

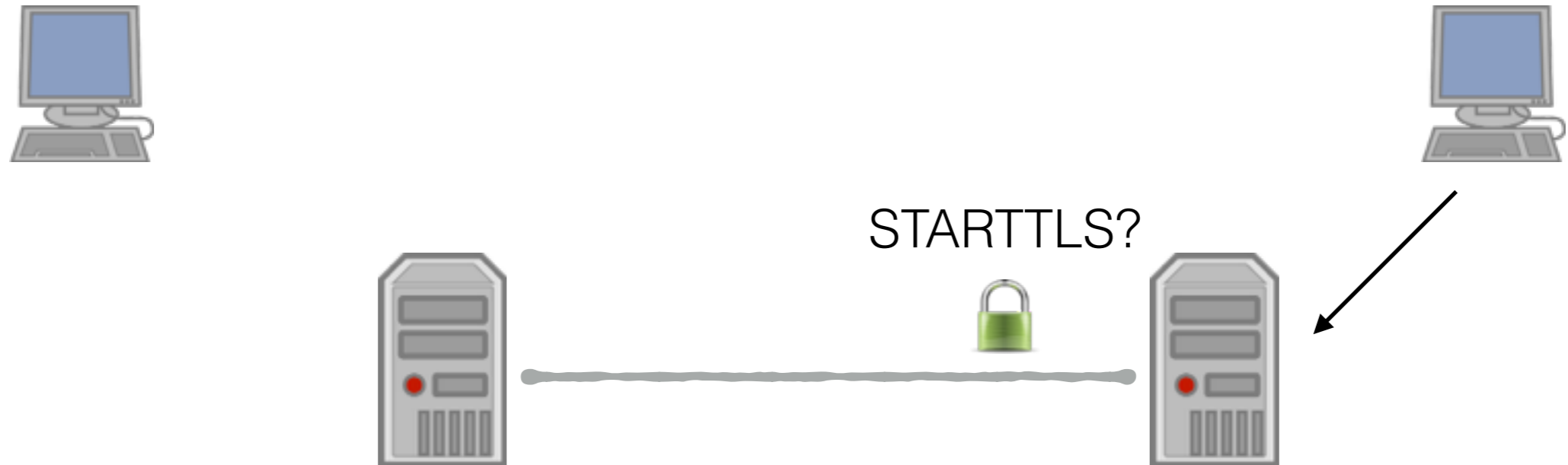
DA(e)NE n lügen nicht

Patrick Ben Koetter
Carsten Strotmann

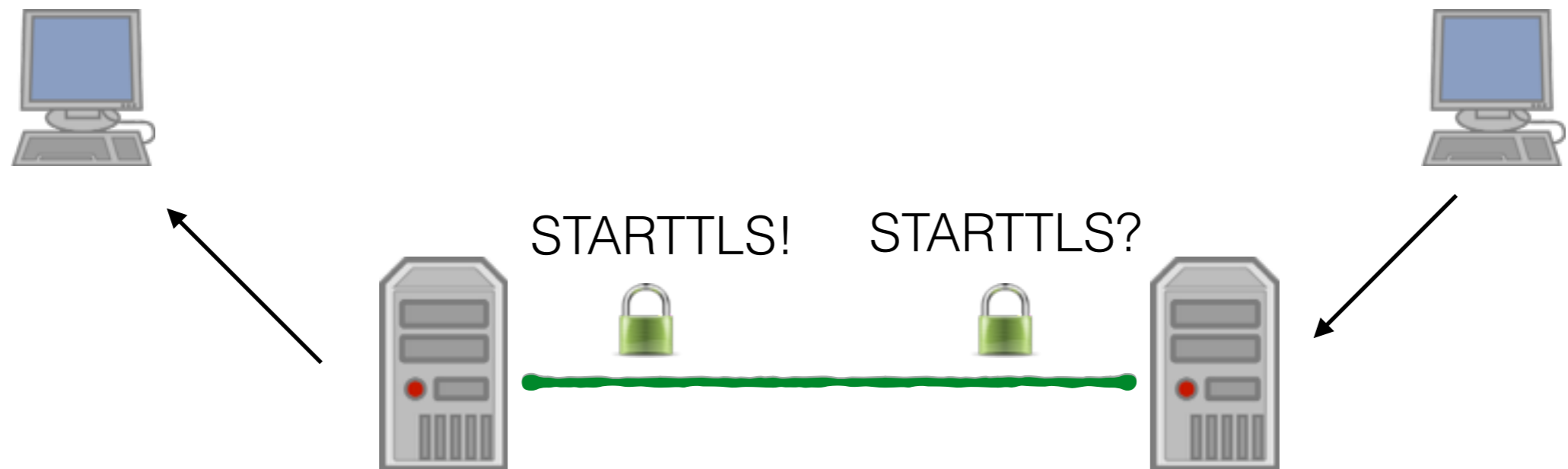
TLS und SMTP



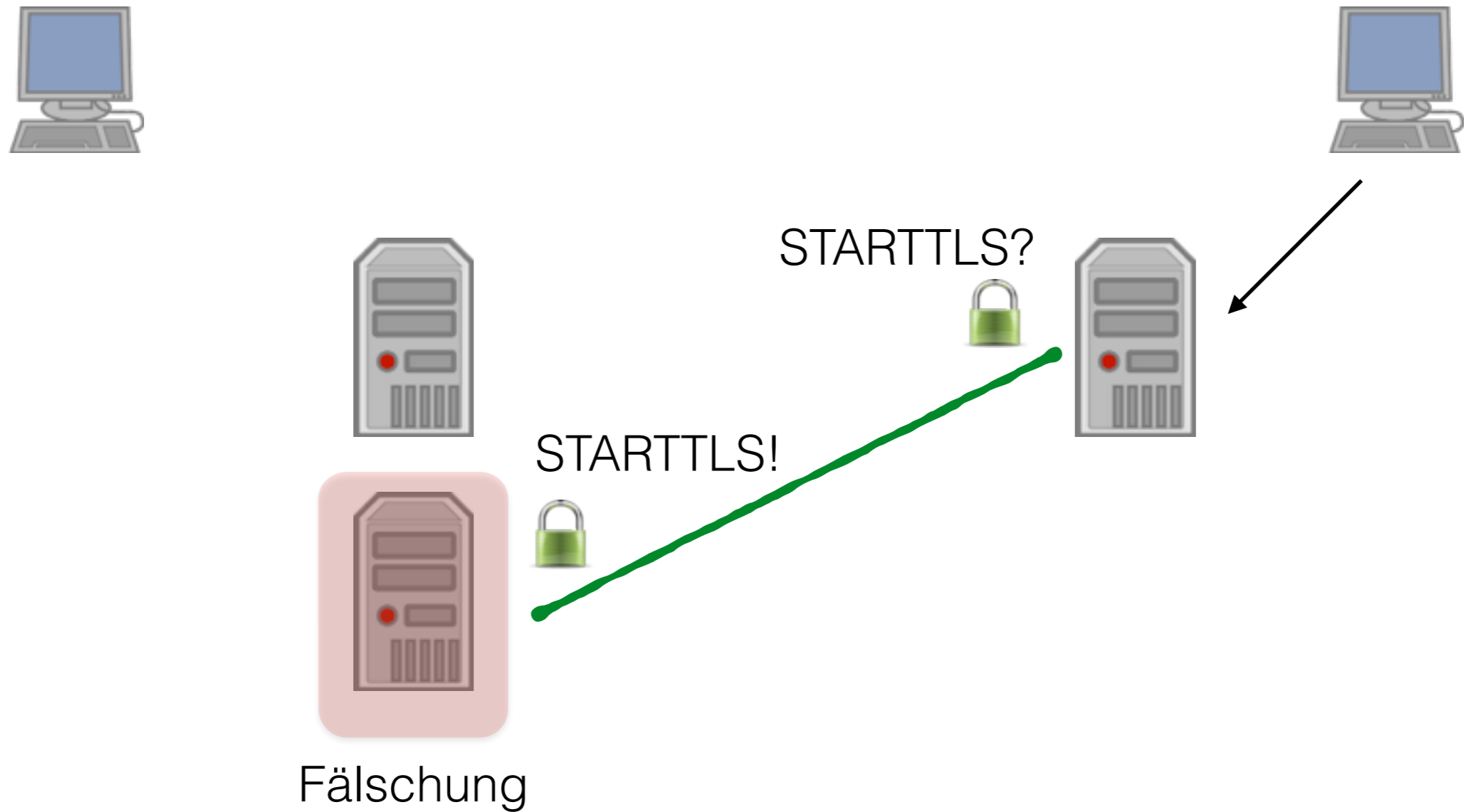
TLS und SMTP



