Fraunhofer SIT

FH MÜNSTER
University of Applied Sciences

Why TLS is better without STARTTLS:

A Security Analysis of STARTTLS in the Email Context

Damian Poddebniak[3], Fabian Ising[1,2], Hanno Böck[3], Sebastian Schinzel[1,2]
@duesee@norden.social @murgi@infosec.exchange @hanno@mastodon.social @seecurity@infosec.exchange

[1] Fraunhofer SIT | ATHENE National Research Center for Applied Cybersecurity

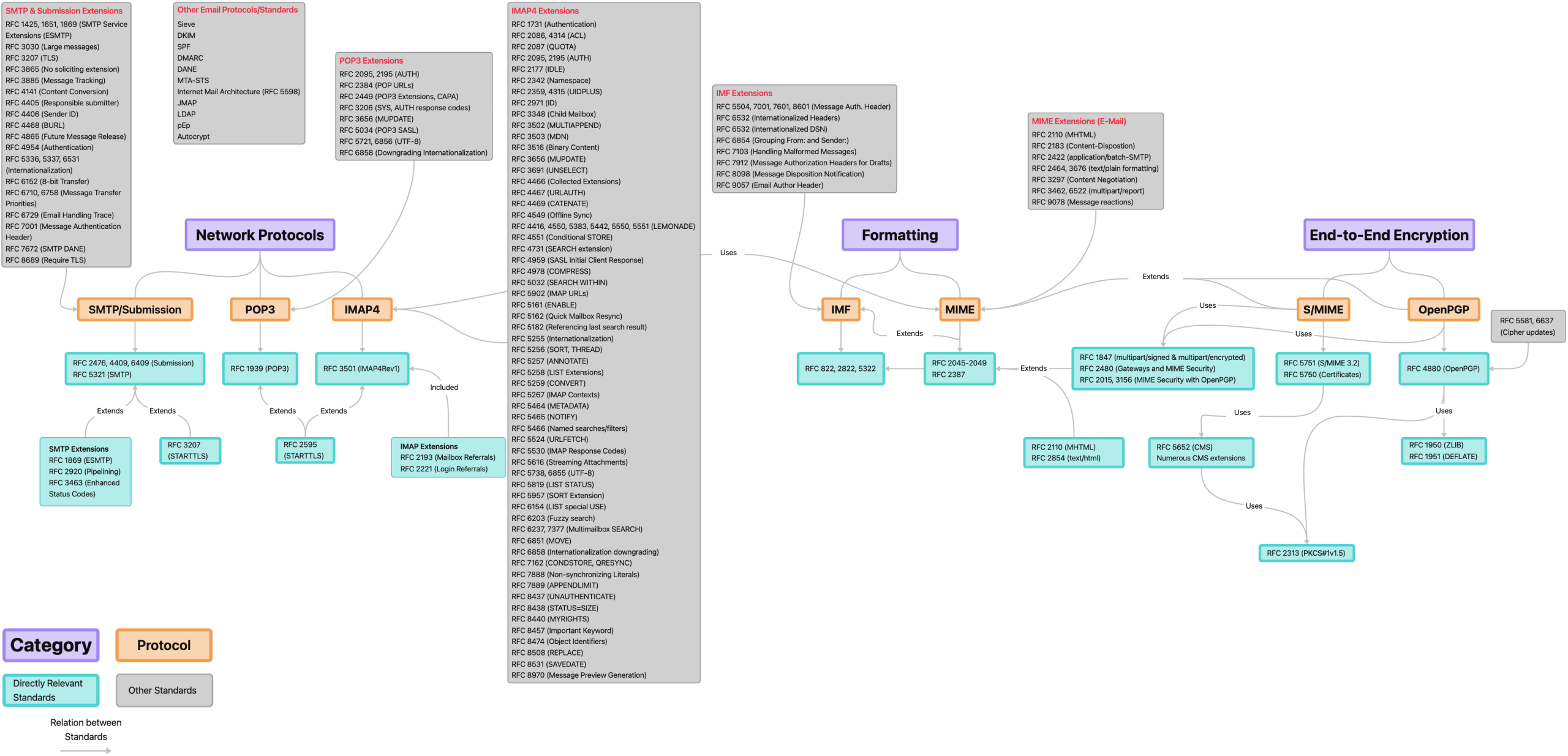
[2] Münster University of Applied Sciences

