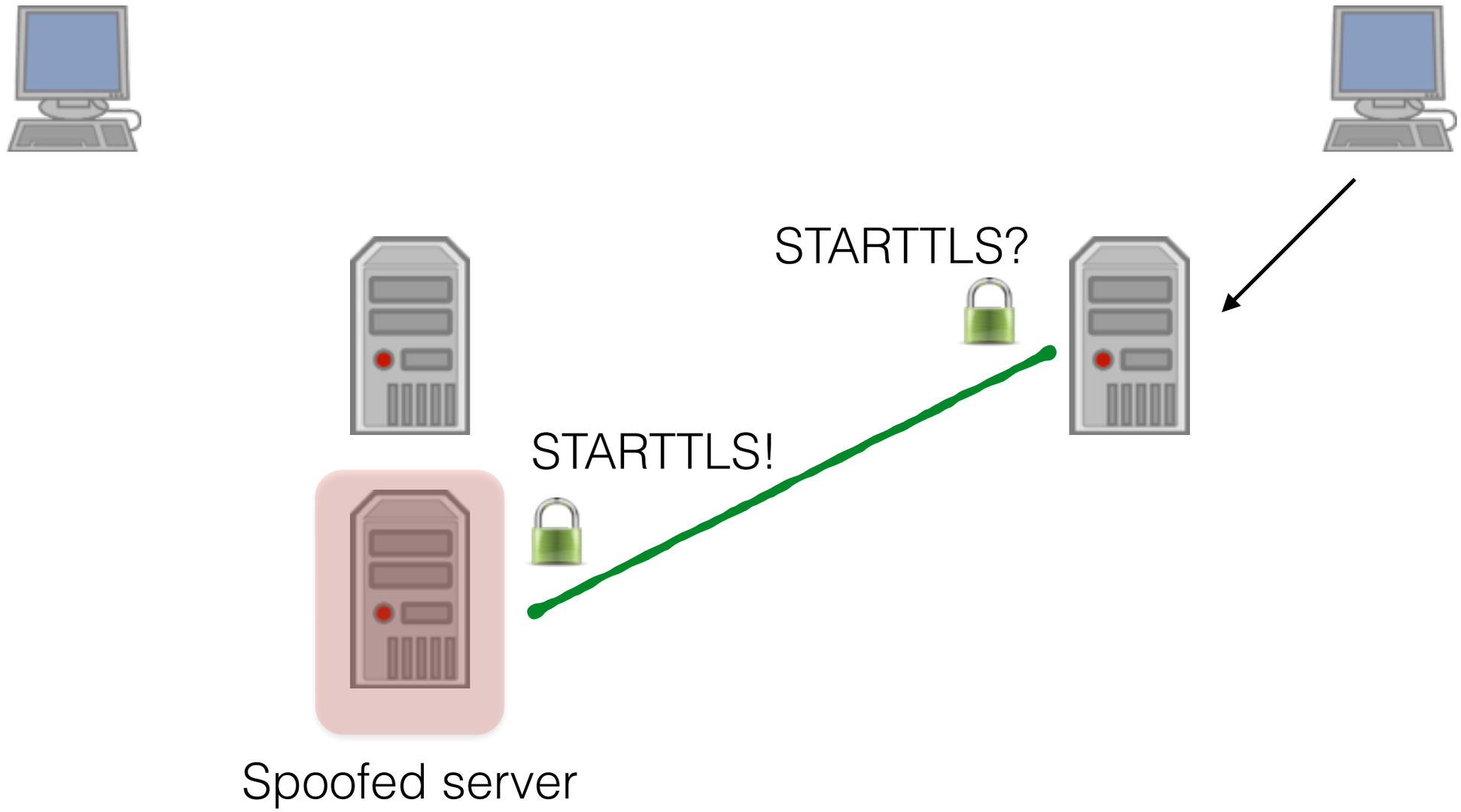
TLS and SMTP



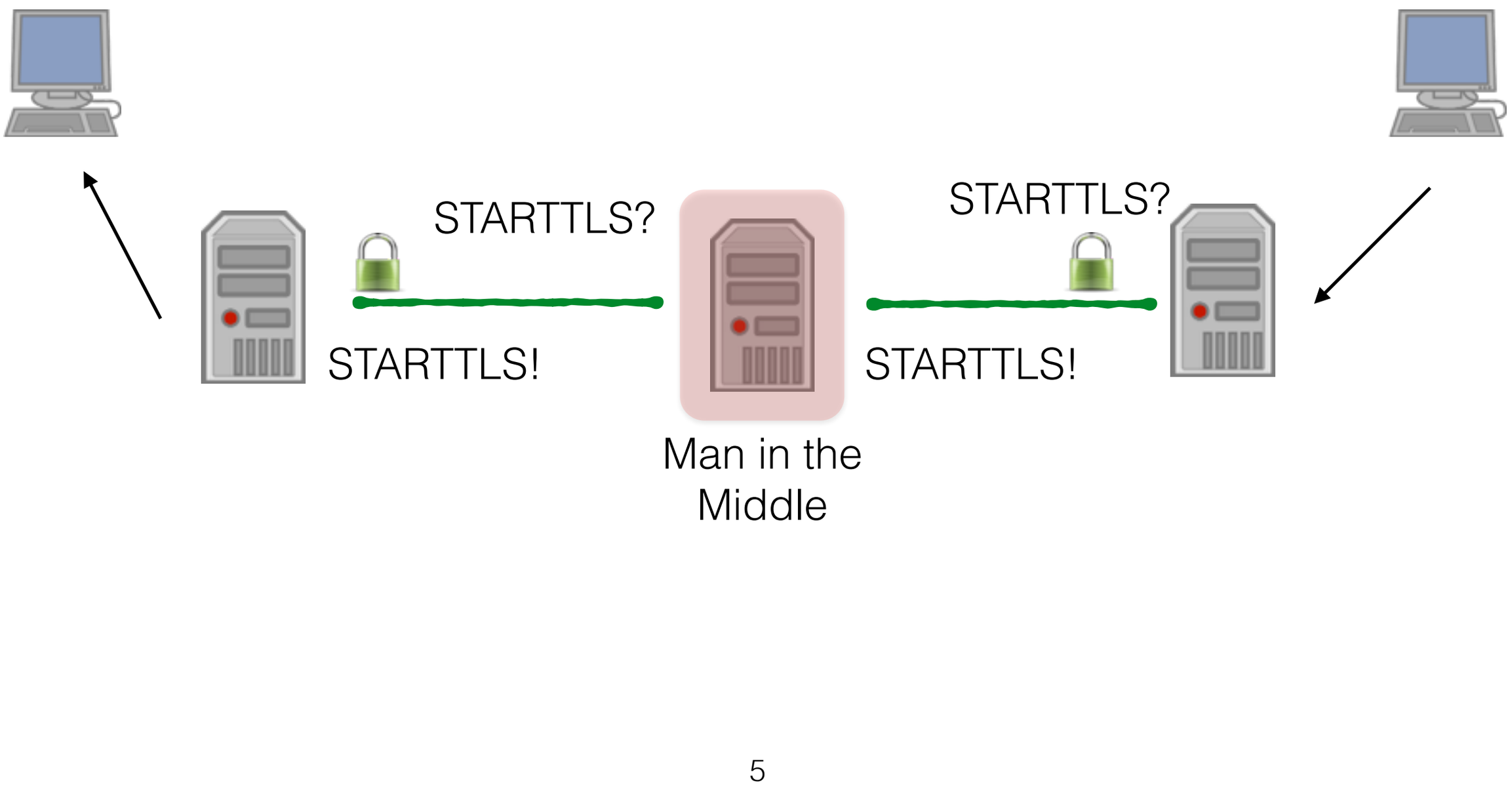
TLS and SMTP



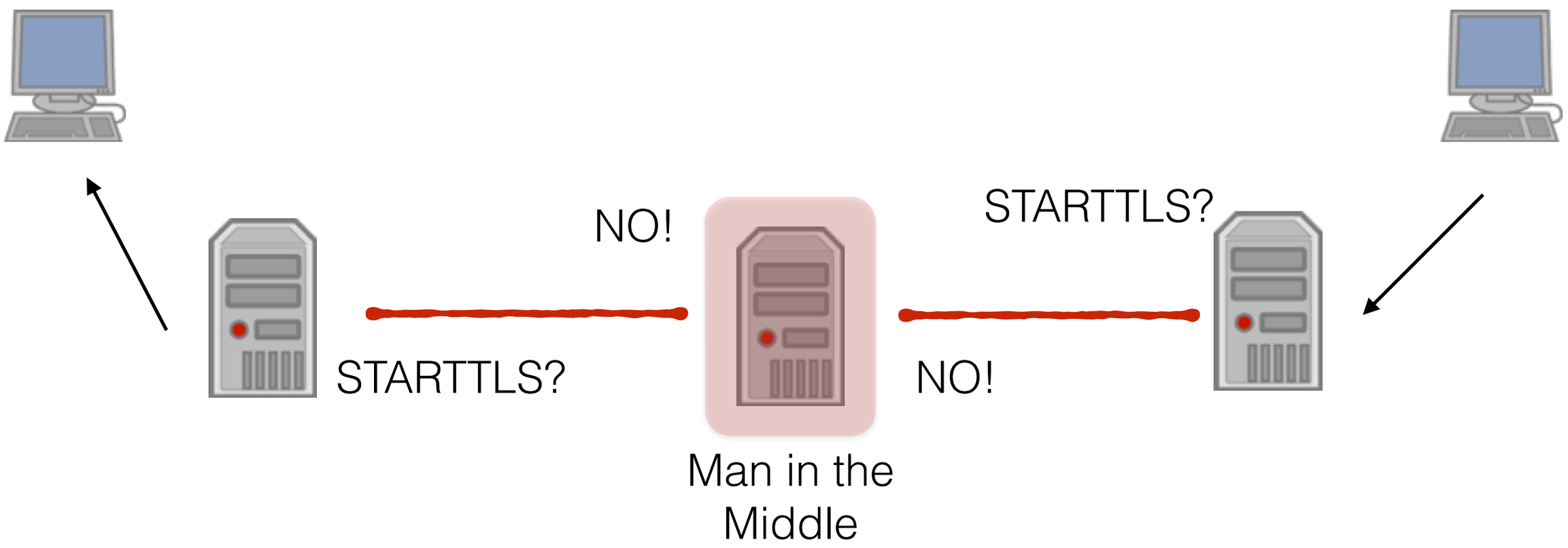
TLS and SMTP



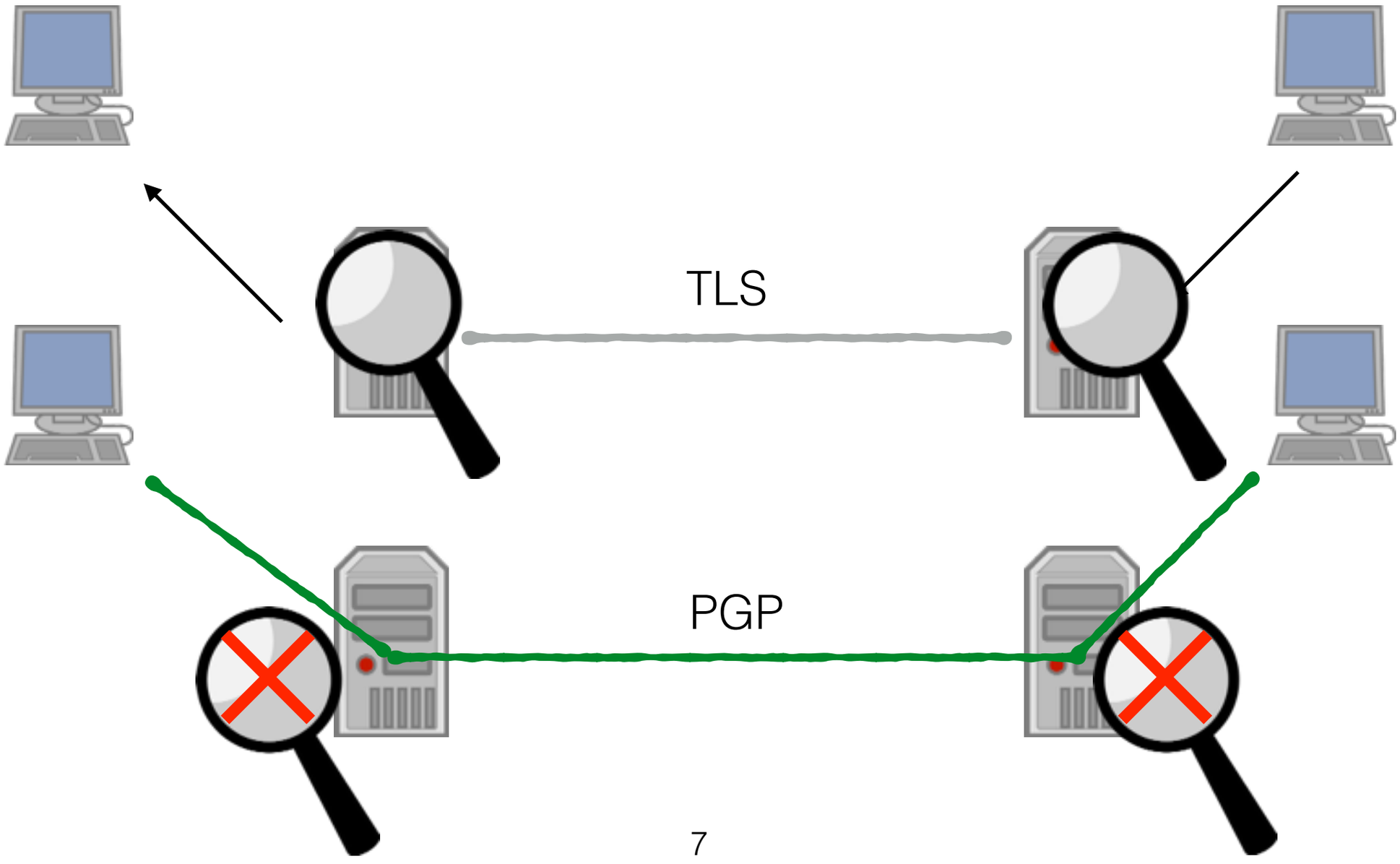
TLS and SMTP



TLS and SMTP



TLS != PGP



TLSA/SMTP

- Validation of TLS certificates via DNS(SEC)
- the hash of an x509 cert (or the full certificate) stored in DNS
- validates: the owner of the domain is the owner of the certificate

