# 50 years of e-mailu

… and we still can't work with him

August 2024

Jan Dušátko (jan.dusatko@cryptosession.cz)
Jan Kopřiva (jan.kopriva@untrustednetwork.net)

https://cryptosession.cz/download/LinuxDays2024EN.pdf

SPAM or E-MAIL

E-MAIL or SPAM

# The state of technology use in 2023

- Estimated load of $3{,}473 \cdot 10^{11}$ e-mails per day, or $1{,}268 \cdot 10^{14}$ e-mails per year
- Year-on-year increase in number of e-mails 4, 3 %
- 85 % of e-mails are marked as spam and 49 % of e-mails are demonstrably spam
- 14,3 % of common e-mail communications are erroneously captured by spam filters
- Approximately 4.3 billion users own about 7.9 billion e-mail accounts
- Year-on-year increase in number of e-mail accounts is 2,7 %
- The average size of e-mail without pictures is 50KB, with pictures 2,5MB
- Reading the average e-mail takes 10s
- Every day, mankind spends about 15,000 man-years just reading received e-mails.
- Almost 700 EB data is transmitted in e-mails every day. Probably almost half of this volume is spam and malware.

Source: https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/

# Junk mail (SPAM)

**Basic facts**

- Junk mail is a subjective evaluation, therefore objective filters can never be perfect

- Organisations require objective evaluation

- Consensual agreement on an accepted form of censorship (refusal, deletion, editing of communications)

- Purpose of protection:
  - primarily to protect against malignant content
  - secondarily to protect against unsolicited (uninteresting, irrelevant or useless) communications, burdensome attention and time consuming

- Rules are determined by the system owner or operator

- Non-compliance may lead to refusal of communication (compliance with standards, socially acceptable behaviour or legislative rules)

# Junk mail (SPAM) and technologies

**Current Technologies Allow**

- Sender to Offer Methods to Authenticate (Providing Tools to Increase Trust and Brand Protection)

- Recipients to Use Methods to Authenticate Sender

- Based on the rules of the recipient and even the sender, reject mail that has not been authenticated

- These technologies only OFFER the possibility of authentication, the recipient should use them in their own interest

- The recipient's free will determines whether to use these possibilities

**Conclusion:**

- The recipient cannot be forced to check the authenticity of emails, but the recipient cannot use the missing mechanisms.

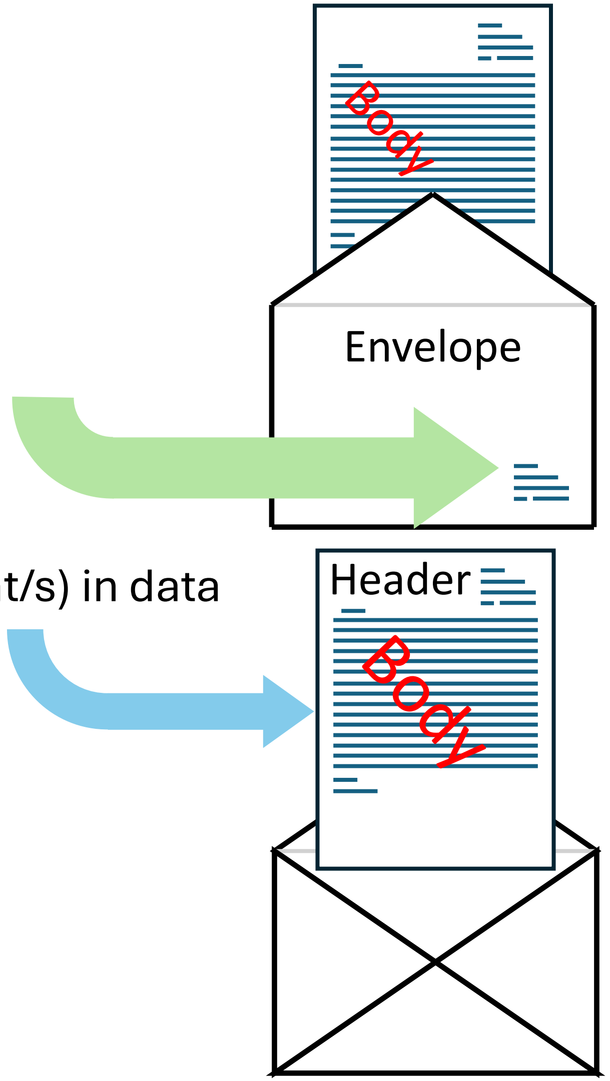
- Providing these mechanisms can be considered a form of good behavior (ethics).

- No one can force you to talk to the indecent. Because behavioral defects can also take financial form.

# E-mail structure

SMTP protocol provide information about envelope

SMTP protocol transfer header and body (text + attachement/s) in data



**RFC:**

- 5321
- 5322

**Mangling** – transcription of headers allows you to edit header records.

**Munging** – masking of e-mail addresses as protection against their collection (usually on web pages).

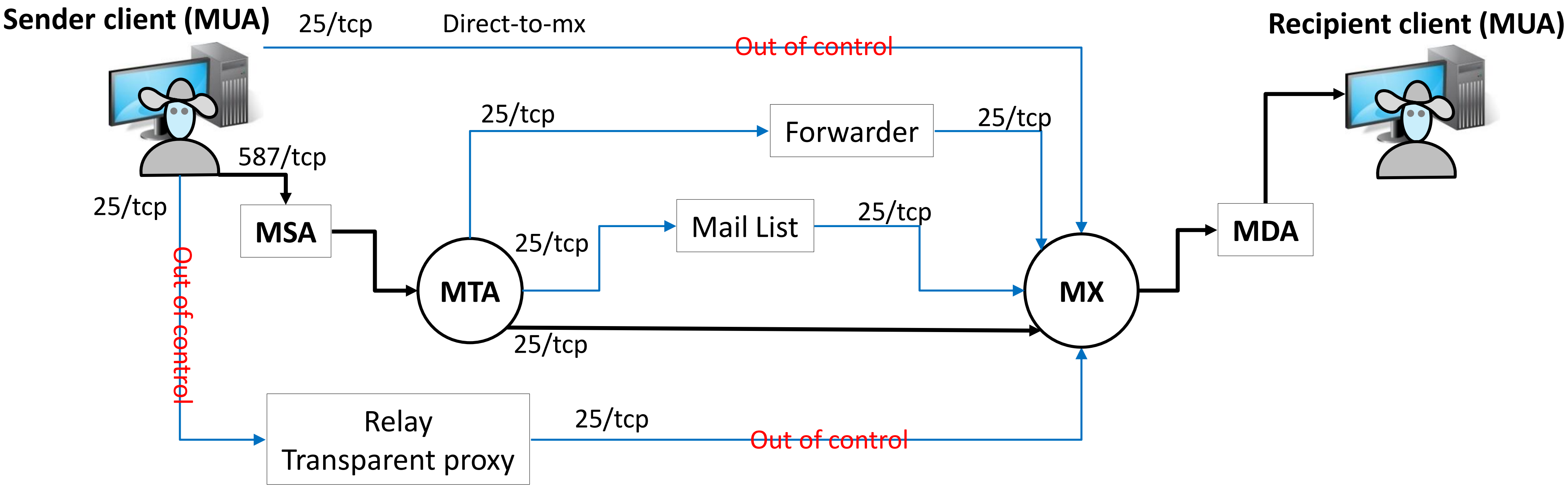
# SMTP communication infrastructure

The SMTP protocol allows protection against communication failure (availability)

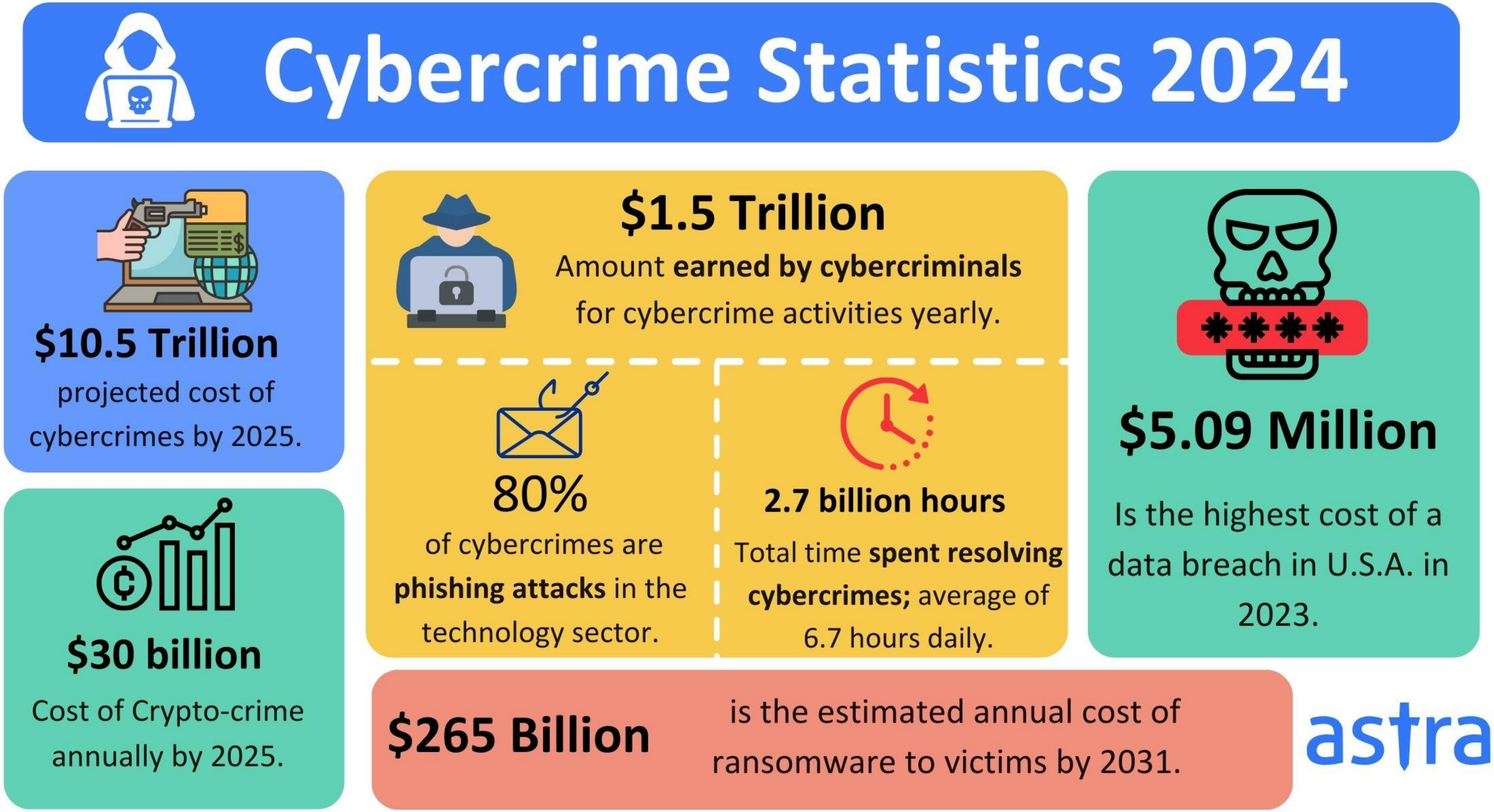
The SMTP protocol DOES NOT ensure delivery to the end user (Silent Drop on MX) or reading of the message by the user

Ensuring protection of the sender's name requires strict control over the provided communication channels

Outside of port 25/tcp (usually STARTTLS), 587/tcp (usually TLS or STARTTLS) and 465/tcp (usually TLS) are used



# Outlook to 2024 and later



## Cybercrime Statistics 2024

**$10.5 Trillion**
projected cost of cybercrimes by 2025.

**$1.5 Trillion**
Amount **earned by cybercriminals** for cybercrime activities yearly.

80%
of cybercrimes are **phishing attacks** in the technology sector.