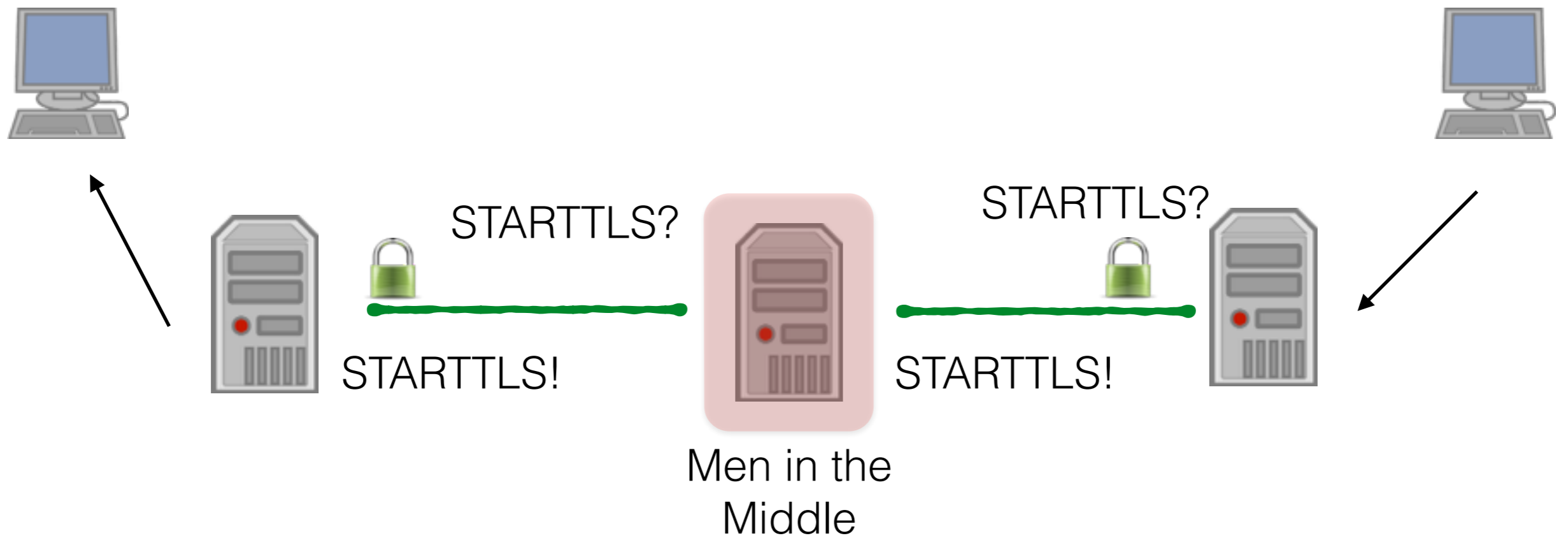
TLS und SMTP



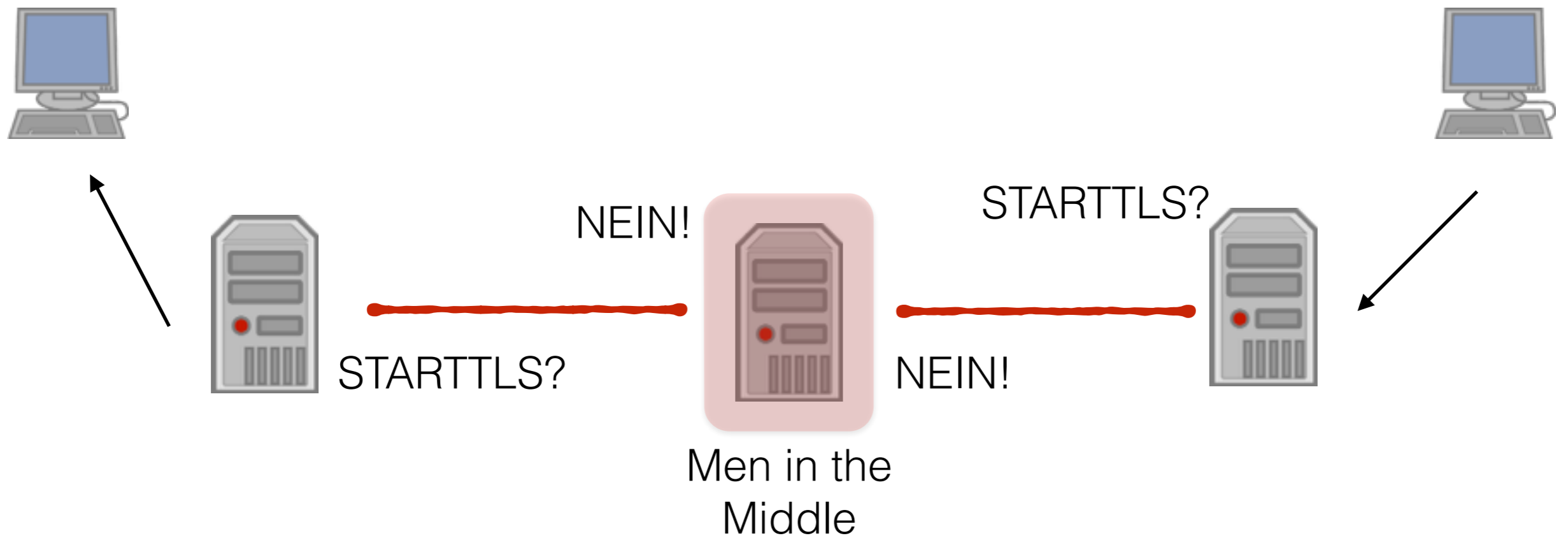
TLS und SMTP



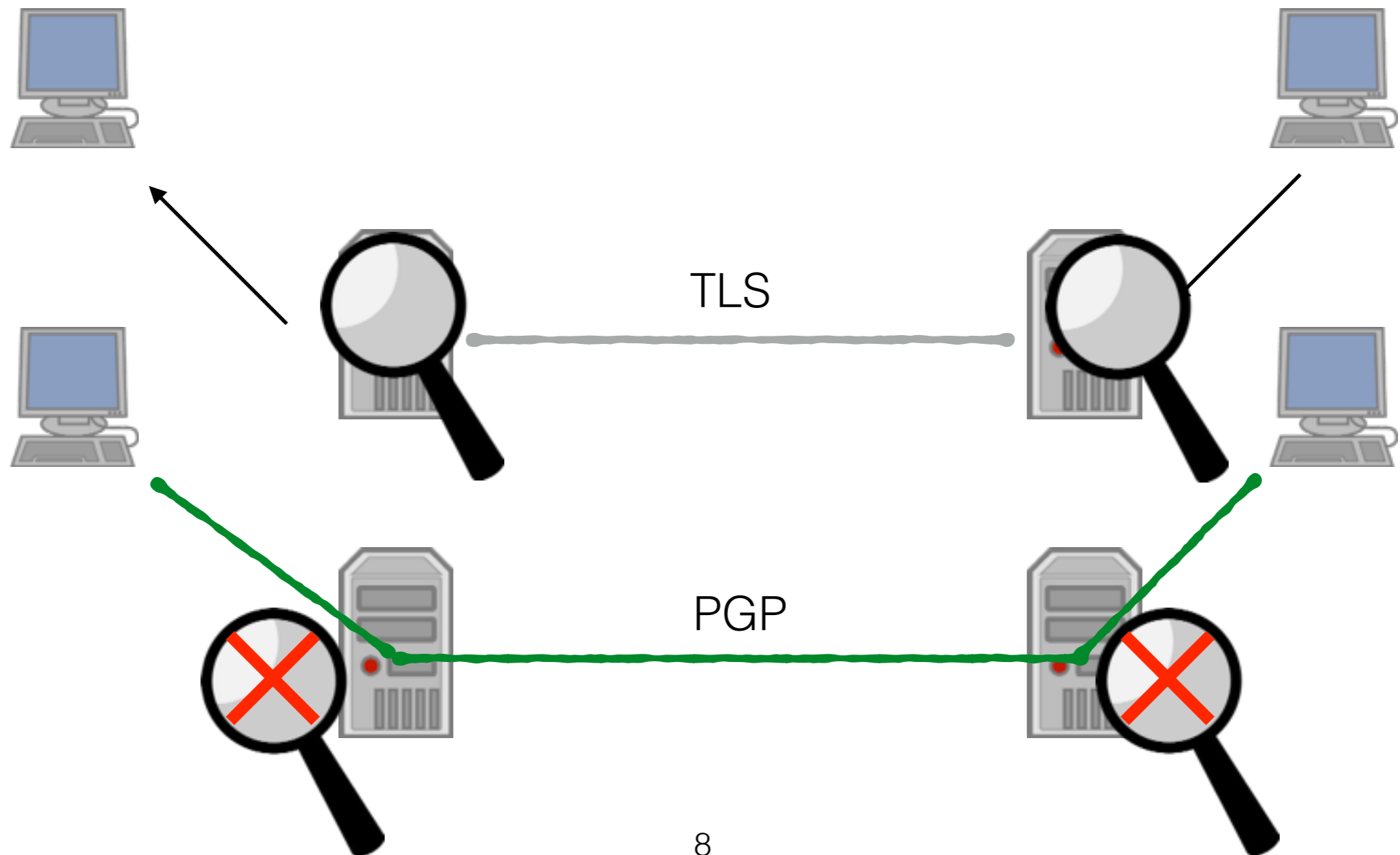
TLS und SMTP



TLS und SMTP



TLS != PGP



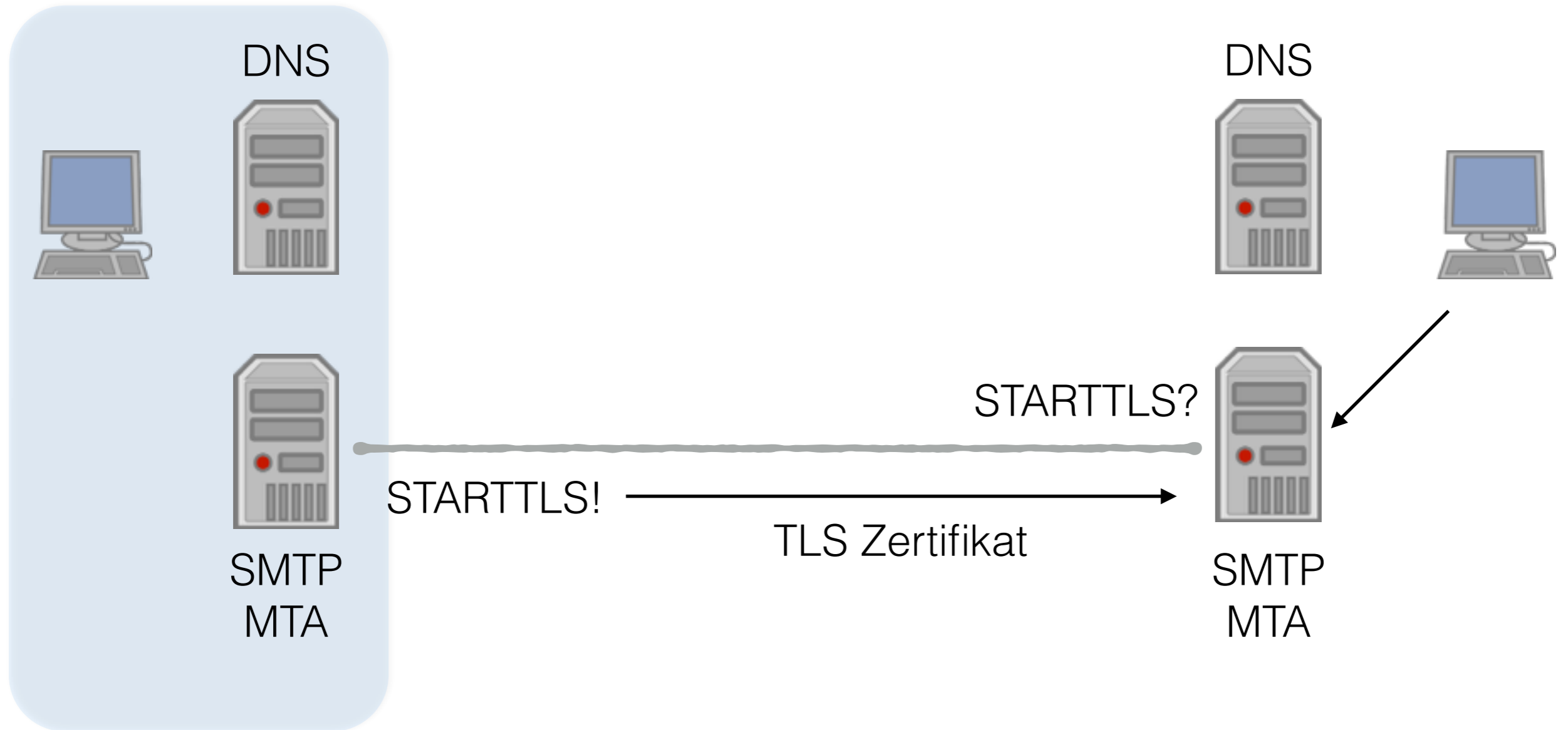
TLSA/SMTP

- **Absicherung von TLS Zertifikaten über DNS(SEC)**
 - **Hash des Zertifikates (oder das ganze Zertifikat) werden im DNS gespeichert**
 - **Annahme: der Besitzer der DNS-Domain ist auch Besitzer des Zertifikates**

