Securing Security - SMTP DANE with Postfix

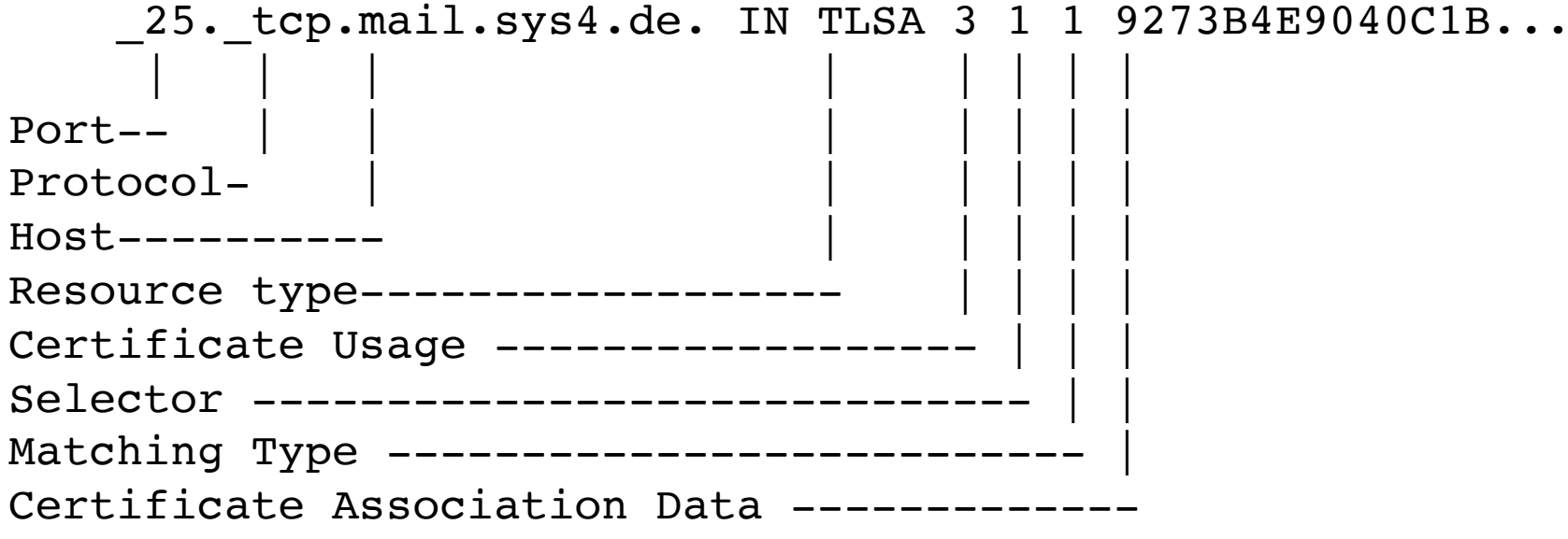
Patrick Koetter und Carsten Strotmann, sys4 AG

CREATED: 2023-10-20 FRI 07:12

Postfix TLS security

- Postfix is an open source Mail-Transfer-Agent (MTA) with a special security architecture (multi process daemon with different privilege level)
- The DANE implementation in Postfix is the reference implementation for DANE-SMTP
- DANE-SMTP inside Postfix has been developed and implemented by Viktor Dukhovni
- Viktor has written the *DANE for SMTP* RFC and lead its standardization inside the IETF
- Postfix is currently the only open source software that implements the full DANE specs

SMTP-DANE - TLSA-Record in DNS



Trust is good - Validation is better

- SMTP TLS without DANE

```
Jul 14 11:03:31 mail postfix/smtp[6477]: Trusted TLS connection established to mx-ha.example.de
  [213.165.67.104]:25: TLSv1.1 with cipher DHE-RSA-AES256-SHA (256/256 bits)
```

- SMTP TLS with DANE

```
Jul 14 11:04:44 mail postfix/smtp[6409]: Verified TLS connection established to mail.sys4.de
  [194.126.158.139]:25: TLSv1 with cipher ECDHE-RSA-AES256-SHA (256/256 bits)
```