[3] Independent Researcher

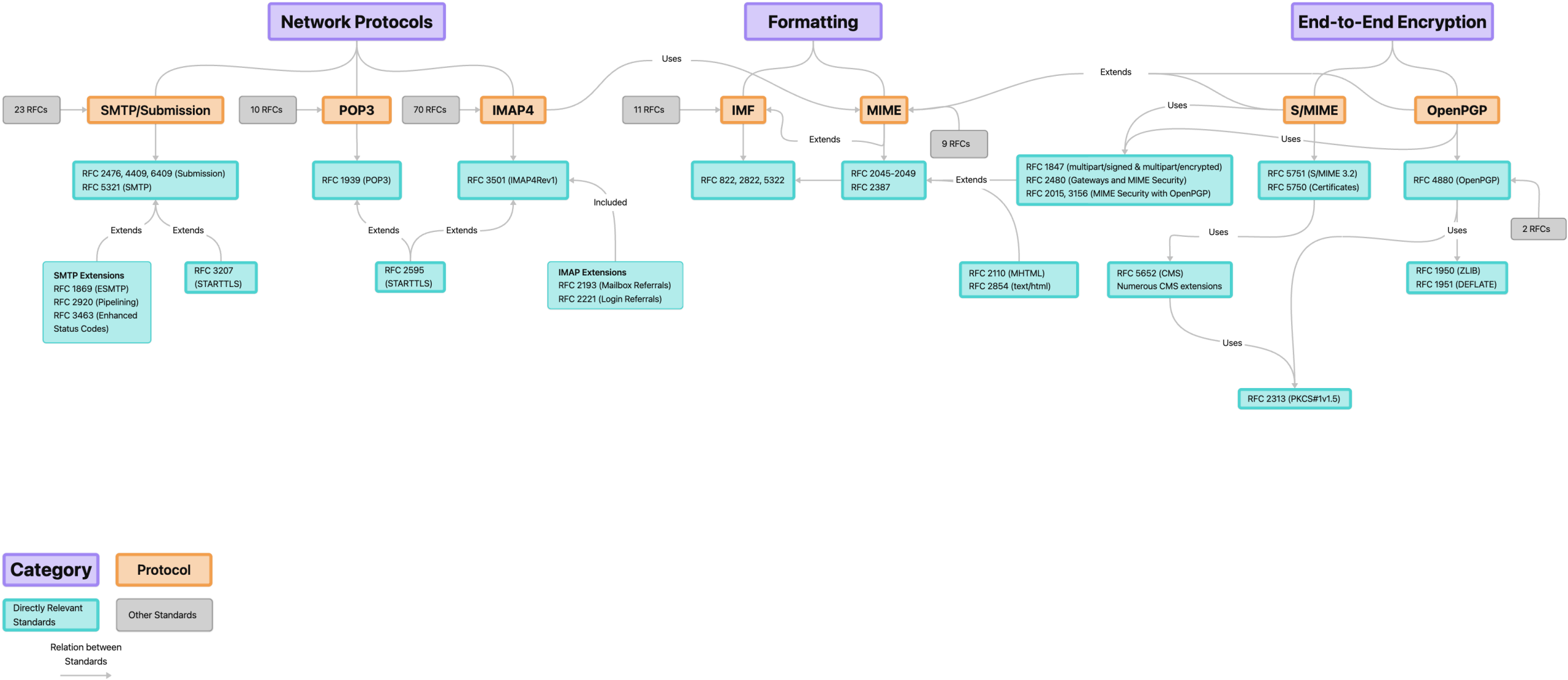
https://nostarttls.secvuln.info/

Client-Side E-Mail Ecosystem

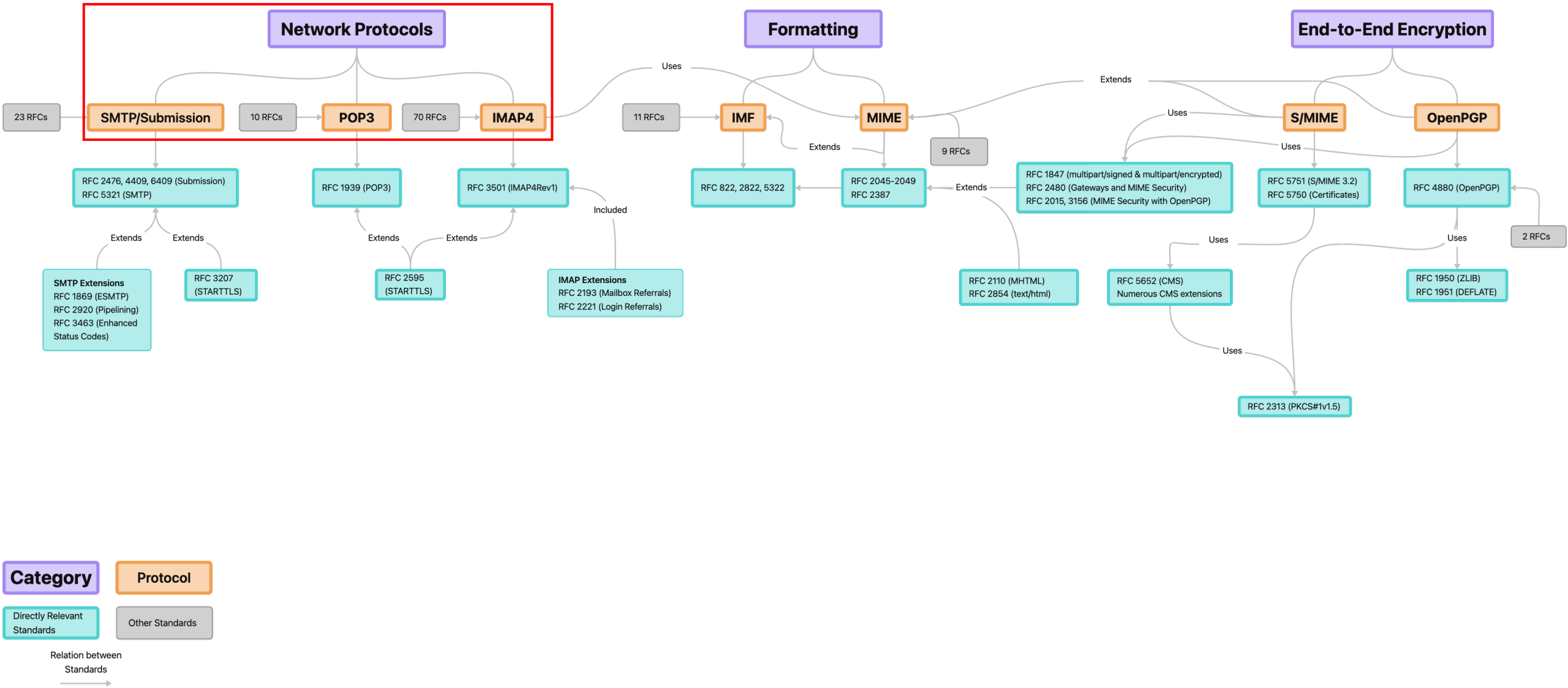
Client-Side E-Mail Ecosystem



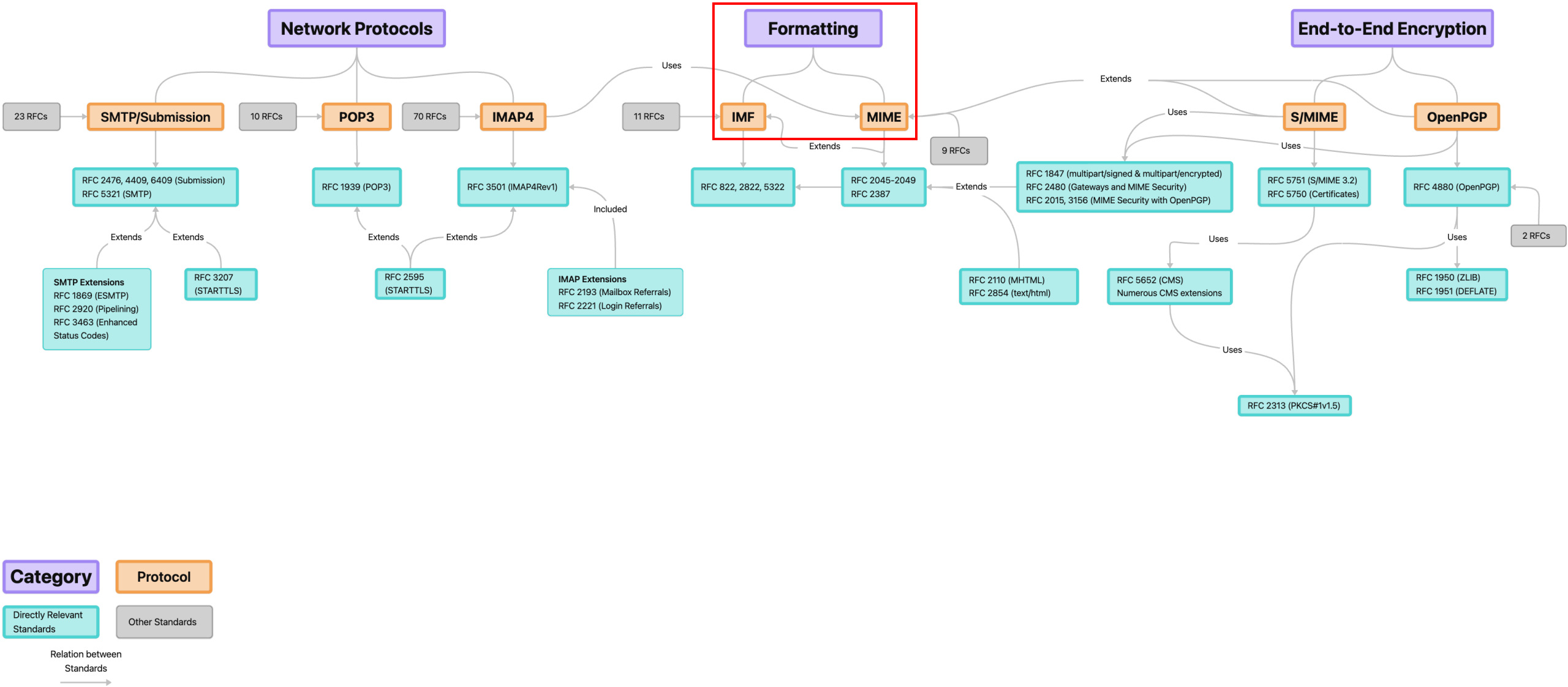
Client-Side E-Mail Ecosystem



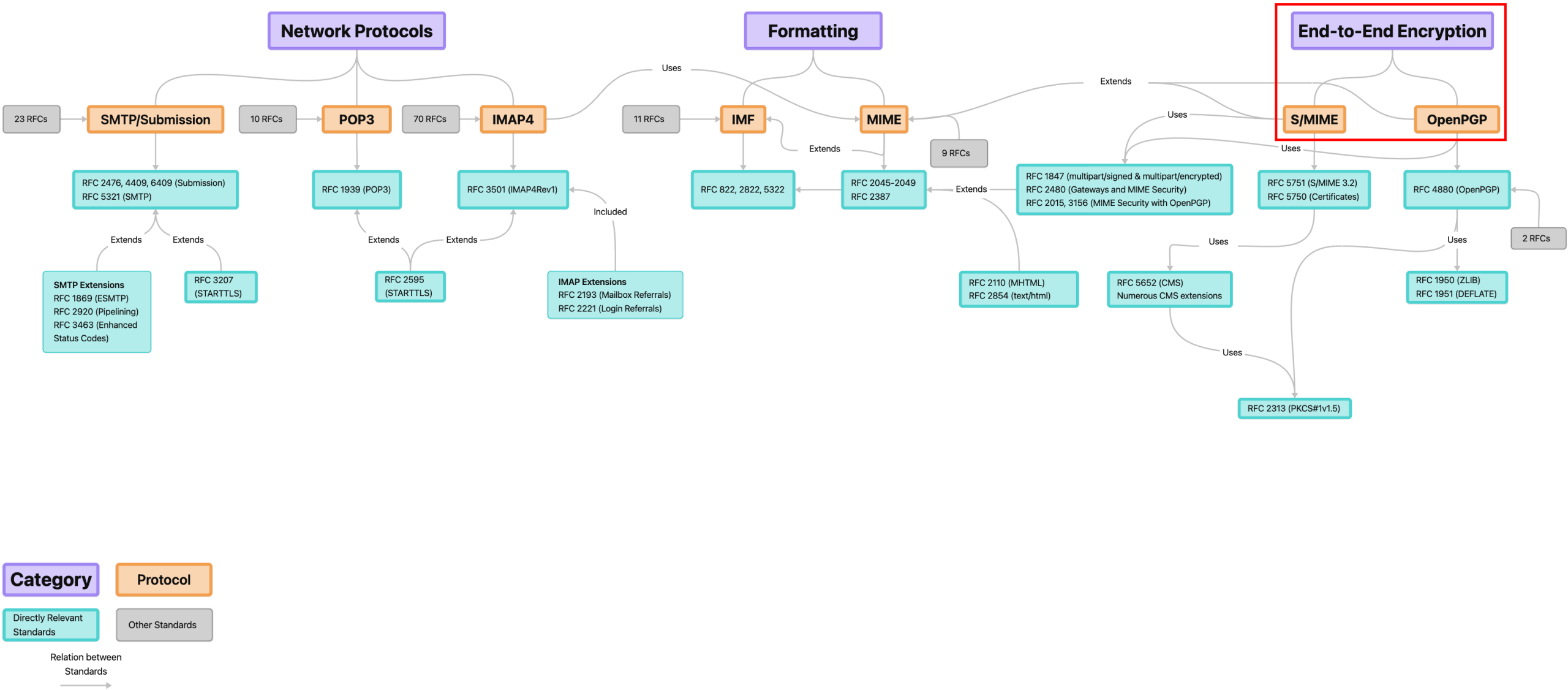
Client-Side E-Mail Ecosystem



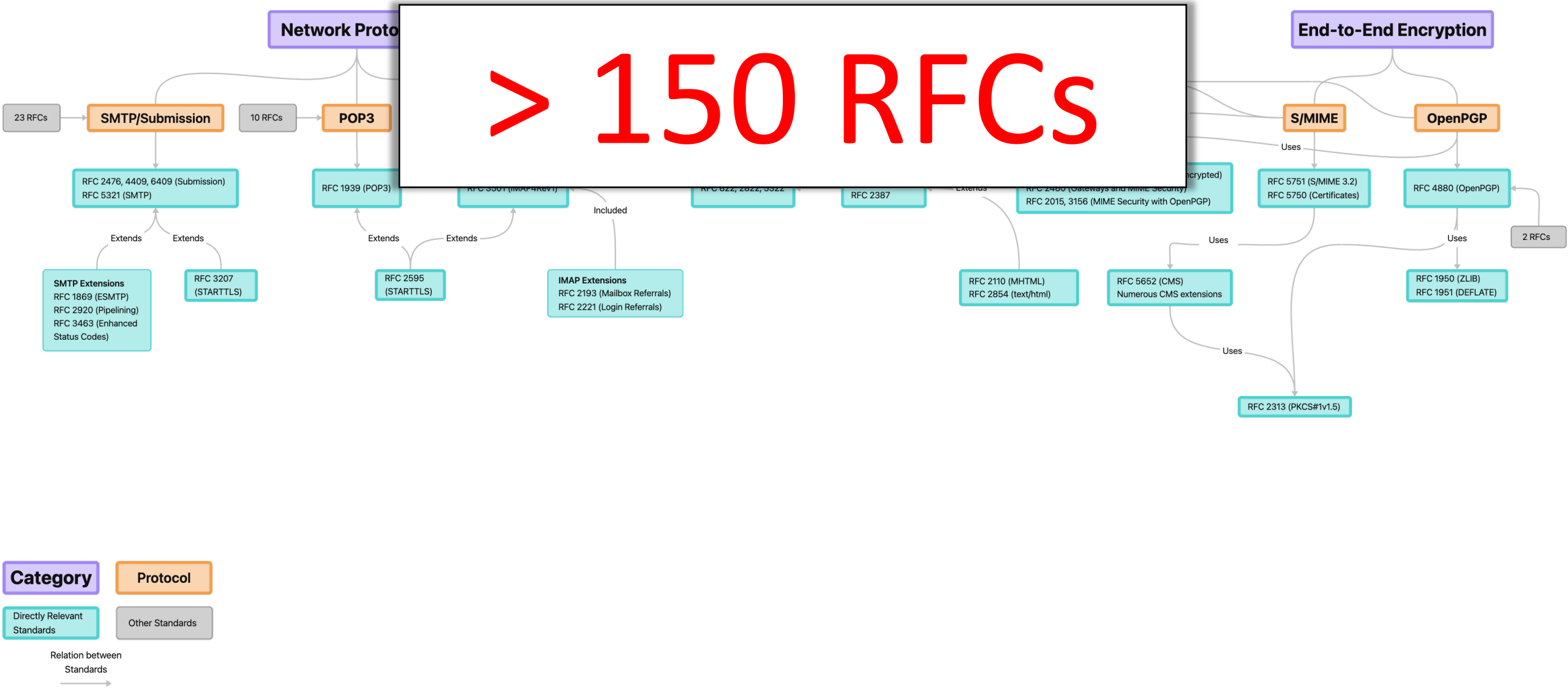