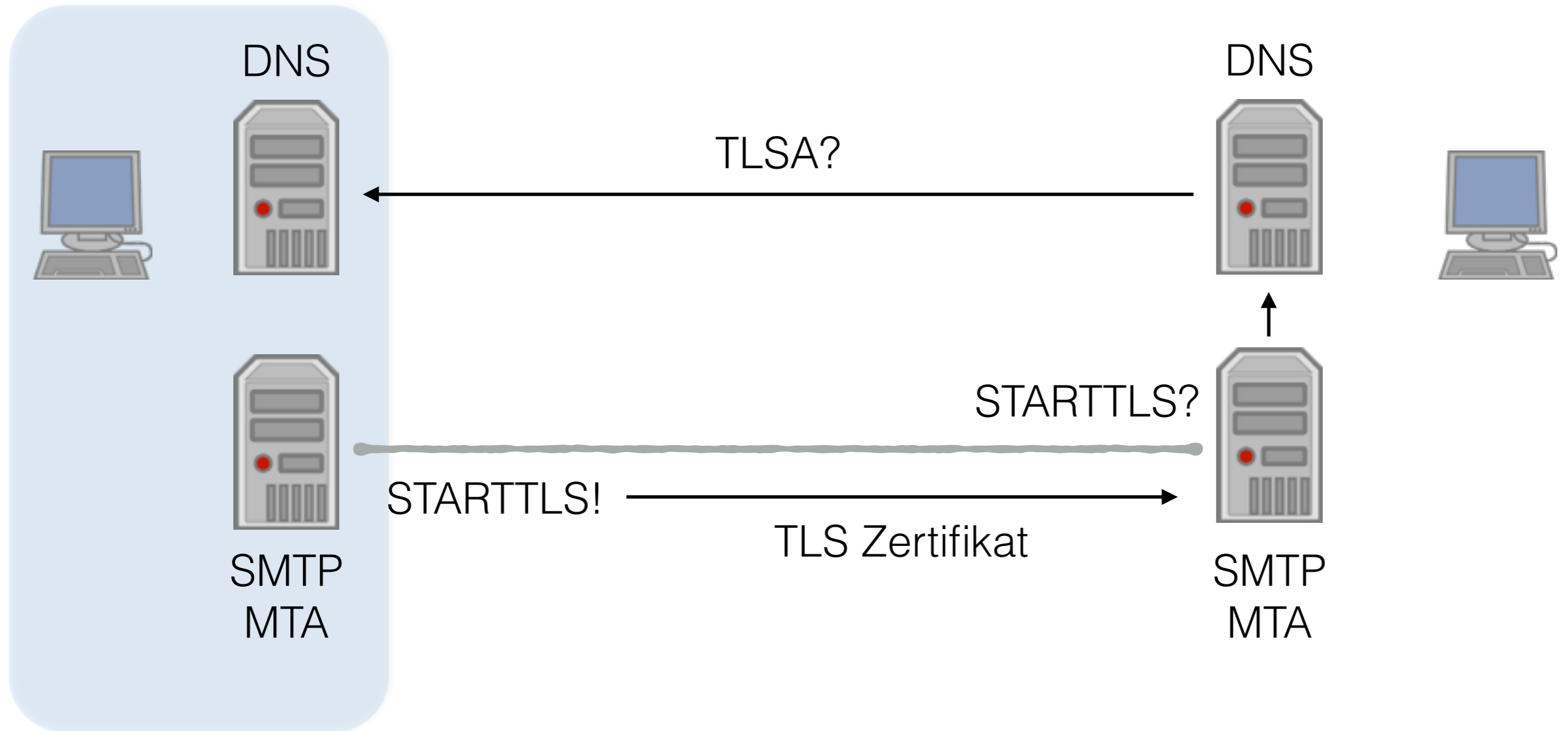
TLSA/SMTP

- **Sicherheitslevel ist vergleichbar mit Domain-(E-Mail) validierten Zertifikaten**
- **TLSA kann self-signed Zertifikate absichern**
- **TLSA kann X509 Zertifikate von Certification Authorities (Symantec, Comodo, StartSSL, CA Cert ...) absichern**