DANE in Postfix step 1 - Creating a TLS certificate

- We create the private (RSA-) key for the x509 certificate

```
# mkdir /etc/postfix/tls
# cd /etc/postfix/tls

# openssl genrsa -out mail.zoneXX.dnslab.org.key 4096
Generating RSA private key, 4096 bit long modulus
.....................................................
.....................................++
..............++
e is 65537 (0x10001)
```

DANE in Postfix step 2 - sign the key to generate a self-signed certificate

- We can use self-signed certificates with DANE-SMTP. These commands sign the public key with the private key to generate a self-signed certificate:

```
# openssl req -new -key mail.zoneXX.dnslab.org.key \
          -out mail.zoneXX.dnslab.org.csr

# openssl x509 -req -days 365 -in mail.zoneXX.dnslab.org.csr \
    -signkey mail.zoneXX.dnslab.org.key -out mail.zoneXX.dnslab.org.crt
Signature ok
subject=/C=de/ST=state/L=city/O=company/CN=mail.zoneXX.dnslab.org/emailAddress=nutzer@zoneXX
Getting Private key

# chmod 400 mail.zoneXX.dnslab.org.*
```

DANE in Postfix step 3 - TLS configuration

- These commands change the Postfix configuration to use the generated certificate and to use DNSSEC and DANE for validating certificates

```
# postconf -e "myhostname = mail.zoneXX.dnslab.org"
# postconf -e "smtp_tls_loglevel = 1"
# postconf -e "smtp_tls_security_level = dane"
# postconf -e "smtp_dns_support_level = dnssec"
# postconf -e "smtpd_tls_security_level = may"
# postconf -e "smtpd_tls_key_file = /etc/postfix/tls/mail.zoneXX.dnsla
# postconf -e "smtpd_tls_cert_file = /etc/postfix/tls/mail.zoneXX.dnsl
# postconf -e "smtpd_tls_loglevel = 1"
# postconf -e "smtpd_tls_received_header = yes"
# postconf -e "smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt"
# postfix reload
# systemctl status postfix
```

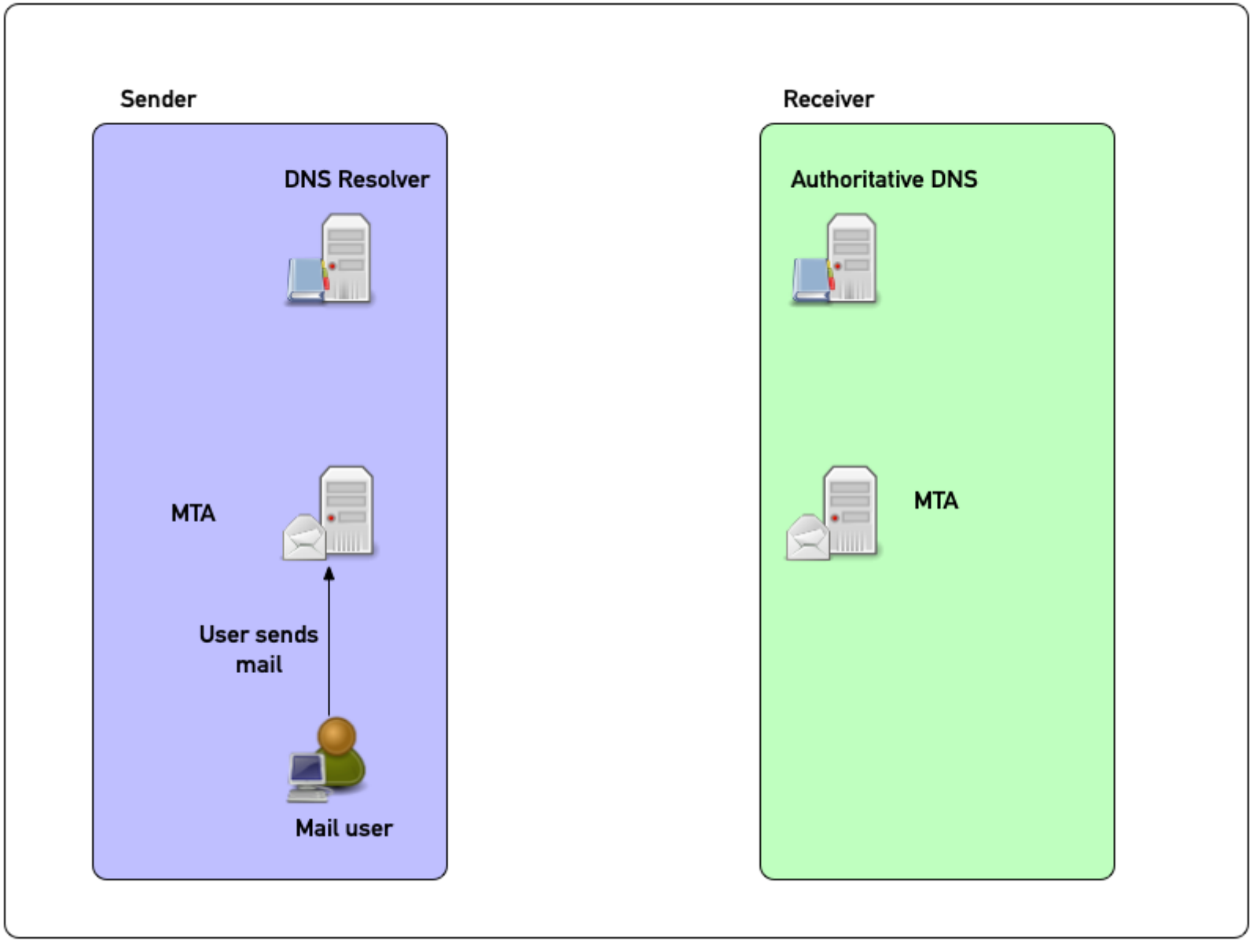
DANE in Postfix step 4 - Testing the TLS connection

