```
> EHLO mail.sba-research.org
> MAIL FROM:<fholzbauer@sba-research.org>
> RCPT TO:<networking.atc22@usenix.org>
> DATA
```

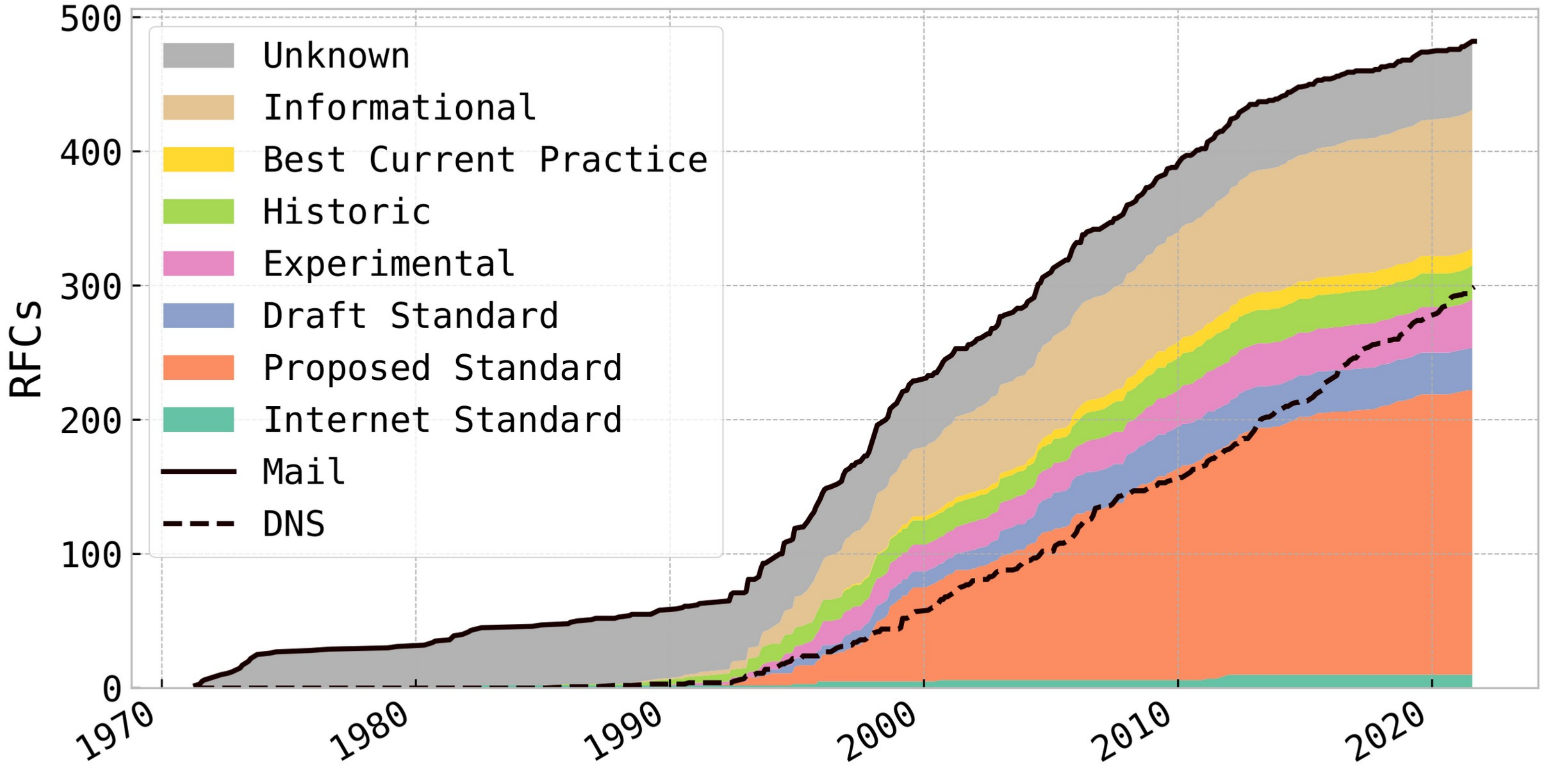
Not that Simple?

Email Delivery in the 21st Century

Florian Holzbauer, Johanna Ullrich, Martina Lindorfer, Tobias Fiebig

.