Client-Side E-Mail Ecosystem



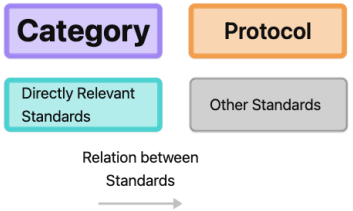
Client-Side E-Mail Ecosystem



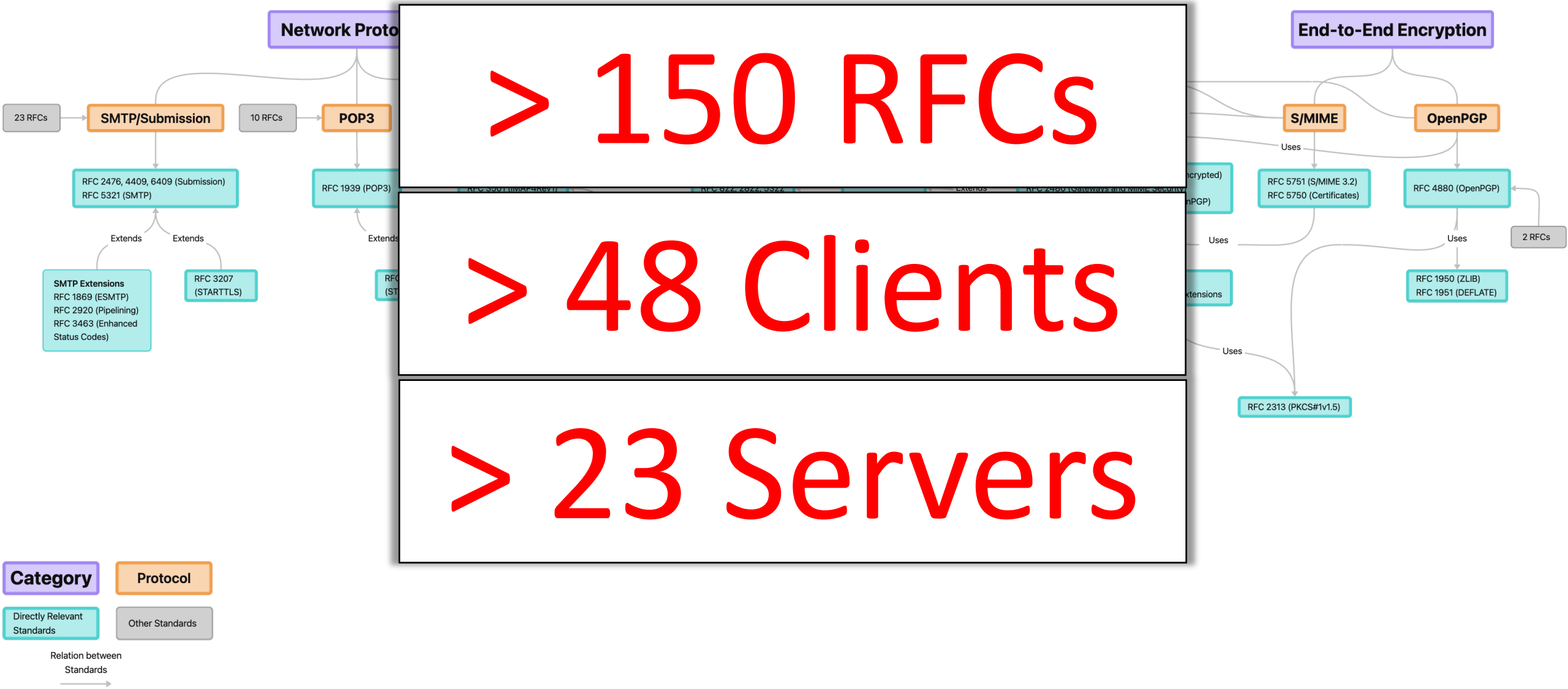
Client-Side E-Mail Ecosystem

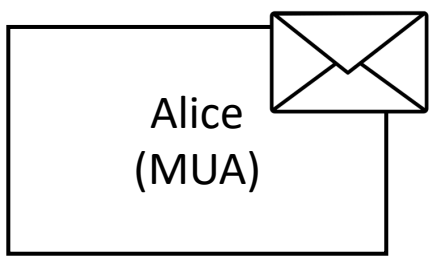


Client-Side E-Mail Ecosystem



Client-Side E-Mail Ecosystem

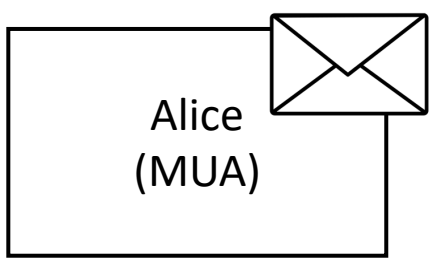




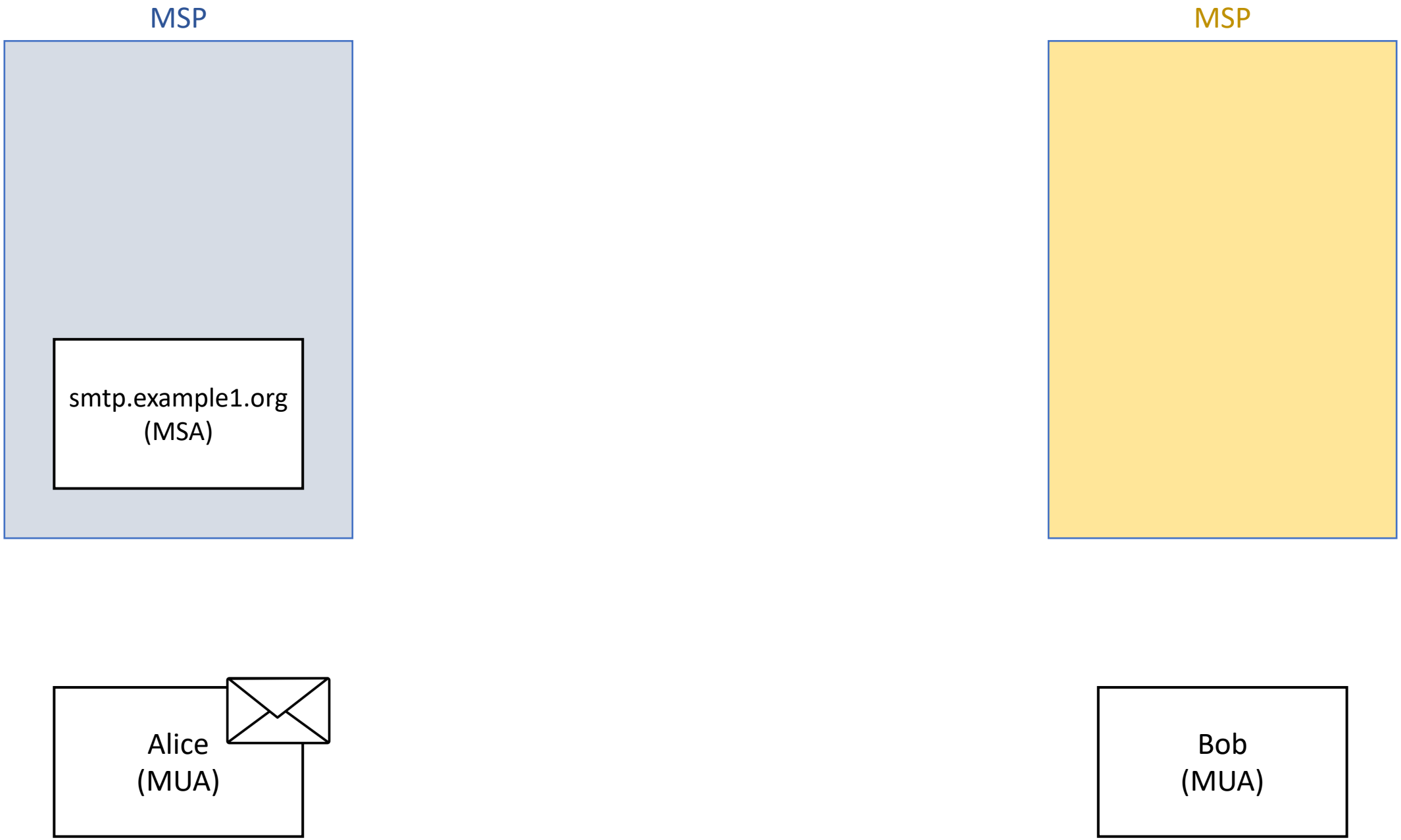
Bob
(MUA)