- We can use the OpenSSL command **`s_client`** to open a TLS secured connection to the Postfix mailserver

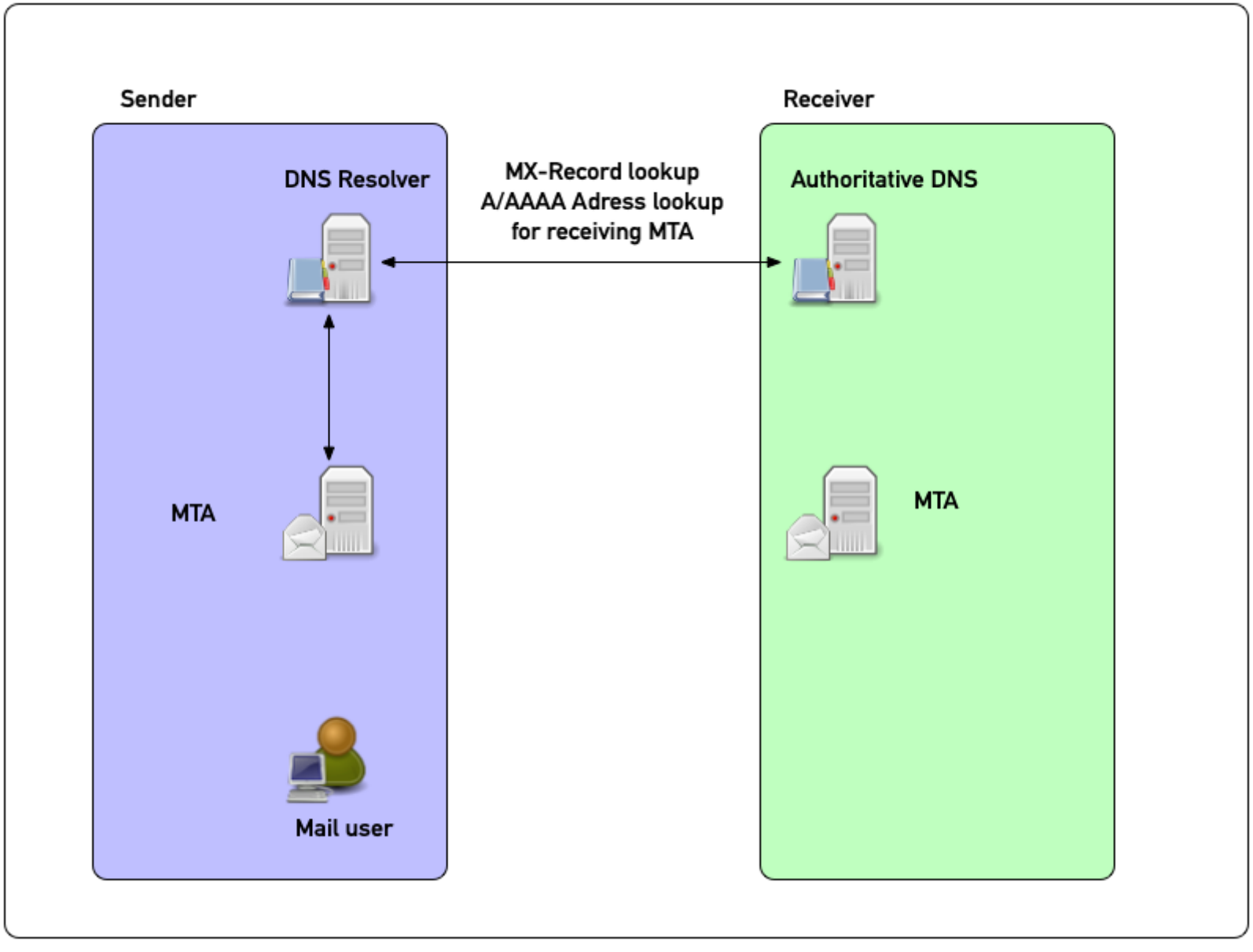
```
# openssl s_client -connect mail.zoneXX.dnslab.org:25 -start
# tail /var/log/maillog
```