**2.7 billion hours**
Total time **spent resolving cybercrimes;** average of 6.7 hours daily.

**$5.09 Million**
Is the highest cost of a data breach in U.S.A. in 2023.

**$30 billion**
Cost of Crypto-crime annually by 2025.

**$265 Billion** is the estimated annual cost of ransomware to victims by 2031.

https://www.getastra.com/blog/security-audit/cyber-crime-statistics/

**GDP 2022**

World
$101,3.10^{12}$ USD

USA
$25,44.10^{12}$ USD

Czech
$0,209.10^{12}$ USD

Slovakia
$0,115.10^{12}$ USD

FASCINATING
TELL ME ALL ABOUT YOUR BEST PRACTICES
makeameme.org

# IETF (Internet Engineering Task Force)

It is an international non-profit industry organisation

It represents academia as well as software/hardware manufacturers

It provides standards (RFCs) governing the operation of the Internet

It provides recommendations (BCP)

Departure from these standards can cause a significant increase in the difficulty of communication

https://www.rfc-editor.org/retrieve/

# M$^3$AAWG and APWG interest group

**M3AAWG** is an international non-profit organization, associating entities providing or using e-mail services (The Messaging, Malware and Mobile Anti Abuse Working Group)

- October 2023: Google and Yahoo announce rules to be joined by Apple, Meta, Microsoft and others ...
- Valid forward and reverse DNS mail server records
- Need to use at least SPF+DKIM+DMARC technologies
- Precedence, List-Unsubscribe-Post, List-Unsubscribe headers required for marketing communications
- Volume of junk mail under 0.3%

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

https://www.m3aawg.org/

**APWG** is an international non-profit organization to increase protection against cybercrime (Anti Phishing Working Group)

APWG

https://apwg.org/

# Solutions in the Czech Republic

NUKIB (CZ) on 11 October 2021 issued a protective measure issued on the basis of § 14 of the Cybersecurity Act No. 181/2014 Coll., on Cybersecurity (reference number: 8477/2021-NÚKIB-E/350):

- The authorities and persons referred to in § 3 (c) to (f) of the Cybersecurity Act … which are also public authorities involved in the Czech Presidency of the Council of the EU … involved in the preparations and performance of the Presidency in 2022, must comply with the points … by 1 July 2022 at the latest.

- The other authorities and persons referred to in § 3 (c) to (f) of the Cybersecurity Act, must comply with the points 1.1. to 1.8. by 1 January 2023 at the latest.

Requirements for compliance:

- Support for DNSSEC and DANE TLSA
- Implementation of SPF, DKIM, DMARC
- MTA-STS and TLS 1.2+, valid certificates

Further changes will probably be based on the implementation of NIS2

# Solutions in the Slovakia Republic

CSIRT (SK) issued:

- „Recommendation for implemetation of authentication and authorization system pre-e-mail servers" on 21.05.2021

- "Methodology for systematic security of public administration organizations in the area of information security" 28.02.2024

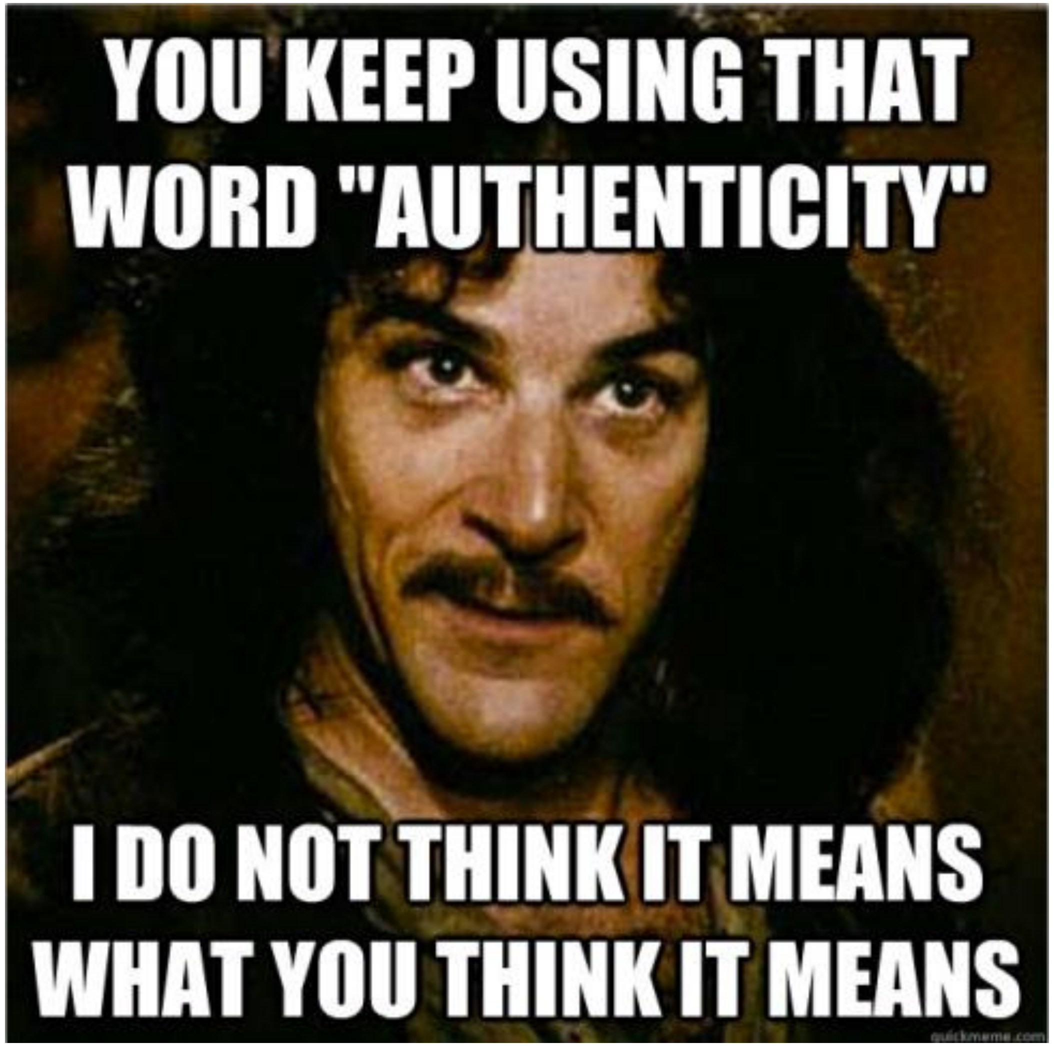
Recommendations for compliance:

- SPF, DKIM, DMARC

Further changes will probably be based on NIS2 implementation

# Technology overview: Source of origin authenticity

- Forward lookup / Reverse lookup / Forward confirmed reverse lookup
- SPF
- SenderID (zastaralé)
- Domainkey (zastaralé)
- DKIM
- ADSP (zastaralé)
- ATPS
- DMARC
- ARC
- BIMI


YOU KEEP USING THAT WORD "AUTHENTICITY"
I DO NOT THINK IT MEANS WHAT YOU THINK IT MEANS
quickmeme.com

# Reverse records and liability

The use of Forward and Reverse Records is required in RFC 5321 , RFC 1912 and RFC 2821

1. The domain has a defined owner
2. The IP addresses in turn have an owner (they are usually part of autonomous systems and subleased)
3. There is no ownership relationship between the IP and DNS
4. The address record can be created by the domain owner in the DNS (Forward lookup)
5. The Reverse Record is established by the IP address owner i.e. rDNS (Reverse lookup)
6. Confirmation of the FCrDNS (Forward Confirmed Reverse Lookup)

Thus, Forward and Reverse Records form a coherent relationship and at the same time a certain level of weak authentication

**RFC:**

- 5321

There is a problem with the determination of liability for next level domains provided by the owner to a third party.
Solution proposal: DBOUND TXT record - https://datatracker.ietf.org/doc/html/draft-levine-dbound-dns

```
_bound.domain.tld IN TXT "bound=1 NOBOUND . domain.tld"
```

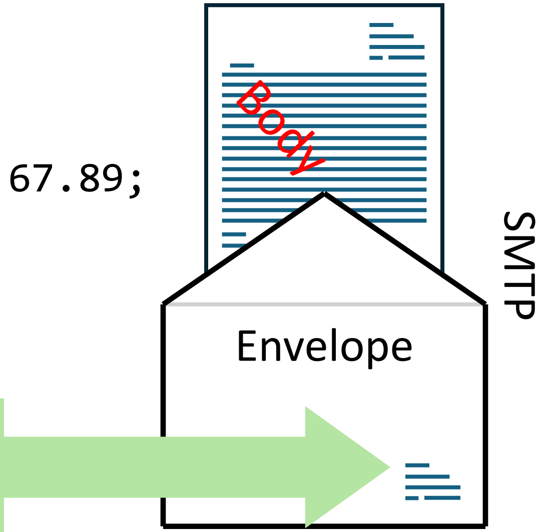
# SPF – Sender Policy Framework

Locator: @ domain.tld

**Header after MTA ...**

```
Received-SPF: pass (mailfrom) identity=mailfrom; client-ip=123.45.67.89;
helo=server.sender.tld; envelope-from=noreply@sender.com;
receiver=<UNKNOWN>
```