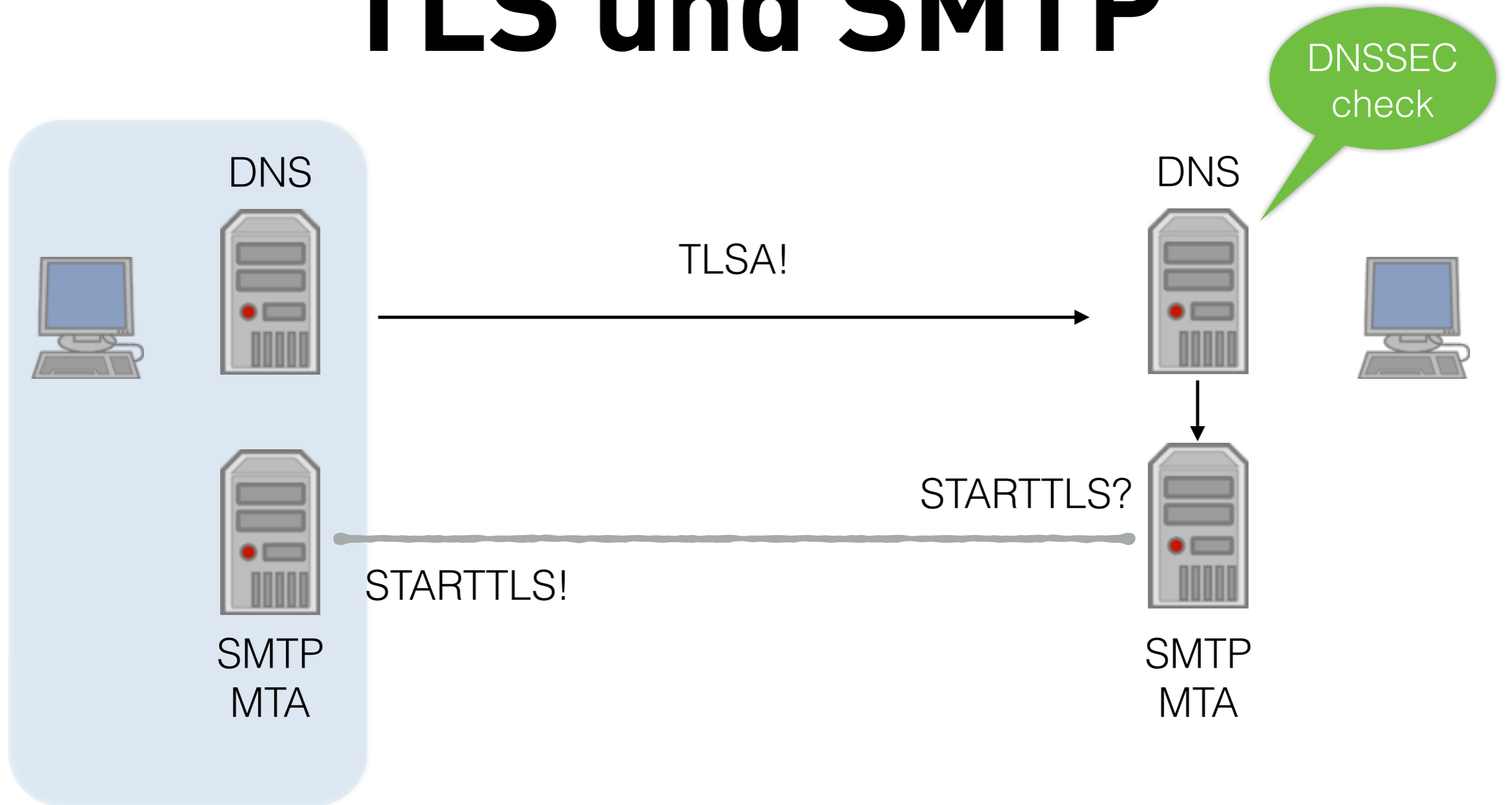
TLS und SMTP



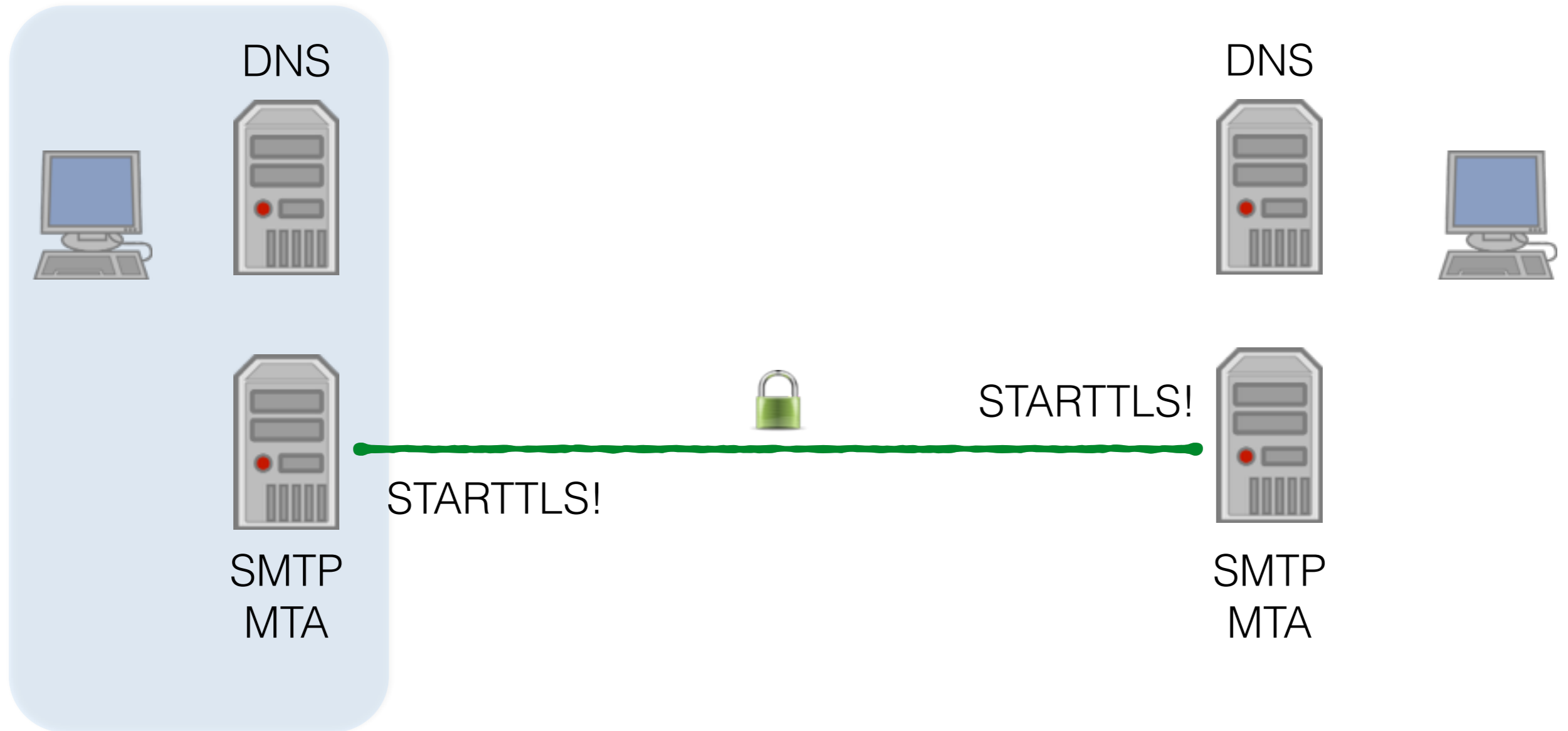
TLS und SMTP



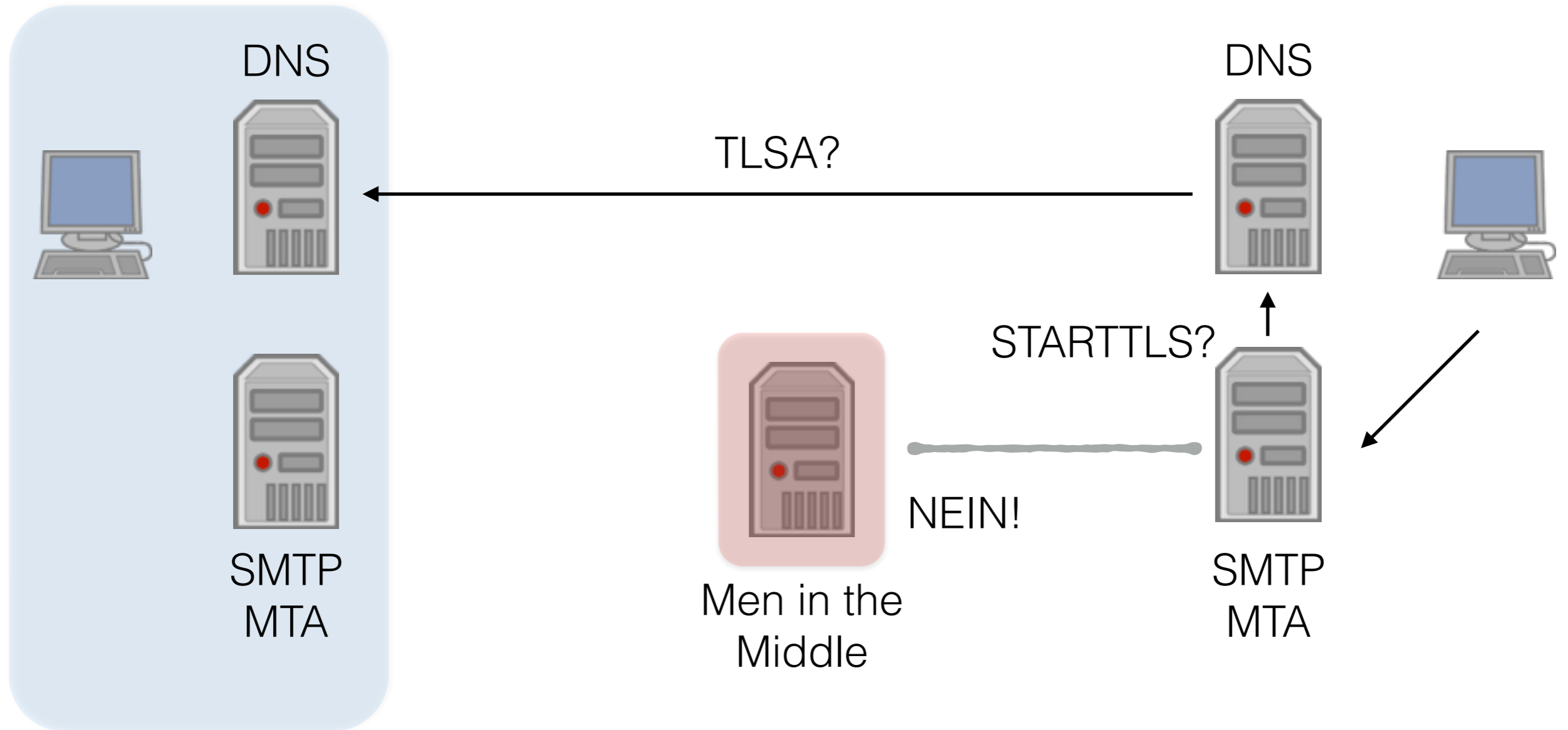
TLS und SMTP



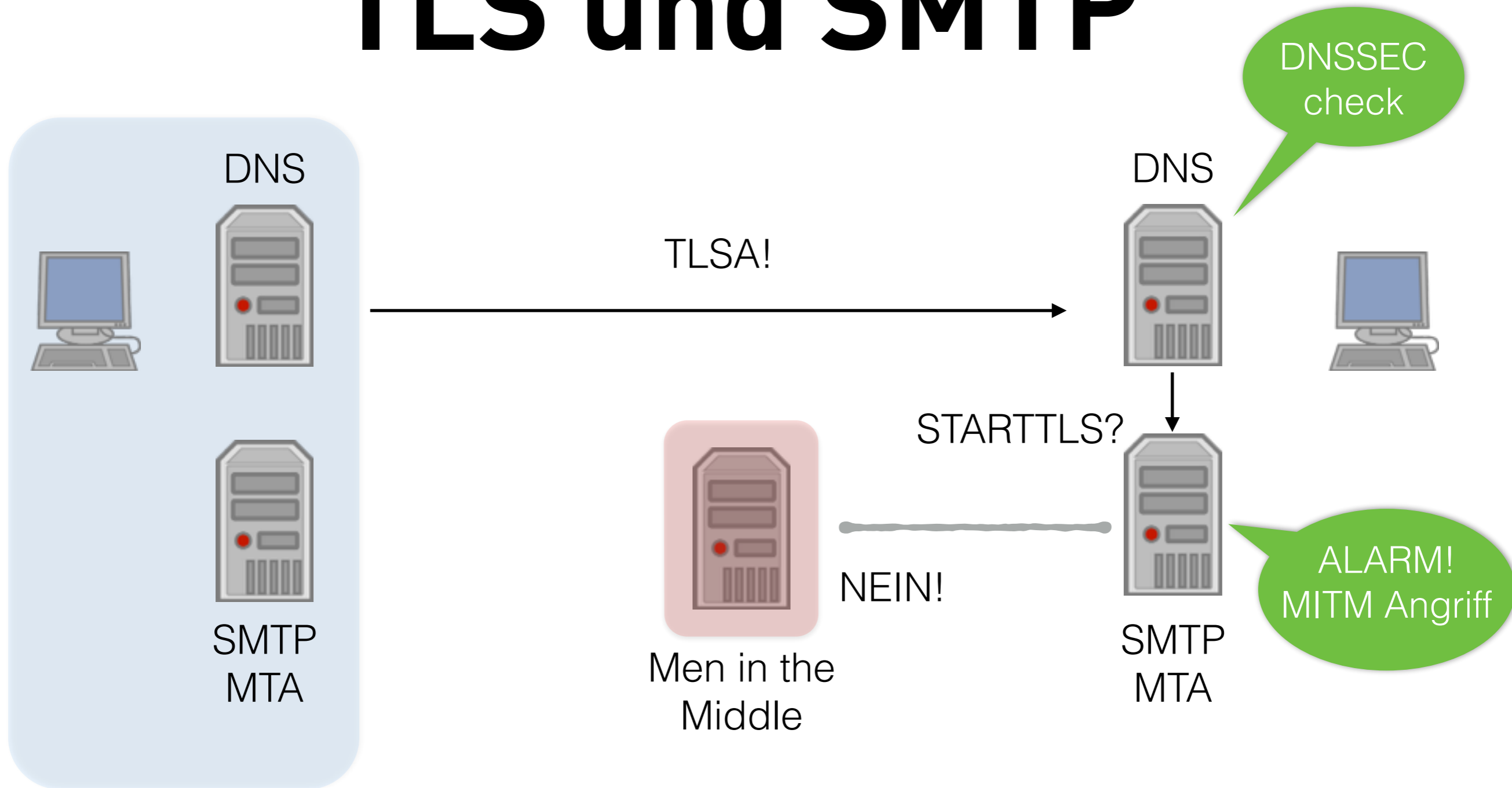
TLS und SMTP



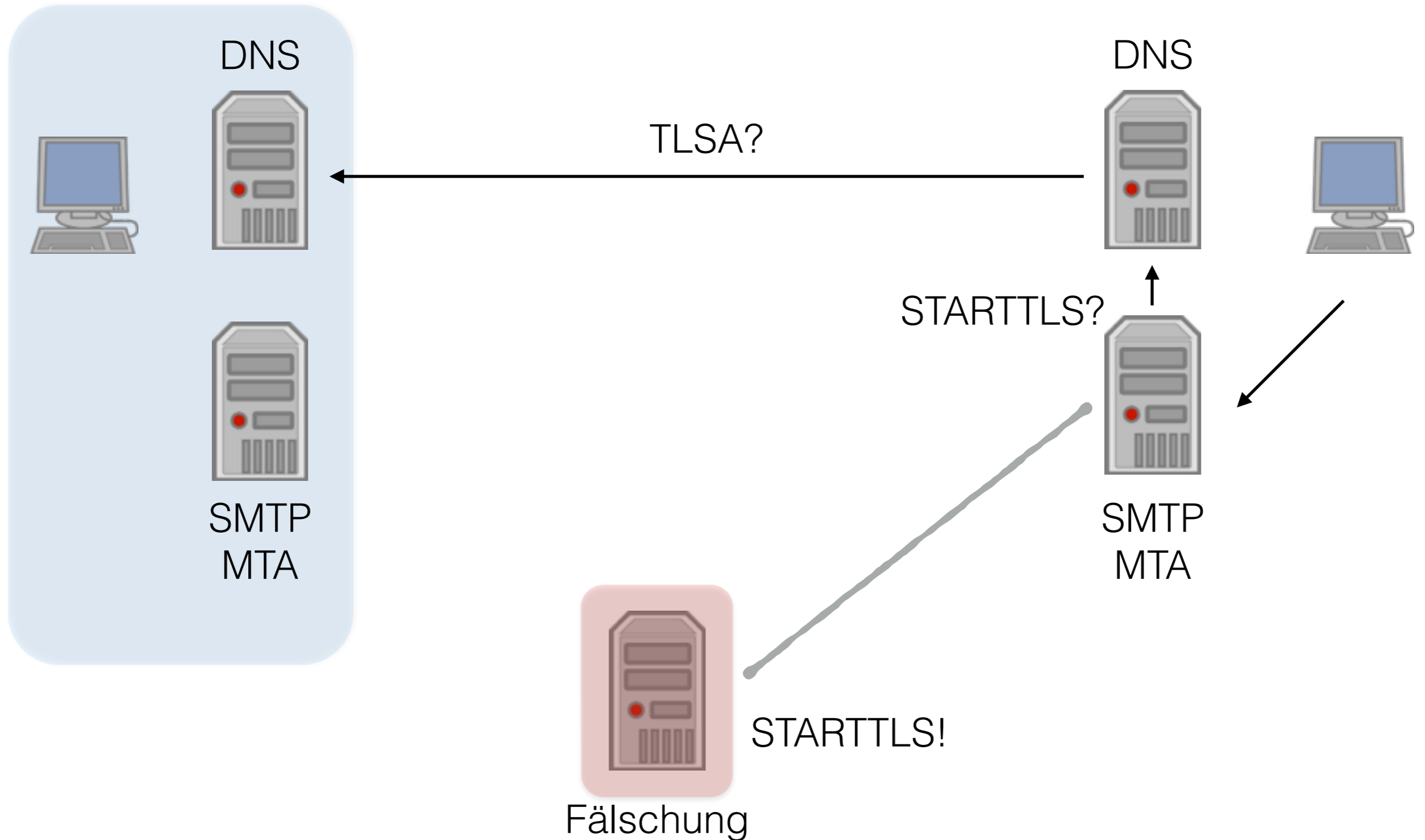
TLS und SMTP