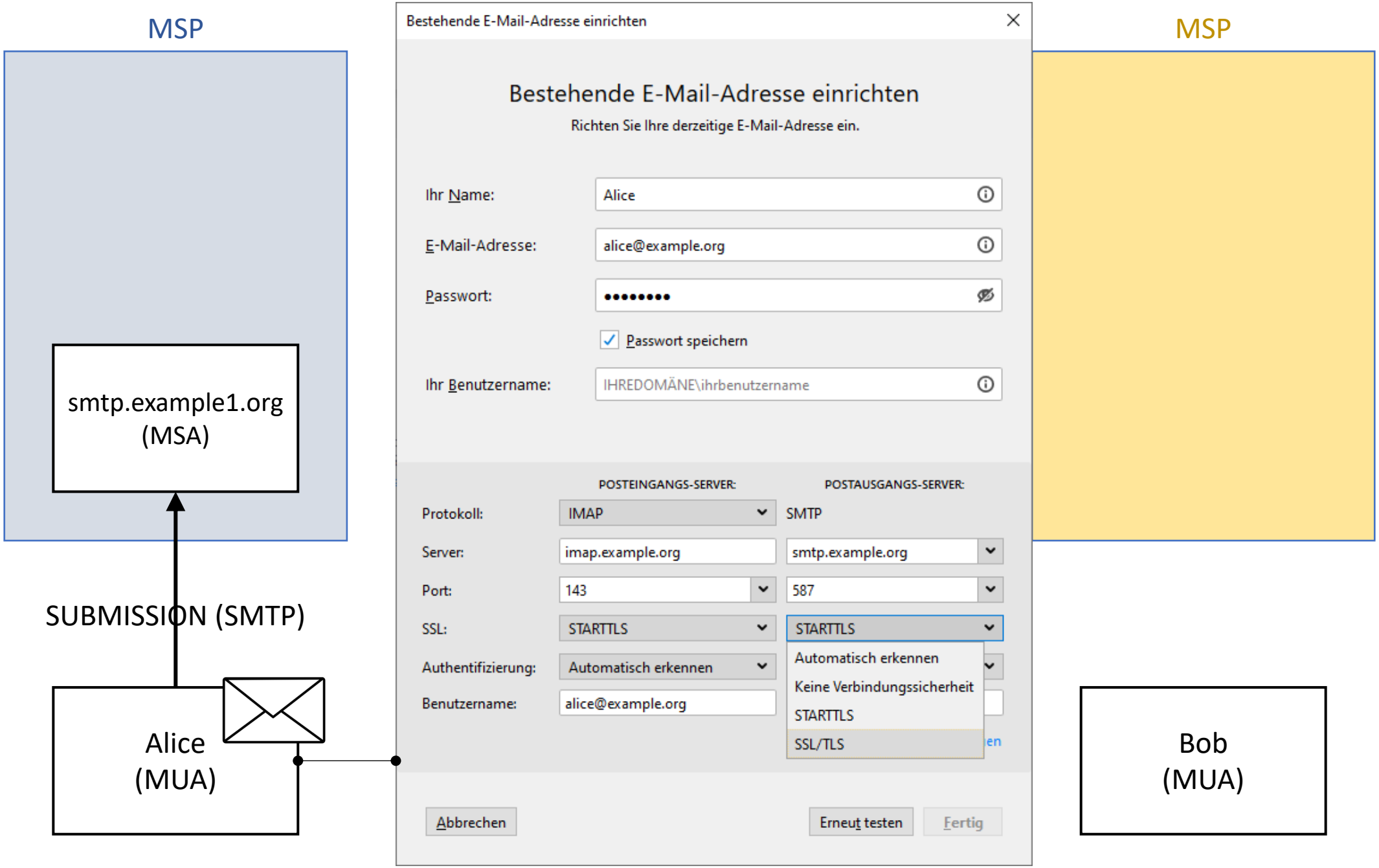
MSP

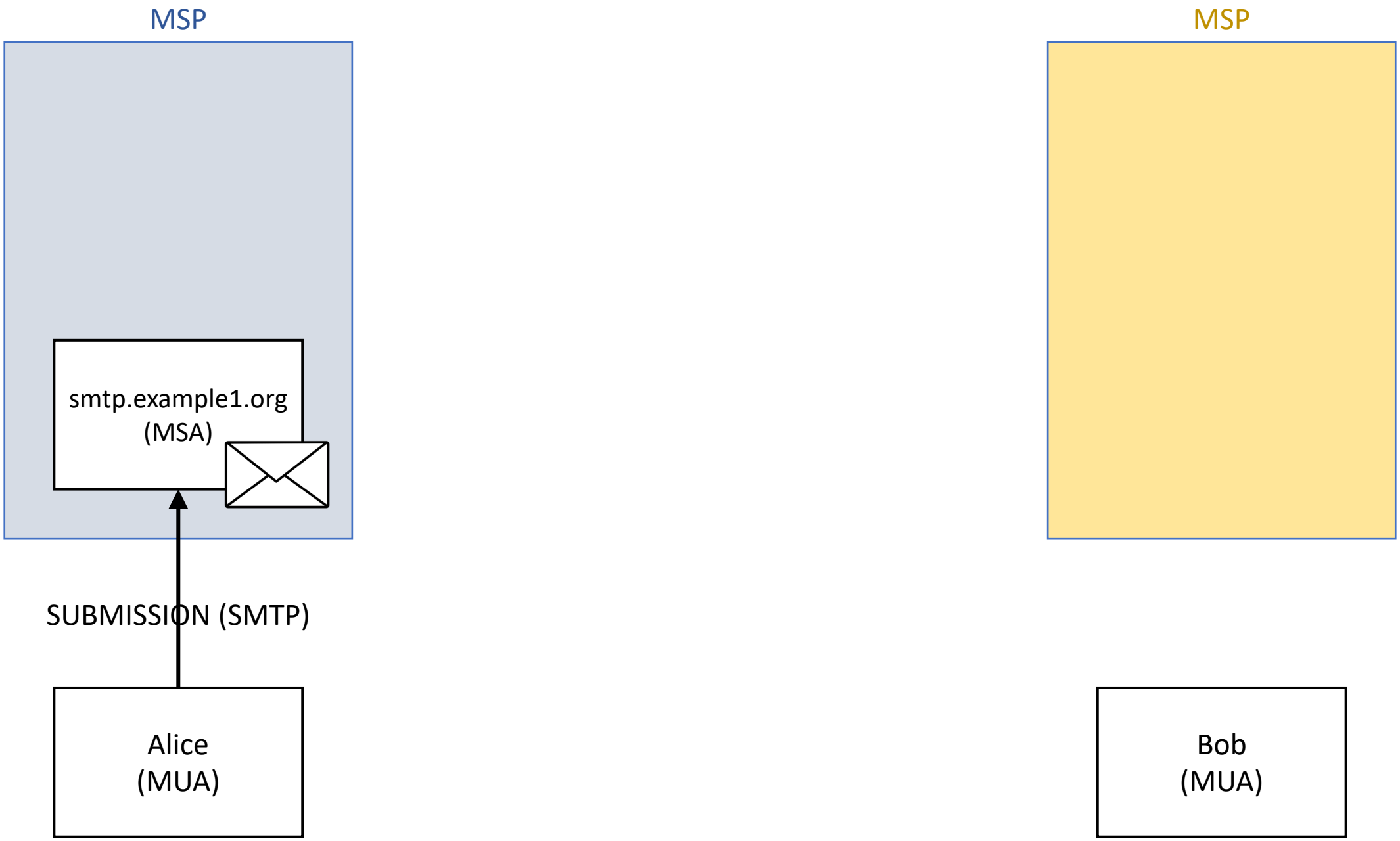
MSP

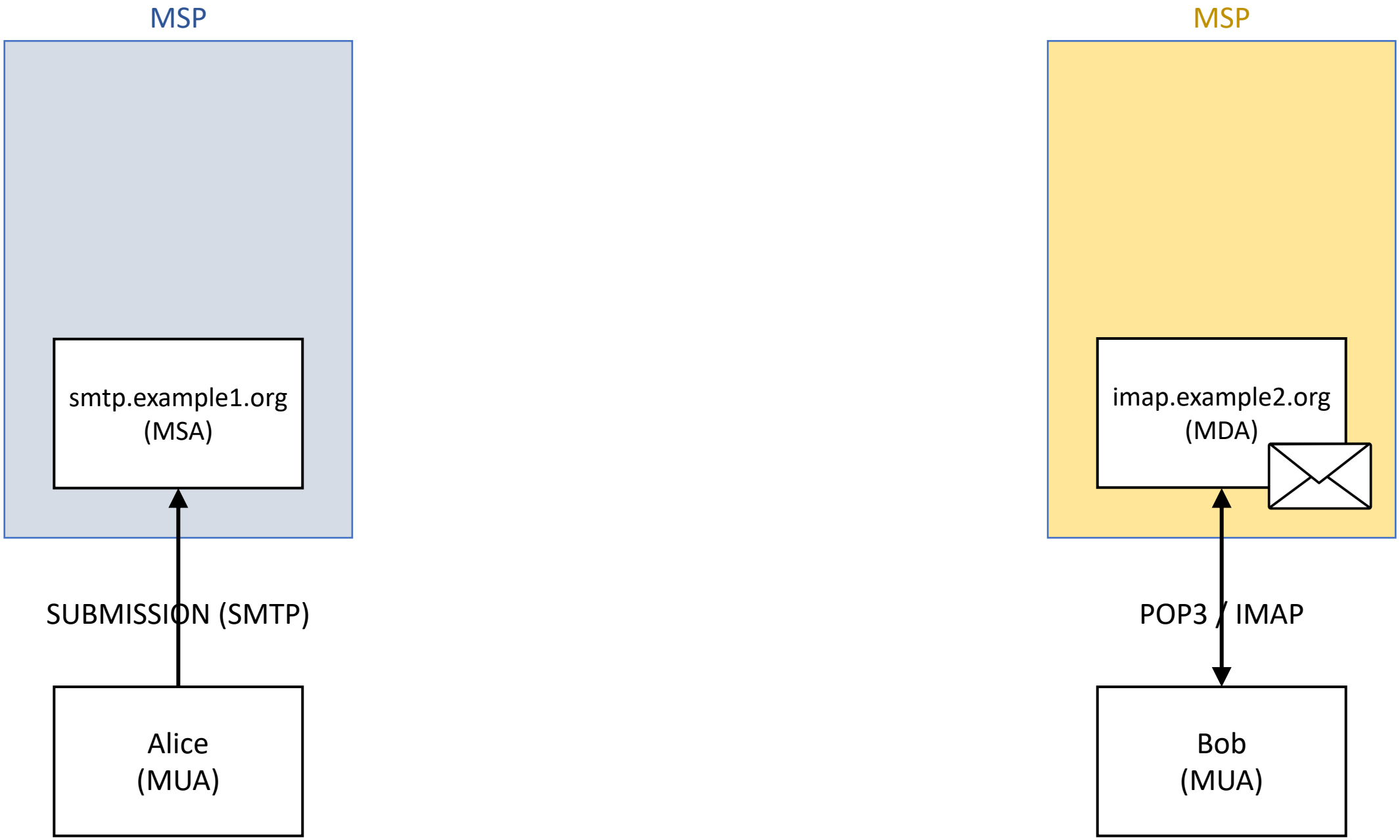


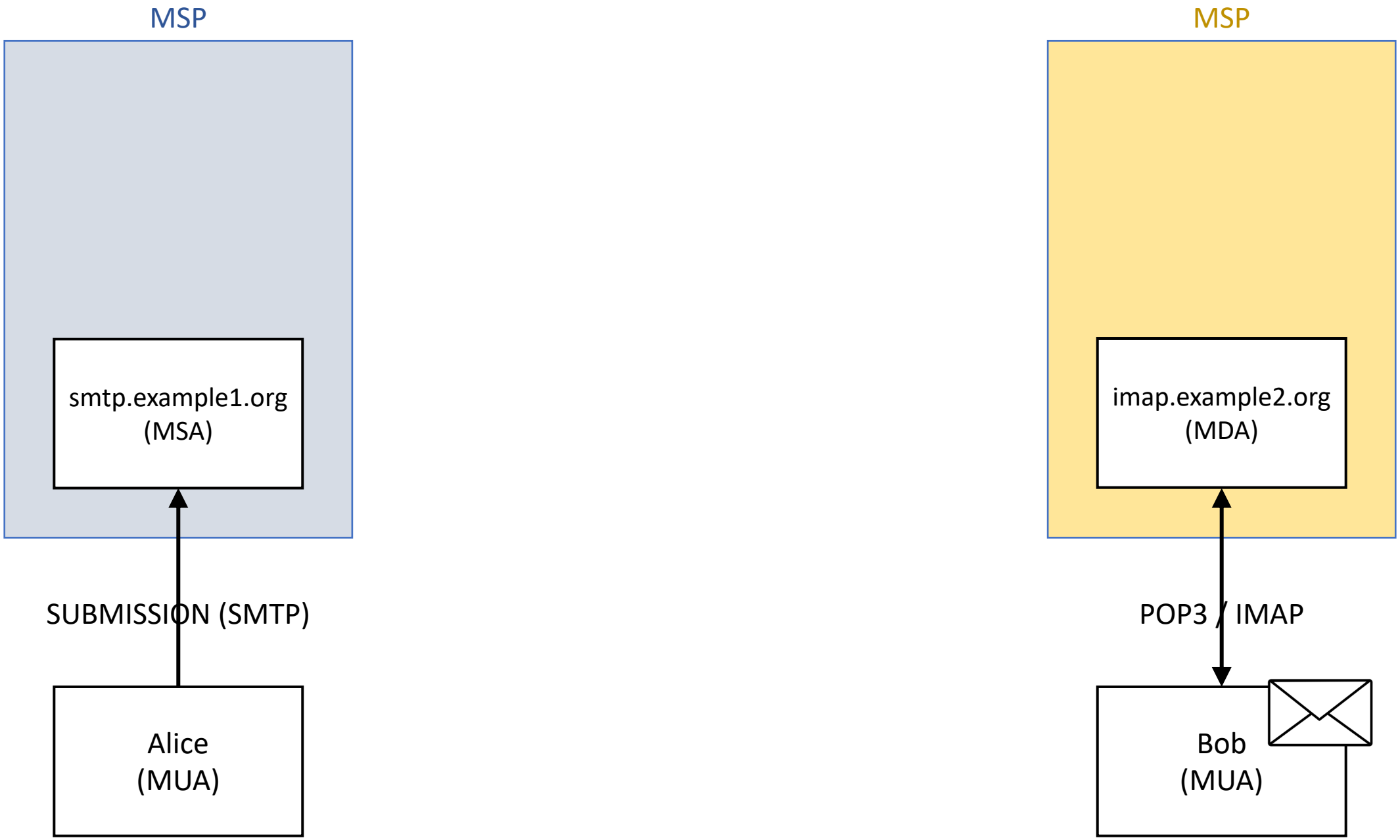
Bob
(MUA)

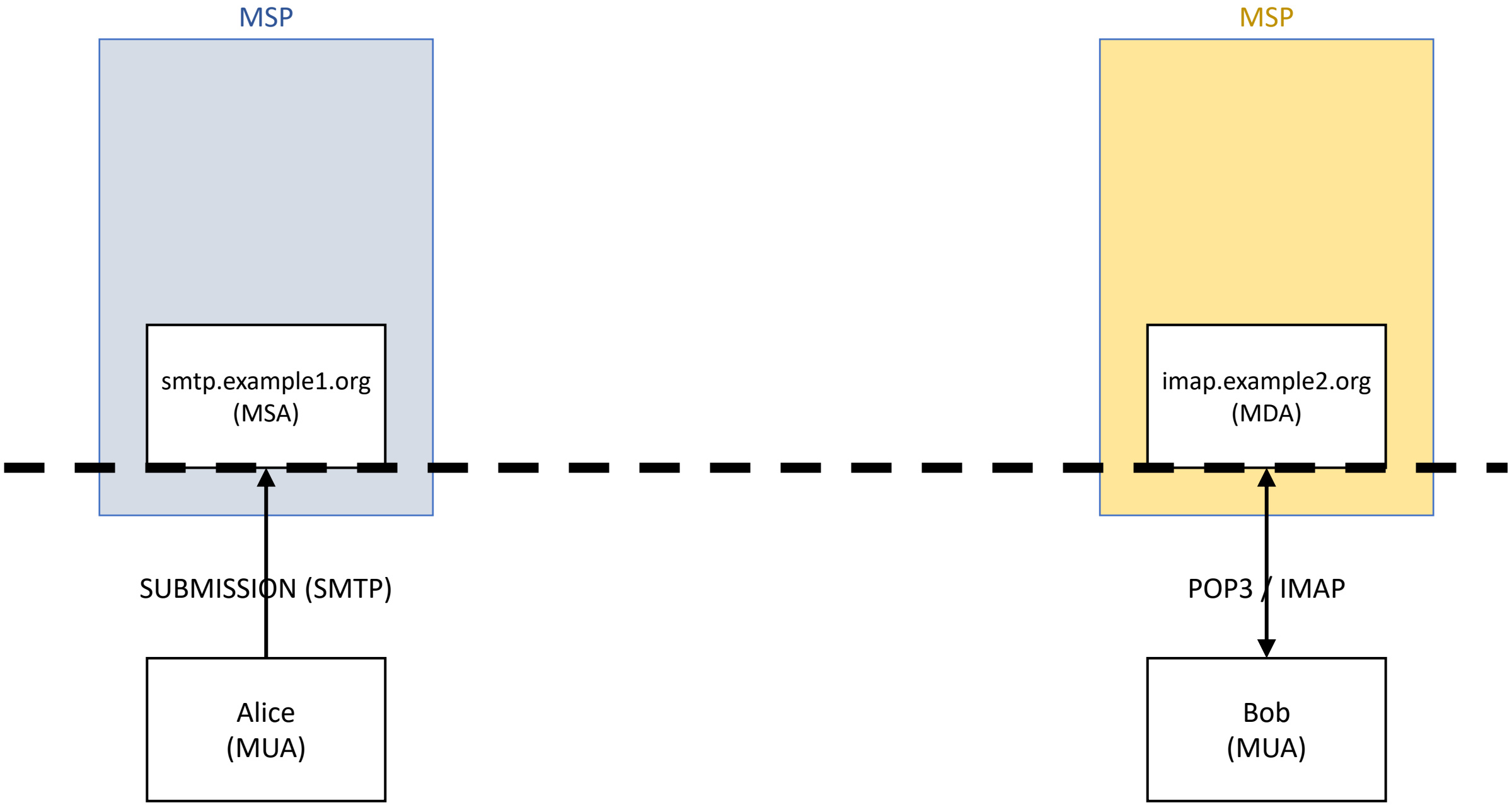

MSP
smtp.example1.org
(MSA)
MSP
Alice
(MUA)
Bob
(MUA)

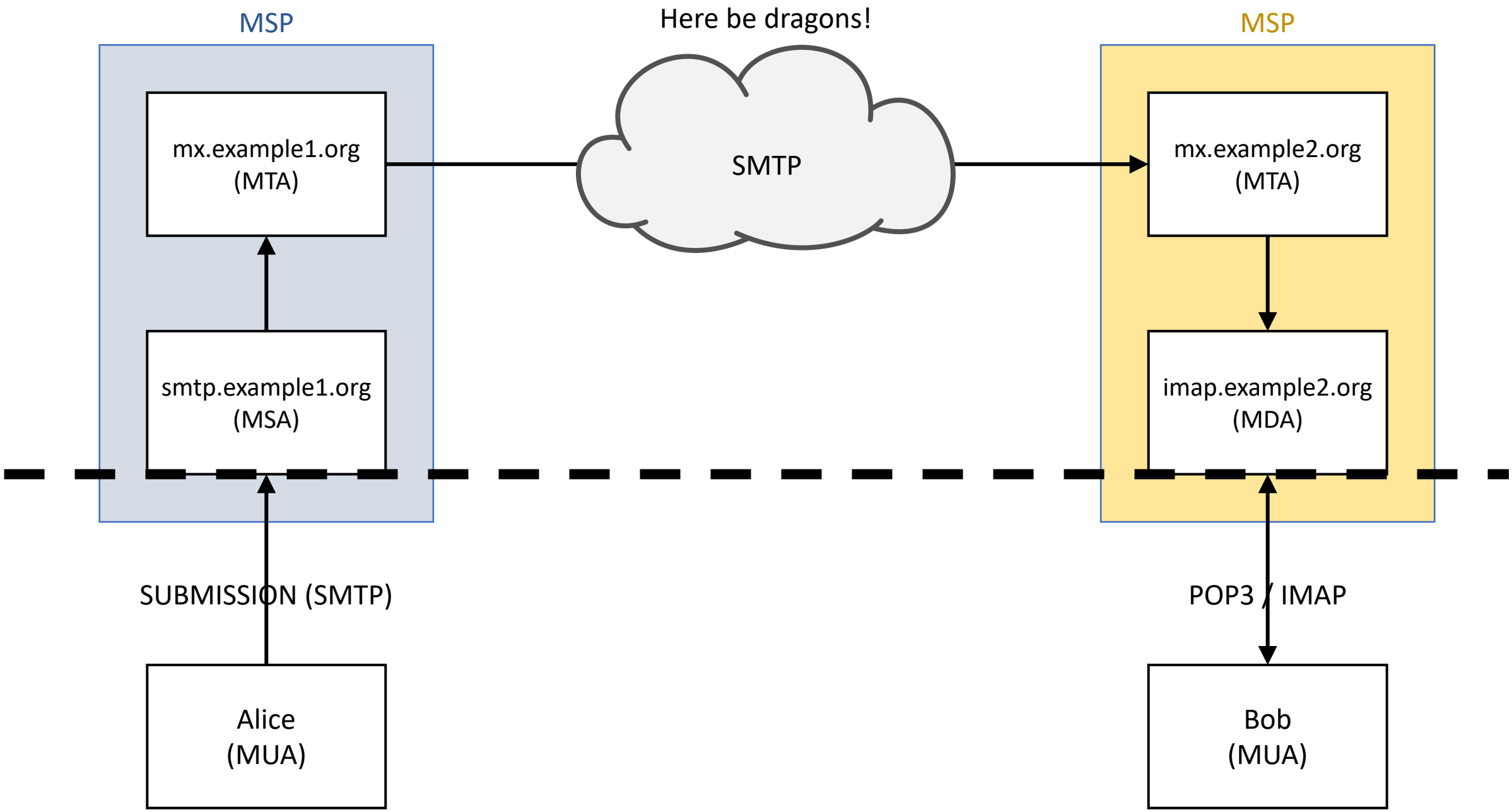

MSP
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
Bestehende E-Mail-Adresse einrichten
Bestehende E-Mail-Adresse einrichten
Richten Sie Ihre derzeitige E-Mail-Adresse ein.
Ihr Name:
Alice
E-Mail-Adresse:
alice@example.org
Passwort:
Passwort speichern
Ihr Benutzername:
IHREDOMÄNE\ihrbenutzername
POSTEINGANGS-SERVER:
POSTAUSGANGS-SERVER:
Protokoll:
IMAP
SMTP
Server:
imap.example.org
smtp.example.org
Port:
143
587
SSL:
STARTTLS
STARTTLS
Authentifizierung:
Automatisch erkennen
Benutzername:
alice@example.org
Automatisch erkennen
Keine Verbindungssicherheit
STARTTLS
SSL/TLS
Abbrechen
Erneut testen
Fertig
MSP
Bob
(MUA)