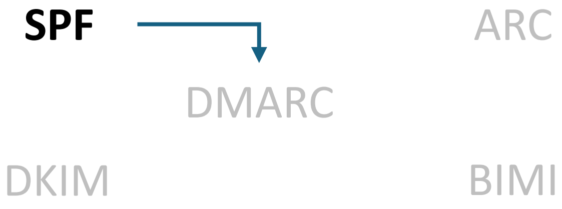
```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM sender@sourcedomain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```



**RFC:**
- 7208

**Service:**
- DNS

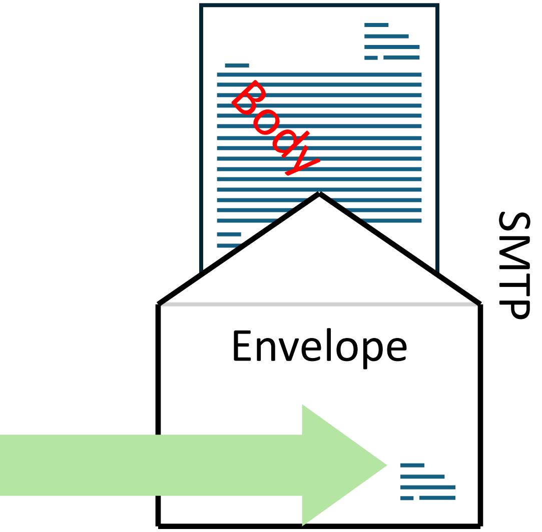
**Protocol:**
- SMTP
- DNS



# SenderID

Locator: @ domain.tld

```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM sender@sourcedomain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```



**RFC:**
- 4406

**Service:**
- DNS

**Protocol:**
- SMTP
- DNS

SPF

ARC

DMARC

DKIM

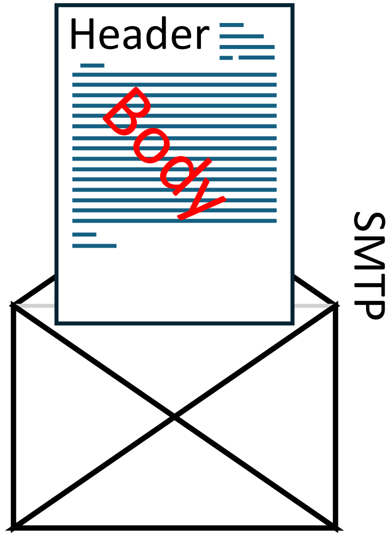
BIMI

# DK (DomainKey)

Locator: *selector*._domainkey.domain.tld

**Headers after MTA …**

**DomainKey-Signature:** a=rsa-sha1; s=selector1; d=domain.tld; c=simple;
q=dns; b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRN
iYzR;



RFC:
- 4870

Service:
- DNS

Protocol:
- SMTP
- DNS

SPF

ARC

DMARC

DKIM

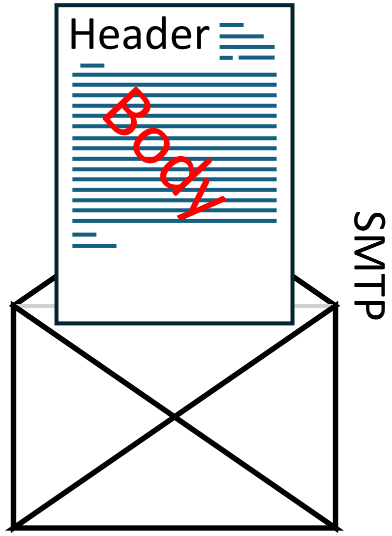
BIMI

# DKIM – Domain Key Identified Mail

Locator: `*selector*._domainkey.domain.tld`

**Headers after MTA …**

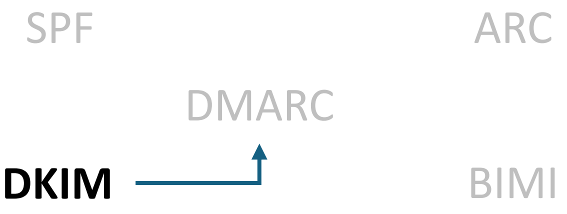
**DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/simple; q=dns/txt; d=sender.tld; i=marketing@sender.tld; s=dkimselector; h=Message-Id:Date:From:To:Subject:CC:Sender:Reply-To:MIME-Version:Content-Type:List-ID:List-Unsubscribe:List-Unsubscribe-Post:Feedback-ID:Precedence; bh=[*digital signature in Base64*]



**RFC:**
- 4871
- 5672
- 6376
- 8301
- 8463
- 8553
- 8616

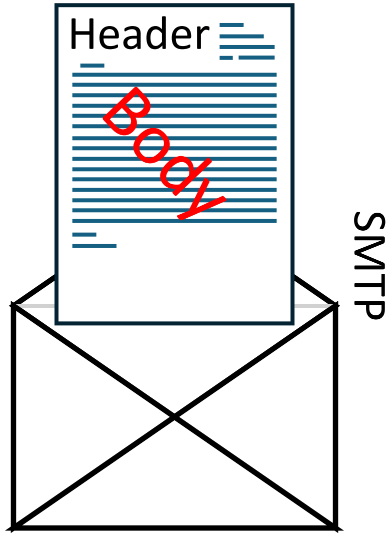
**Service:**
- DNS

**Protocol:**
- SMTP
- DNS



# ADSP – Author Domain Signing Practice

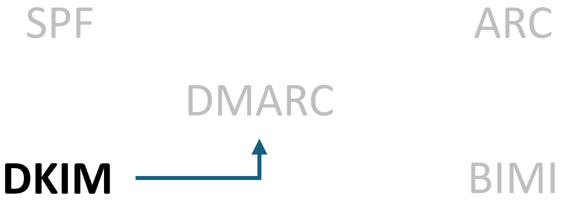
Locator: `_adsp.domain.tld`



**RFC:**
- 5617

**Service:**
- DNS

**Protocol:**
- SMTP
- DNS

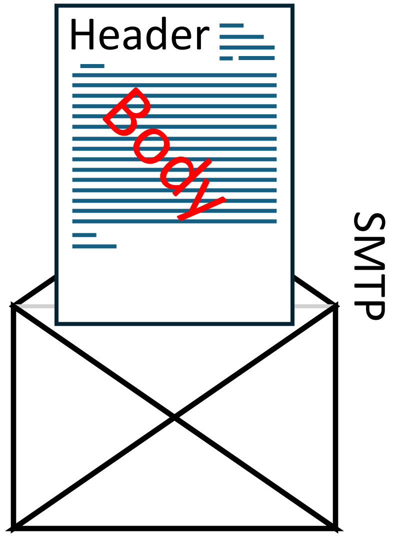


# ATPS – Authorized Third Party Signature

Locator: domain.tld._atps.3rdparty.tld
[*hash_názvu_domény*]._atps.3rdparty.tld

**Headers after MTA …**

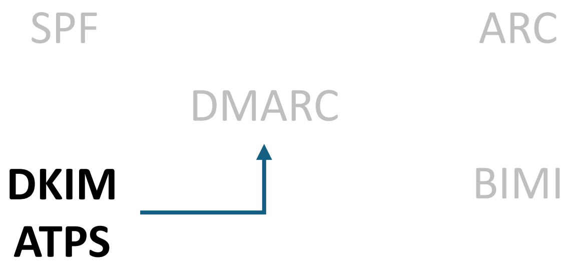
**DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/simple; q=dns/txt; d=sender.tld; i=marketing@sender.tld; s=dkimselector; h=Message-Id:Date:From:To:Subject:CC:Sender:Reply-To:MIME-Version:Content-Type:List-ID:List-Unsubscribe:List-Unsubscribe-Post:Feedback-ID:Precedence; bh=[*digital signature in Base64*]; **atps=3party.tld; atpsh=none**



**RFC:**
- 6541

**Service:**
- DNS

**Protocol:**
- SMTP
- DNS

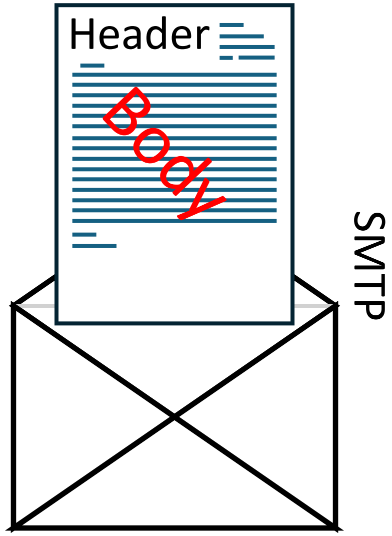


# DMARC – Domain-based Message Authentication, Reporting and Conformance

Locator: `_dmarc.domain.tld`

**Headers after MTA …**

```
Authentication-Results: server.targetdomain.tld; dkim=pass (2048-bit
key; unprotected) header.d=sourcedomain.tld header.i=@sourcedomain.tld
header.a=rsa-sha256 header.s=selector header.b=aabbccdd; dkim-
atps=neutral
```

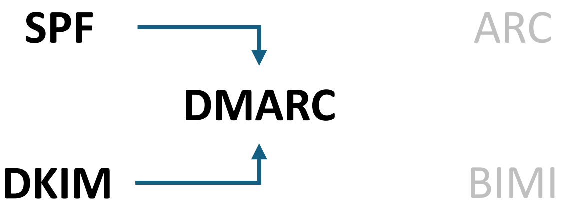


**RFC:**
- 7489
- 7601
- 8601
- 8616
- 9091

**Service:**
- DNS
- SPF

  *or*
- DKIM

**Protocol:**
- SMTP
- DNS

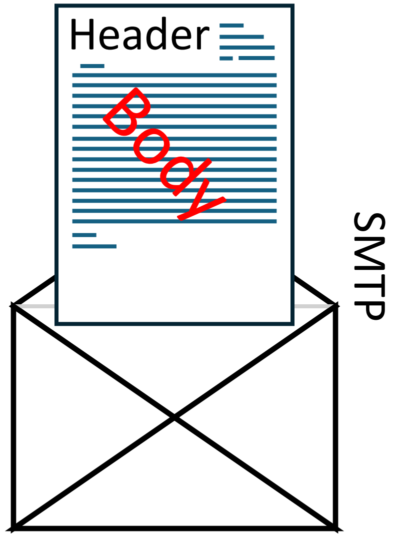


# ARC – Authenticated Receive Chain

Locator: *selector*._domainkey.domain.tld

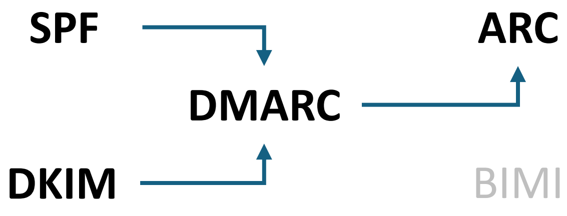
**Headers after MTA …**

**ARC-Seal:** i=1; a=rsa-sha256; s=arcselector; d=trusted.1$_{st}$1hop.tld; cv=none; b=[*digital signature in Base64*]
**ARC-Message-Signature:** i=1; a=rsa-sha256; c=relaxed/relaxed; d= sourcedomain.tld; s=arcselector; h=Message-Id:Date:From:To:Subject: CC:Sender:Reply-To:MIME-Version:Content-Type:List-ID:List-Unsubscribe: List-Unsubscribe-Post:Feedback-ID:Precedence; bh=[*digital signature in Base64*]
**ARC-Authentication-Results:** i=1; trusted.1$_{st}$1hop.tld 1; spf=pass smtp.mailfrom=sourcedomain.tld; dmarc=pass action=none header.from=sourcedomain.tld; dkim=pass header.d=sourcedomain.tld; arc=none