DANE for SMTP (TLSA-Record for x509 certificates)

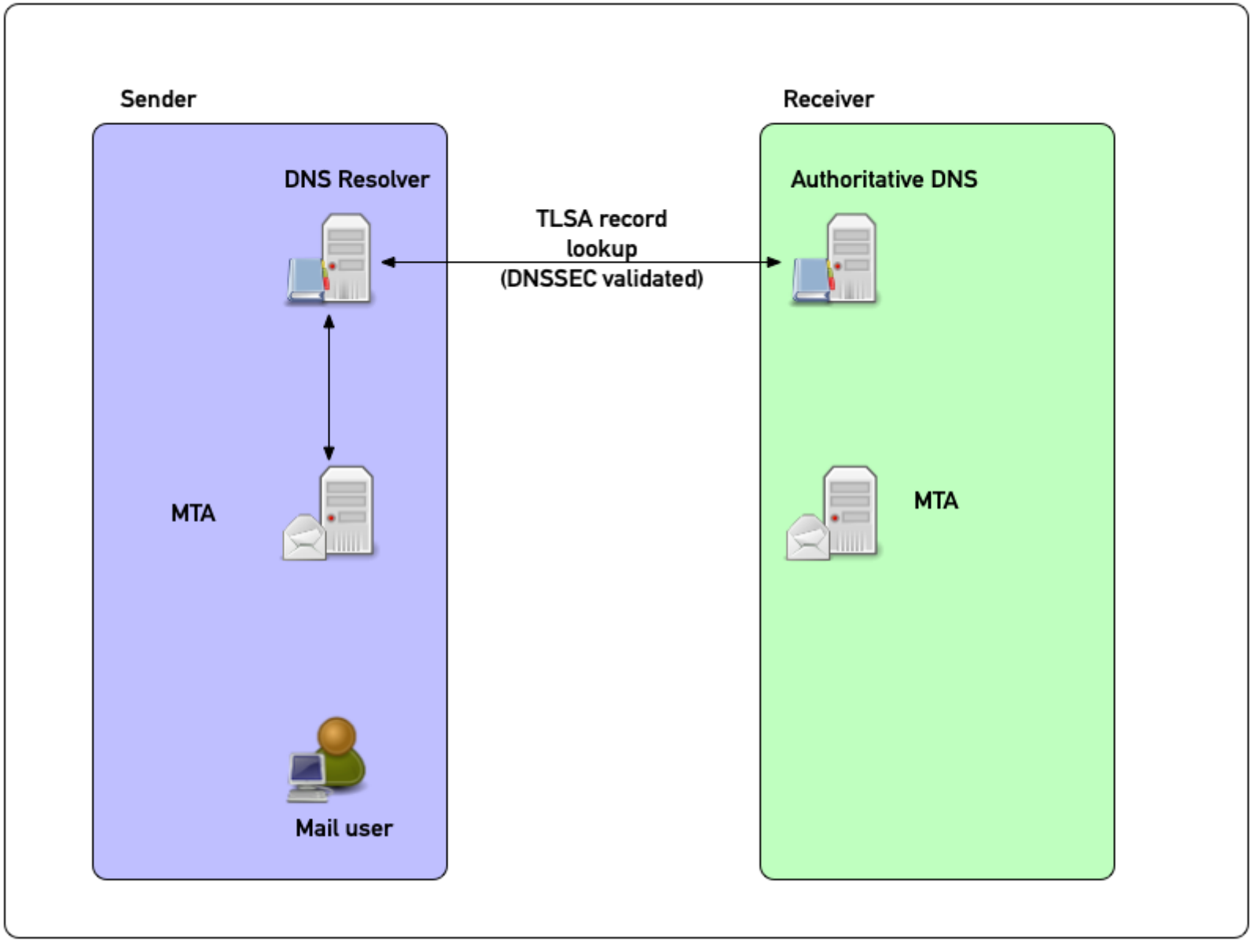
DANE in pictures (1)