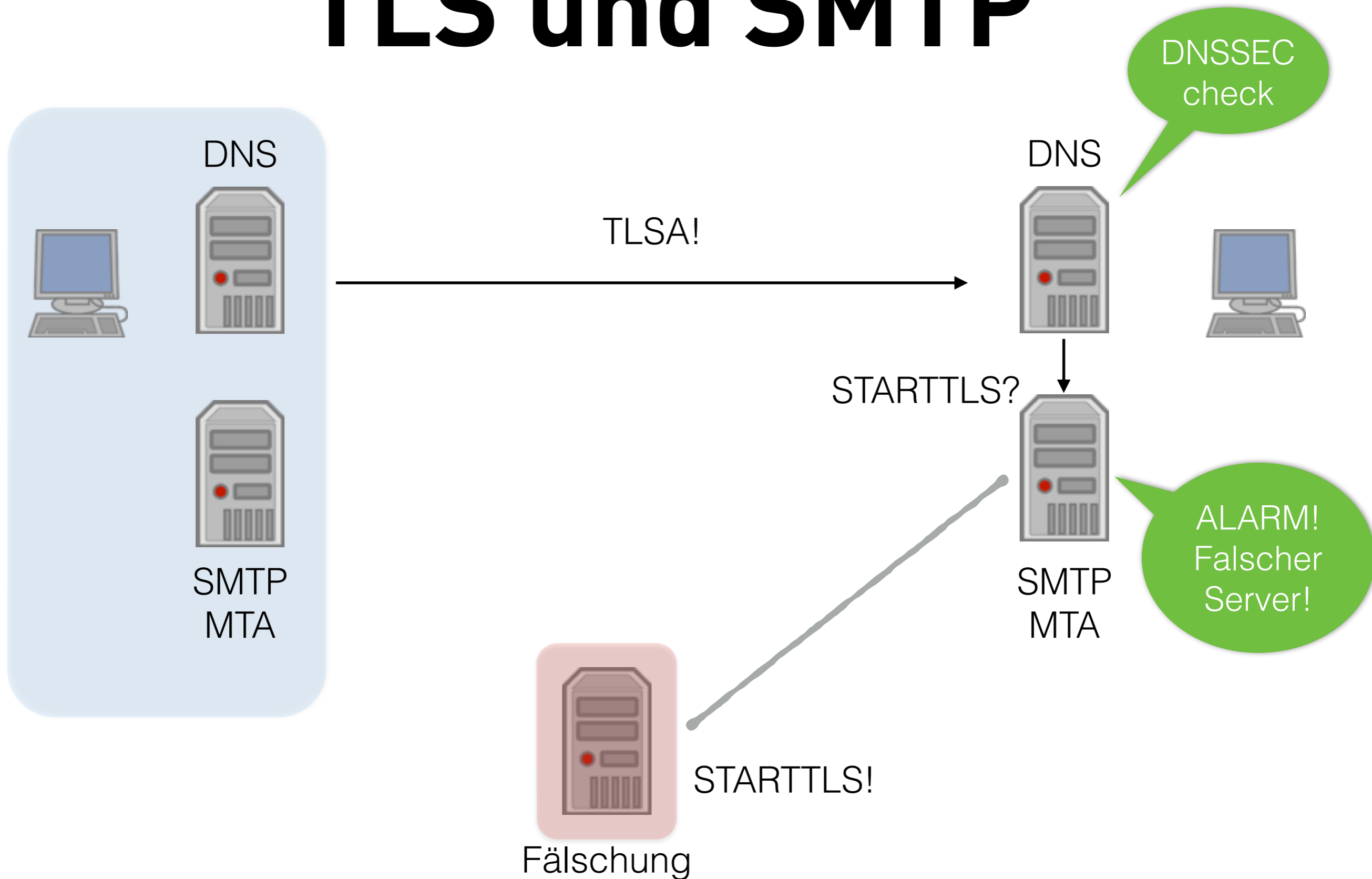
TLS und SMTP



TLS und SMTP



TLS und SMTP



Infrastruktur DNS

- **DNSSEC Validierung (Caching DNS Resolver)**
 - **BIND 9, Unbound, dnsmasq, Windows 2012**
- **DNSSEC signierte Zonen (Authoritativer DNS Server)**
 - **BIND 9, NSD, Knots, Y.A.D.I.F.A., PowerDNS, Bundy-DNS, Windows 2012**

Infrastruktur Mail

- **MTA mit TLSA Unterstützung**
 - **Postfix 2.11, Exim (in Vorbereitung)**
- **TLS Zertifikate**
 - **EV-Zertifikat (Extended Validation)**
 - **DV-Zertifikat (Domain Validation)**
 - **Self-signed Zertifikat**