Email-related RFCs



Outline

- Scope
- Email Delivery
- Measurement Setup
- Datasets & Findings

Scope

1. Is the sender able to reach the receiver?

2. How do additional standards impact delivery?

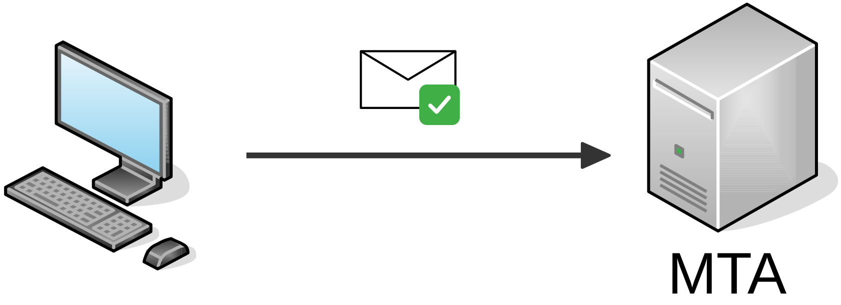
Sender

Receiver

3. Should the receiver accept the incoming email?

Related Measurements
(see Paper) ✓

Email Delivery

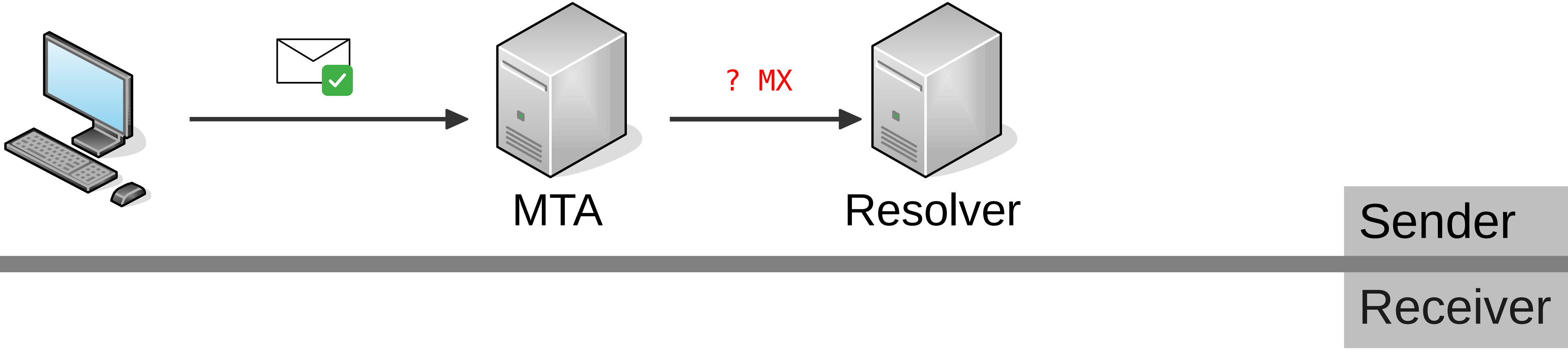


MTA

Sender

Receiver

Email Delivery



? MX

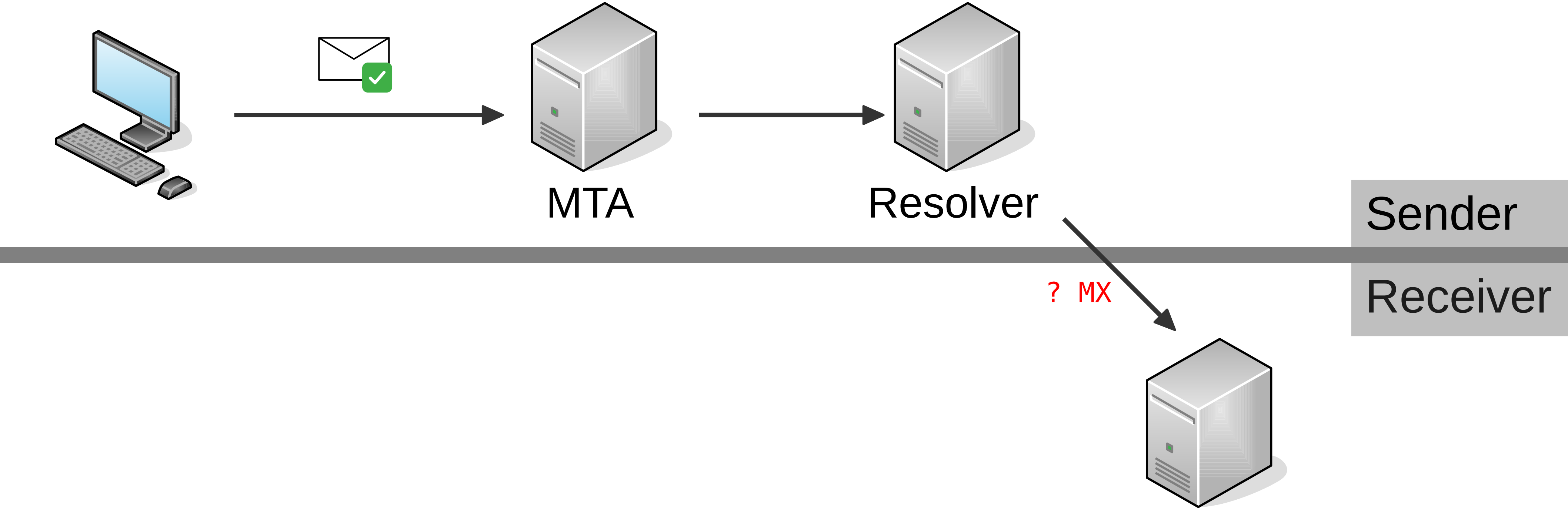
MTA

Resolver

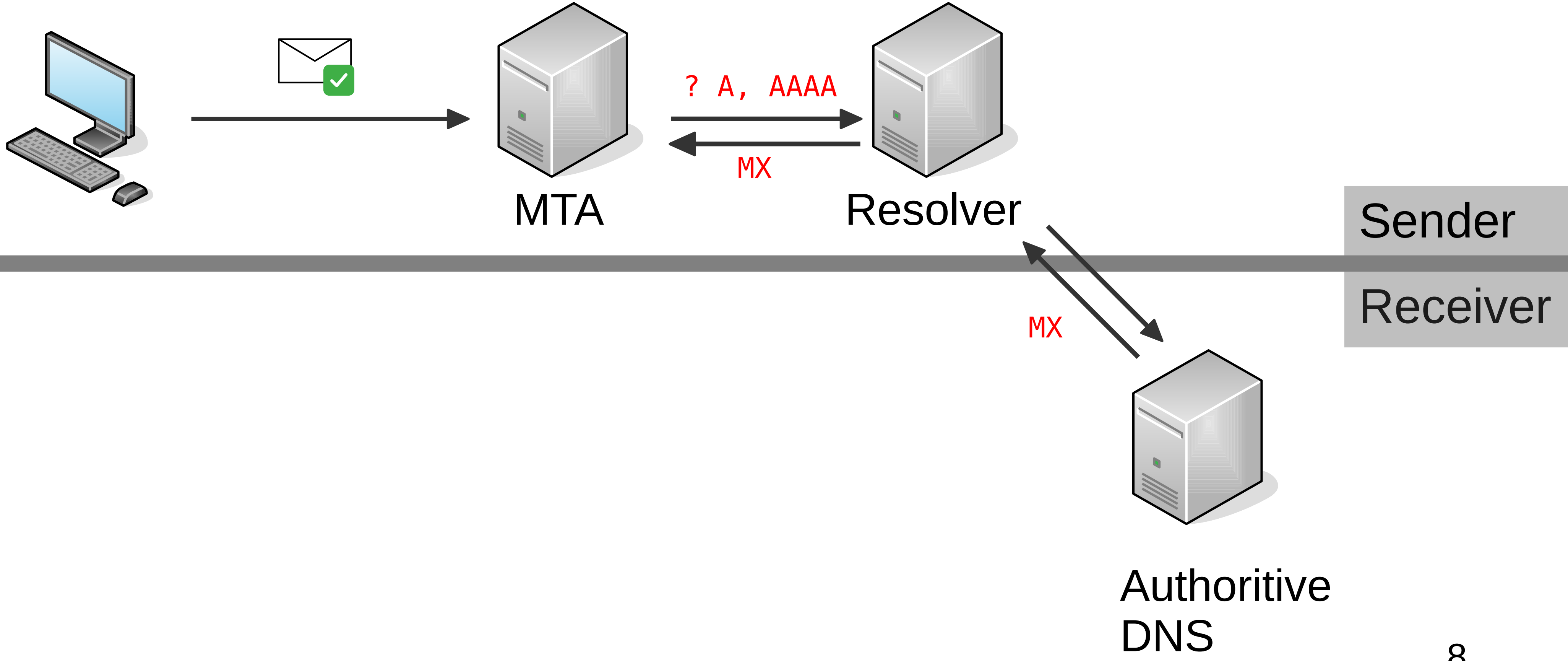
Sender

Receiver

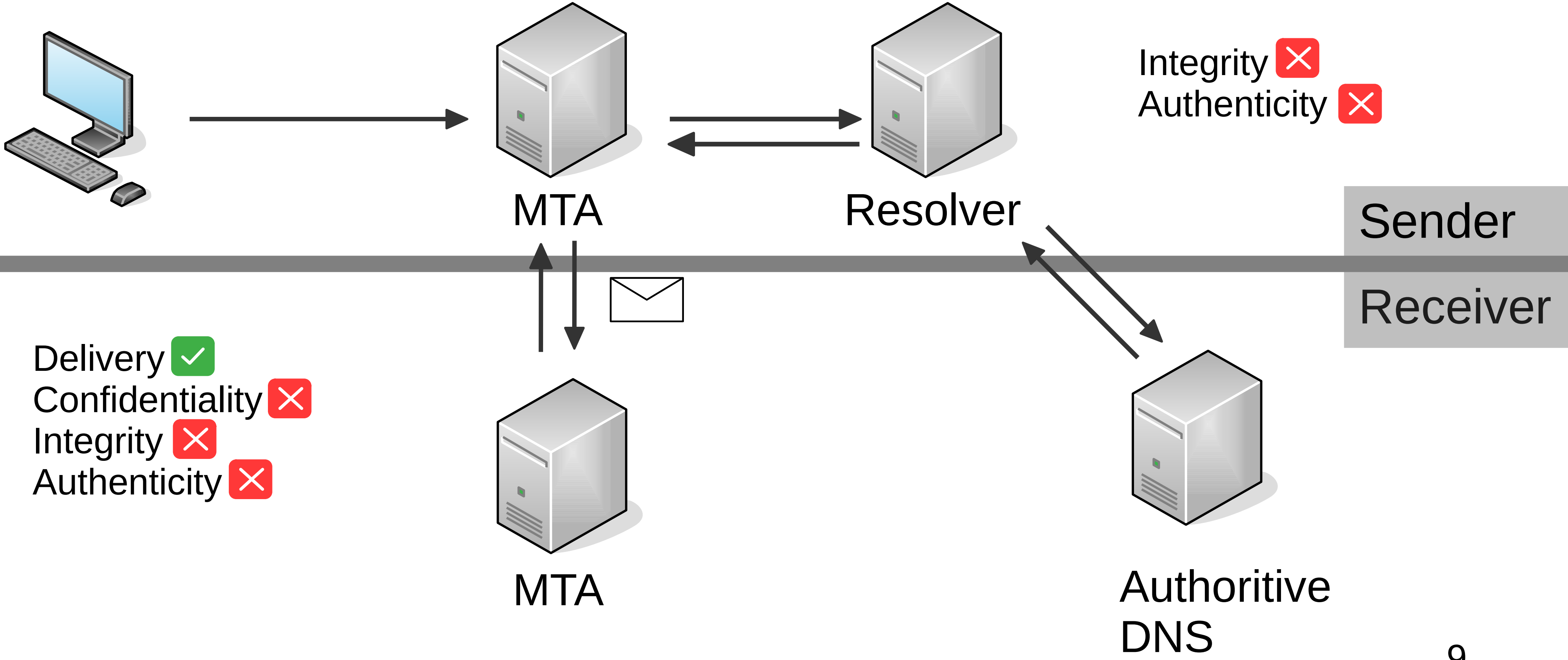
Email Delivery



Email Delivery



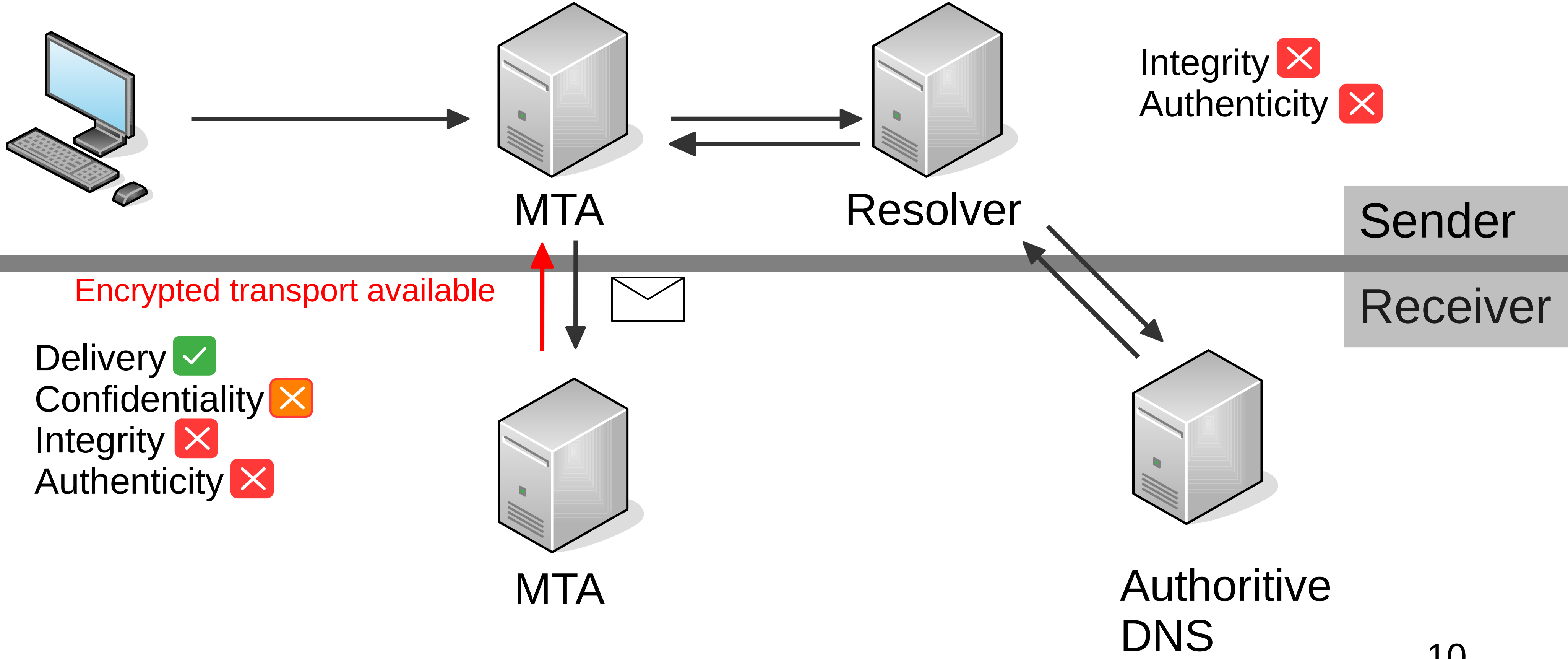
Email Delivery



Integrity ✗
Authenticity ✗

Delivery ✓
Confidentiality ✗
Integrity ✗
Authenticity ✗

Email Delivery: STARTTLS

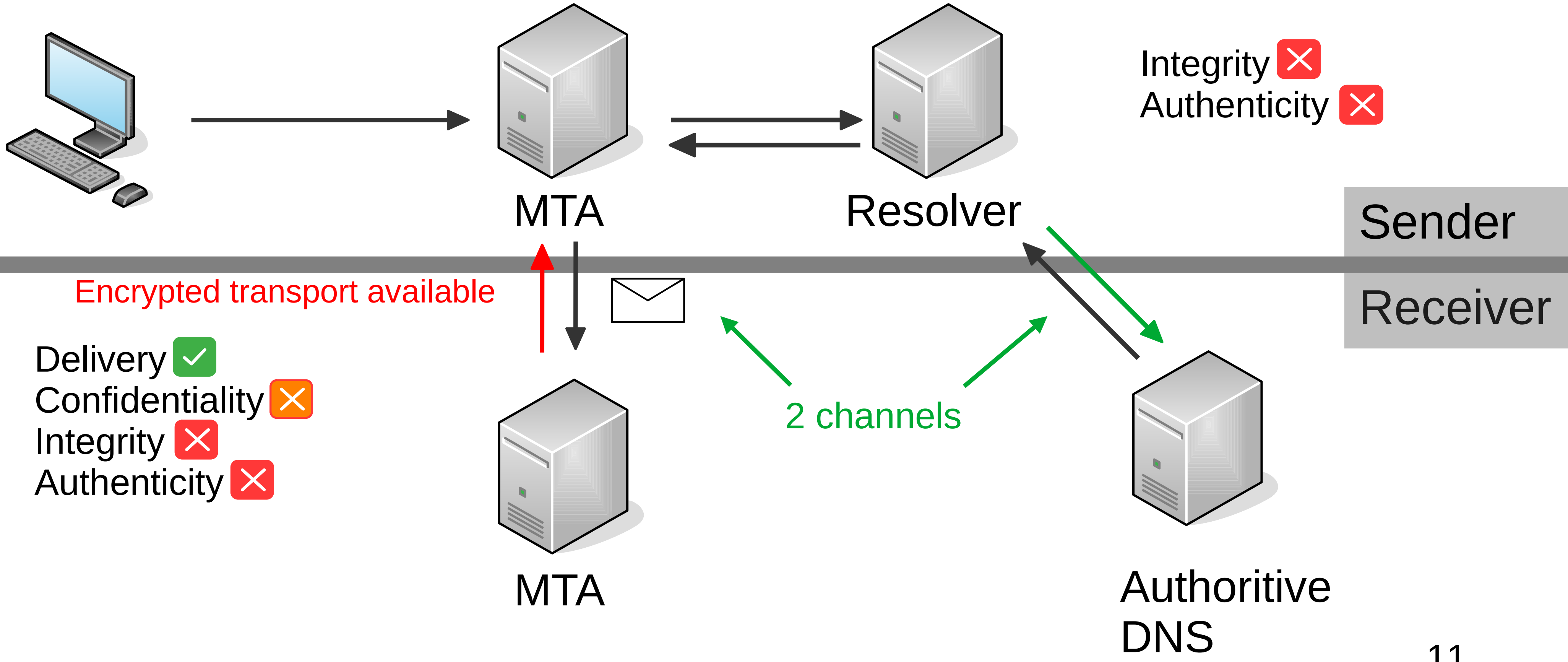


Integrity ✗
Authenticity ✗

Encrypted transport available

Delivery ✓
Confidentiality ✗
Integrity ✗
Authenticity ✗

Email Delivery



MTA

Resolver