**RFC:**

- 8617



**Service:**

- DMARC
- DNS

**Protocol:**

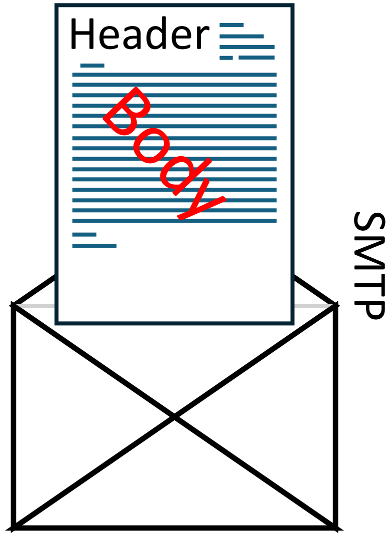
- SMTP
- DNS

# BIMI – Brand Message Mail Identification

Locator: `*selector*._bimi.domain.tld`
Default: `default._bimi.domain.tld`

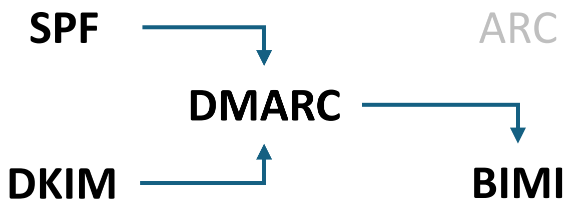
**Headers before MTA …**

```
BIMI-selector: v=BIMI1;s=selector
```



**RFC:**
- 3709
- 5280
- 6110
- 6170
- 6962
- 9399
- draft

RFC 3709: GIF, JPEG, MP3
RFC 6170: GIF, JPEG, PDF, PNG, SVG
RFC 9399: GIF, JPEG, PDF, PNG, SVG, SVG+GZIP



**Service:**
- DMARC
- DNS
- HTTPs
- X.509

**Protocol:**
- SMTP
- DNS
- HTTPs

# Technology overview: Bounce address protection

- BATV
- VERP
- SRS

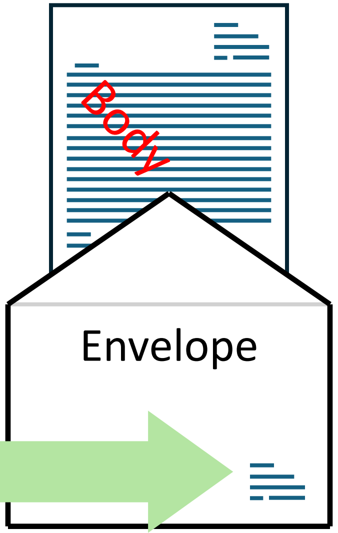
# Bounce address protection - BATV

Locator:

**Header after MTA …**

```
Received-SPF: pass (mailfrom) identity=mailfrom; client-ip=123.45.67.89;
helo=server.sender.tld; envelope-from=prvs=sender/1123ABCDEF@domain.tld;
receiver=<UNKNOWN>
```

```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM prvs=sender/1123ABCDEF@domain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```



**RFC:**
- draft

**Service:**

**Protocol:**
- SMTP

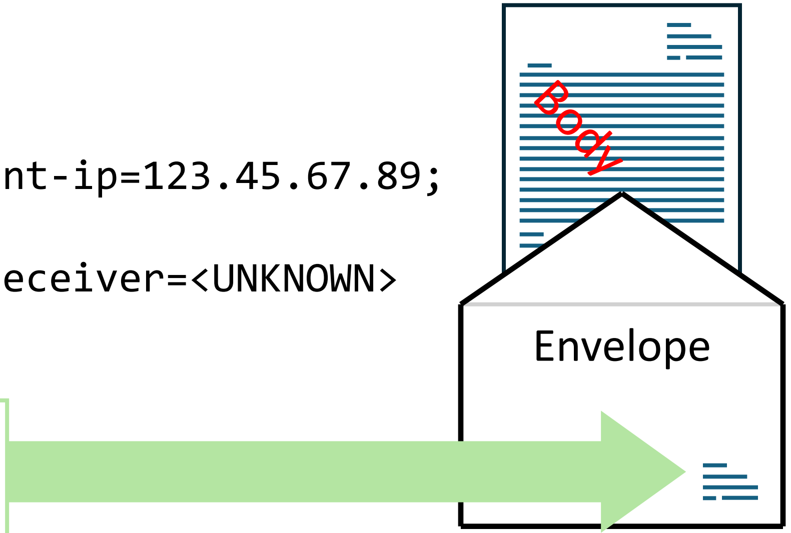
# Variable Envelope Return Path - VERP

Locator:

**Header after MTA …**

```
Received-SPF: pass (mailfrom) identity=mailfrom; client-ip=123.45.67.89;
helo=server.sender.tld; envelope-from=
sender+recipient=targetdomain.tld@sourcedomain.tld; receiver=<UNKNOWN>
```

```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM sender+recipient=targetdomain.tld@sourcedomain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```



**RFC:**
- 3464

**Service:**

**Protocol:**
- SMTP

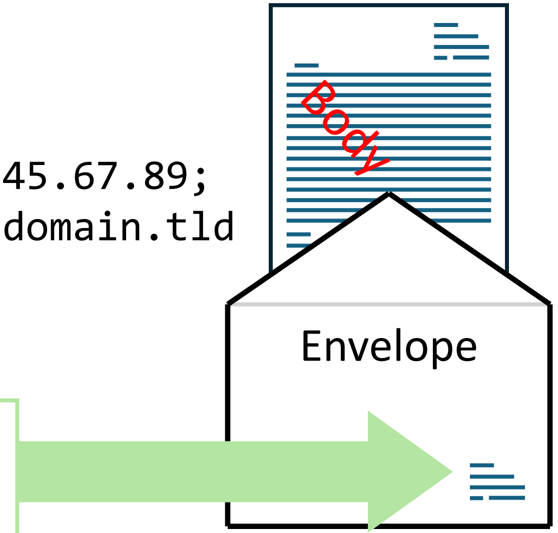
# Sender Rewriting Scheme - SRS

Locator:

**Header after MTA ...**

```
Received-SPF: pass (mailfrom) identity=mailfrom; client-ip=123.45.67.89;
helo=server.sender.tld; envelope-from=SRS0=01..ef=01..89=sourcedomain.tld
=sender@recipientdomain.tld; receiver=<UNKNOWN>
```

```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM SRS0=01..ef=01..89=sourcedomain.tld=sender@recipientdomain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```



**RFC:**
- draft

**Service:**

**Protocol:**
- SMTP

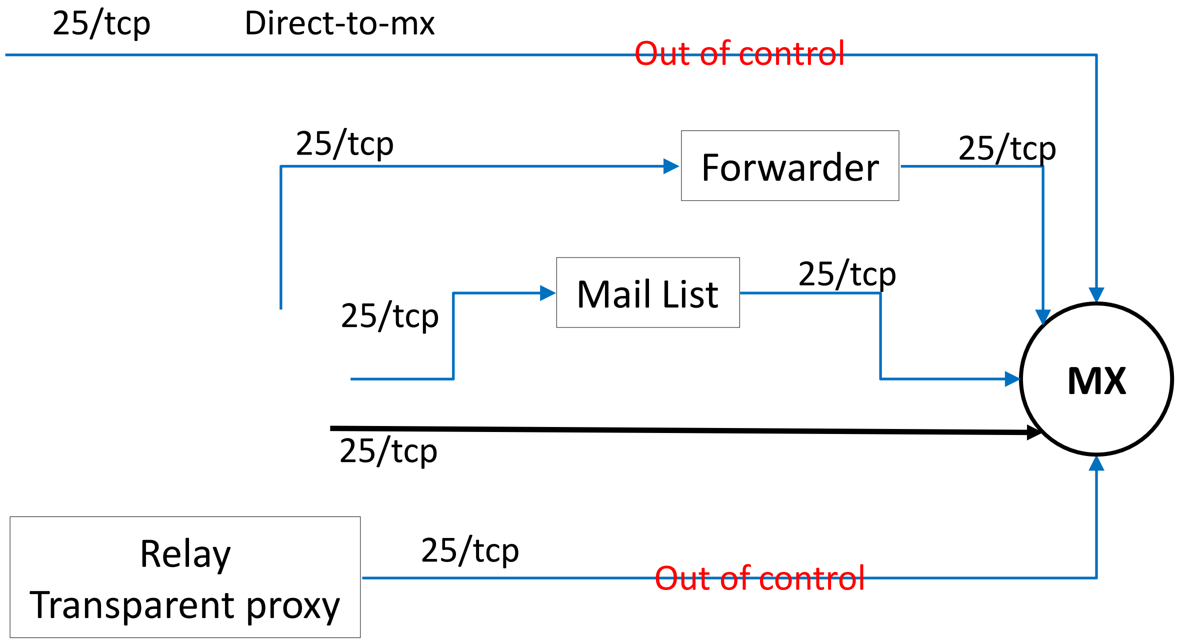
# Technology overview: Ensuring transport security

- MTA-STS
- DANE TLSA

# MTA-STS