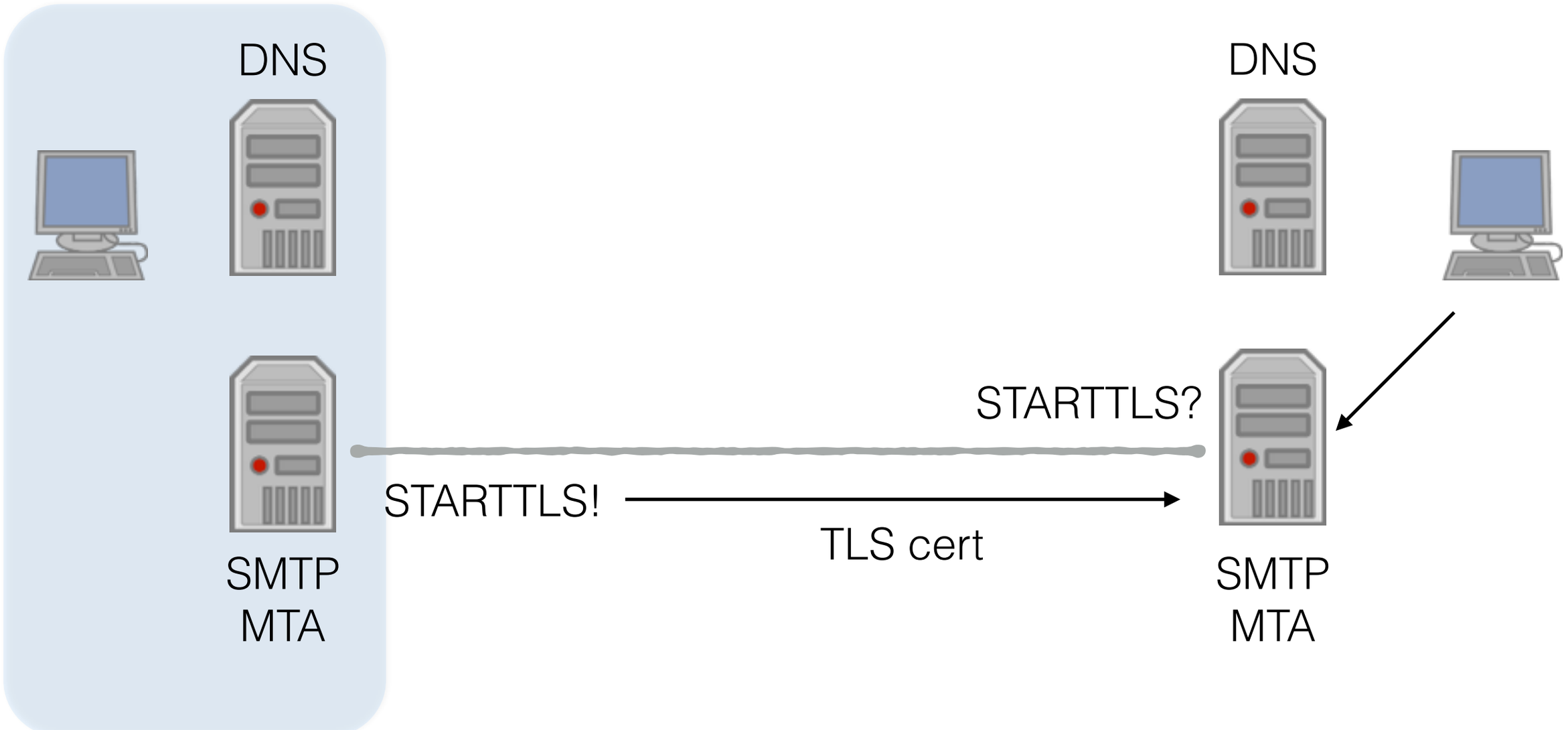
TLSA/SMTP

- the security-level similar to domain-validated x509 certificates

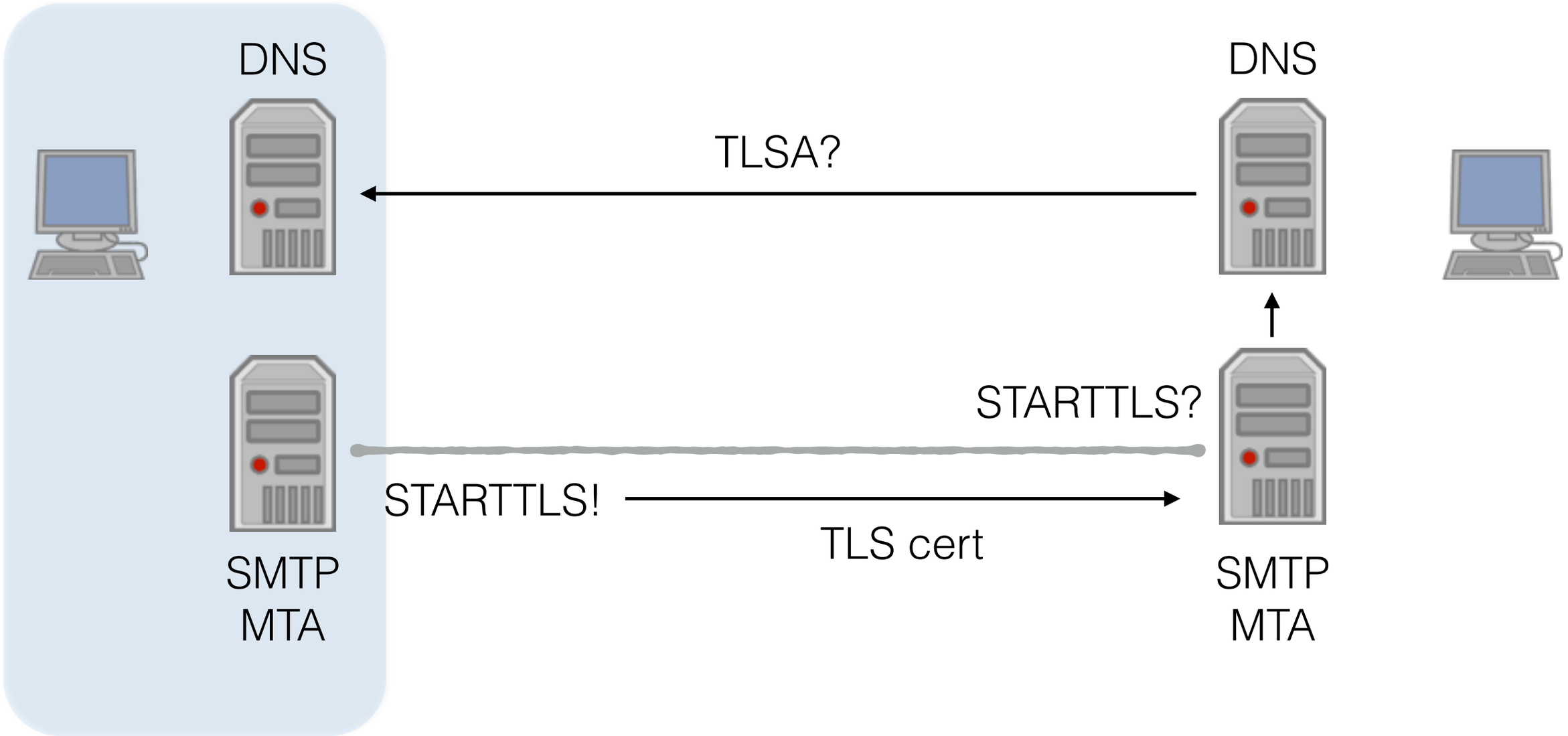
- TLSA can be used to validate self-signed certificates

- TLSA can be used to validate X509 certificates from certification authorities (Symantec, Comodo, StartSSL, CACert . . .)