Integrity ✗

Authenticity ✗

Sender

Receiver

Encrypted transport available

Delivery ✓

Confidentiality ✗

Integrity ✗

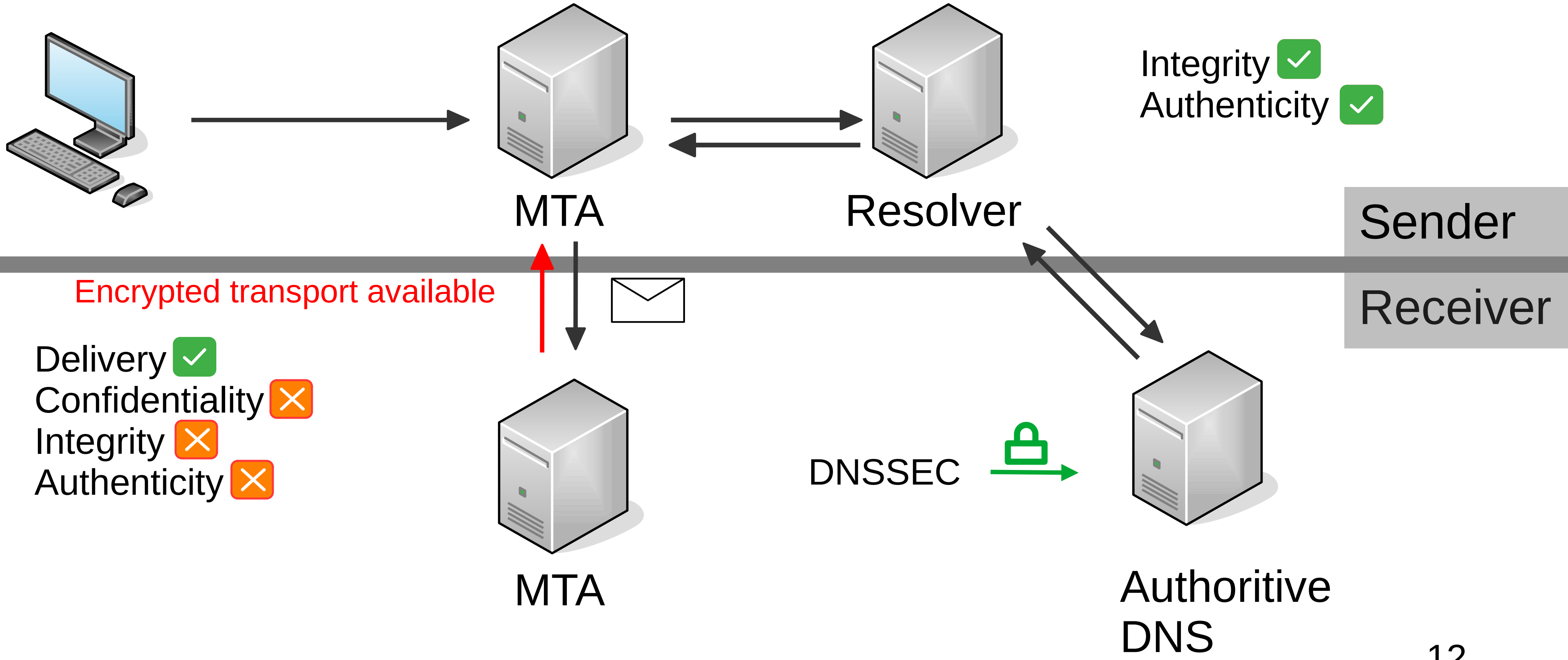
Authenticity ✗

2 channels

MTA

Authoritive DNS

Email Delivery: DNSSEC



MTA

Resolver

Integrity ✓
Authenticity ✓

Sender

Receiver

Encrypted transport available

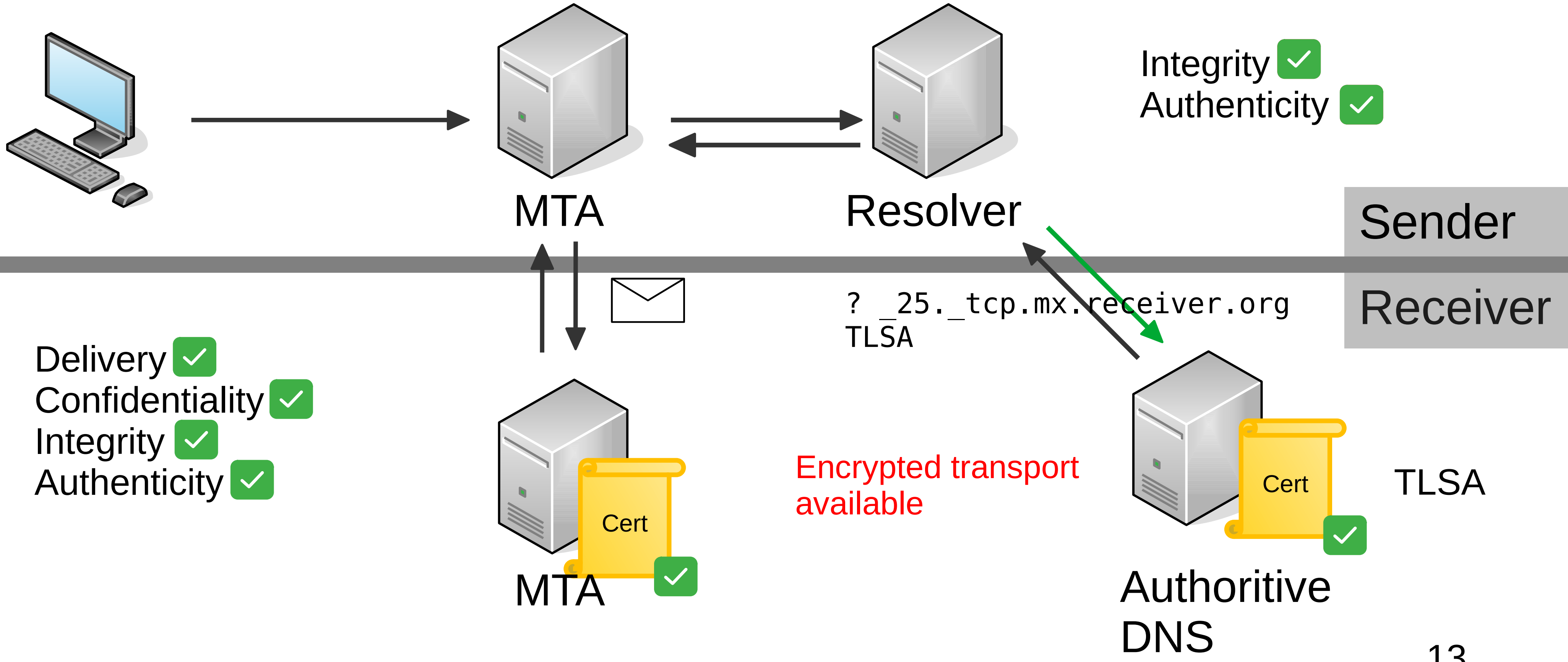
Delivery ✓
Confidentiality ✗
Integrity ✗
Authenticity ✗

MTA

DNSSEC

Authoritive
DNS

Email Delivery: DANE



MTA

Resolver

Integrity ✓
Authenticity ✓

Sender

Receiver

```
? _25._tcp.mx.receiver.org
TLSA
```

Delivery ✓
Confidentiality ✓
Integrity ✓
Authenticity ✓

MTA

Cert ✓

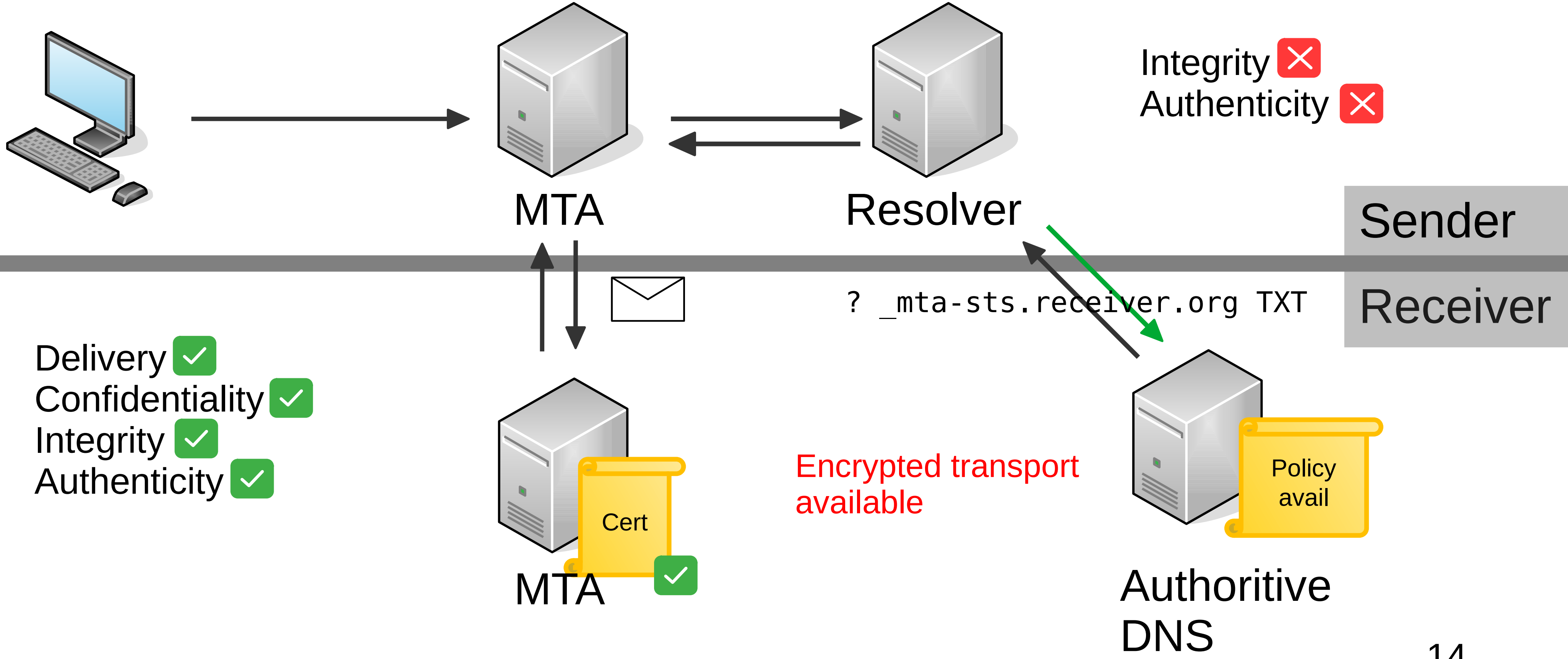
Encrypted transport available

Cert ✓

TLSA

Authoritive DNS

Email Delivery: MTA-STS



Integrity ✗
Authenticity ✗

MTA

Resolver

Sender

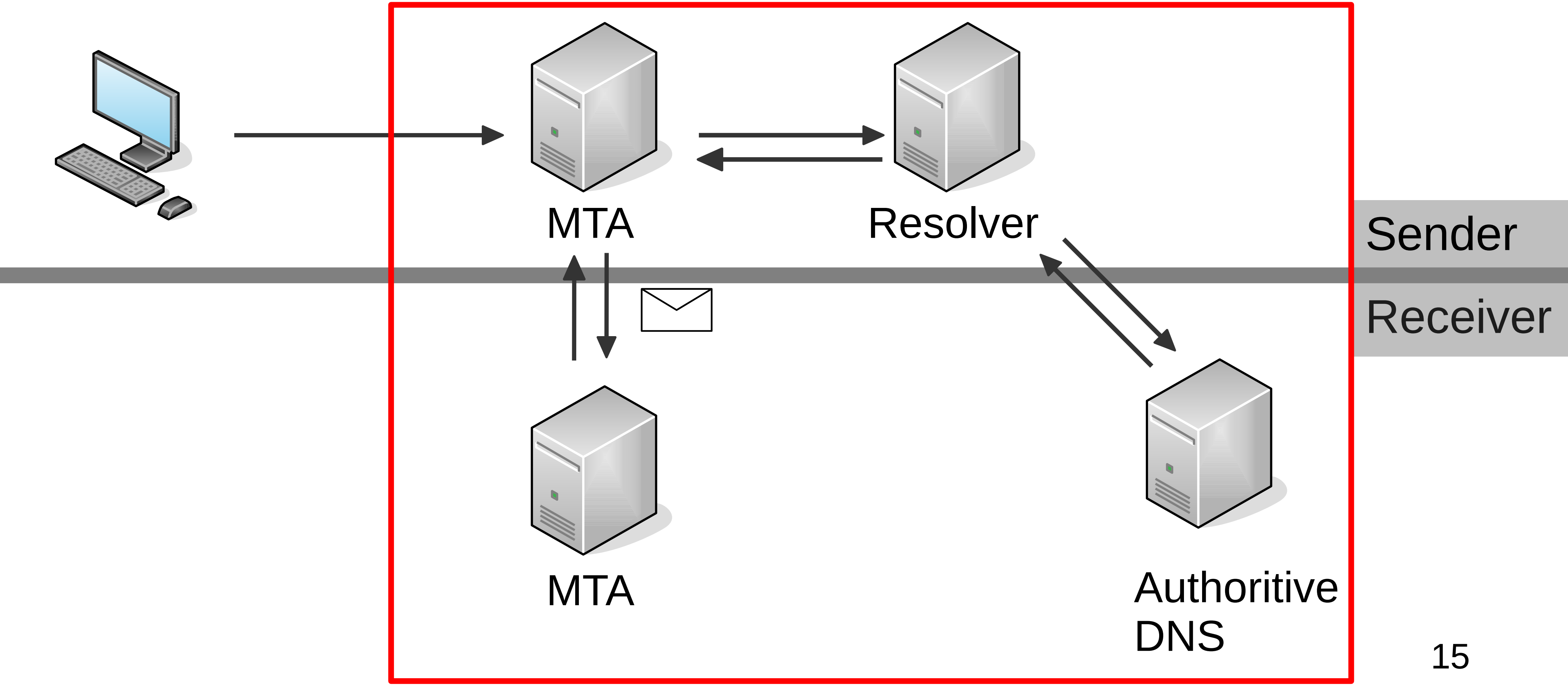
Receiver

`? _mta-sts.receiver.org TXT`

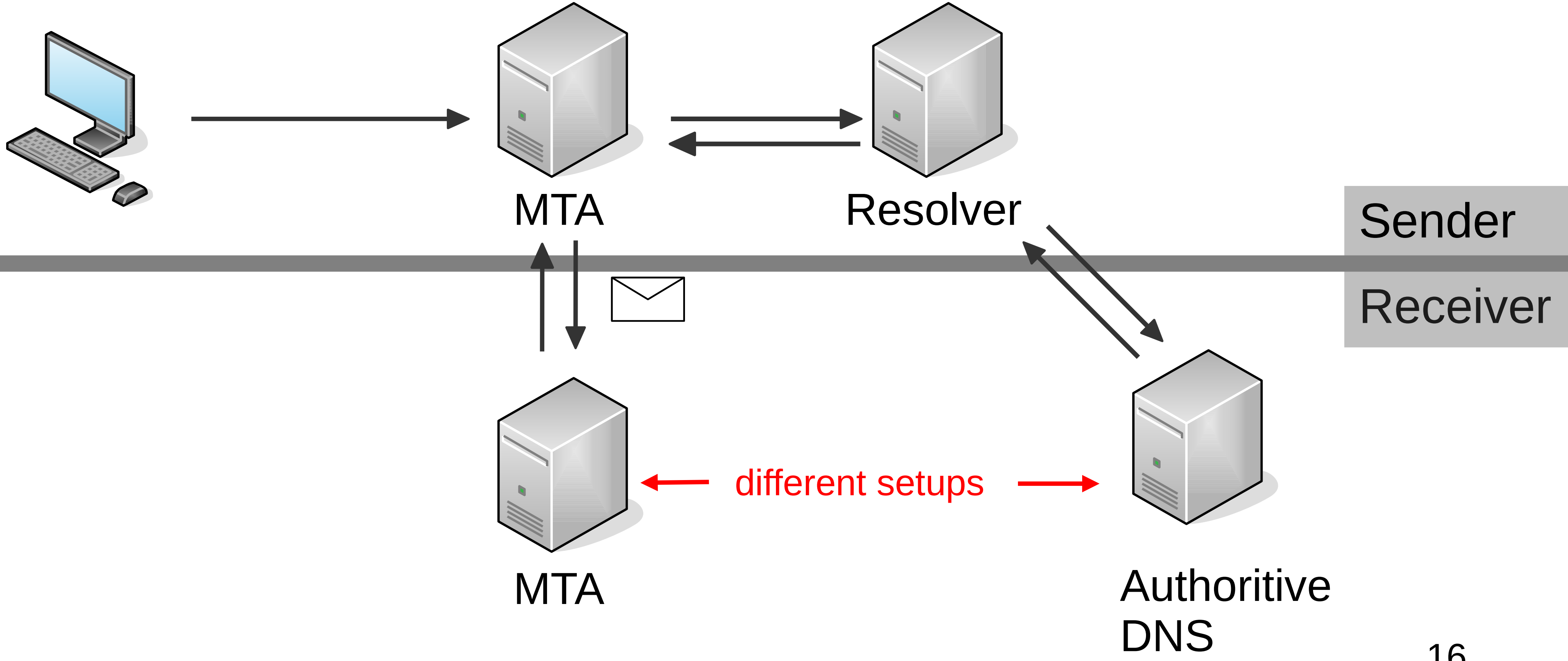
Delivery ✓
Confidentiality ✓
Integrity ✓
Authenticity ✓