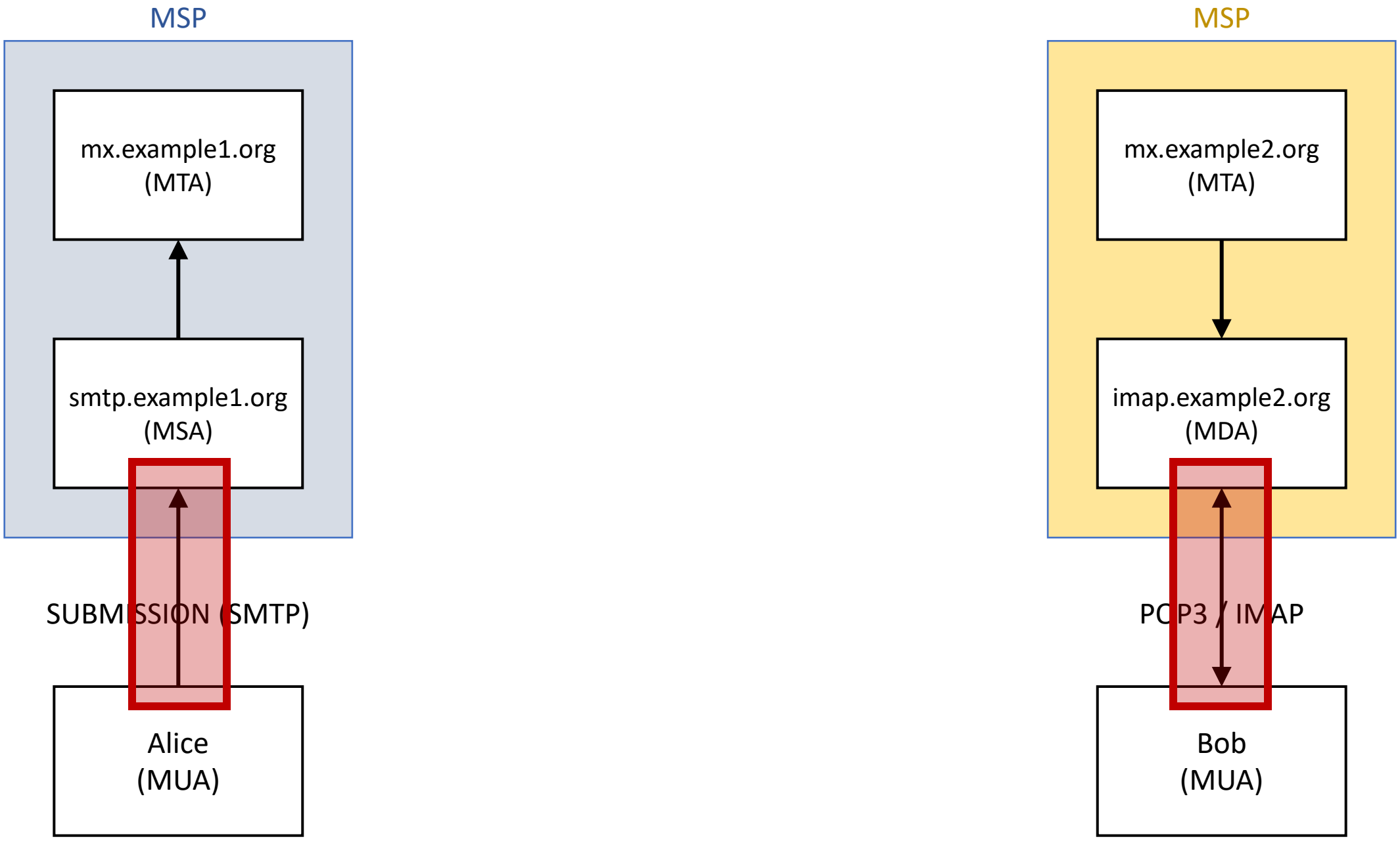

MSP
MSP
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
Bob
(MUA)


MSP
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
MSP
imap.example2.org
(MDA)
POP3 / IMAP
Bob
(MUA)


MSP
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
MSP
imap.example2.org
(MDA)
POP3 / IMAP
Bob
(MUA)


MSP
MSP
smtp.example1.org
(MSA)
imap.example2.org
(MDA)
SUBMISSION (SMTP)
POP3 / IMAP
Alice
(MUA)
Bob
(MUA)


MSP
Here be dragons!
MSP
mx.example1.org
(MTA)
SMTP
mx.example2.org
(MTA)
smtp.example1.org
(MSA)
imap.example2.org
(MDA)
SUBMISSION (SMTP)
POP3 / IMAP
Alice
(MUA)
Bob
(MUA)


MSP
mx.example1.org
(MTA)
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
MSP
mx.example2.org
(MTA)
imap.example2.org
(MDA)
POP3 / IMAP
Bob
(MUA)

Introduction to IMAP & STARTTLS

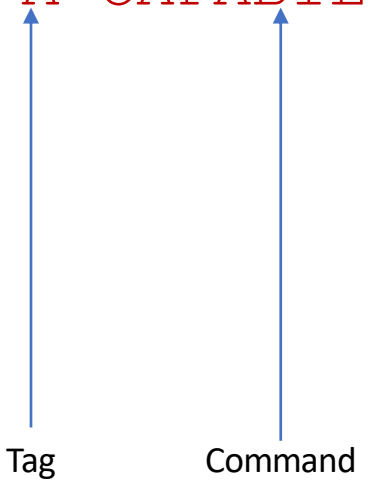
IMAP

```
S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]
```


Greeting

IMAP

```
S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]
C: A CAPABILITY
```



IMAP

```
S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]
C: A CAPABILITY
S: * CAPABILITY IMAP4REV1 AUTH=LOGIN
```

Untagged Response

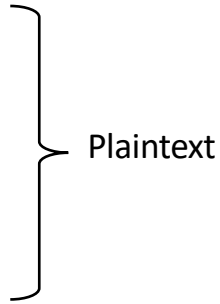
IMAP

```
S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]
C: A CAPABILITY
S: * CAPABILITY IMAP4REV1 AUTH=LOGIN
S: A OK
```

Tagged Response

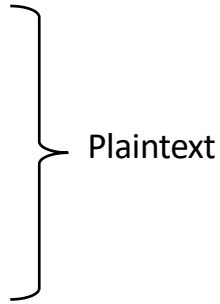
STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
```



STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
```



STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```

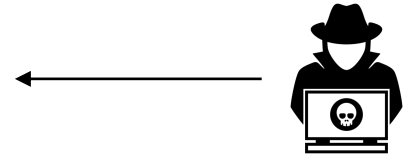
Plaintext

Encrypted

STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```

Plaintext



Encrypted

STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```

Plaintext

Encrypted

STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```

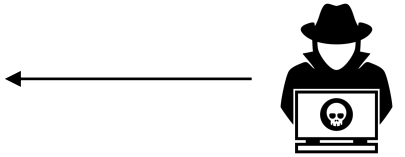
Plaintext

Encrypted

STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```

Plaintext



Encrypted

STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```

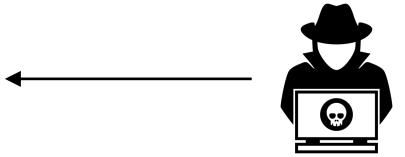
Plaintext

Encrypted

STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```

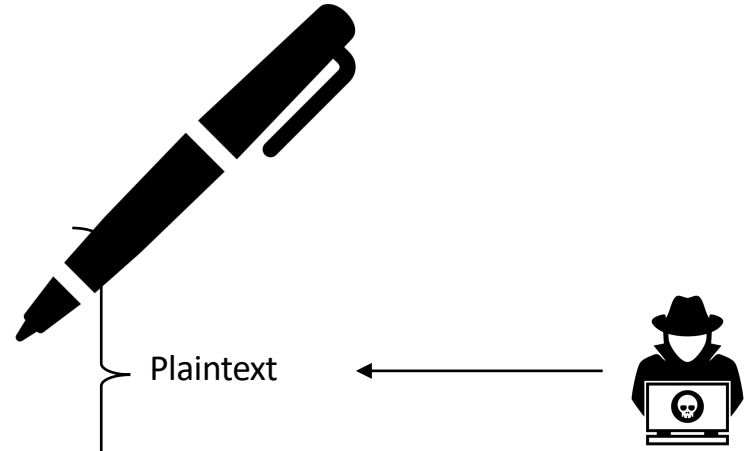
Plaintext



Encrypted

STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```



Encrypted

Why TLS is better without STARTTLS: A Security Analysis of STARTTLS in the Email Context

Damian Poddebniak and Fabian Ising, *Münster University of Applied Sciences;* Hanno Böck, *Independent Researcher;* Sebastian Schinzel, *Münster University of Applied Sciences*

https://www.usenix.org/conference/usenixsecurity21/presentation/poddebniak

Questions

Are modern clients opportunistic?

Questions

Are modern clients opportunistic?

What data is sent in plaintext?

Questions

Are modern clients opportunistic?

What data is sent in plaintext?

What is retained from the plaintext phase?

Questions

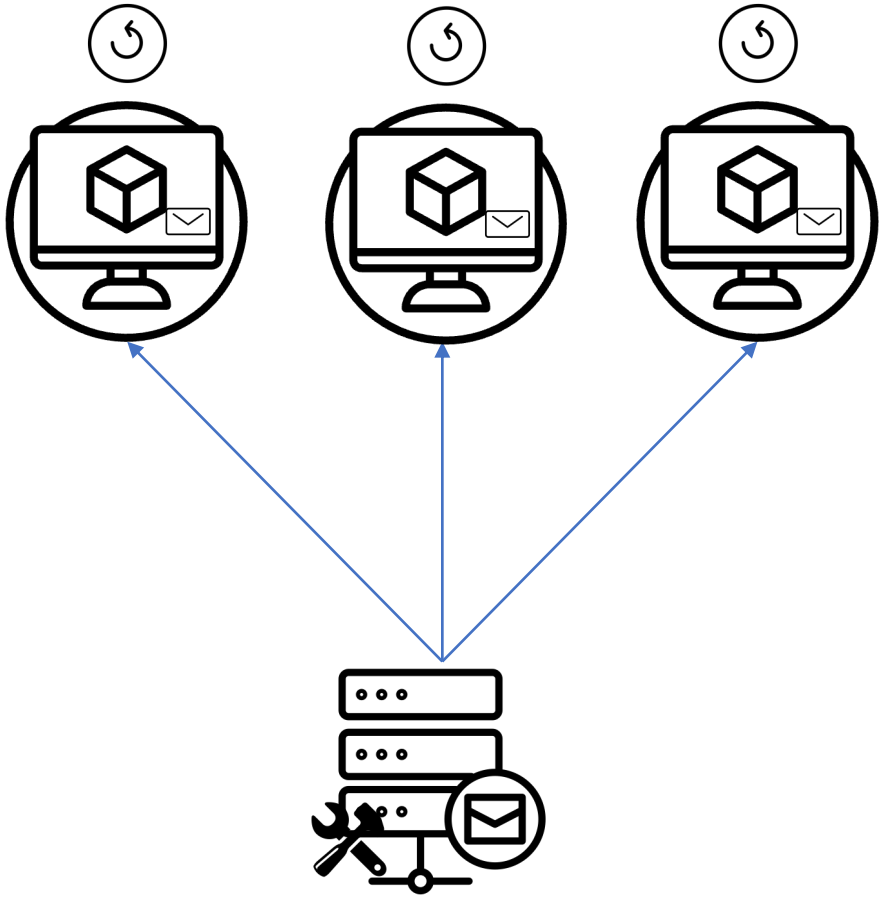
Are modern clients opportunistic?