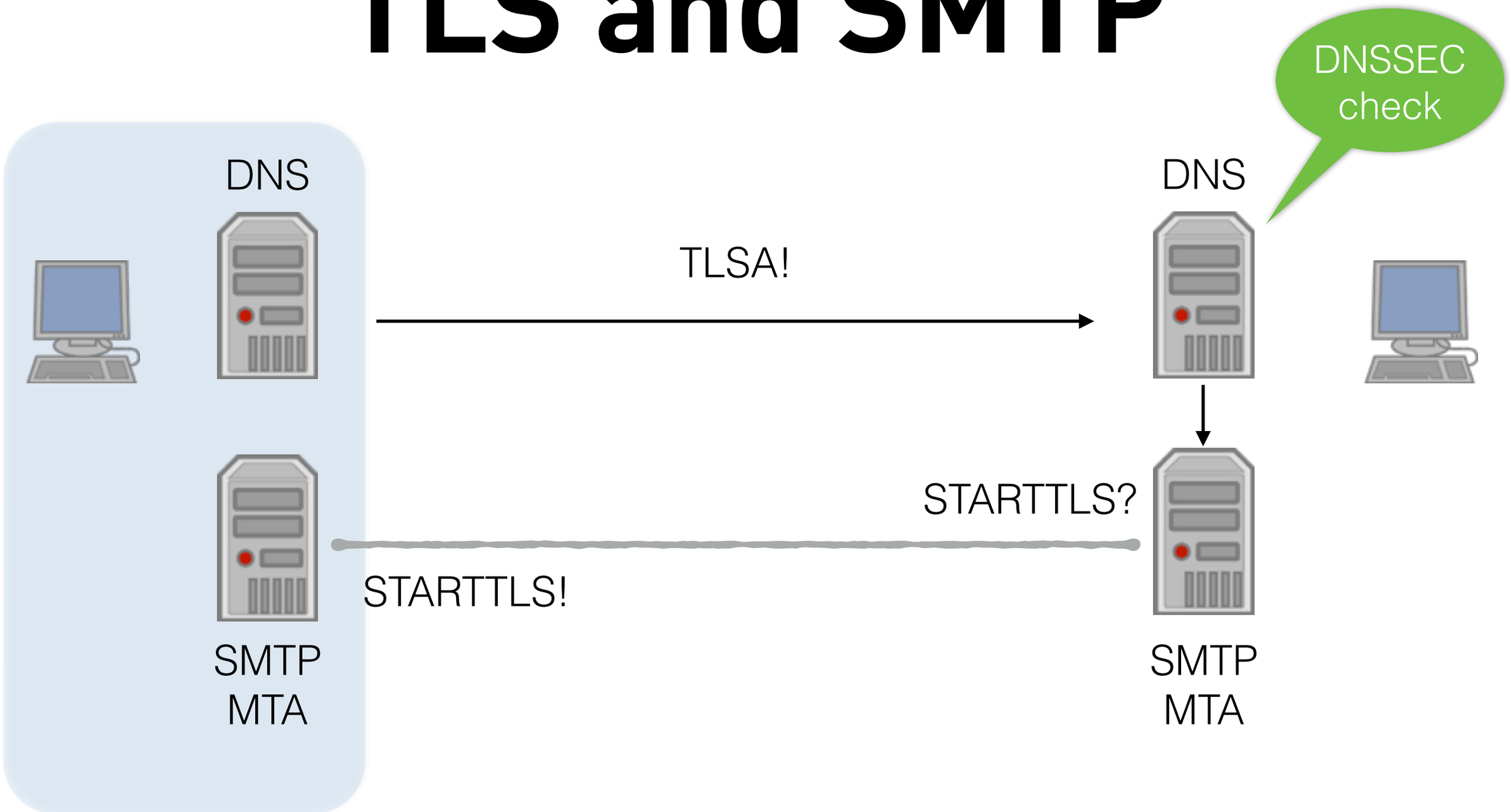
TLS and SMTP



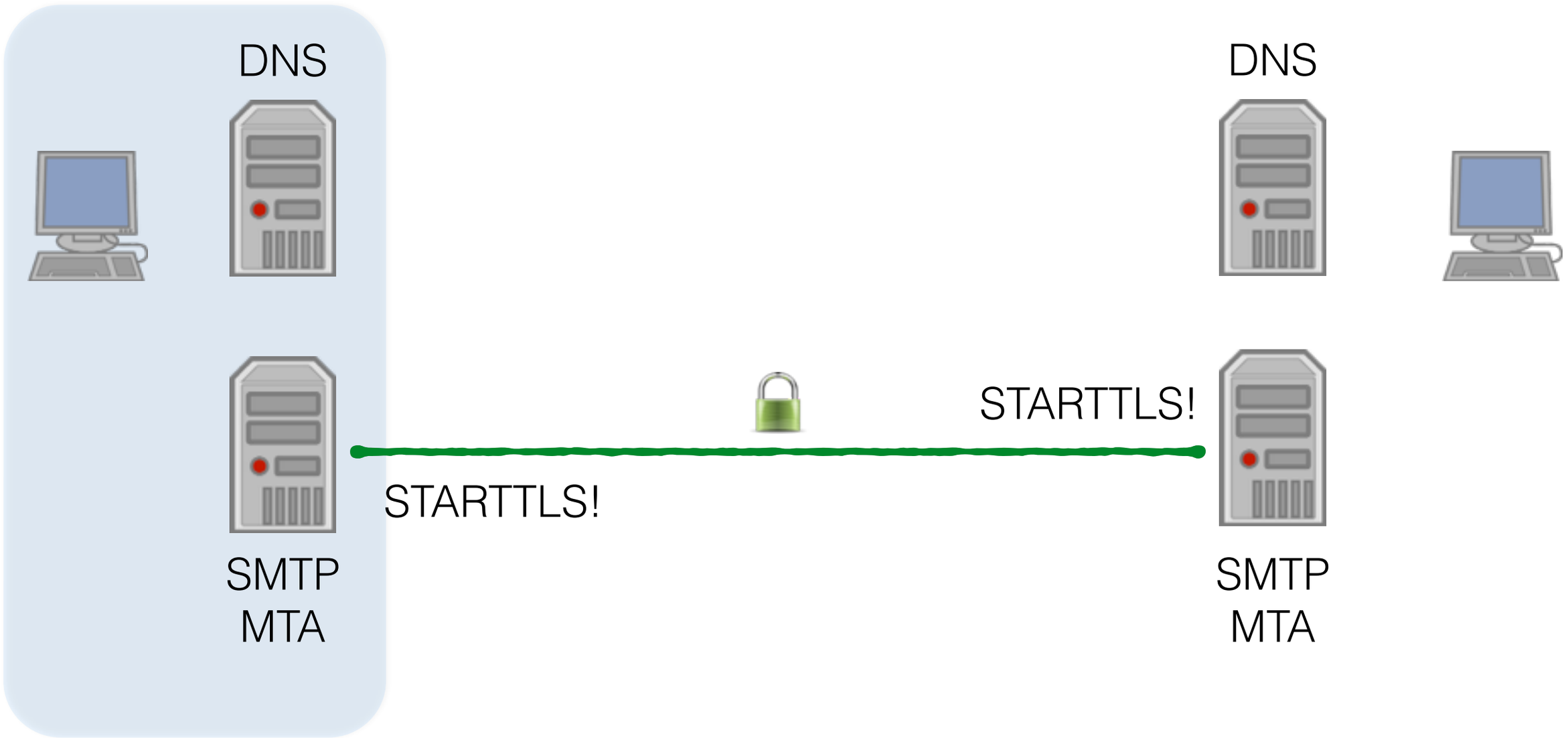
TLS and SMTP



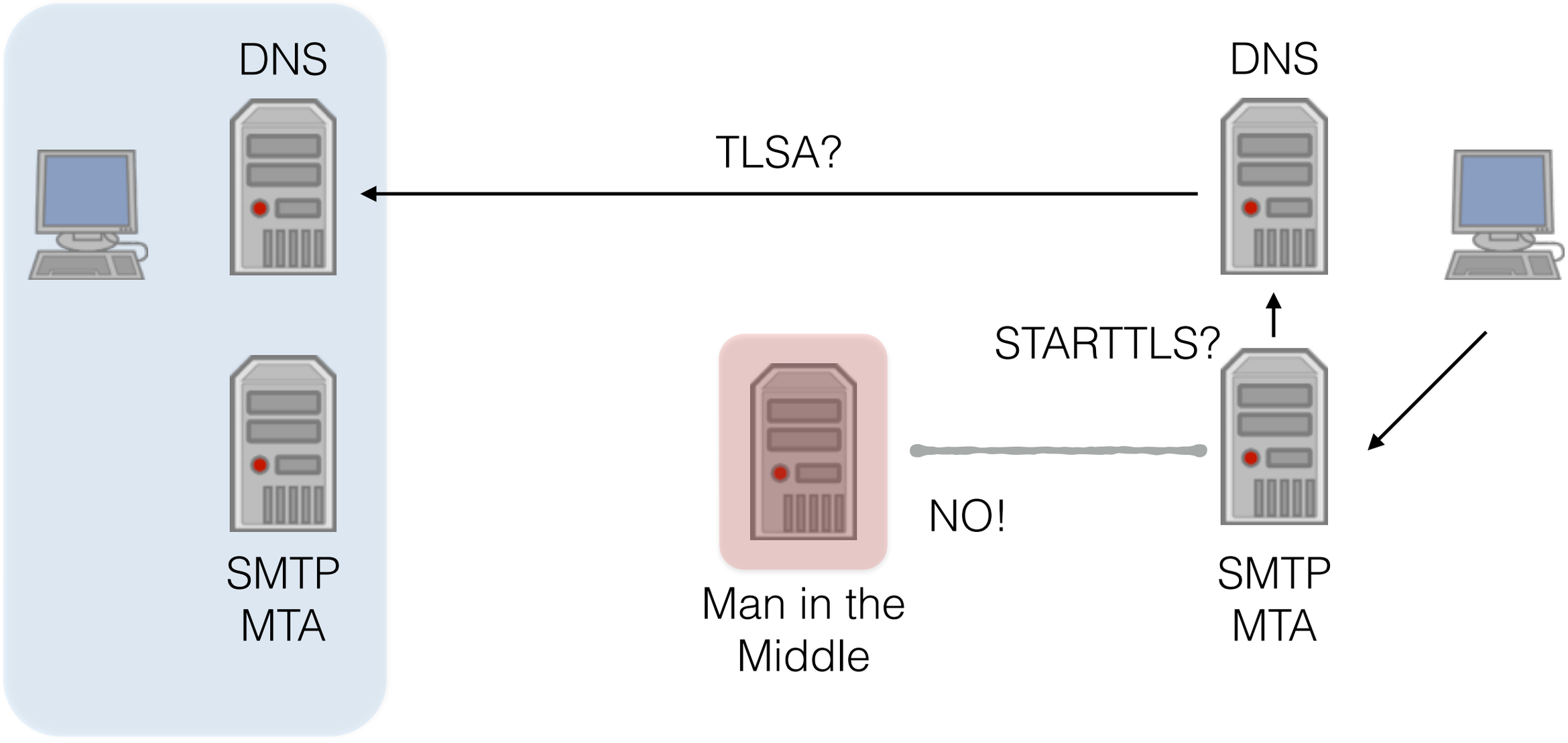
TLS and SMTP


DNS
DNS
DNSSEC check
TLSA!
STARTTLS?
STARTTLS!
SMTP MTA
SMTP MTA

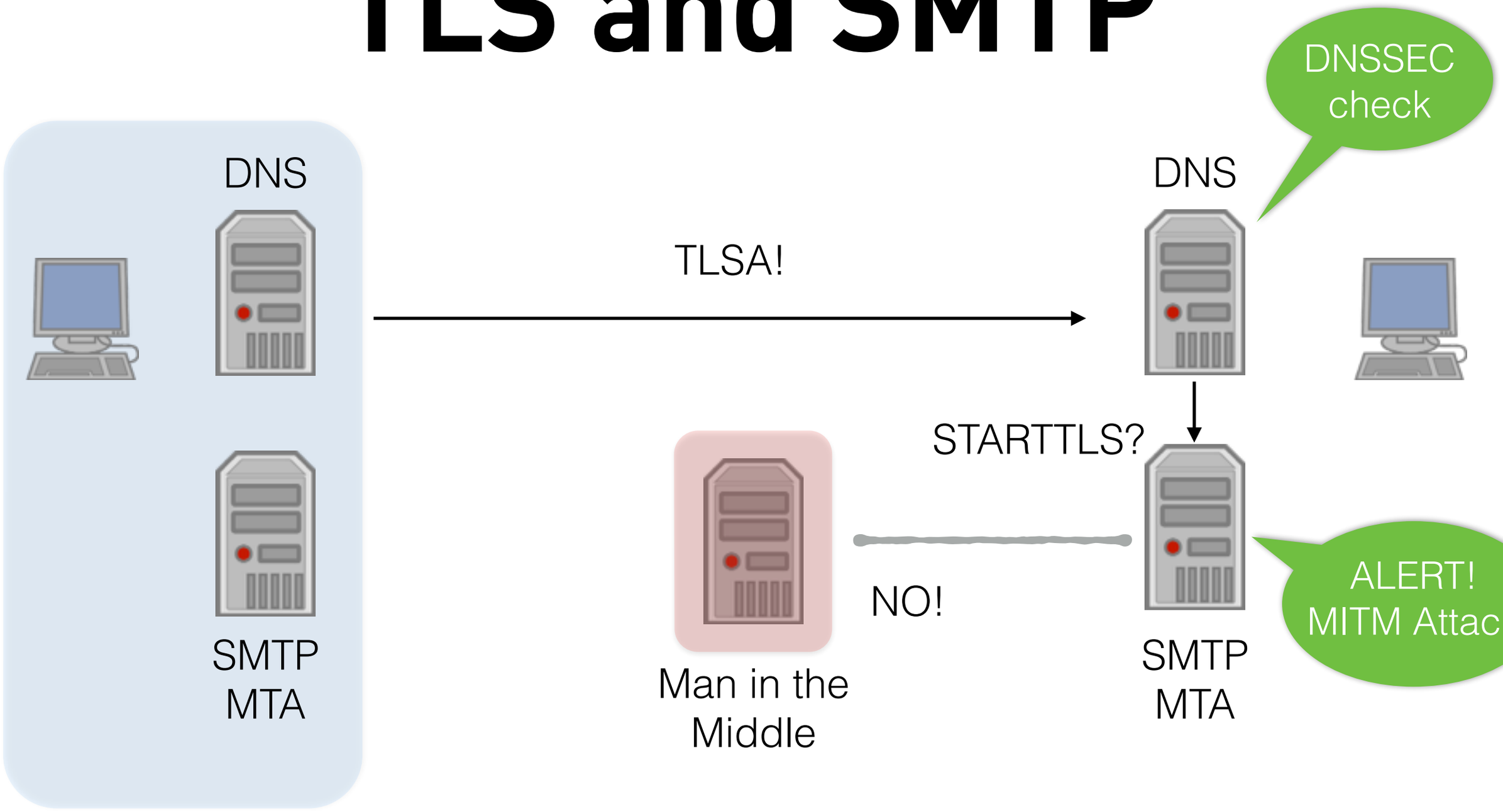
TLS and SMTP