Encrypted transport available

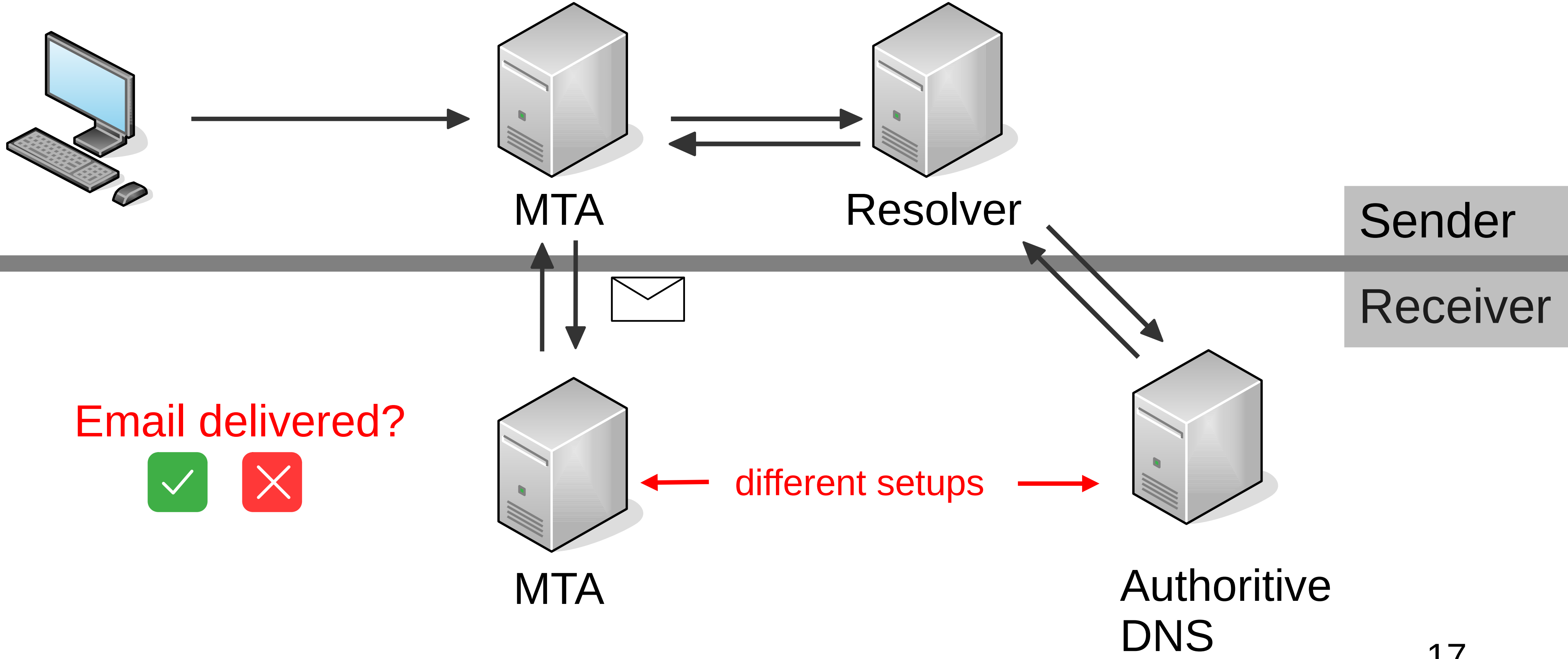
Measurement Target



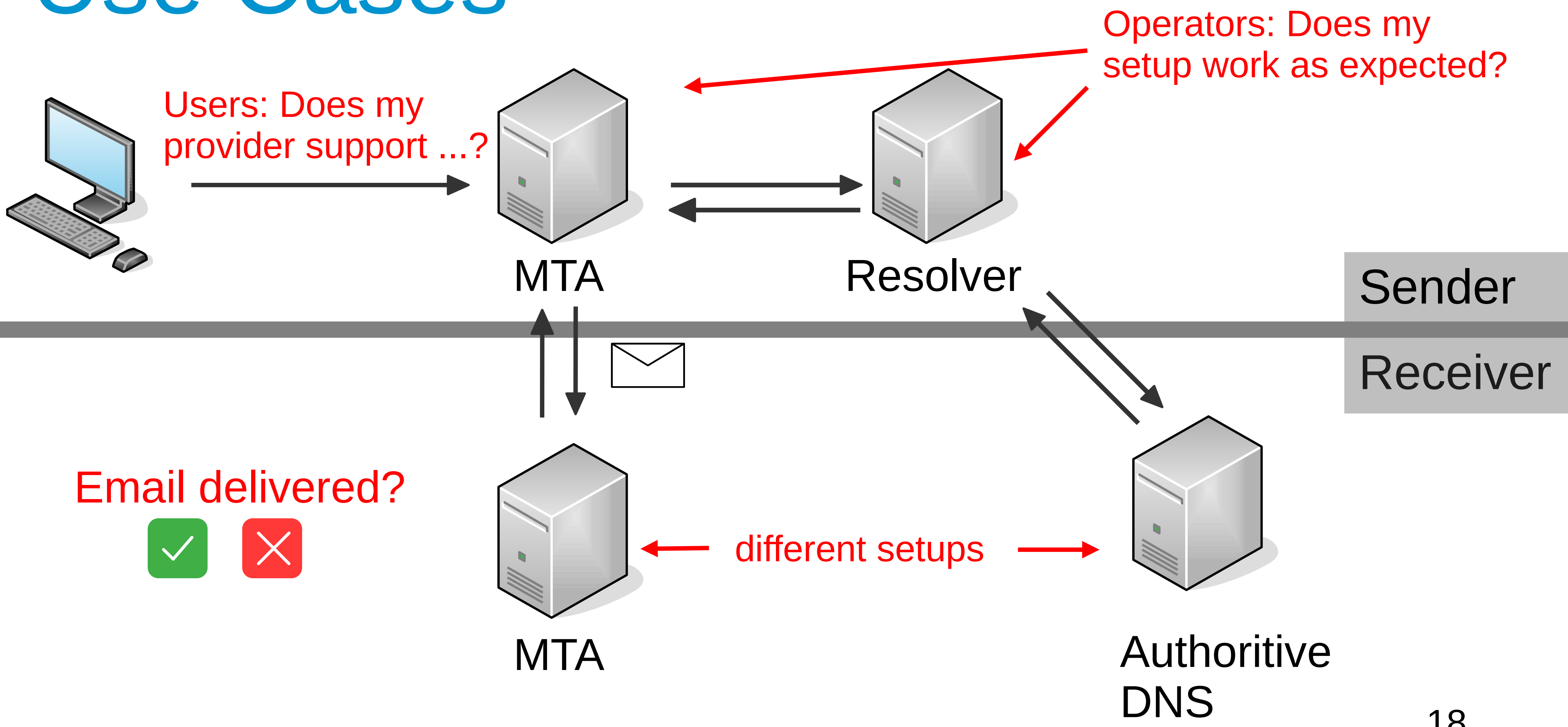
Measurement Setup



Measurement Setup



Use Cases

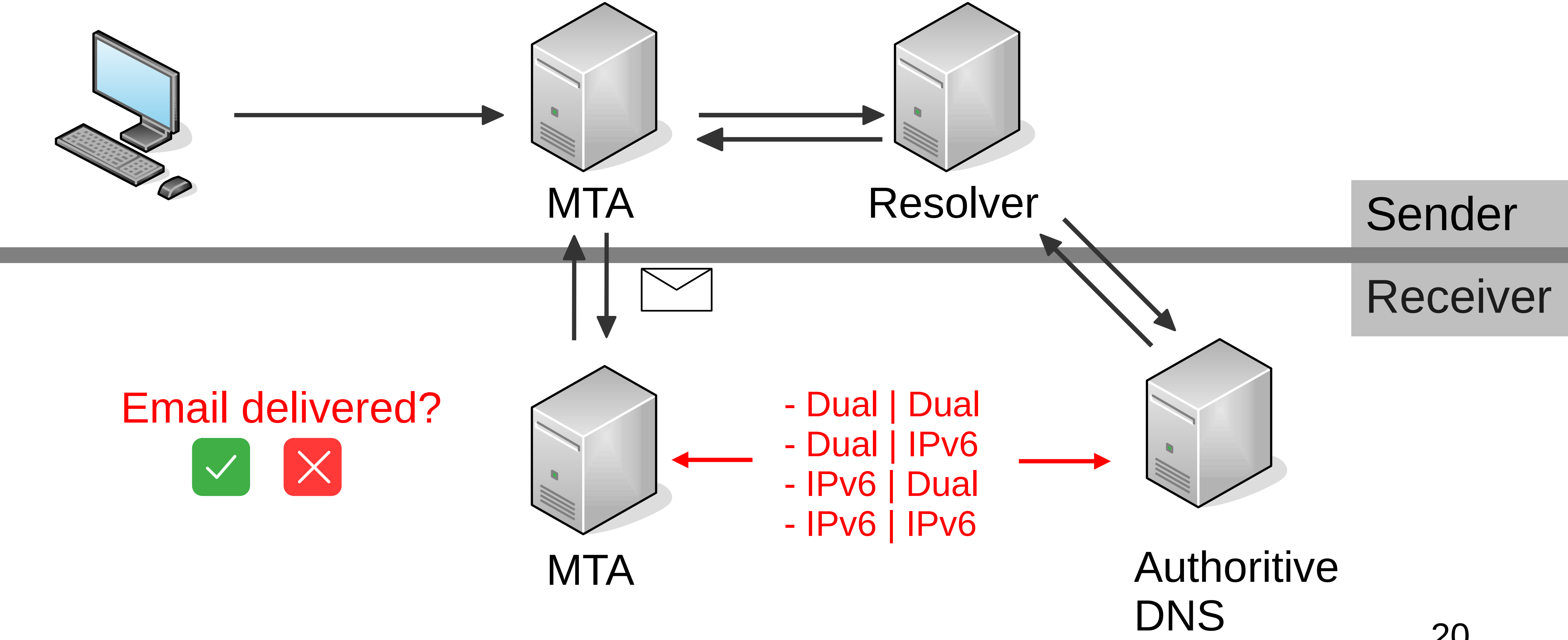

Users: Does my provider support ...?
Operators: Does my setup work as expected?
MTA
Resolver
Sender
Receiver
Email delivered?
✓ ✗
different setups
MTA
Authoritive DNS

Measurement Goals

1) Ongoing transition to IPv6

- MTAs vs. Resolvers

Measurement Setup (1)

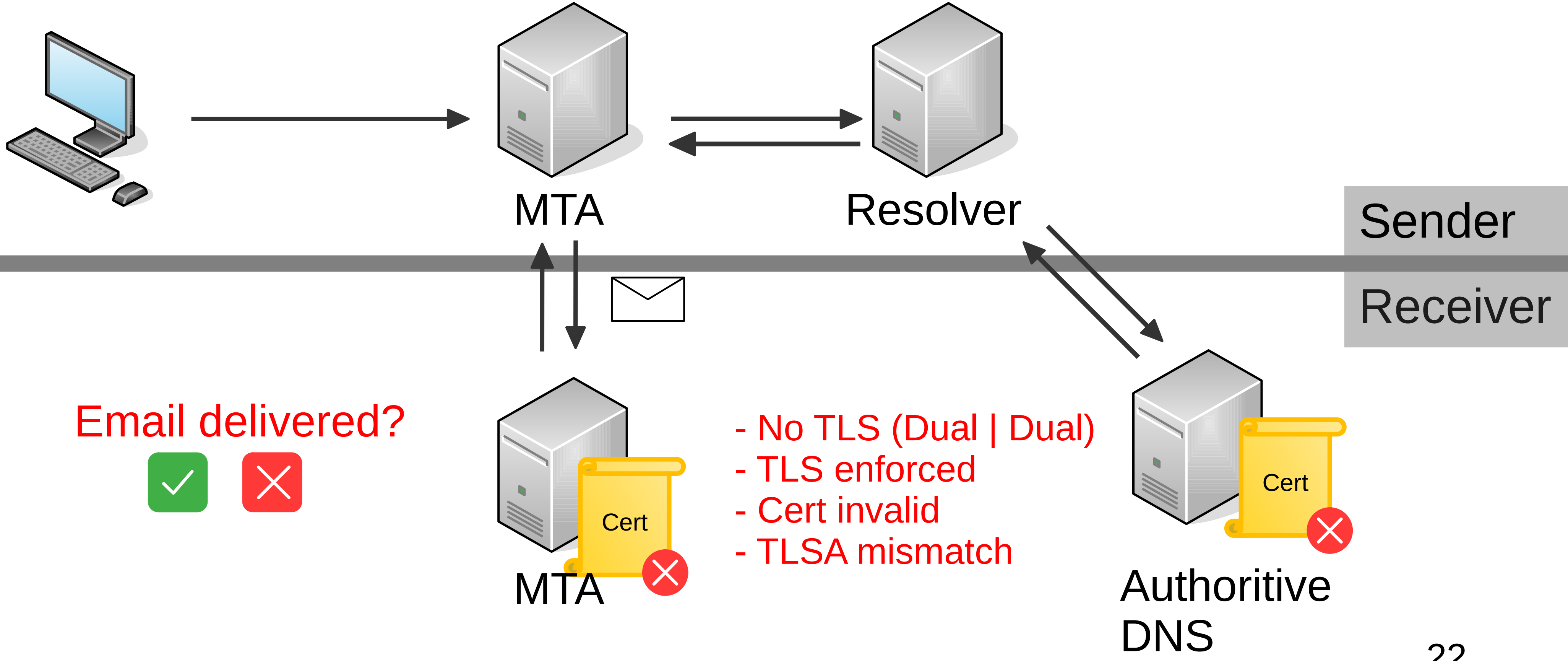


Measurement Goals

1) Ongoing transition to IPv6
   - MTAs vs. Resolvers

2) Opportunistic vs strict TLS
   - Plaintext delivery vs TLS enforcement
   - Certificate validation
   - Downgrade/MITM protection