```
Locator: _mta-sts.domain.tld.  TXT    "v=STSv1; id=20201231;"
         mta-sts.domain.tld.   A      IP.AD.DR.ES
         https://mta-sts.domain.tld/.well-known/mta-sts.txt
```

**RFC:**
- 8640
- 8641



**MTA-STS web:**

About SMTP supported:

- Plaintext only
- **Support TLS**
- **Enforce TLS**

**Service:**
- SMTP
- DNS
- HTTPs
- X.509
- TLS

**Protocol:**
- SMTP
- DNS
- HTTPs

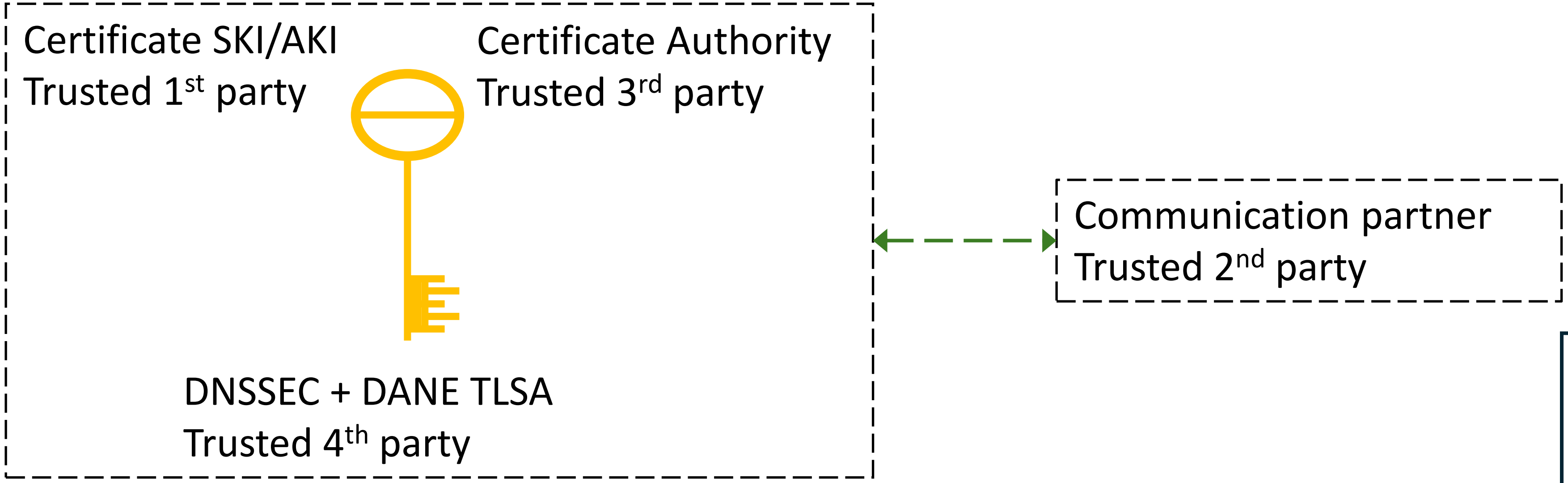
# DANE TLSA

Locator: `_587._tcp.mail.domain.tld IN TLSA 3 0 1`