Sender
Receiver
DNS Resolver
Authoritative DNS
MTA
MTA
User sends mail
Mail user

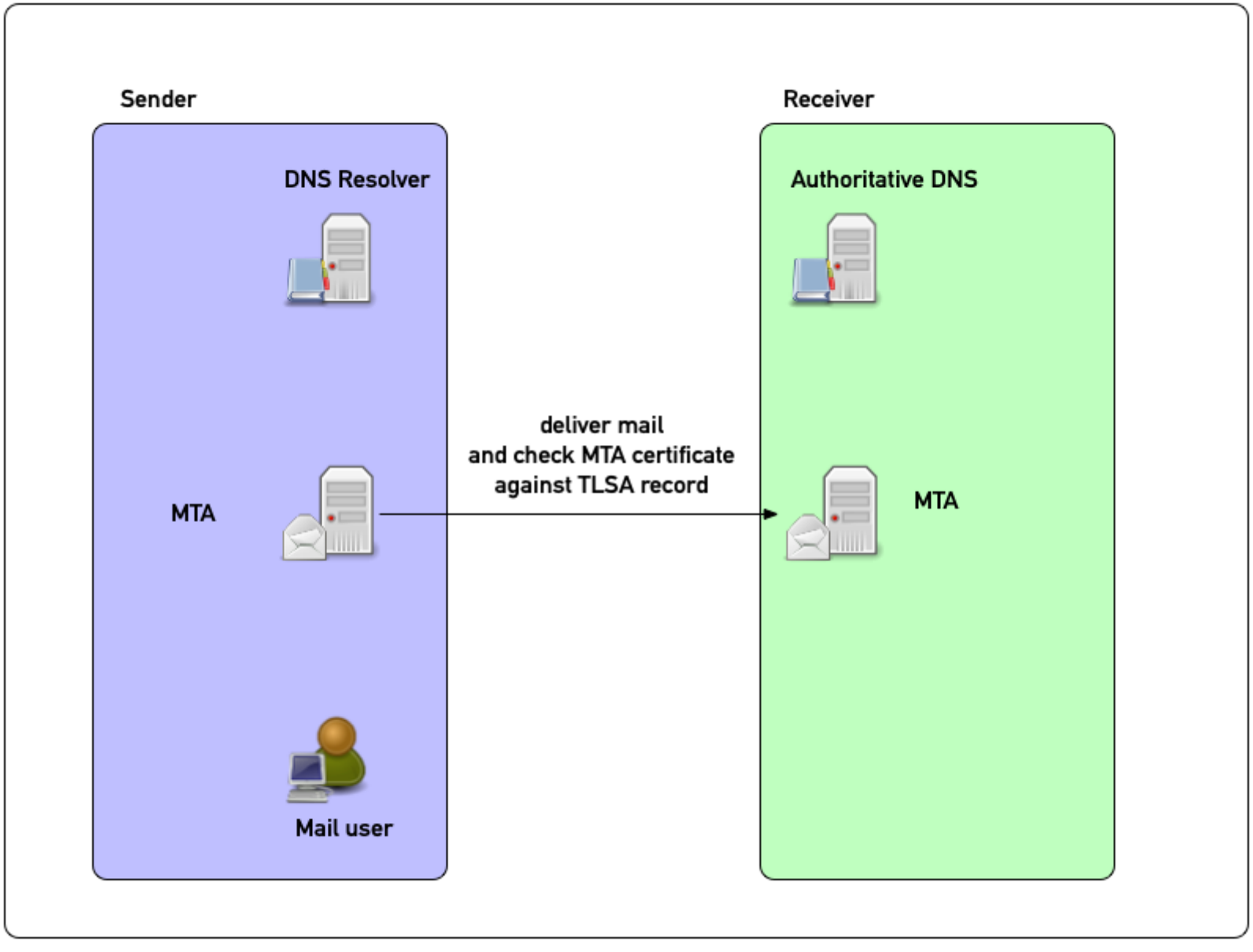
DANE in pictures (2)