What data is sent in plaintext?

What is retained from the plaintext phase?

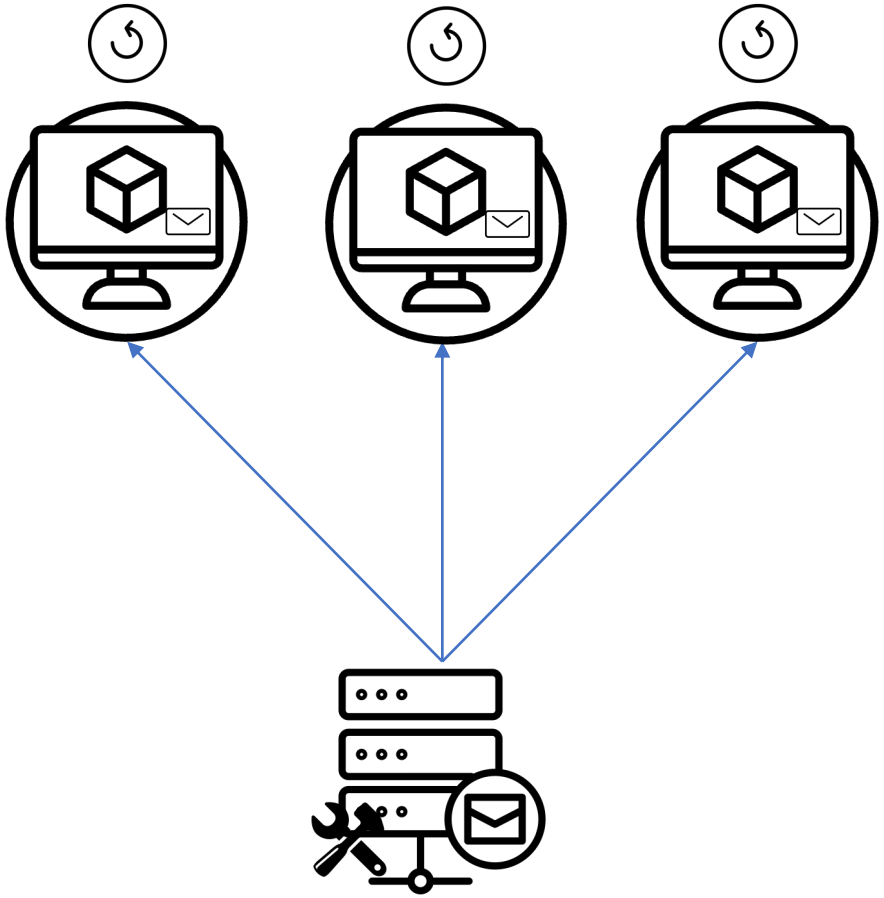
What happens in error cases?

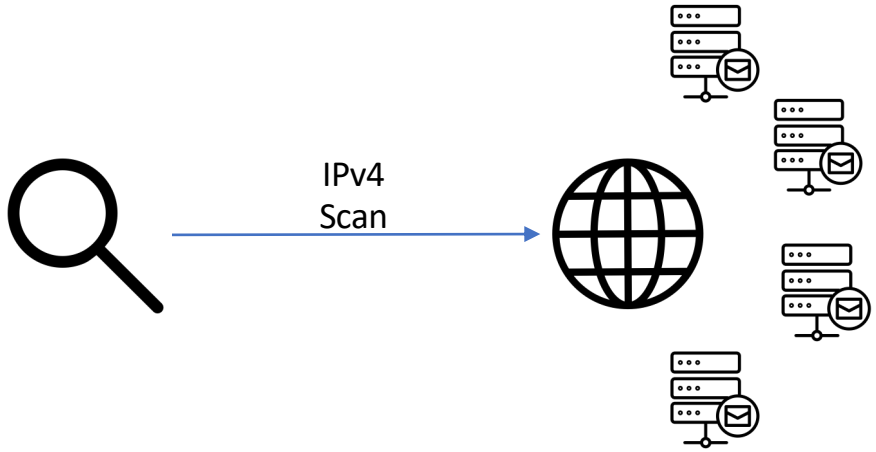
EAST Framework



https://github.com/FHMS-ITS/EAST

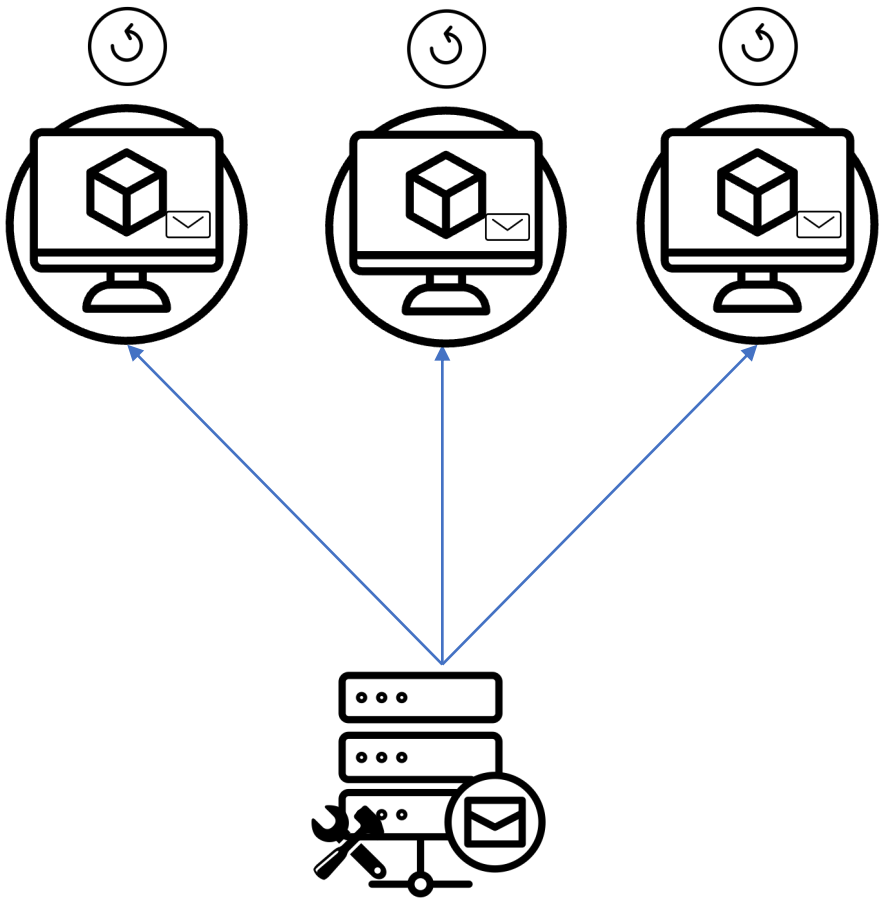
EAST Framework

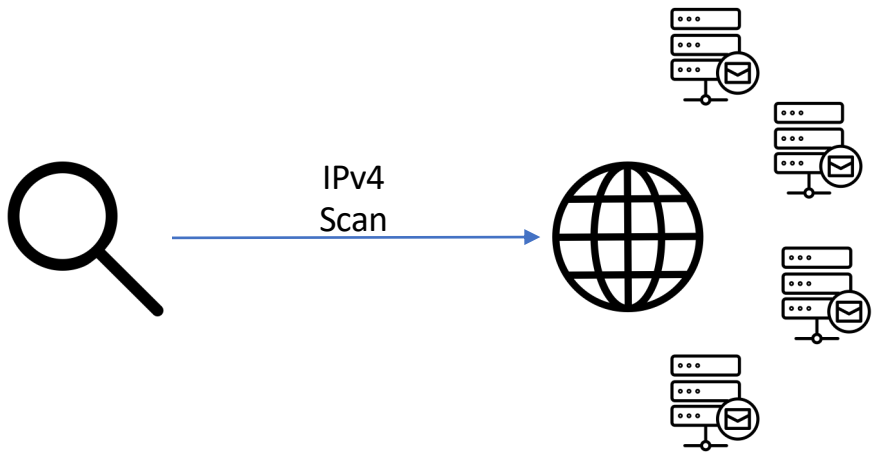


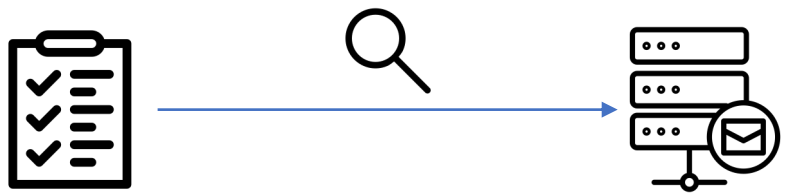


https://github.com/FHMS-ITS/EAST

EAST Framework







https://github.com/FHMS-ITS/EAST

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"
```

```
S: * PREAUTH
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"
```

```
S: * PREAUTH
C: A STARTTLS
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"
```

> In addition to the universal commands (CAPABILITY, NOOP, and LOGOUT), the following commands are valid in the not authenticated state: STARTTLS, AUTHENTICATE and LOGIN. See the Security Considerations section for important information about these commands.

```
C: A STARTTLS
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 ~~STARTTLS~~]
C: A STARTTLS
S: A ~~OK~~ NO
C: B LOGIN "victim" "password"
```

```
S: * PREAUTH
C: ~~A STARTTLS~~
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"
```

```
S: * PREAUTH
C: A STARTTLS
C: B APPEND Sent {250}
S: +
C: From: victim@example.org
.. Subject: Sensitive Mail [...]
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"
```

15/28 Clients

```
C: A STARTTLS
C: B APPEND Sent {250}
S: +
C: From: victim@example.org
.. Subject: Sensitive Mail [...]
```

Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails
  - Only one library **opportunistic**

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"
```

```
S: * PREAUTH
C: A STARTTLS
C: B APPEND Sent {250}
S: +
C: From: victim@example.org
.. Subject: Sensitive Mail [...]
```

Key Findings

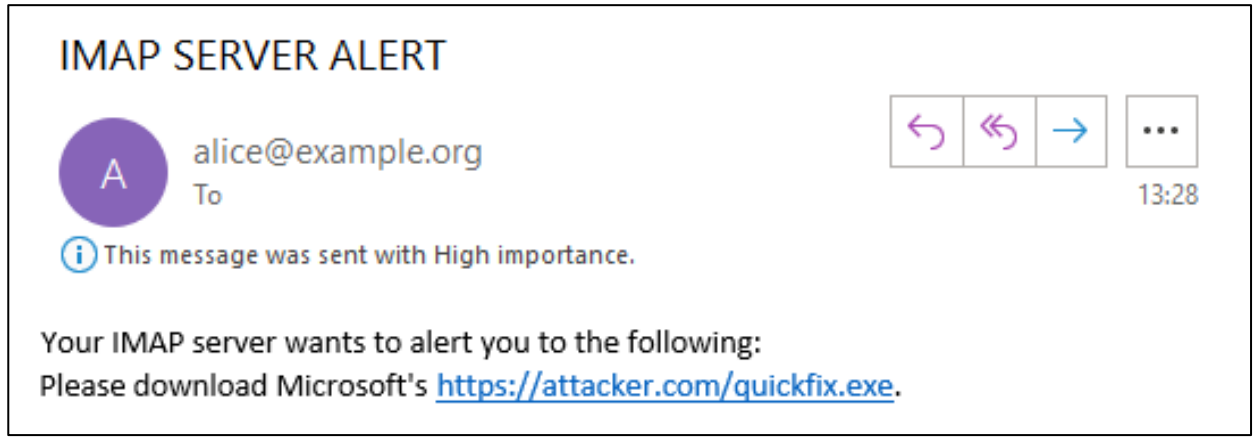
- Clients can be tricked into not using STARTTLS
- Many clients process unauthenticated data

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
S: * [ALERT] Please download [...]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
```

Key Findings

- Clients can be tricked into not using STARTTLS
- Many clients process unauthenticated data

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
S: * [ALERT] Please download [...]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
```