```
5494492464623acb8155a1b1949000ef334c968dd1d5351a3e3baae737c0c1ab
```

**RFC:**

- 8640
- 8641



Certificate SKI/AKI
Trusted 1st party

Certificate Authority
Trusted 3rd party

DNSSEC + DANE TLSA
Trusted 4th party

Communication partner
Trusted 2nd party

**Service:**

- DNS
- X.509
- TLS

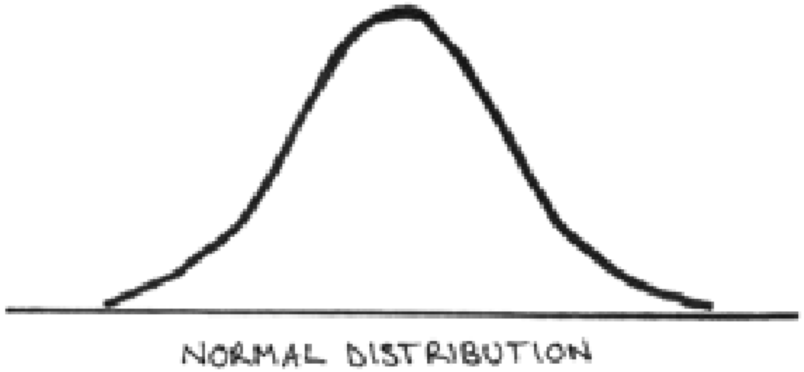
**Protocol:**

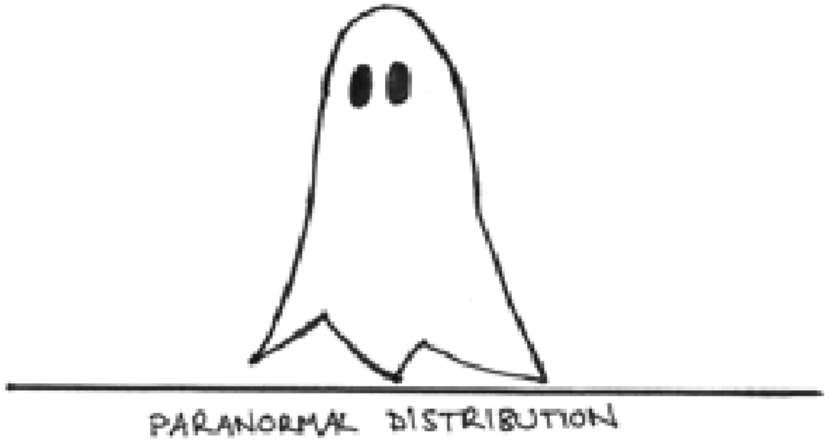
- DNS

**Implementation of TLSA without DNSSEC is a nonsense!**

# Overview of technologies applicable to feedback collection

- Bounces
- DMARC report
- TLS report
- DKIM report
- ADSP report





# Bounces

Important information is custom error messages, where codes or possibly extended error codes provided by the mail server should be evaluated. Unfortunately, some of the messages are sent only in a textual state.

| | |
|---|---|
| **220** | Successfully delivered |
| **421** | Service not available, closing transmission channel |
| **422** | The recipient’s mailbox is over quota |
| **431** | The recipient’s server is temporarily unavailable |
| **432** | The recipient’s server is not accepting messages at this time |
| **450** | Requested action not taken; mailbox unavailable |
| **451** | Temporary server error; try again later |
| **452** | Insufficient system storage |
| **453** | No mail |
| **454** | Temporary authentication failure |
| **550** | Non-existent email address or domain |
| **551** | User not local; please try forwarding |
| **552** | Mailbox full; exceeded storage allocation |
| **553** | Invalid recipient address format |
| **554** | Transaction failed; message refused |
| **555** | Syntax error in parameters or arguments |
| **556** | Domain does not exist (DNS) |