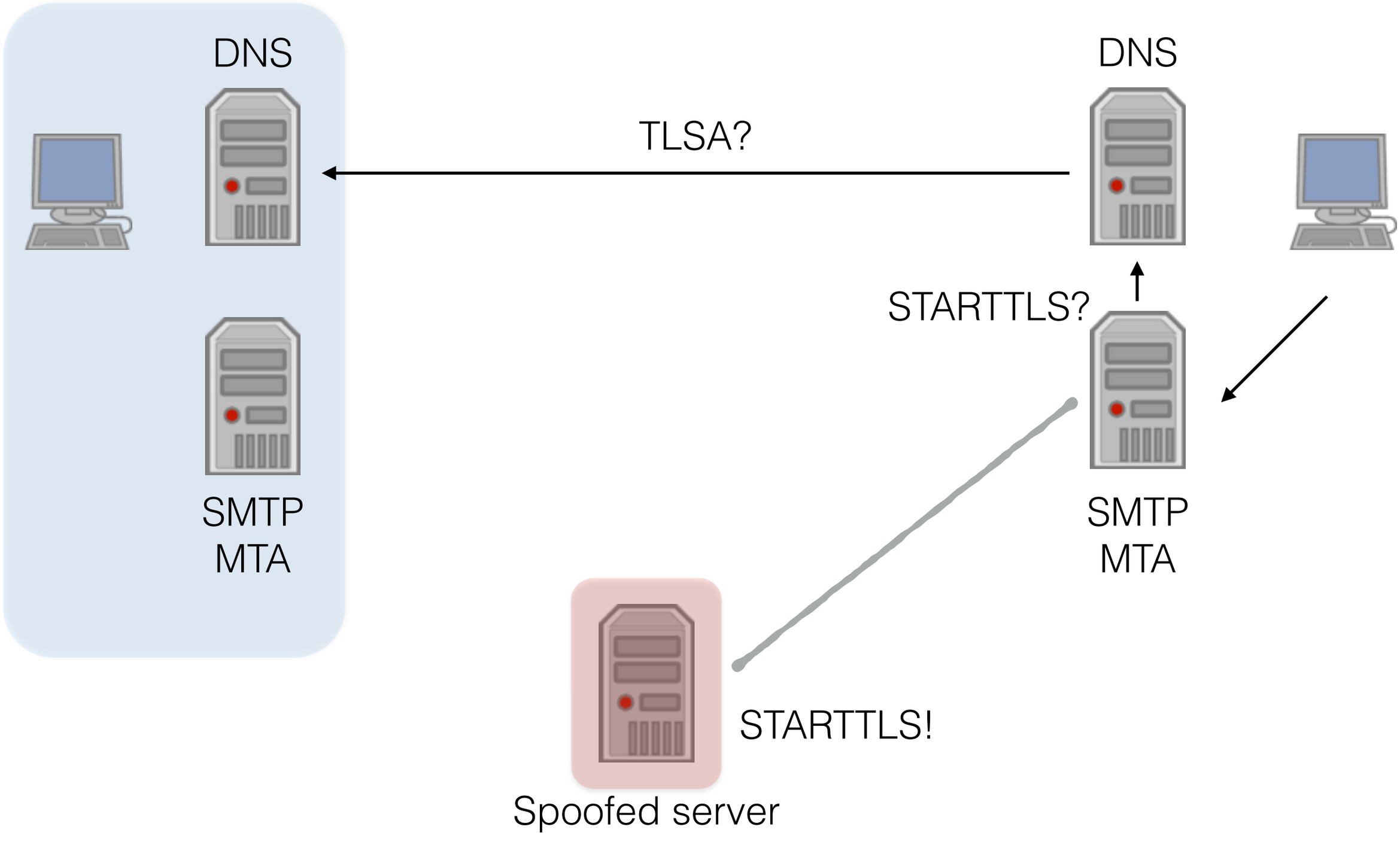
TLS and SMTP



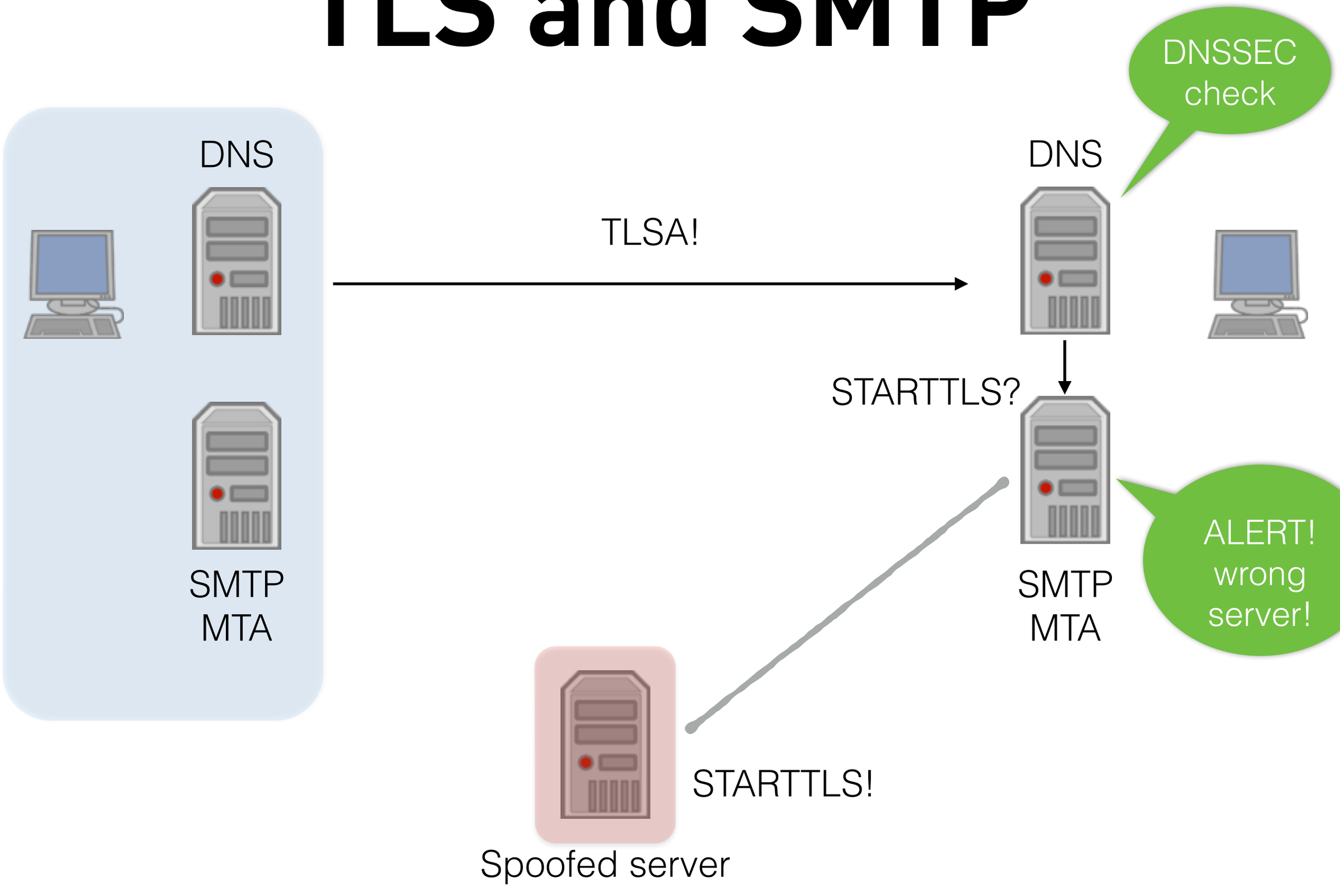
TLS and SMTP


DNS
SMTP
MTA
TLSA!
DNS
DNSSEC
check
STARTTLS?
Man in the
Middle
NO!
SMTP
MTA
ALERT!
MITM Attack

TLS and SMTP


DNS
DNS
TLSA?
STARTTLS?
SMTP
MTA
SMTP
MTA
STARTTLS!
Spoofed server

TLS and SMTP


DNS
SMTP
MTA
TLSA!
DNS
DNSSEC
check
STARTTLS?
SMTP
MTA
ALERT!
wrong
server!
STARTTLS!
Spoofed server

Infrastructure DNS

- DNSSEC validation (caching DNS resolver)
  - BIND 9, Unbound, dnsmasq, Windows 2012
- DNSSEC signed zones (authoritative DNS Server)
  - BIND 9, NSD, Knots, Y.A.D.I.F.A., PowerDNS, Bundy-DNS, Windows 2012

Infrastructure Mail

- MTA with TLSA Support
  - Postfix 2.11, Exim (in development)
- TLS certificates
  - EV-certificate (Extended Validation)
  - DV-certificate (Domain Validation)
  - Self-signed certificate