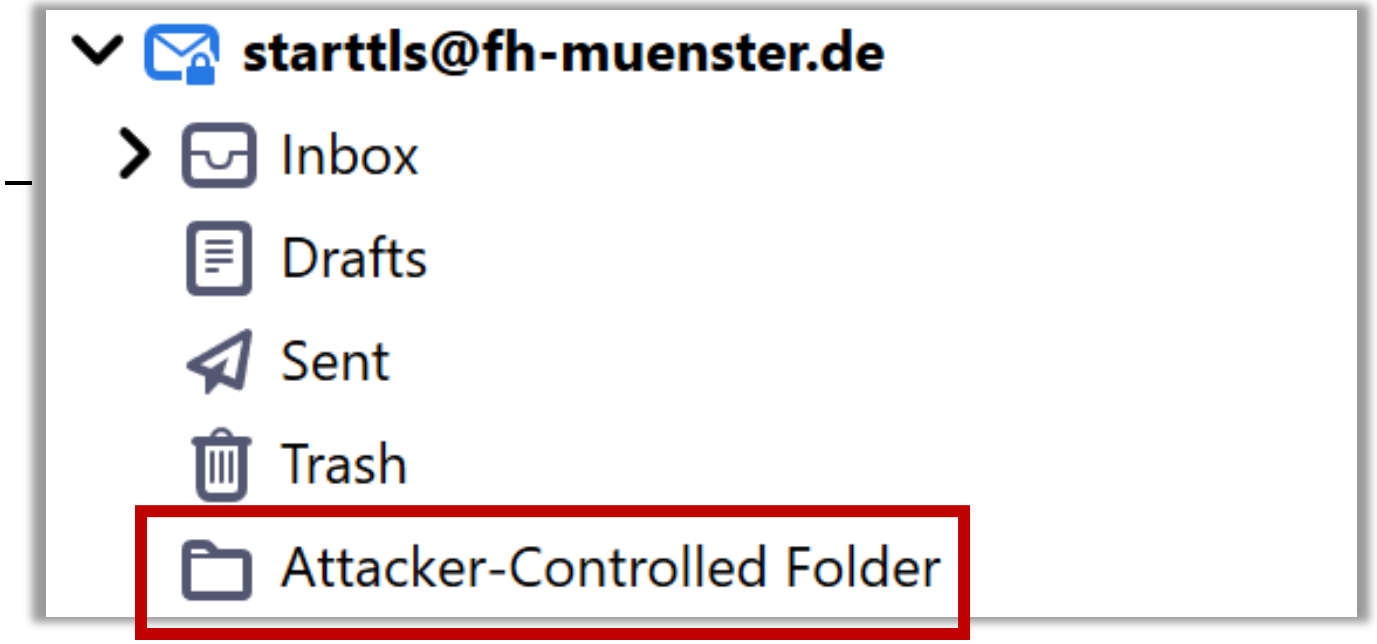


More Unauthenticated Data

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
.. * LIST () “Attacker-Controlled Folder”
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: ...
```

More Unauthenticated Data

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
.. * LIST () “Attacker-Controlled Folder”
C: A STARTTLS
S: A OK
// ------------
C: ...
```



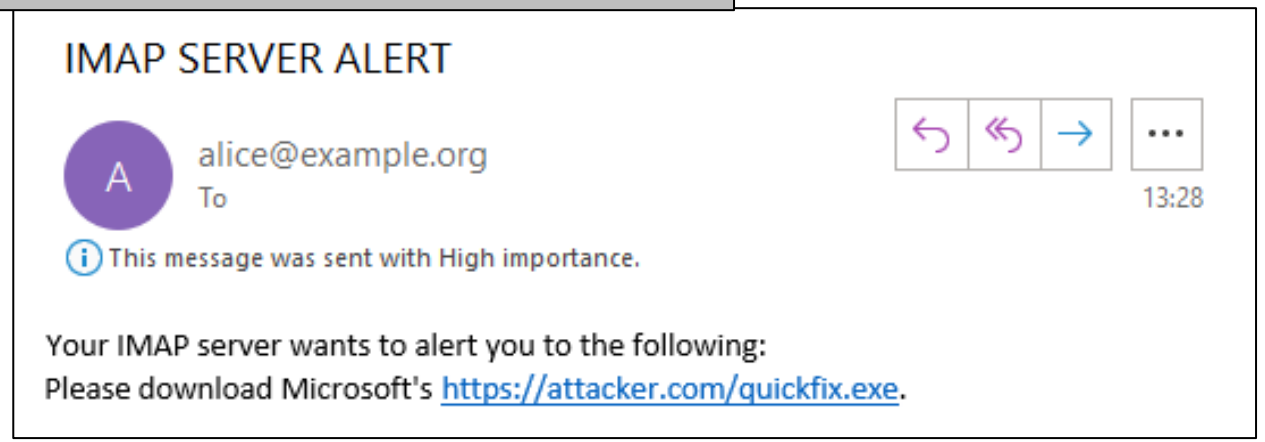
Key Findings

- Clients can be tricked into not using STARTTLS
- Many clients p
  unauthenticate

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
S: * [ALERT] Please download [...]
C: A STARTTLS
```

11/28 Clients

shake ----------



Key Findings

- Clients can be tricked into not using STARTTLS
- Many clients process unauthenticated data
- Servers vulnerable to known bug

FreeBSD: postfix -- plaintext command injection with SMTP over TLS (CVE-2011-0411)

Command Injection

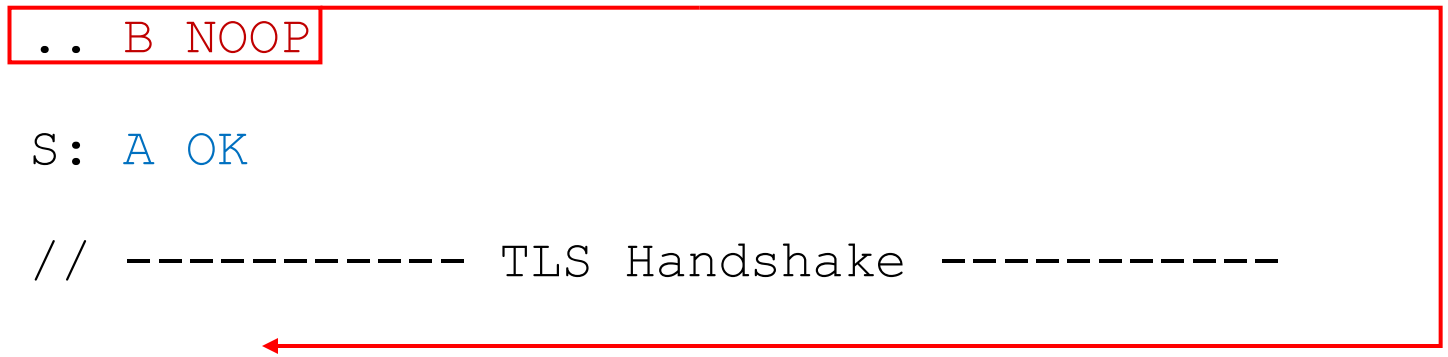
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]

C: A STARTTLS

.. B NOOP

S: A OK

// ----------- TLS Handshake -----------
```

Command Injection

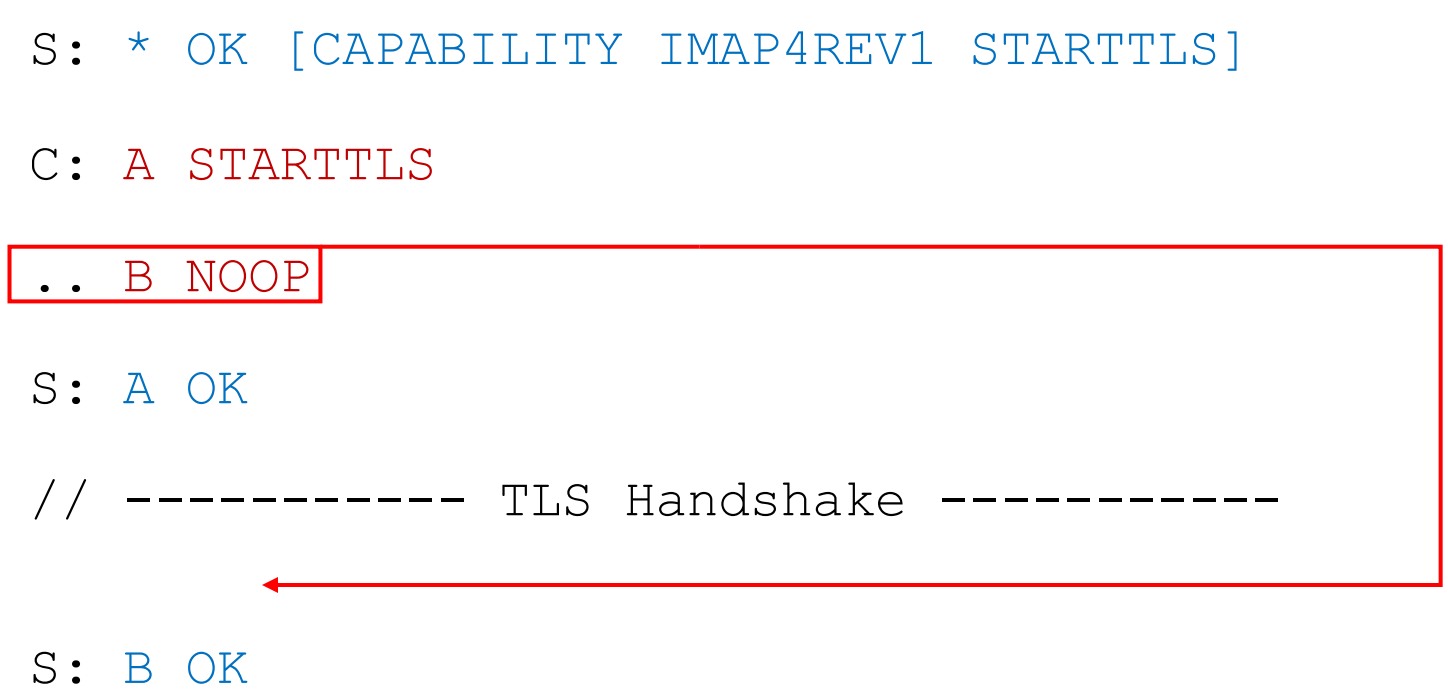
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]

C: A STARTTLS

.. B NOOP

S: A OK

// ----------- TLS Handshake -----------
```

Command Injection

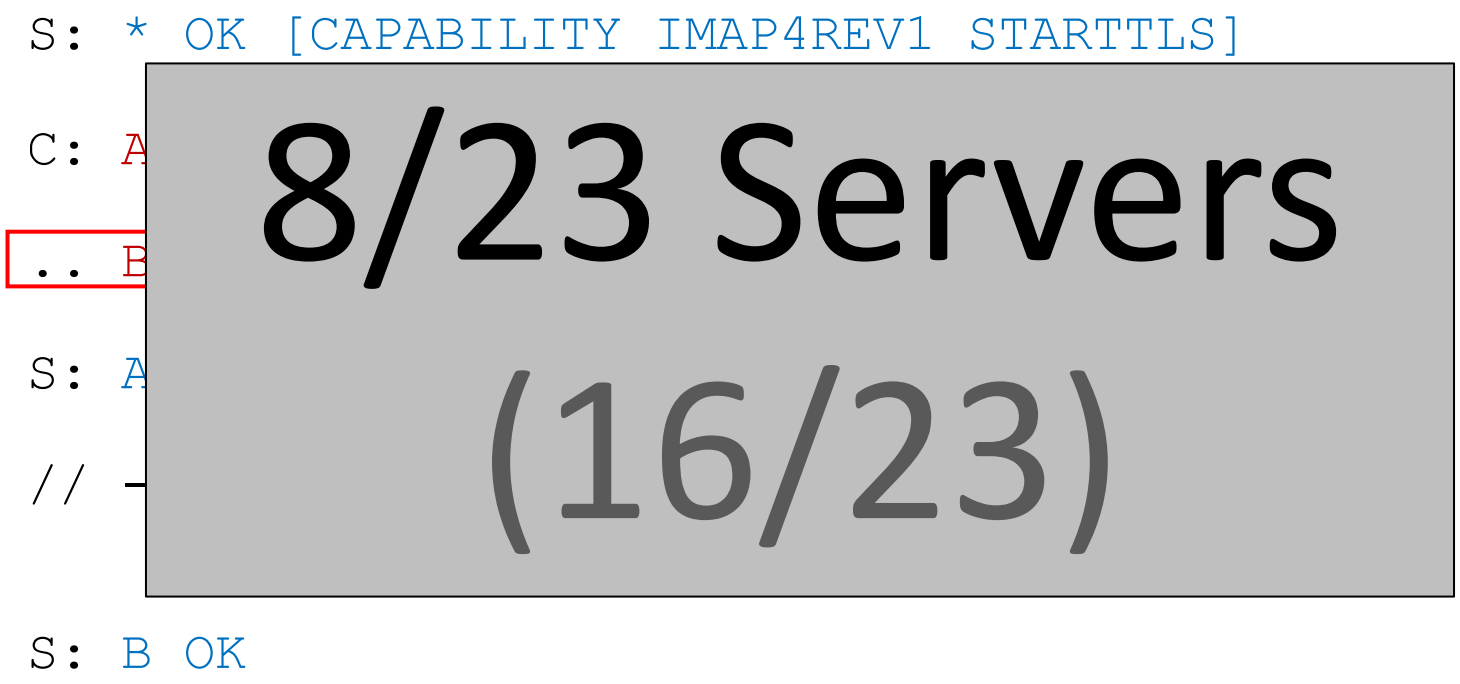
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]

C: A STARTTLS

.. B NOOP

S: A OK

// ----------- TLS Handshake -----------
```