| **557** | Recipient's mailbox is full |
| **558** | Mail server requires authentication |

| | |
|---|---|
| **2.X.X** | Successful delivery |
| **4.1.X** | Temporary delivery - addressing issues |
| **4.2.X** | Temporary delivery - mailbox issues |
| **4.3.X** | Temporary delivery - mail system issues |
| **5.1.X** | Permanent delivery - addressing issues |
| **5.2.X** | Permanent delivery - mailbox issues |
| **5.3.X** | Permanent delivery - mail system issues |

# Reporting

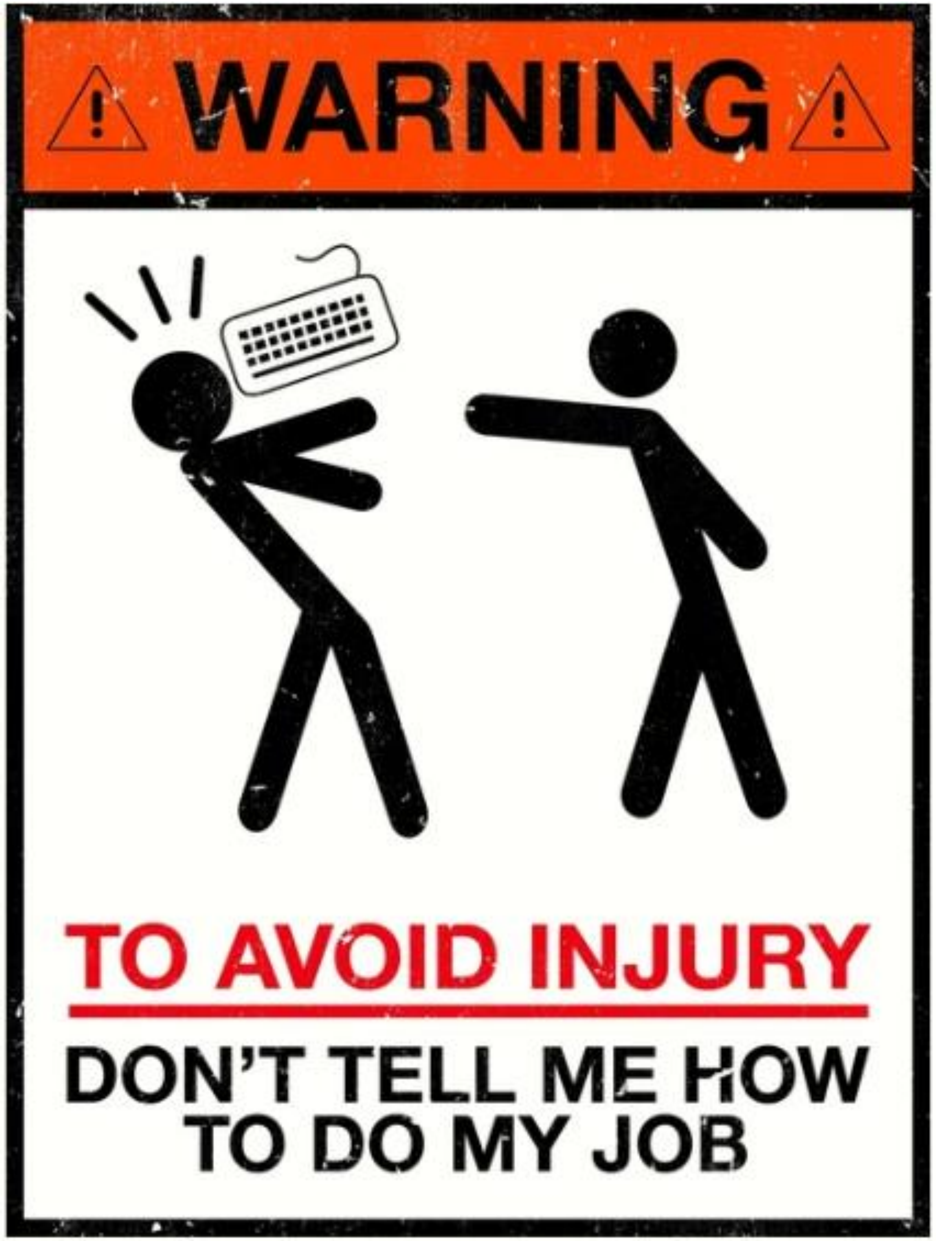
- **DMARC** (RFC 7489)
  - Part of DMARC setup
  - Analytical (rua), creates overview reports for periods
  - Forensic (ruf), possibility to create a report for each wrong evaluation
  - "v=DMARC1;...;rua=mailto:postmaster@domain.tld;ruf=mailto:postmaster@domain.tld„

- **TLS** (RFC 8460, RFC 8461)
  - Relative to MTA-STS, report problems when establishing a secure connection
  - _smtp._tls.domain.tld.   IN   TXT   "v=TLSRPTv1;rua=mailto:postmaster@domain.tld„

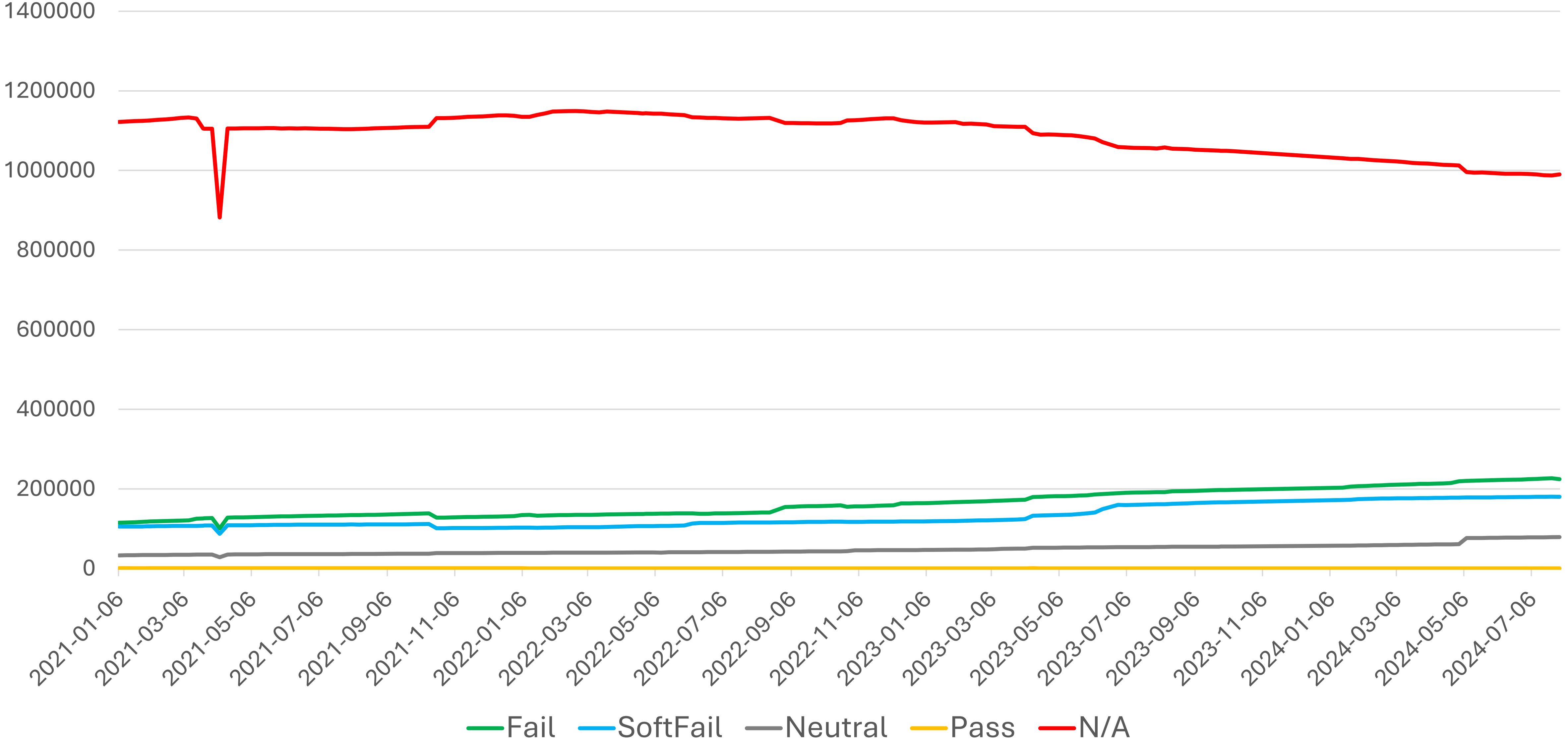
- **DKIM** (RFC 6651)
  - Relative to DKIM, reports signature verification problems to a specific user of the reported domain
  - _report._domainkey.domain.tld.   3600   IN   TXT "ra=dkim-report;„

- **ADSP** (obsolete, RFC 6651)
  - Related to DKIM and ADSP, reports problems when verifying signatures to a specific user of this domain
  - _adsp._domainkey.domain.tld.   3600   IN   TXT "dkim=all;ra=adsp-report;"

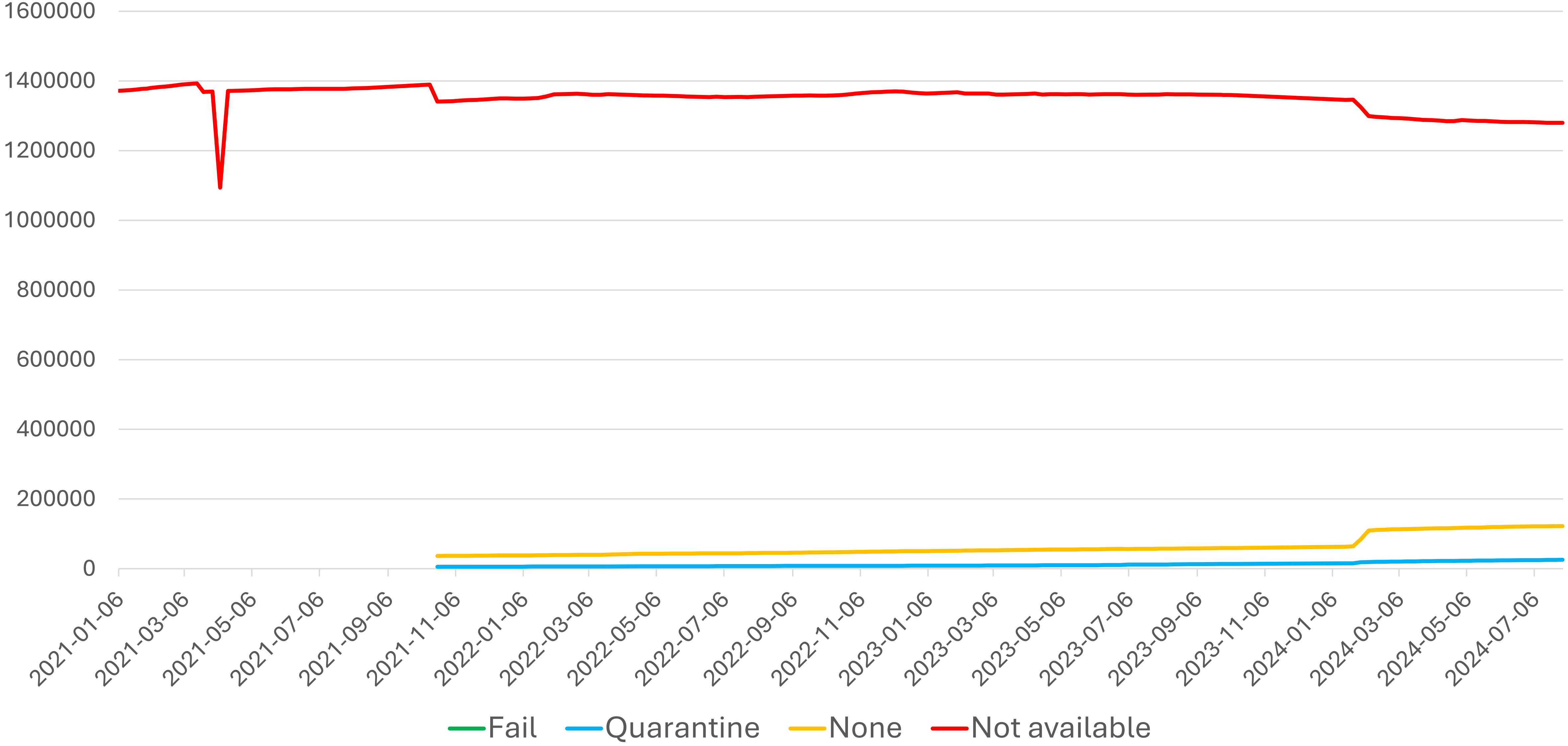
# Reality?



# A little bit of statistics from the Czech Republic: Change in number and type of SPF with time



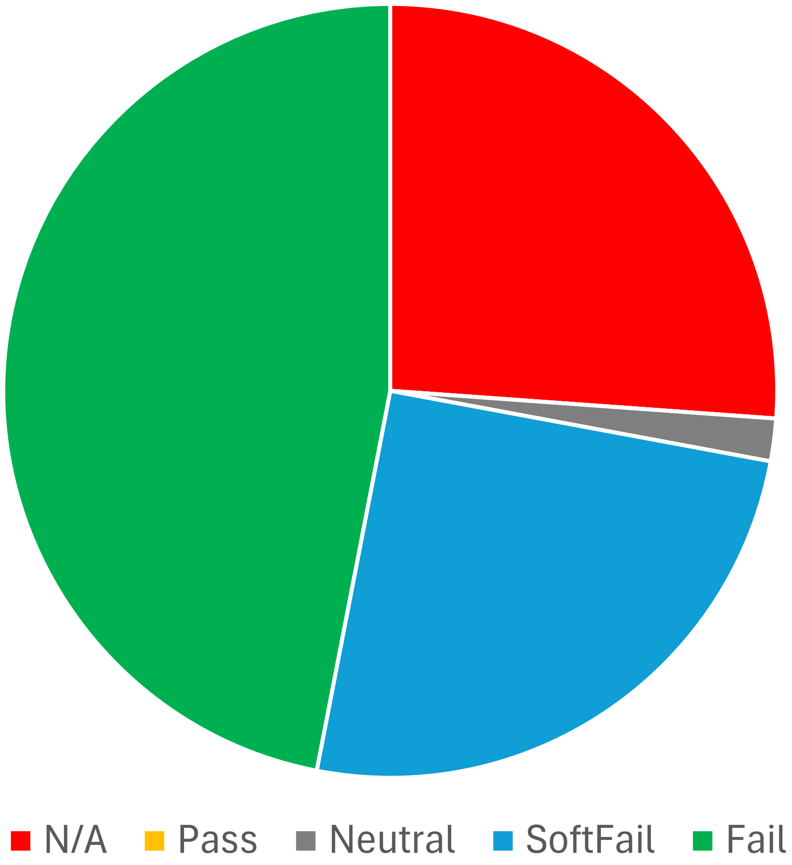