BIND 9.9.x DNSSEC

- **enable DNSSEC validation:**

```
options {
    …
    dnssec-validation auto;
    dnssec-lookaside auto;
};
```

TLSA-Record

- **manual creation of a TLSA record hash:**

```
$ openssl x509 -in mail.example.de.crt -outform DER | openssl sha256  (stdin)=
8cb0fc6c527506a053f4f14c8464bebbd6dede2738d11468dd953d7d6a3021f1
```

- **TLSA record:**

```
_25._tcp.mail.example.de.  3600 IN TLSA 3 0 1 (
                                8cb0fc6c527506a053f4f14c8464bebbd6dede
                                2738d11468dd953d7d6a3021f1 )
```

test TLSA-Record

DNSSEC check OK

TLSA Record

DNSSEC signature

```
shell> dig _25._tcp.ma                                  sec +m
 ; <<>> DiG 9.9.5 <<>> _                               mple.de TLSA +dnssec +m
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13973
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;_25._tcp.mail.example.de. IN TLSA

;; ANSWER SECTION:
_25._tcp.mail.example.de.  3588 IN TLSA 3 1 1 (
                                8cb0fc6c527506a053f4f14c8464bebbd6dede
                                2738d11468dd953d7d6a3021f1 )
_25._tcp.mail.example.de.  3588 IN RRSIG TLSA 8 5 3600 (
                                20140324063111 20140317121843 4390 example.de.
                                RBgAAzQx3gks0KKJHuJ7qKd61jpY8E6dwDM6inPPa6Ee
                                xV8OBnAzhF4RMKSabHF0LNwRzWqE5xNfPibMQFDoDRKJ
                                /QiNgux/IXti3JqtH4BkT0w7Ooi+8DZsil9BTjg6WkaX
                                1FuJ4rJ2r3hXS7eIOFWtOF7pPVPdIIaRB6xp+1A= )

;; Query time: 9 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Mar 17 19:29:45 CET 2014
;; MSG SIZE  rcvd: 142
```

Postfix configuration

- **Postfix configuration for TLSA validation:**

```
shell> postconf -e "smtpd_use_tls = yes"
shell> postconf -e "smtp_dns_support_level = dnssec"
shell> postconf -e "smtp_tls_security_level = dane"
```

Postfix log (untrusted TLS)

- **Postfix log TLS without DNSSEC TLSA validation (DANE):**

```
Mar 16 19:10:55 m3 postfix/qmgr[25923]: 2B1A680337:
from=<root@myinfrastructure.org>, size=291, nrcpt=1 (queue active)

Mar 16 19:11:03 m3 postfix/smtp[25929]: Untrusted TLS connection established to
mail1.example.de[2001:db8:100::25]:25: TLSv1 with cipher ECDHE-RSA-AES256-SHA
(256/256 bits)

Mar 16 19:11:05 m3 postfix/smtp[25929]: 2B1A680337: to=<benutzer@example.de>,
relay=mail1.example.de[2001:db8:100::25]:25, delay=16, delays=6.2/0.01/7.9/2.1,
dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 3fn80C2DP5zTT)

Mar 16 19:11:05 m3 postfix/qmgr[25923]: 2B1A680337: removed
```

Postfix log
(DNSSEC secured TLS)

- **Postfix log TLS with DNSSEC TLSA validation (DANE):**

```
Mar 16 19:20:01 m3 postfix/qmgr[26122]: 8FBEE80337:
from=<root@myinfrastructure.org>, size=285, nrcpt=1 (queue active)

Mar 16 19:20:01 m3 postfix/smtp[26131]: Verified TLS connection established to
mail.example.de[2001:db8:100::25]:25: TLSv1 with cipher ECDHE-RSA-AES256-SHA
(256/256 bits)

Mar 16 19:20:03 m3 postfix/smtp[26131]: 8FBEE80337: to=<benutzer@example.de>,
relay=mail.example.de[2001:db8:100::25]:25, delay=149, delays=147/0.03/0.13/1.8,
dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 3fn8BY3ltPzTT)

Mar 16 19:20:03 m3 postfix/qmgr[26122]: 8FBEE80337: removed
```

DANE TLSA Benefits

- authenticated encrypted connection between SMTP server
- prevents STARTTLS "downgrade" attacks
- secures against fake/spoofed TLS/SSL certificates
- no CRL/OCSP required to "revoke" a certificate (just replace the TLSA record)

Mail-ISP deploys DANE/SMTP


News Newsticker 7-Tage-News Archiv Foren

Topthemen: Heartbleed Fritzbox Windows XP NSA Bitcoin

heise online > News > 2014 > KW 20 > Verschlüsselter Mail-Transport: Posteo setzt als erste

12.05.2014 15:37

heise Netze « Vorige | Nächste »

Verschlüsselter Mail-Transport: Posteo setzt als erster Provider DANE ein

vorlesen / MP3-Download

Damit schlägt die kleine Firma den großen Anbietern erneut ein Schnippchen: Anders als etwa die Konkurrenz von "E-Mail made in Germany" setzt Posteo auf einen offenen Standard, dessen Implementierung obendrein nicht teuer zertifiziert werden muss.

Das Berliner Unternehmen Posteo setzt seit dem heutigen Montag als vermutlich weltweit erster Mail-Dienstleister die moderne DANE-Technik ein, um den

~500.000 Mails/day, ~50.000 Mailboxes

MEN&MICE

[*]
We do ASCII

[?]

Patrick Ben Koetter — p@sys4.de
Carsten Strotmann — carsten@menandmice.com

Links

- **Sys4 -** `http://www.sys4.de`
- **Men & Mice -** `http://www.menandmice.com`
- **DNSWorkshop -** `http://dnsworkshop.org`
- **Postfix TLS Readme-** `http://www.postfix.org/TLS_README.html`
- **Wietse Venema "Postfix 2.11" FOSDEM 2014 Video -**
  `https://fosdem.org/2014/schedule/event/postfix_lessons_learned_and_recent_developments/`
- **IETF "DANE" working group -** `http://datatracker.ietf.org/wg/dane/`
  - **TLSA RFC 6698 -** `http://datatracker.ietf.org/doc/rfc6698/`
  - **TLSA/SMTP Draft -** `http://datatracker.ietf.org/doc/draft-ietf-dane-smtp-with-dane/`
- **c't Issue 11/2014 - Page 194 "Geleitschutz"**
- **TLSA generator webpage -** `https://www.huque.com/bin/gen_tlsa`
- **"hash-slinger" by Paul Wouters (Red Hat) -** `http://people.redhat.com/pwouters/hash-slinger/`
- **DNSSEC Training —**
  `http://www.menandmice.com/support-training/training/dnssec-workshop/`