Command Injection

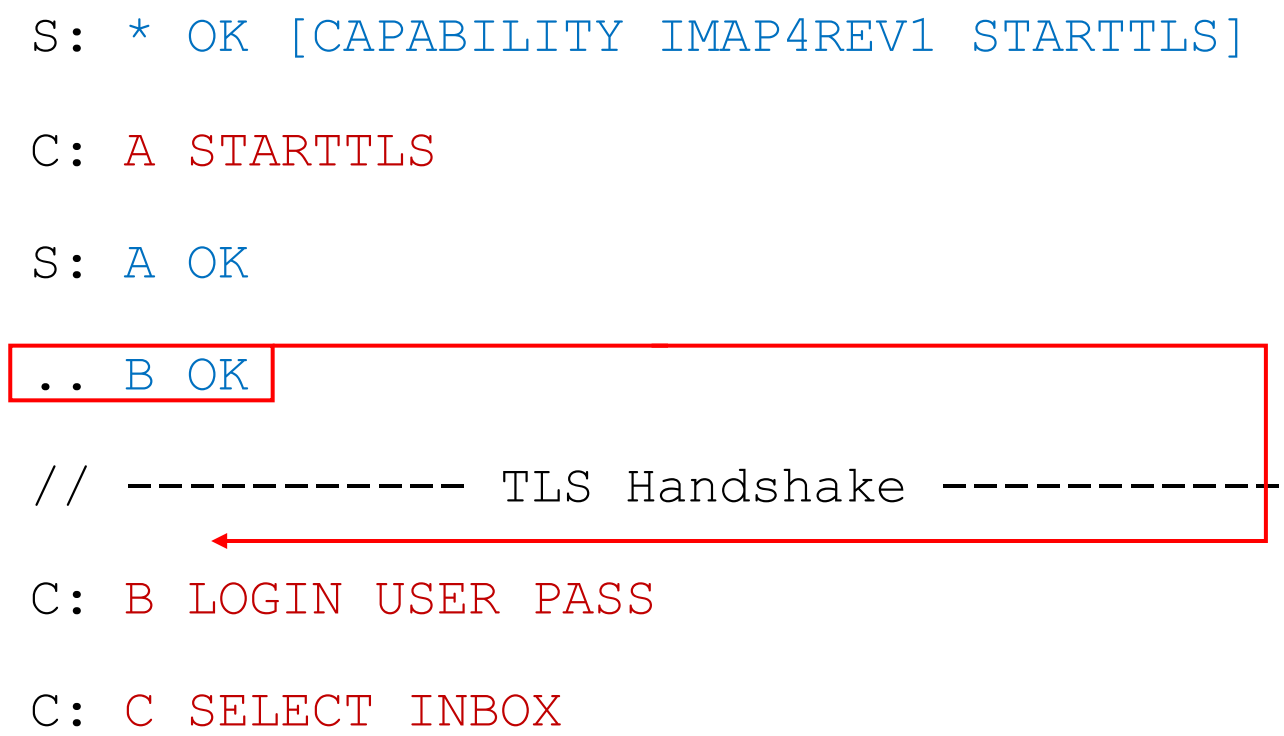


Command Injection



Key Findings

- Clients can be tricked into not using STARTTLS
- Many clients process unauthenticated data
- Servers vulnerable to known bug
  - Many clients vulnerable to a variant



Key Findings

- Clients can be tricked into not using STARTTLS
- Many clients p
  unauthenticate
- Servers vulnerable to known bug
  - Many clients vulnerable to a variant

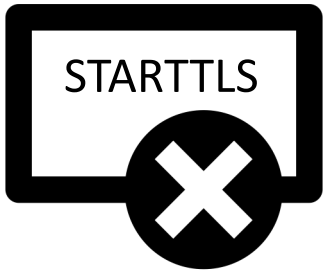
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
                                    ndshake ----------
C: B LOGIN USER PASS
C: C SELECT INBOX
```

16/28 Clients

Impact

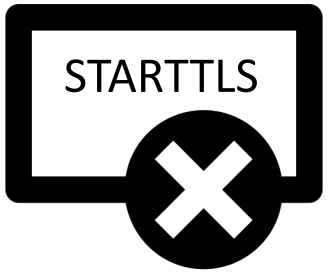
Attack/Protocol	POP3	IMAP	SMTP
Credential Stealing	-	X	X
Stealing Sent/Drafted Mails	-	X	X
Tampering with the Mailbox	X	X	-
UI Spoofing	X	X	X
HTTPS Hosting	-	X	-

Mitigation



Disable STARTTLS

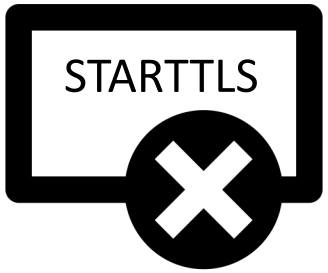
Mitigation



Disable STARTTLS

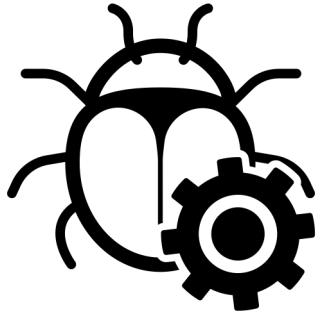
Isolating the
Plaintext Phase

Mitigation



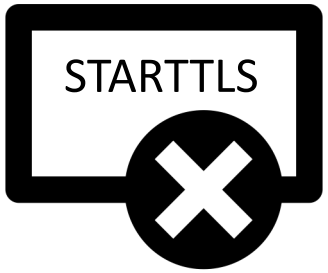
Disable STARTTLS

Isolating the
Plaintext Phase

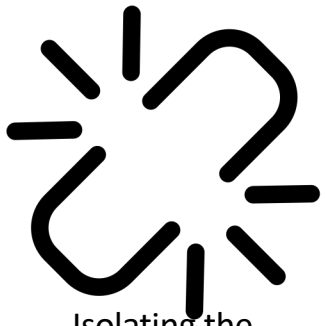


Fix Buffering
Issues

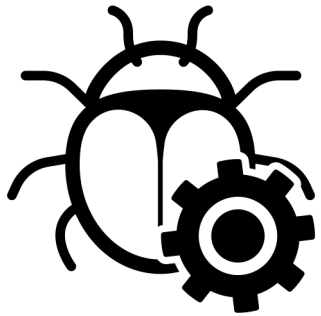
Mitigation



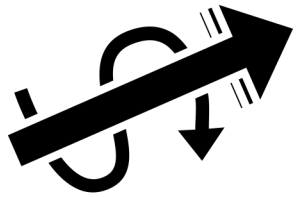
Disable STARTTLS



Isolating the Plaintext Phase



Fix Buffering Issues



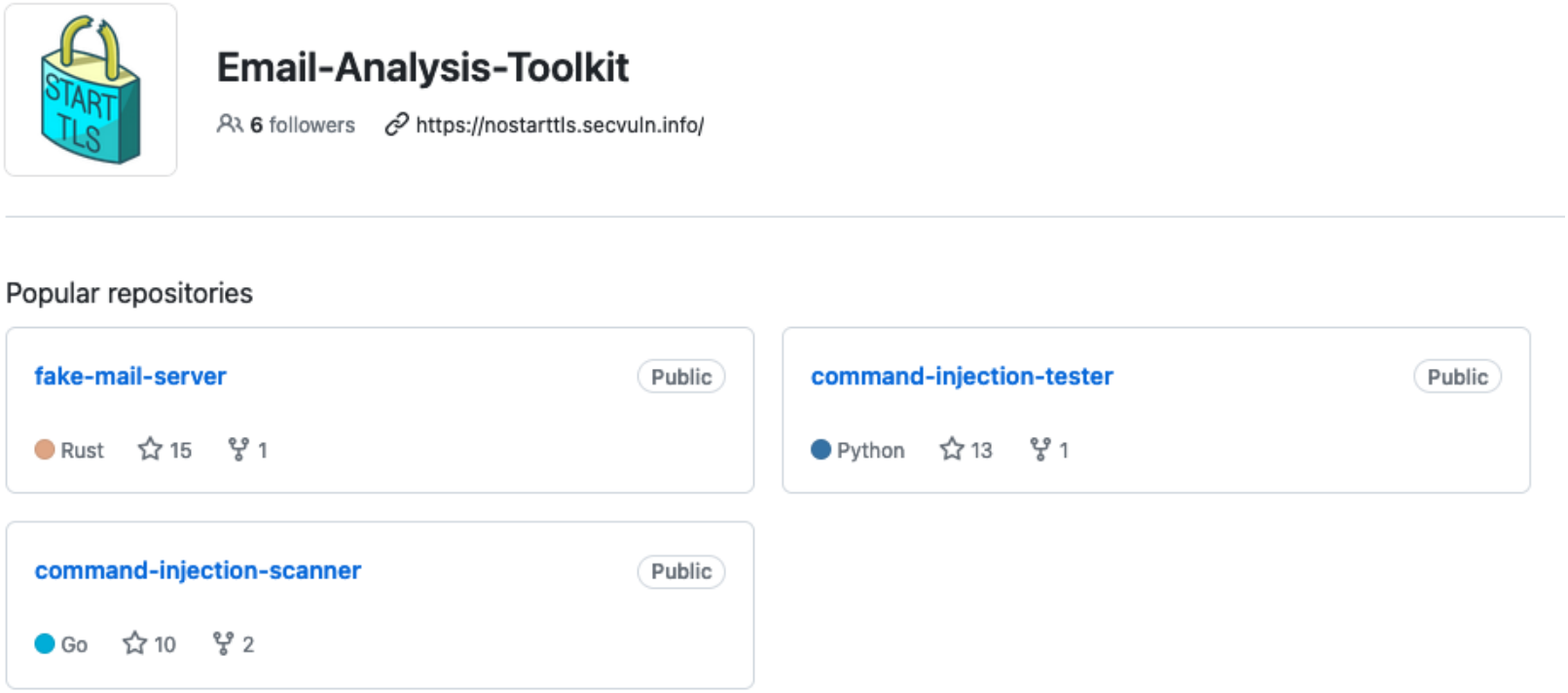
Streamline Negotiation

A thank you to the FOSS Developers!

- Response time to bug reports for FOSS Developers was phenomenal!
  - Much better than most commercial vendors ;-)

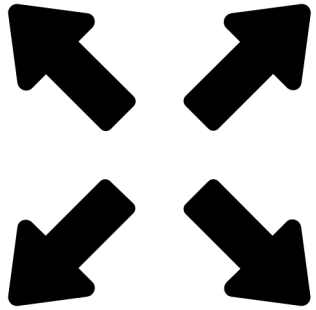
A thank you to the FOSS Developers!

- Response time to bug reports for FOSS Developers was phenomenal!
  - Much better than most commercial vendors ;-)

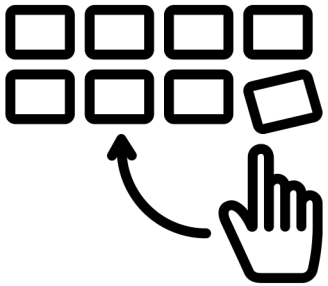


https://github.com/Email-Analysis-Toolkit

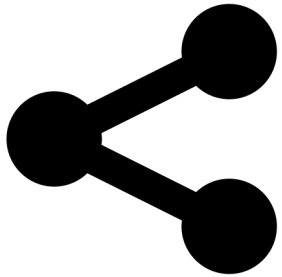
Conclusion



STARTTLS extends the attack surface

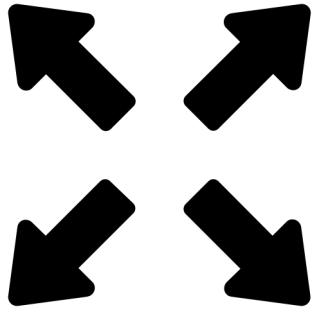


STARTTLS issues are widespread

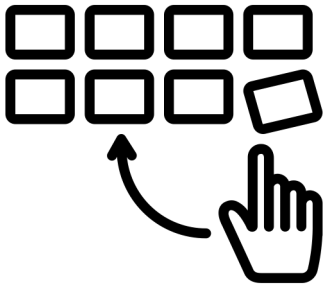


Cross-Protocol Attacks are possible

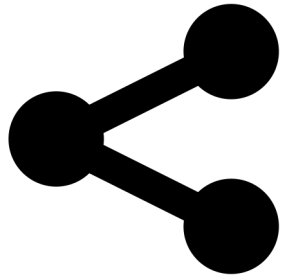
Conclusion



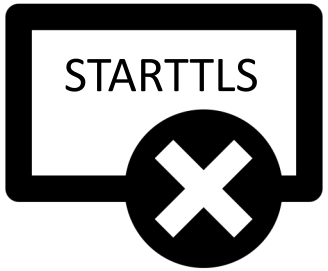
STARTTLS extends the attack surface



STARTTLS issues are widespread



Cross-Protocol Attacks are possible



TLS is better without STARTTLS

Fraunhofer SIT

FH MÜNSTER
University of Applied Sciences

Why TLS is better without STARTTLS:

A Security Analysis of STARTTLS in the Email Context

Damian Poddebniak[3], Fabian Ising[1,2], Hanno Böck[3], Sebastian Schinzel[1,2]

@duesee@norden.social @murgi@infosec.exchange @hanno@mastodon.social @seecurity@infosec.exchange

[1] Fraunhofer SIT | ATHENE National Research Center for Applied Cybersecurity

[2] Münster University of Applied Sciences

[3] Independent Researcher

https://nostarttls.secvuln.info/