BIND 9.9.x DNSSEC

- **DNSSEC Validierung einschalten:**

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

TLSA-Record

- **TLSA hash manuell erstellen:**

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

- **TLSA Record:**

```
_25._tcp.mail.example.de. 3588 IN TLSA 3 1 1 (  
8cb0fc6c527506a053f4f14c8464bebbd6dede  
2738d11468dd953d7d6a3021f1 )
```

TLSA-Record testen

```
shell> dig _25._tcp.mail.example.de TLSA +dnssec +m
; <<>> DiG 9.9.5 <<>> _25._tcp.mail.example.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
      xV80BnAzhF4RMKSabHF0LNwRzWqE5xNfPibMQFDoDRKJ
      /QiNgux/IXti3JqtH4BkT0w70oi+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
```

DNSSEC
check OK

TLSA
Record

DNSSEC
Signatur

Postfix Konfiguration

- **TLSA Prüfung in der Postfix Konfiguration:**

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


STARTTLS testen

- **Test einer STARTTLS-Verbindung zum Mailserver:**

```
shell> openssl s_client -connect mail1.example.de:25 -starttls smtp
CONNECTED(00000003)
---
Certificate chain
 0 s:/C=DE/ST=State/L=City/O=Company/OU=Mailserver/CN=mail1.example.de
  i:/C=DE/ST=State/L=City/O=Company/OU=Mailserver/CN=mail1.example.de
---
Server certificate
-----BEGIN CERTIFICATE-----
[...]
    Start Time: 1394991261
    Timeout    : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
221 2.0.0 Bye
closed
shell>
```

Postfix log (ungesichertes TLS)

- **Postfix log TLS ohne DNSSEC TLSA Prüfung (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 gesichertes TLS)

- **Postfix log TLS mit DNSSEC TLSA Prüfung (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 3fn8BY31tPzTT)
```

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

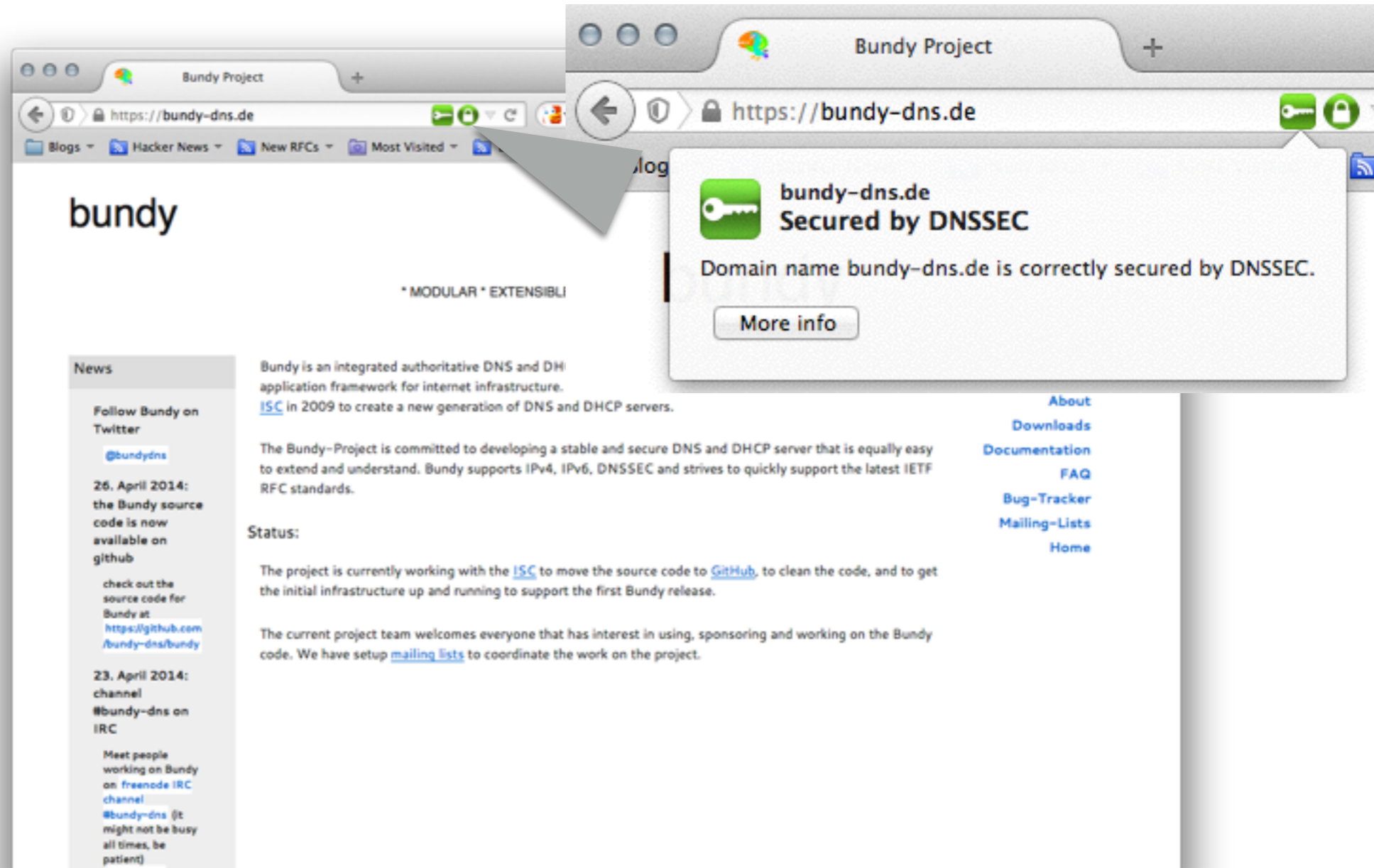
DANE TLSA Vorteile

- **Verschlüsselte Verbindung zwischen Server wird authentisiert**
- **STARTTLS "downgrade" Angriffe werden verhindert**
- **TLS/SSL Zertifikate sind gegen Fälschung abgesichert**
- **CRL/OCSP wird nicht benötigt, um TLS/SSL Zertifikate auszutauschen**

Mehr als nur SMTP

- **TLSA für HTTPS**
- **OPENPGPKEY — PGP Schlüssel im DNS**
- **IPSECKEY — IPSEC Schlüssel im DNS**
- **SSHFP — SSH Server Fingerprints**
- **S/MIME**
- **SRV — DNS Service Discovery**

www.dnssec-validator.cz



MEN&MICE



[?]

Patrick Ben Koetter — p@sys4.de

Carsten Strotmann — carsten@menandmice.com
cs@sys4.de

Links

- **Sys4 Blog** - <http://blog.sys4.de>
- **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" Arbeitsgruppe** - <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 Ausgabe 11/2014 - Seite 194 "Geleitschutz"**
- **TLSA generator webpage** - https://www.huque.com/bin/gen_tlsa
- **"hash-slinger" von Paul Wouters (Red Hat)** - <http://people.redhat.com/pwouters/hash-slinger/>
- **DNSSEC Schulungen** —
<http://www.linuxhotel.de/kurs/dnssec/>
<http://www.menandmice.com/support-training/training/dnssec-workshop/>