Measurement Setup (2)



- No TLS (Dual | Dual)
- TLS enforced
- Cert invalid
- TLSA mismatch

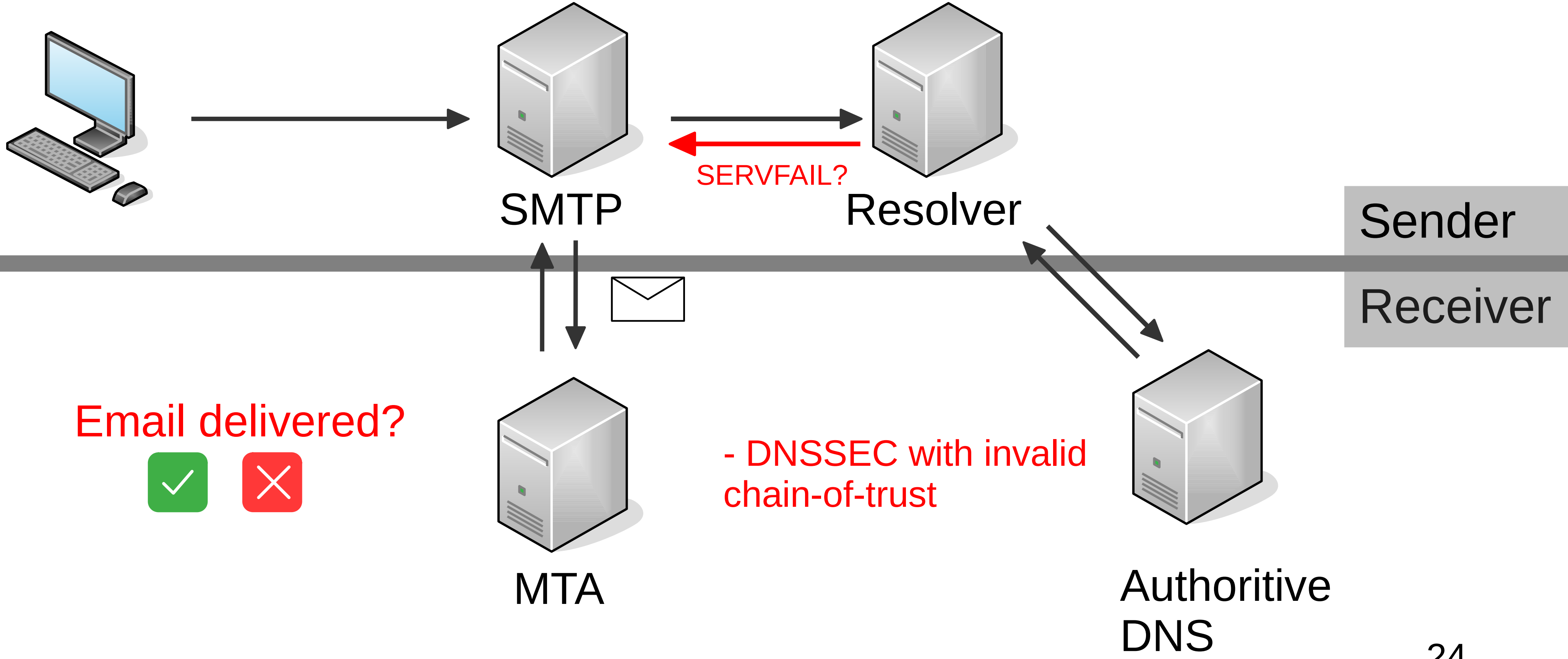
Measurement Goals

1) Ongoing transition to IPv6
   - MTAs vs. Resolvers

2) Opportunistic vs strict TLS
   - Plaintext delivery vs TLS enforcement
   - Certificate validation
   - Downgrade/MITM-Protection

3) Resolver
   - DNSSEC validation

Measurement Setup (3)



Email delivered?

✓ ✗

- DNSSEC with invalid chain-of-trust

Measurement Goals

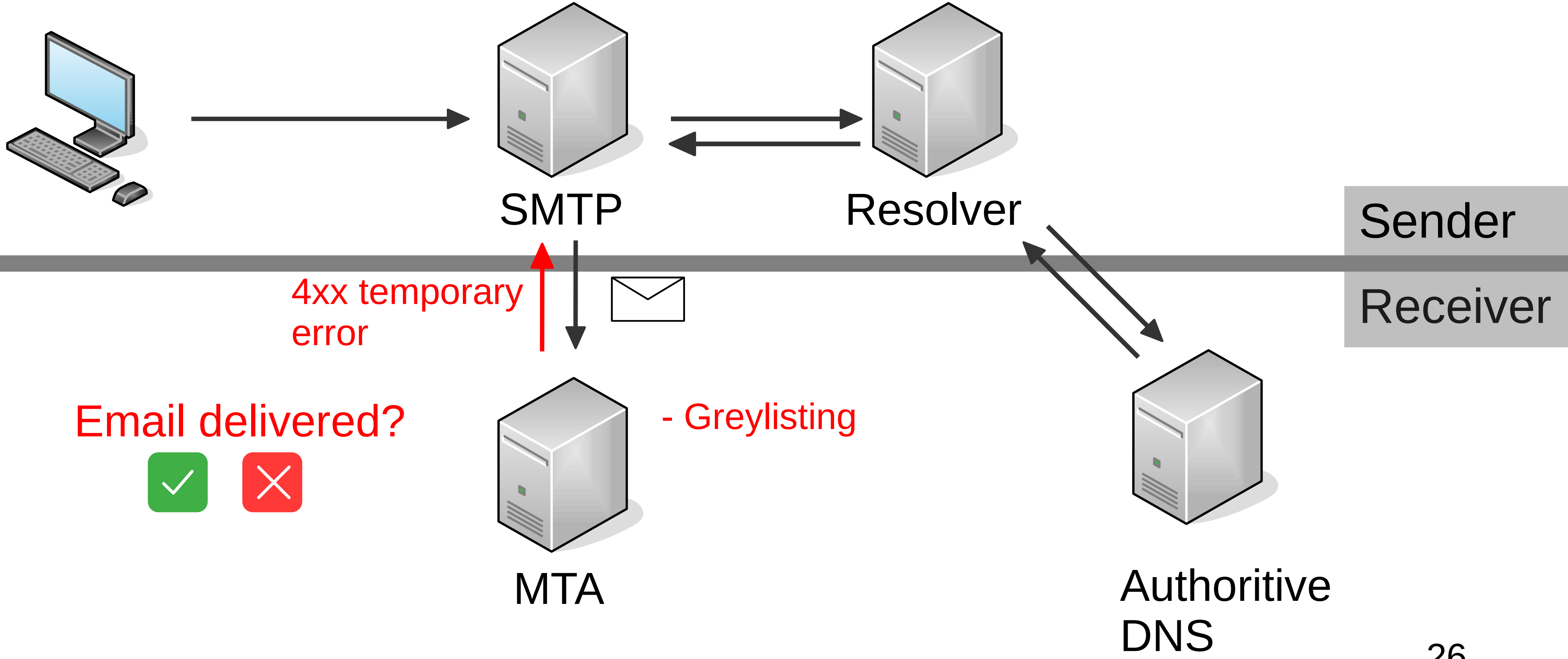
1) Ongoing transition to IPv6
   - MTAs vs. Resolvers

2) Opportunistic vs strict TLS
   - Plaintext delivery vs TLS enforcement
   - Certificate validation
   - Downgrade/MITM protection

3) Resolver
   - DNSSEC validation

4) Redelivery in case of Greylisting

Measurement Setup (4)



Datasets

1. Regular Provider

2. Large Provider

3. Spammers

Regular Provider

- Active Promotion
- July, 2020 – October, 2021
- 622 participants; 436 provider; 53 countries
- 6842 attempted deliveries, 4660 emails received
- Requirement
  - Receive at least one email
  - All target addresses in To: Header
    - Pre-filtering (5,5%)

Large Provider

- Farsight passive DNS[43]
  - 1 Month (November, 2020)
  - 73M MX lookups

Provider	% Domains
Google	14.08
Microsoft	5.95
GoDaddy	3.78
OVHCloud	1.99
Enom	1.34
Total	**27%**

Large Provider

Measurement	Year	Overlap	Large Provider	Methodology
Foster [17]	2015	3	22	Adobe Leak
Durumeric [14]	2015	6	19	Manually
Hu [22]	2018	1	35	Manually
Lee [31]	2020	2	29	Adobe Leak
Tatang [45]	2021	2	25	Manually
Liu [32]	2021	11	15	Custom
This work	2022		15	Passive DNS

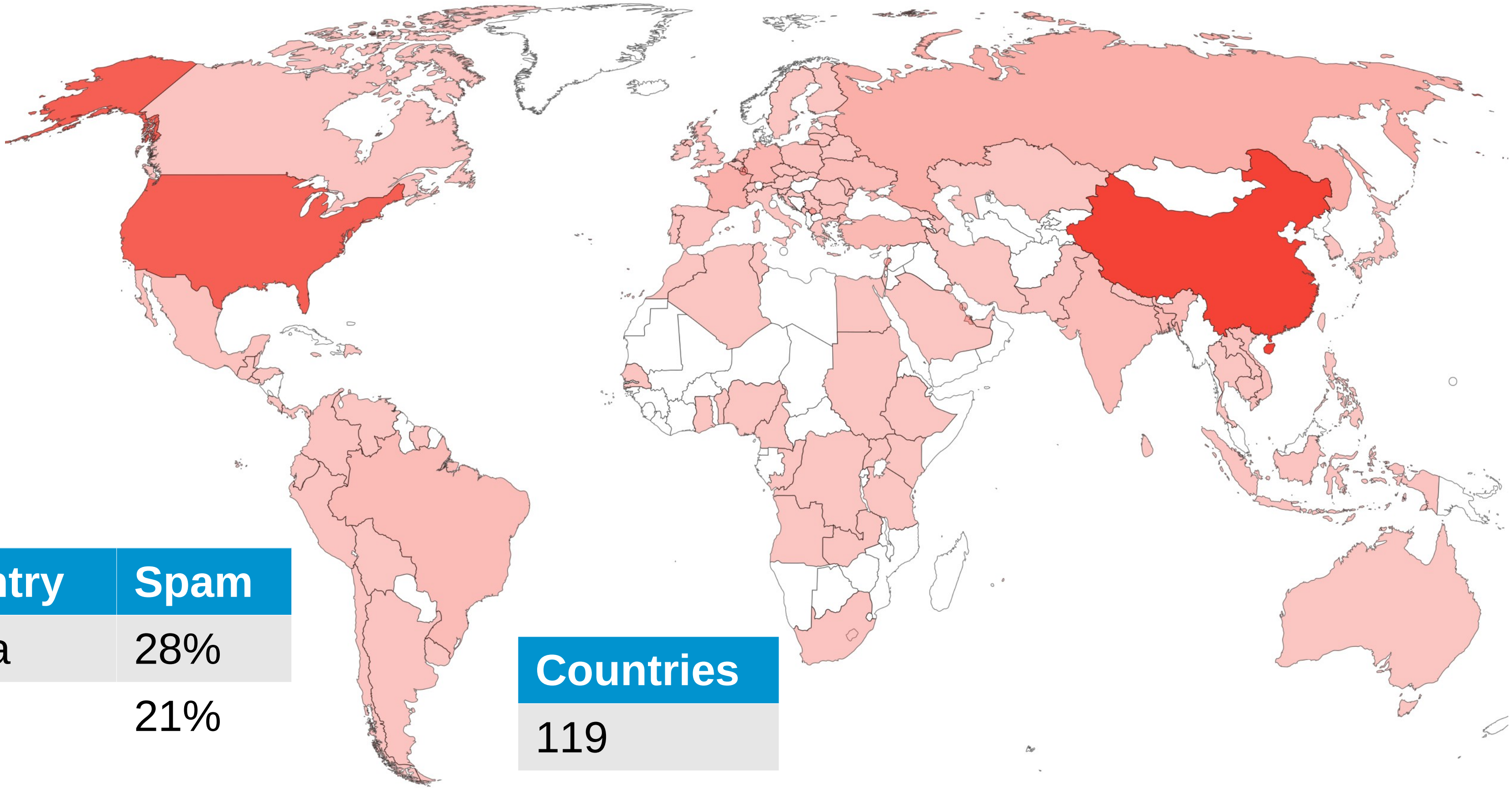
Spammers

Category	Description	% of domains that receive spam multiple days a week
1990s	Domains with the first screenshot available on Archive.org between 1990 and 2000 (= “birth year”)	50%
alexa	Domains selected based on Alexa traffic rank	28.5%
backlinks	Domains based on number of Majestic external backlinks	0%
dmoz	Domains found in the latest snapshot of dmoz.org (~2017)	38%
majestic	Domains with low Majestic million global rank	12.5%
wiki	Domains with high numbers of Wikipedia links	0%