Sender
Receiver
DNS Resolver
MX-Record lookup
A/AAAA Adress lookup
for receiving MTA
Authoritative DNS
MTA
MTA
Mail user

DANE in pictures (3)


Sender
Receiver
DNS Resolver
Authoritative DNS
TLSA record
lookup
(DNSSEC validated)
MTA
MTA
Mail user

DANE in pictures (4)


Sender
Receiver
DNS Resolver
Authoritative DNS
deliver mail
and check MTA certificate
against TLSA record
MTA
MTA
Mail user

DANE - generate the TLSA record for the certificate on the mail-server

- We use the command **`ldns-dane`** to create a DANE-TLSA record from the self-signed certificate and add the record to our zone file

```
# ldns-dane -c /etc/postfix/tls/mail.zoneXX.dnslab.org.crt  \
      create mail.zoneXX.dnslab.org 25 3 1 1 >> /var/named/zoneXX.dnslab.org
```

- Next we need to increment the SOA serial number in the zonefile and reload the new zone into the server

```
# rndc reload zoneXX.dnslab.org
```

DANE - Verify that the TLSA record in visible in DNS

- Query the new TLSA-record from a DNSSEC validating resolver. Make sure the DNS answer is DNSSEC secured (AD-Flag!)

```
# dig _25._tcp.mail.zoneXX.dnslab.org tlsa +dnssec +multi @9.9.9.9

[..]
;; ANSWER SECTION:
_25._tcp.mail.zoneXX.dnslab.ORG. 2490 IN TLSA 3 1 1 (
                                 5B9909E641FAB068A193A66B98E3FB0646CBE1AE88D9
                                 01D63F24B9E4778D31D1 )
_25._tcp.mail.zoneXX.dnslab.ORG. 2490 IN RRSIG TLSA 8 6 3600 (
                                 20151104204359 20151005194359 57864 zoneXX.dnslab.org.
                                 1A0uzC9Iglsq9xZzMAPzq3N984fRBH2Yes+TQ3OgQXDO
                                 MstWO22SHvR95gnpv4hPY+b9J6RvMhI4pyzlHFXTIXy3
                                 FVGWR1Gha4sa64ZZHCFBnekFou9WtK9unYagY1q59c3F
                                 wg3Bb7mNy3zO1Mepysx+tW1ZyCvZoeqvAzN0P+agj0ED
                                 m8gt3cO/dRVgi7RgGlyDC8p2o4GvdyykU84Nd+J0zEP6
                                 /irpyHRPfjBQNpaHLW2D7ILLCvSyGpXHPTLg )
```

End

Questions ? Answers !