Spammers

- 50 expired Domains
- Default spam volume
  - 3 weeks Mail-v4-Baseline
- One week rotations
  - Point MXes to a measurement server

Spammers



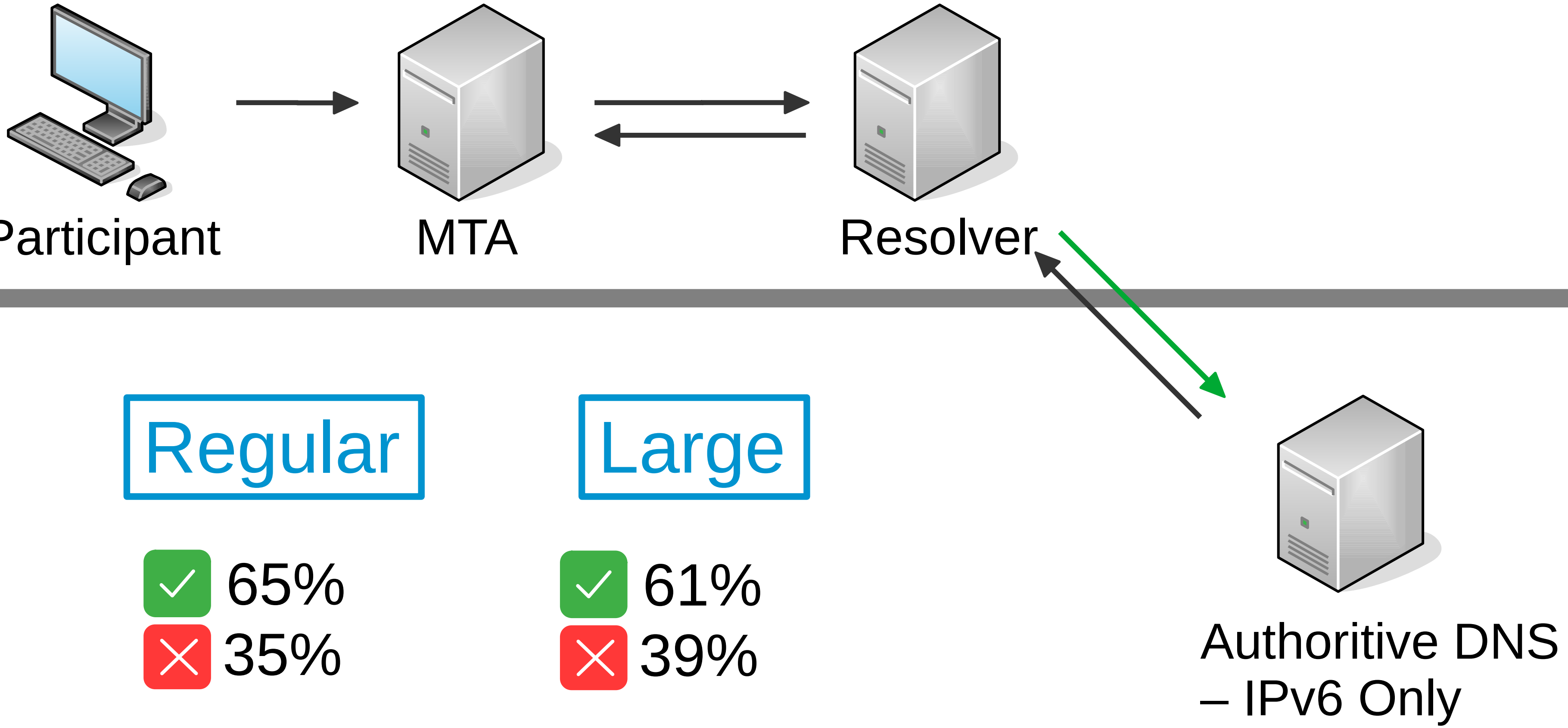
Country	Spam
China	28%
USA	21%

Countries
119

Findings:

- IPv6 Delivery

Resolver: IPv6 Support



Regular

✓ 65%

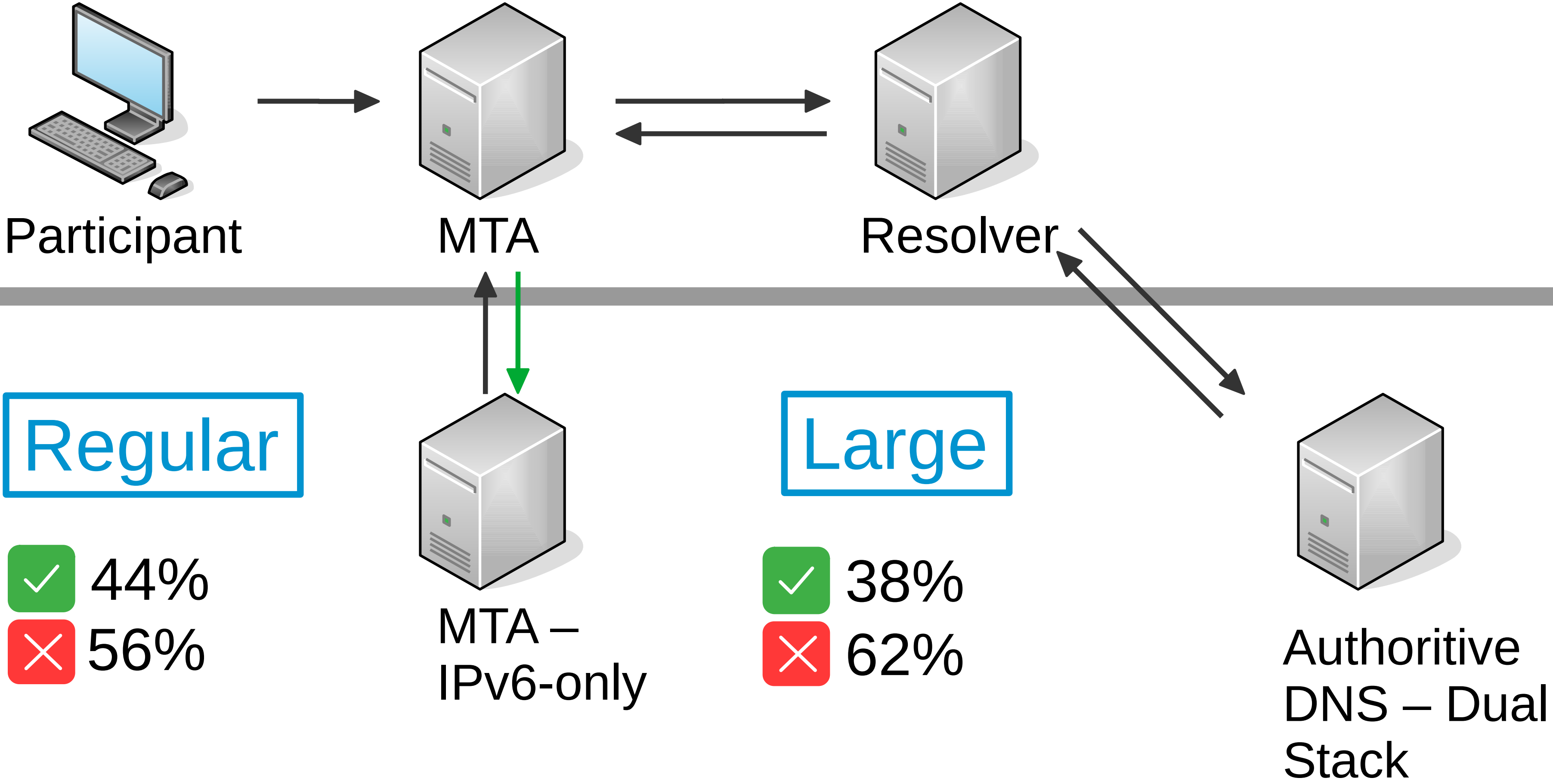
✗ 35%

Large

✓ 61%

✗ 39%

MTA: IPv6 Support



Participant

MTA

Resolver

MTA –
IPv6-only

Authoritive
DNS – Dual
Stack

Regular

✓ 44%

✗ 56%

Large

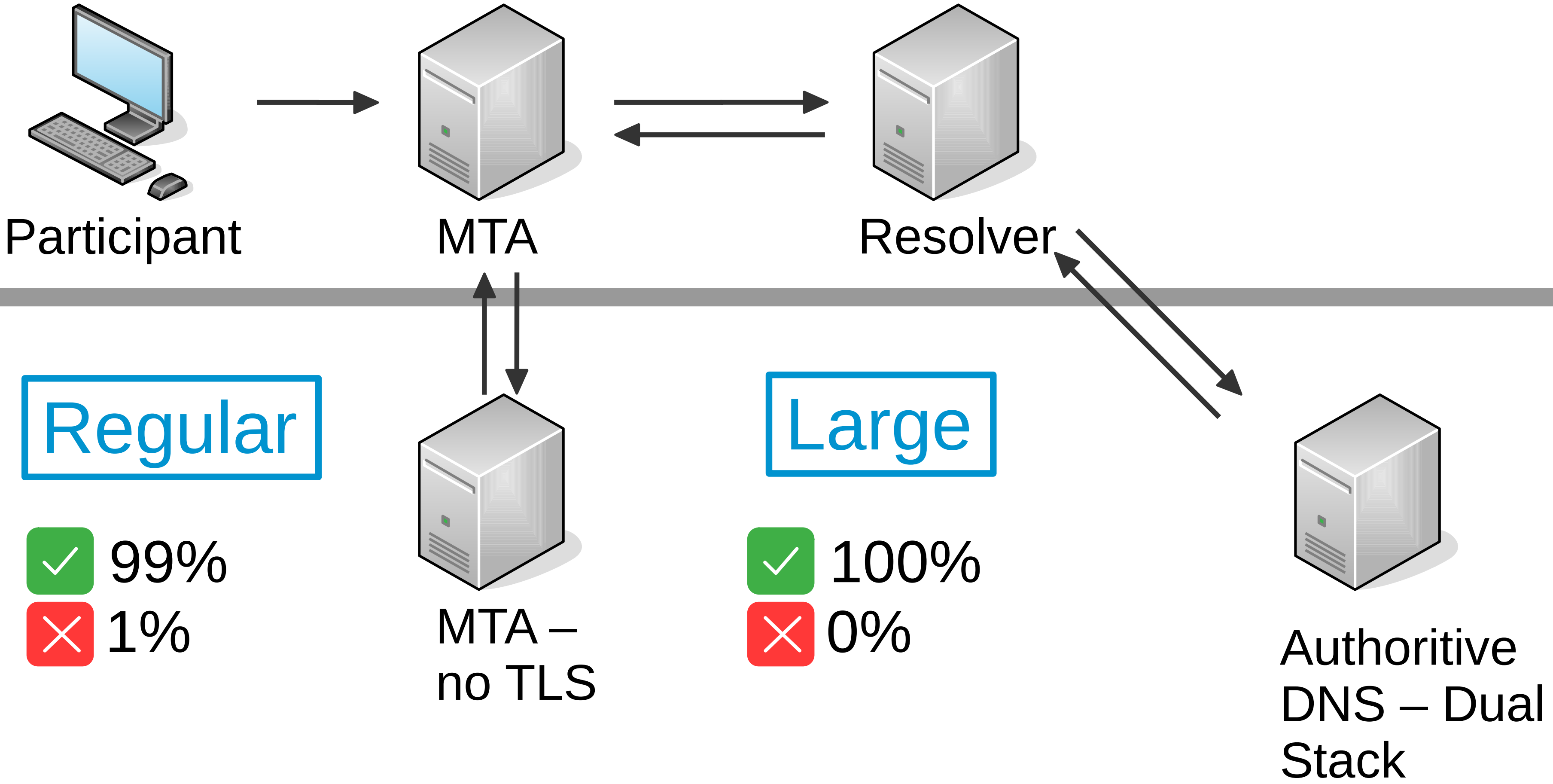
✓ 38%

✗ 62%

Findings

- IPv6 delivery
- TLS configuration

MTA: Plaintext Delivery



Participant

MTA

Resolver

MTA –
no TLS

Authoritive
DNS – Dual
Stack

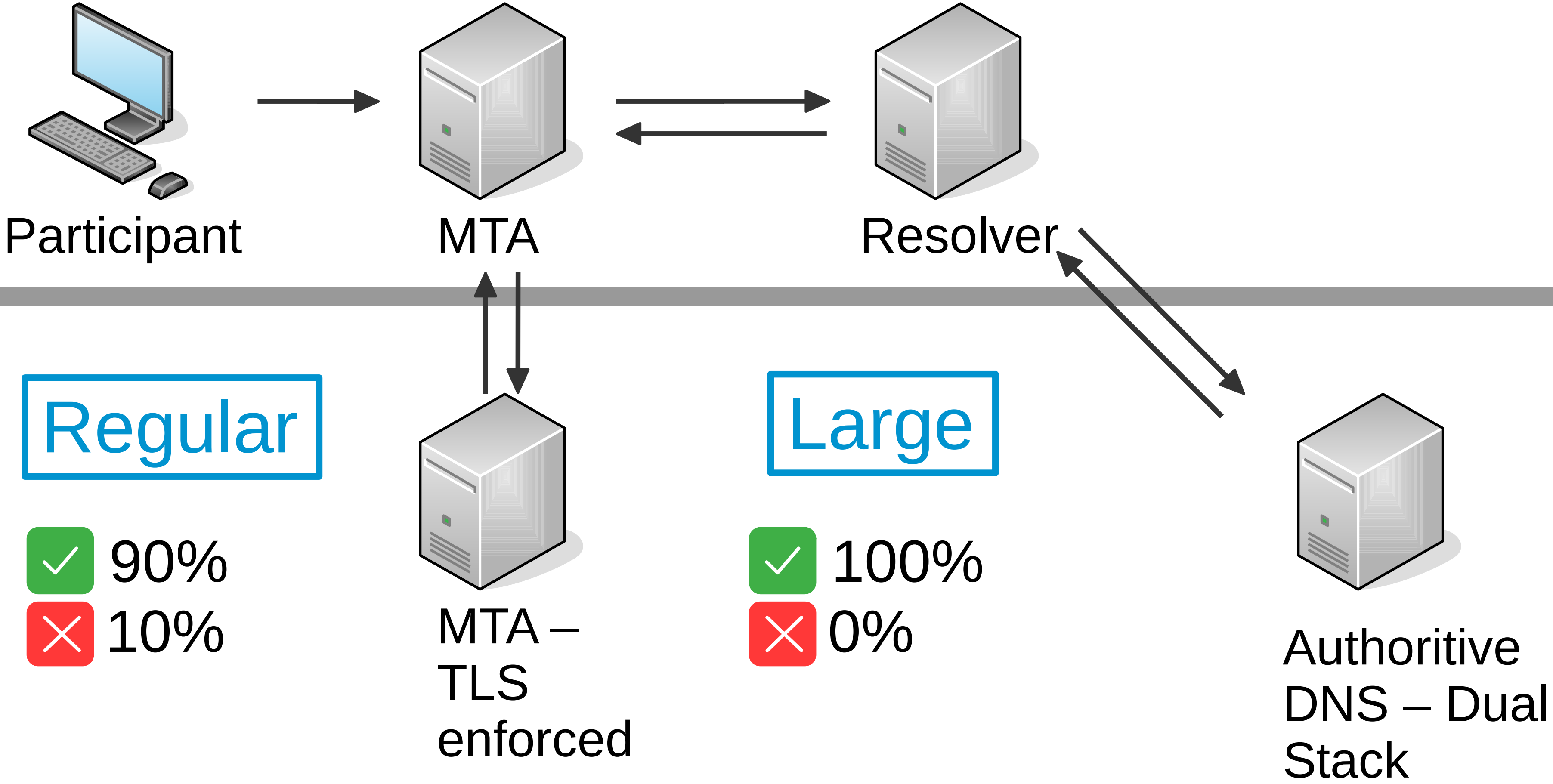
Regular

✓ 99%
✗ 1%

Large

✓ 100%
✗ 0%

MTA: STARTTLS Enforced



Participant

MTA

Resolver

Regular

✓ 90%

✗ 10%

MTA – TLS enforced

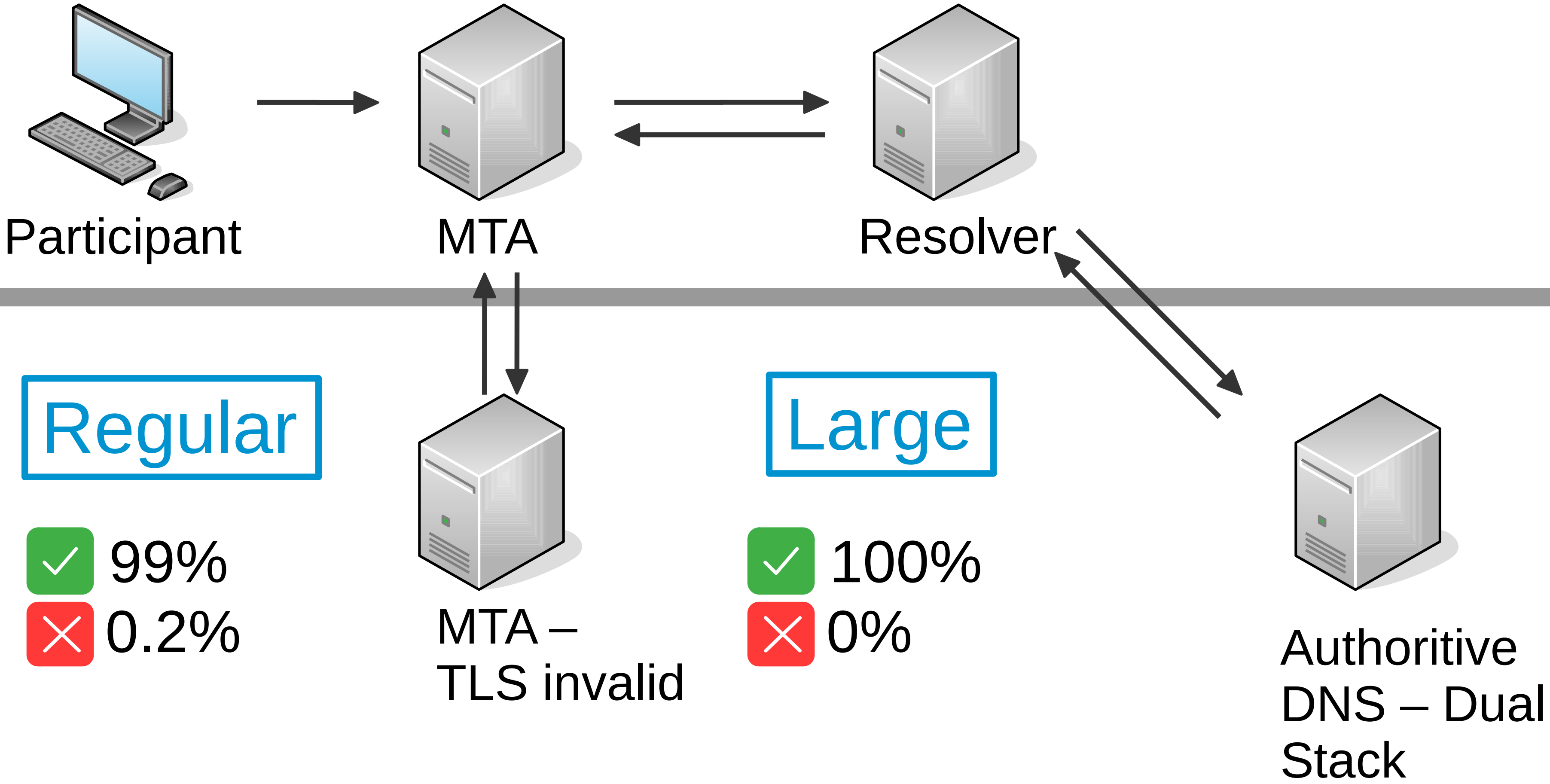
Large

✓ 100%

✗ 0%

Authoritive DNS – Dual Stack

MTA: Invalid Certificate



Regular

✓ 99%

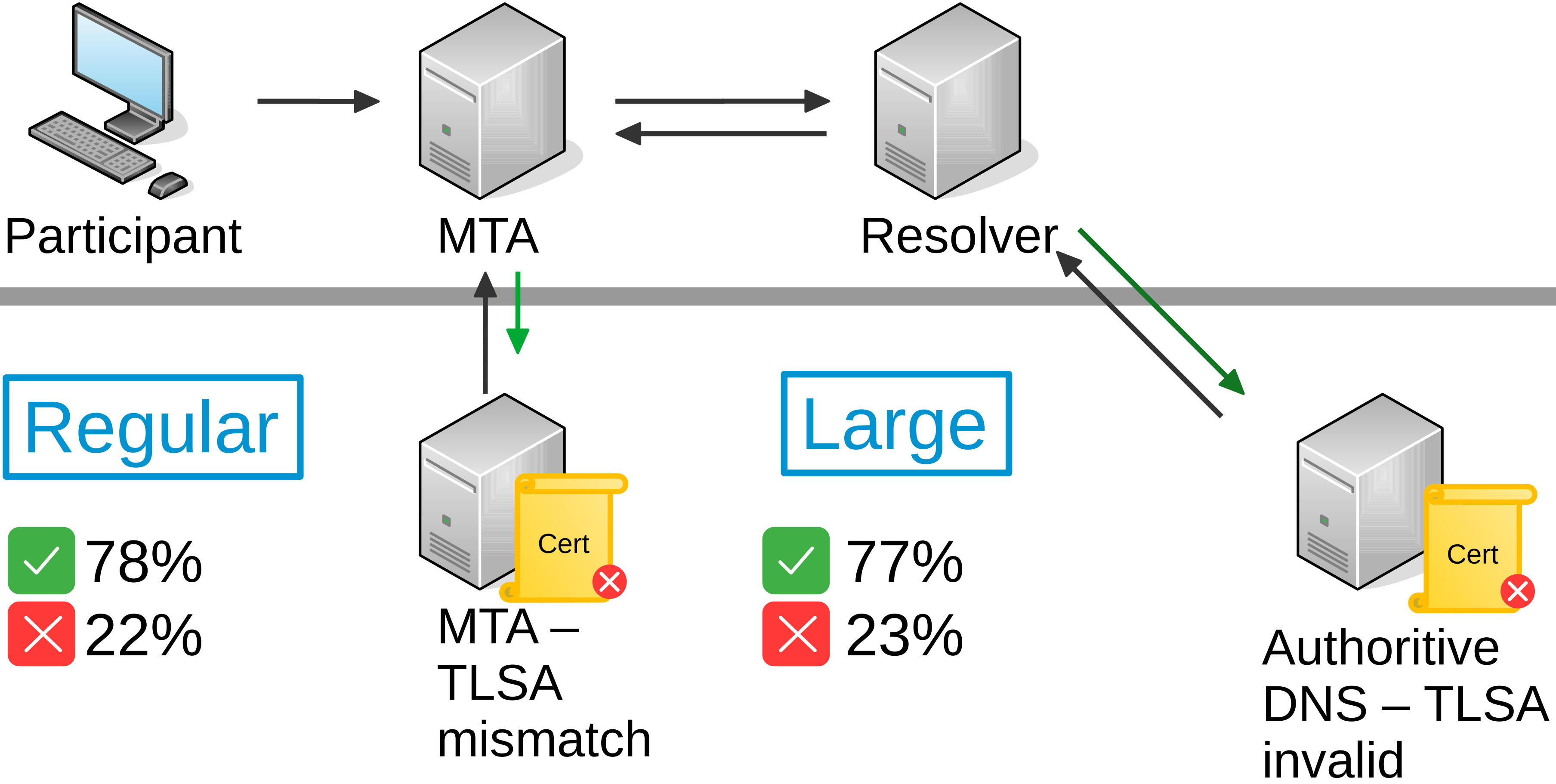
✗ 0.2%

Large

✓ 100%

✗ 0%

MTA: DANE Mismatch



Regular

✓ 78%

✗ 22%

Large

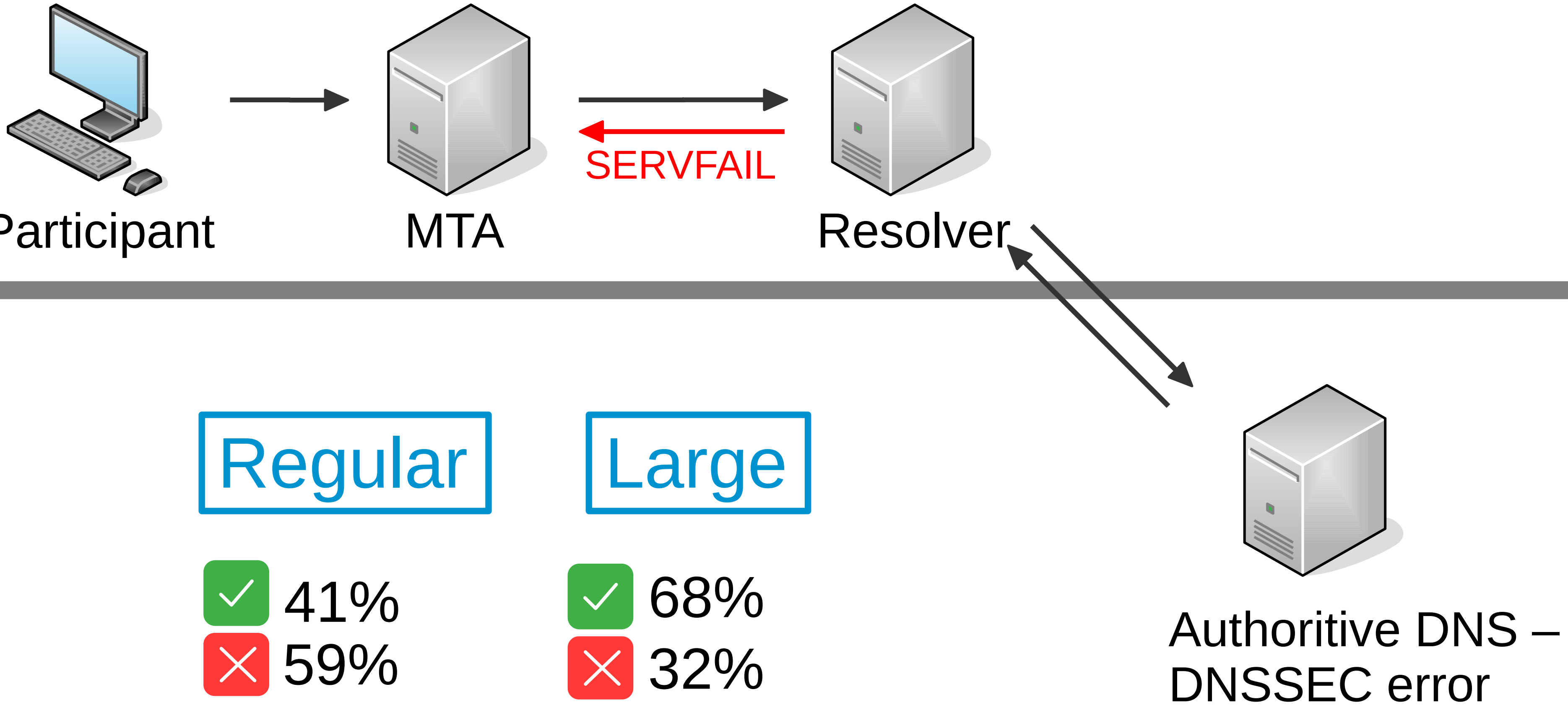
✓ 77%

✗ 23%

Findings

- IPv6 delivery
- TLS configuration
- DNSSEC validation

Resolver: DNSSEC Validation



Regular	Large
✓ 41%	✓ 68%
✗ 59%	✗ 32%

Spam Volume

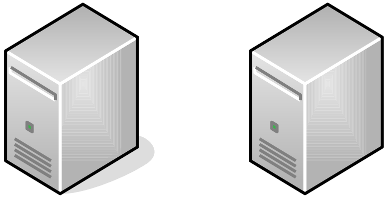
Greylisting	↓	- 37%	
IPv6 (Resolver)	↓	- 54%	(Public Resolvers)
TLS-enforced	↓	- 66%	(No TLS handshakes supported)
IPv6 (MTA)	↓	- 93%	

Conclusion

- IPv6 support: MTAs != Resolver
- Increasing support for enforcing TLS
  - Announce TLSA records, but check validity
- Large vs. small providers
- Security while keeping reachability
  - Not that simple

Questions?

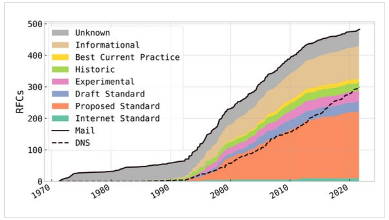
Artifact Available:



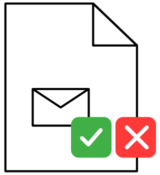
Measurement Setup

```
https://github.com/
ichdasich/email-
measurement-toolchain
```

Stay Tuned:



RFC Search Tool



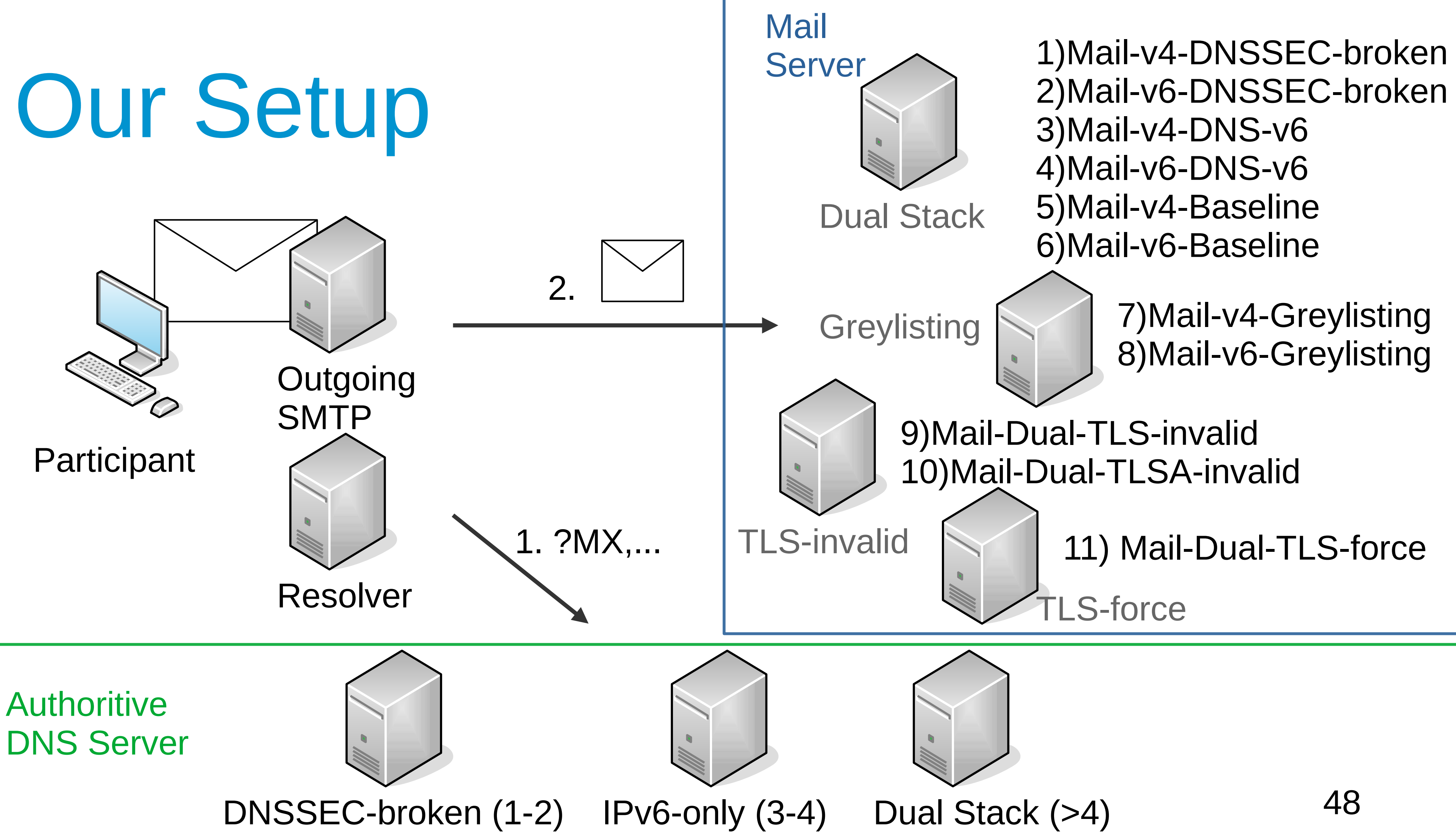
Email Delivery
Report Web-app

@holzsec

Useful Tools

- Generate TLSA records
  - https://ssl-tools.net/tlsa-generator
- Rank your email receiving capabilities
  - https://internet.nl
- Email security assessment
  - https://mecsa.jrc.ec.europa.eu/

Our Setup



Participant

Outgoing SMTP

Resolver

1. ?MX,...

2.

Mail Server

Dual Stack

1)Mail-v4-DNSSEC-broken
2)Mail-v6-DNSSEC-broken
3)Mail-v4-DNS-v6
4)Mail-v6-DNS-v6
5)Mail-v4-Baseline
6)Mail-v6-Baseline

Greylisting

7)Mail-v4-Greylisting
8)Mail-v6-Greylisting

TLS-invalid

9)Mail-Dual-TLS-invalid
10)Mail-Dual-TLSA-invalid

TLS-force

11) Mail-Dual-TLS-force

Authoritive DNS Server

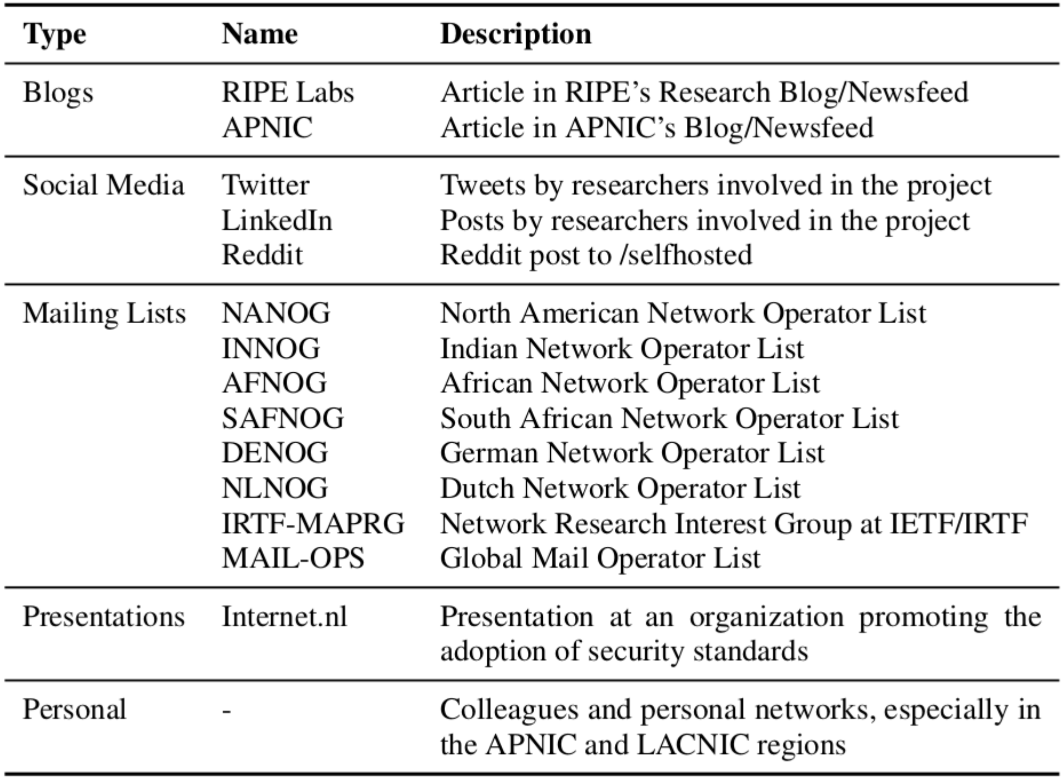
DNSSEC-broken (1-2)

IPv6-only (3-4)

Dual Stack (>4)

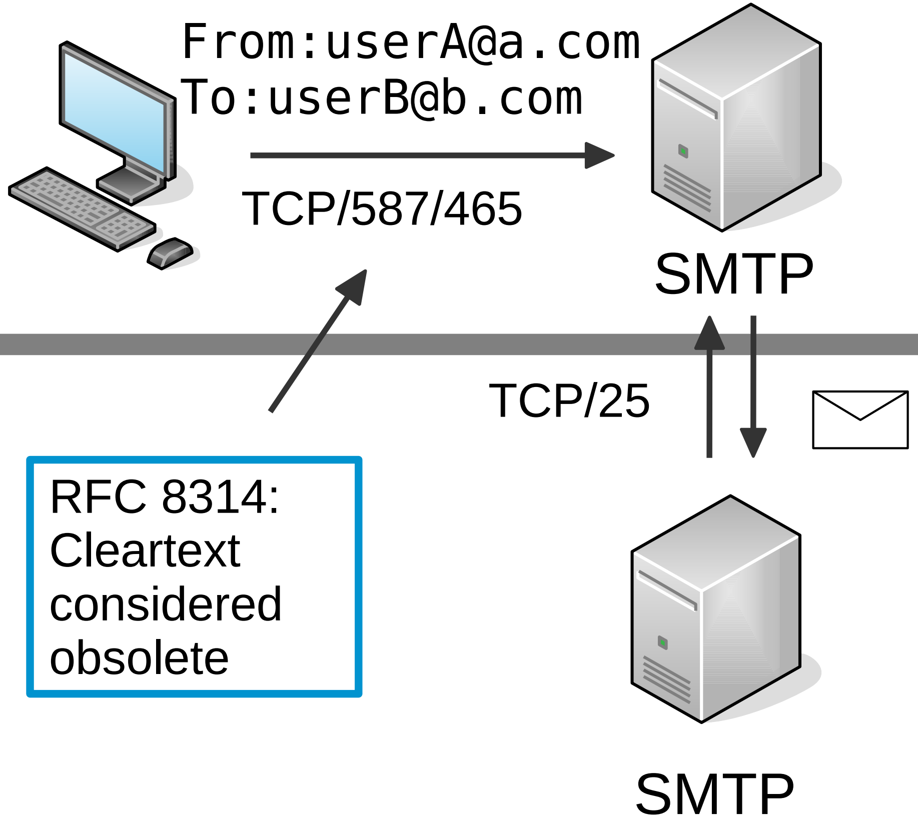
Regular Provider

- Promotion channels



Type	Name	Description
Blogs	RIPE Labs APNIC	Article in RIPE's Research Blog/Newsfeed Article in APNIC's Blog/Newsfeed
Social Media	Twitter LinkedIn Reddit	Tweets by researchers involved in the project Posts by researchers involved in the project Reddit post to /selfhosted
Mailing Lists	NANOG INNOG AFNOG SAFNOG DENOG NLNOG IRTF-MAPRG MAIL-OPS	North American Network Operator List Indian Network Operator List African Network Operator List South African Network Operator List German Network Operator List Dutch Network Operator List Network Research Interest Group at IETF/IRTF Global Mail Operator List
Presentations	Internet.nl	Presentation at an organization promoting the adoption of security standards
Personal	-	Colleagues and personal networks, especially in the APNIC and LACNIC regions

Email Submission



From:userA@a.com
To:userB@b.com

TCP/587/465

SMTP

TCP/25

SMTP

RFC 8314: Cleartext considered obsolete

```
< 220 mail.b.com ESMTP Postfix
> EHLO mail.a.com
< 250-mail.b.com
…
< 250-STARTTLS
< 250 CHUNKING
> STARTTLS
< 220 2.0.0 Ready to start TLS
```

Future Work

- Add measurement addresses for new protocols
  - TLSRPT
  - MTA-STS
- Extend reporting functionality for users and operators

Happy to collaborate on ...

- Building measurement systems
- Internet-measurements