# A little bit of statistics from the Czech Republic: Change in number and type of DMARC with time



# A little bit of statistics from the Czech Republic: SPF

SPF records of original state domains (currently migrating to gov.cz)

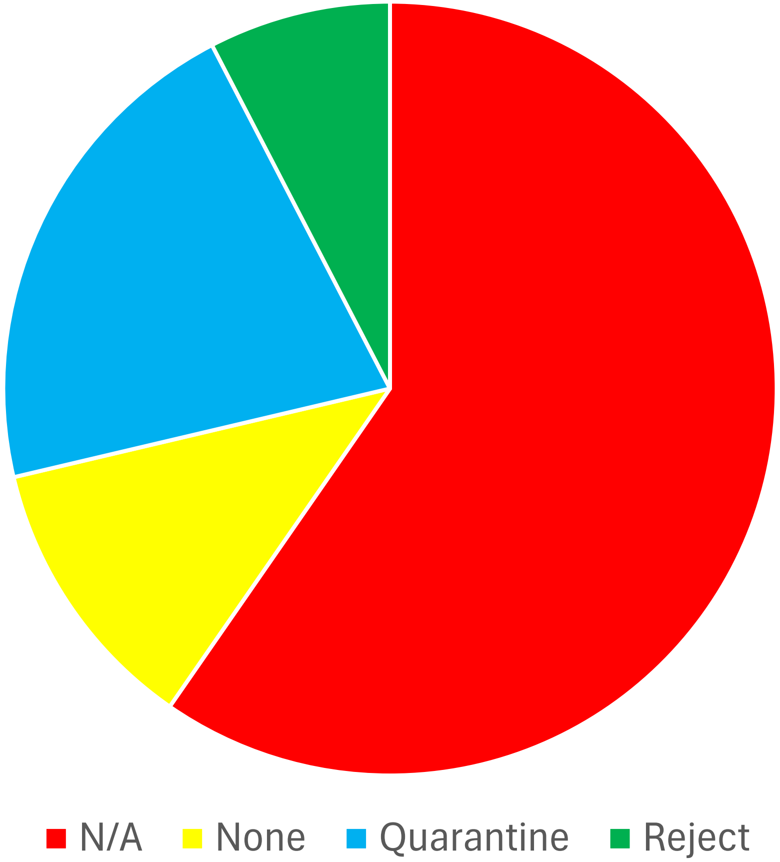
Number of tested domains and subdomains: 436



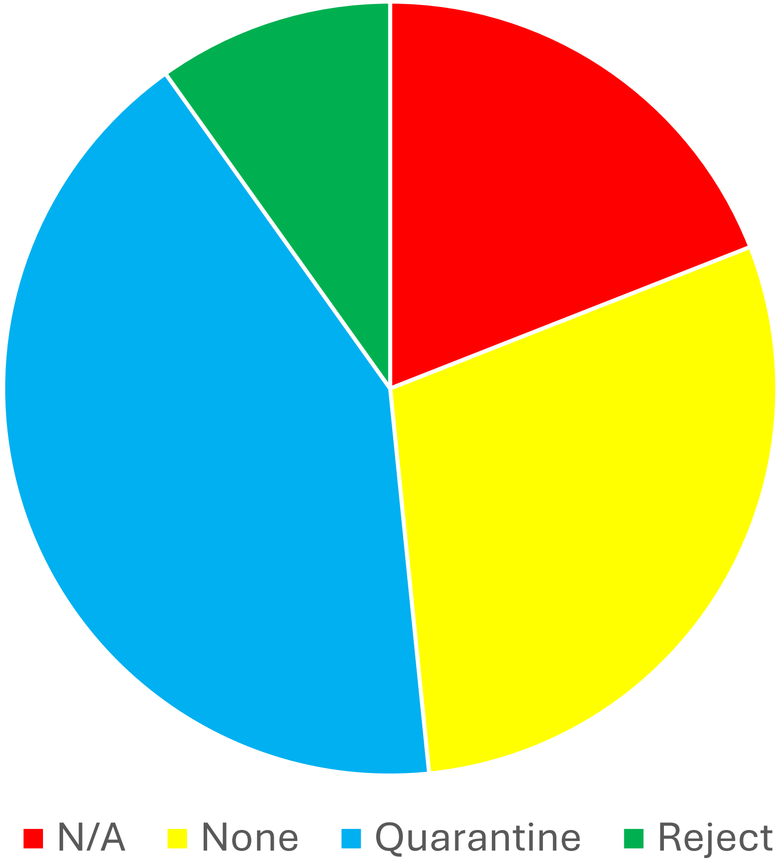
# A little bit of statistics from the Czech Republic: DMARC

DMARC records of original state domains (currently migrating to gov.cz)

Number of tested domains and subdomains:



Policies in domain/subdomain only



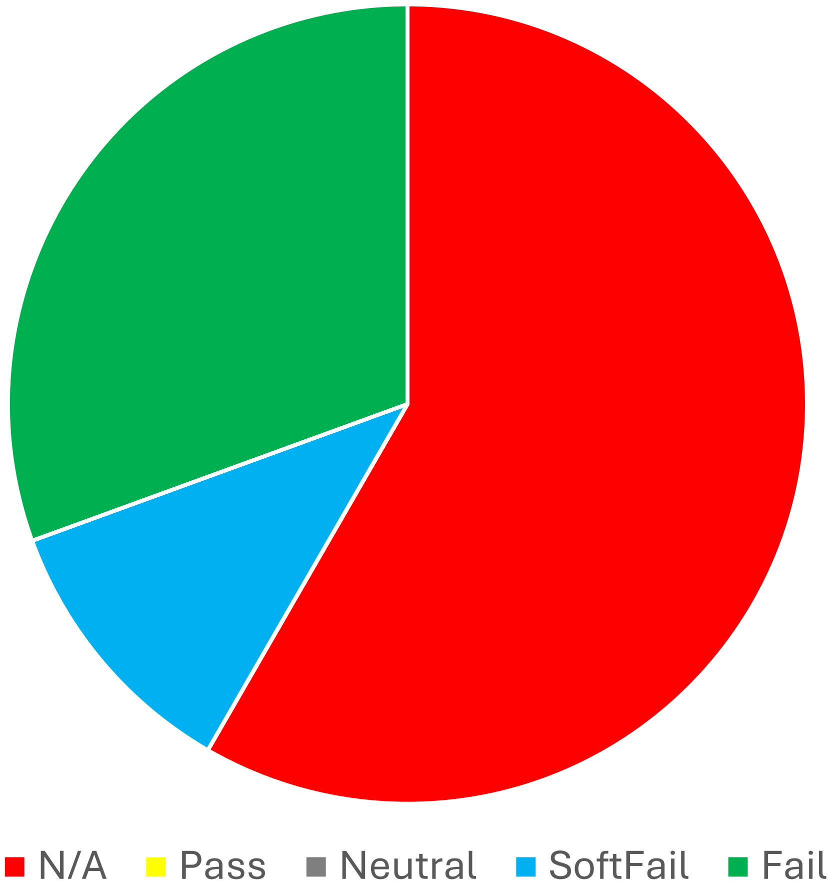
Policies in domain structure

# A little bit of statistics from the Czech Republic: SPF

SPF záznamy známých státních domén v rámci gov.cz

Počet testovaných domén a subdomén: 72

*Migration is still ongoing, this may be a temporary situation*



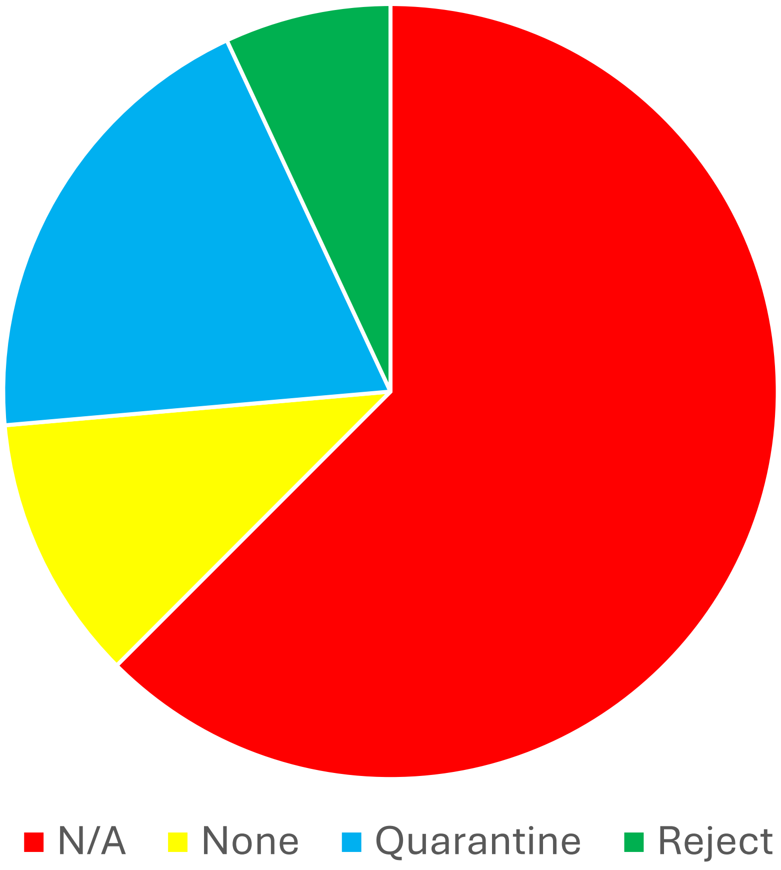
# A little bit of statistics from the Czech Republic: DMARC

DMARC records of known state domains within gov.cz

Number of tested domains and subdomains: 72

*Migration is still ongoing, this may be a temporary situation*

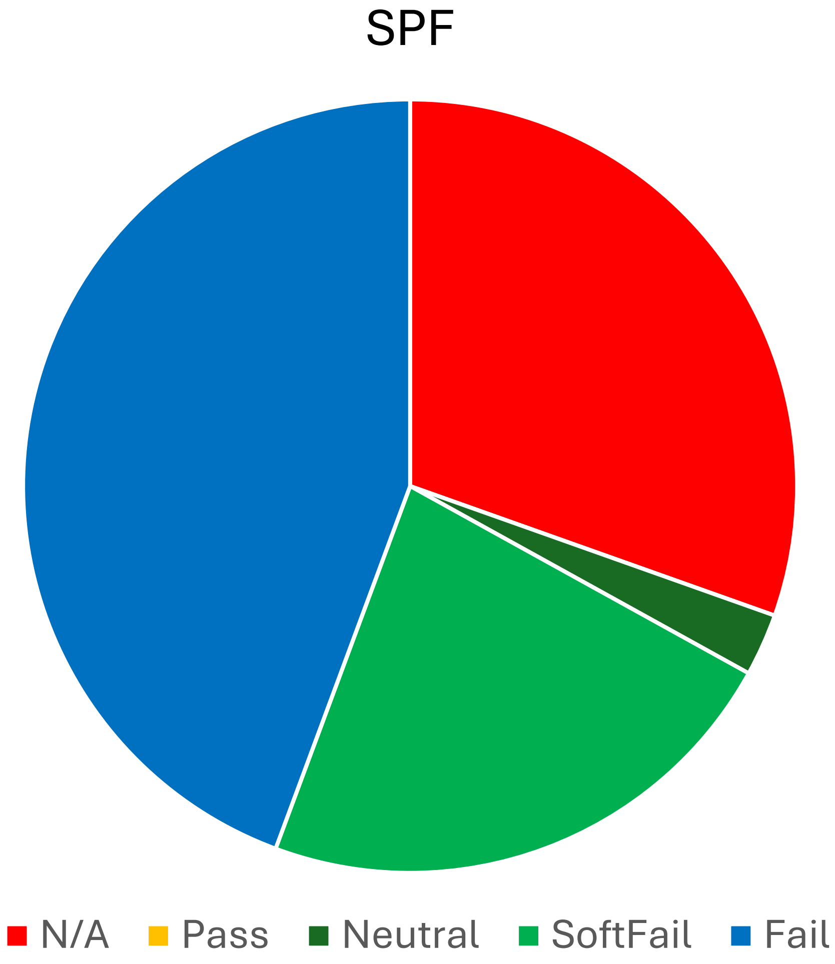
Domain gov.cz DOES NOT have DMARC set

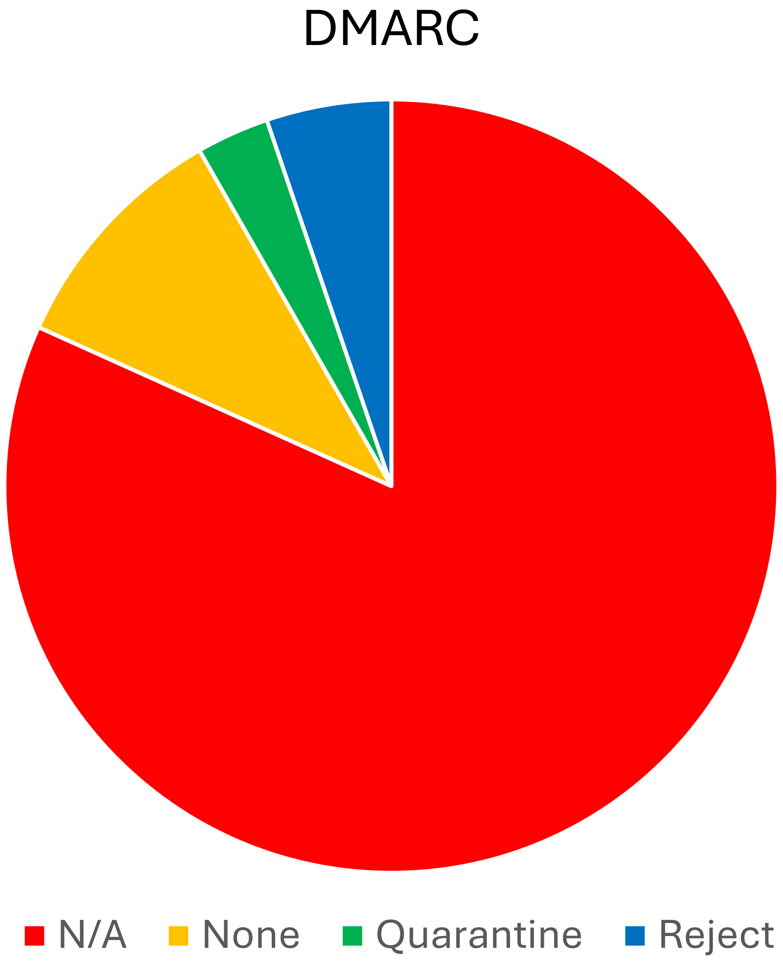


# A little bit of statistics from the Czech Republic – Industry and services

SPF and DMARC records of MPO list of sensitive subjects

Number of domains and subdomains tested: 247

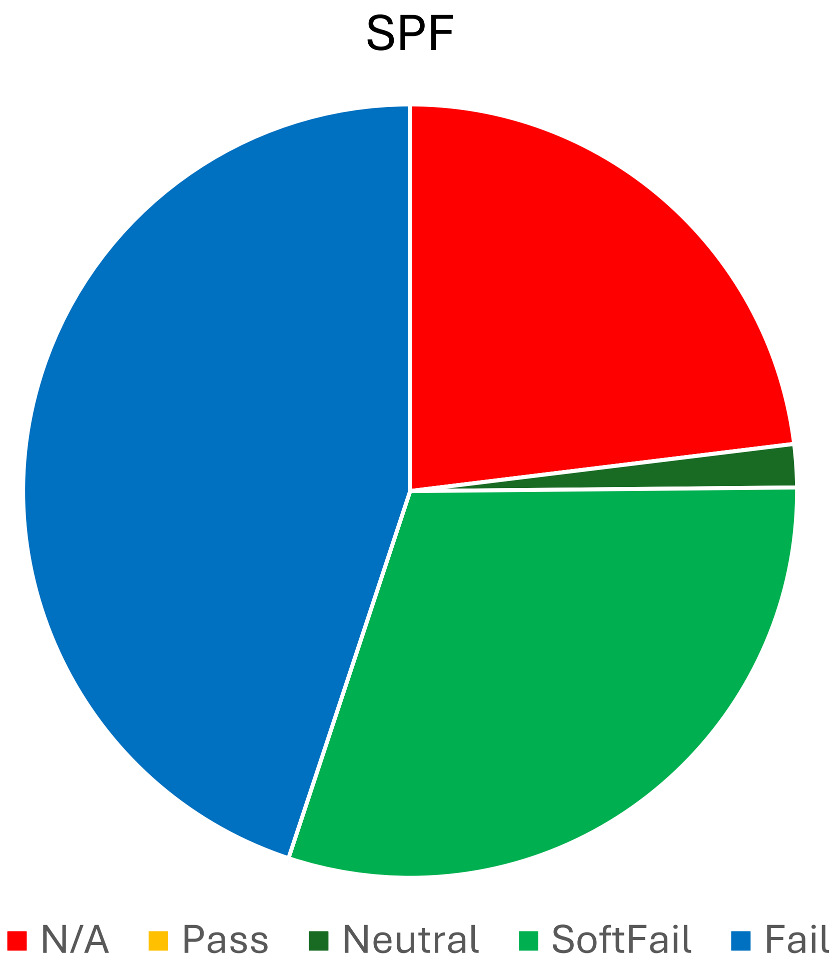


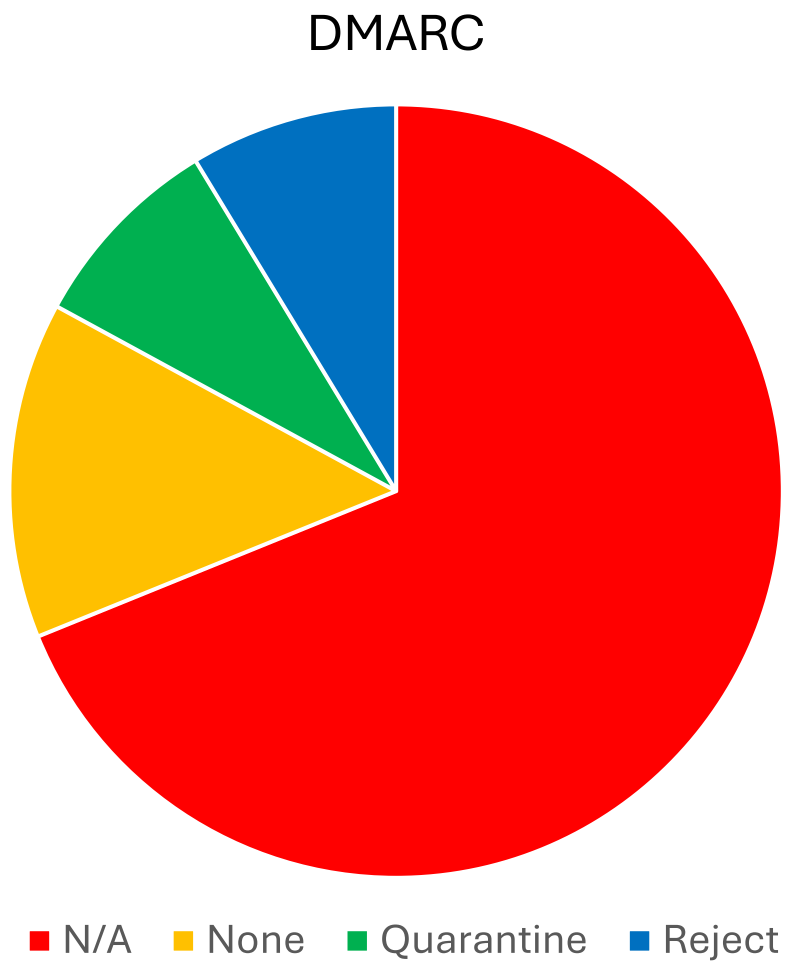


# A little bit of statistics from the Czech Republic – Industry and services

SPF and DMARC records of next MPO list of sensitive subjects

Number of domains and subdomains tested: 360

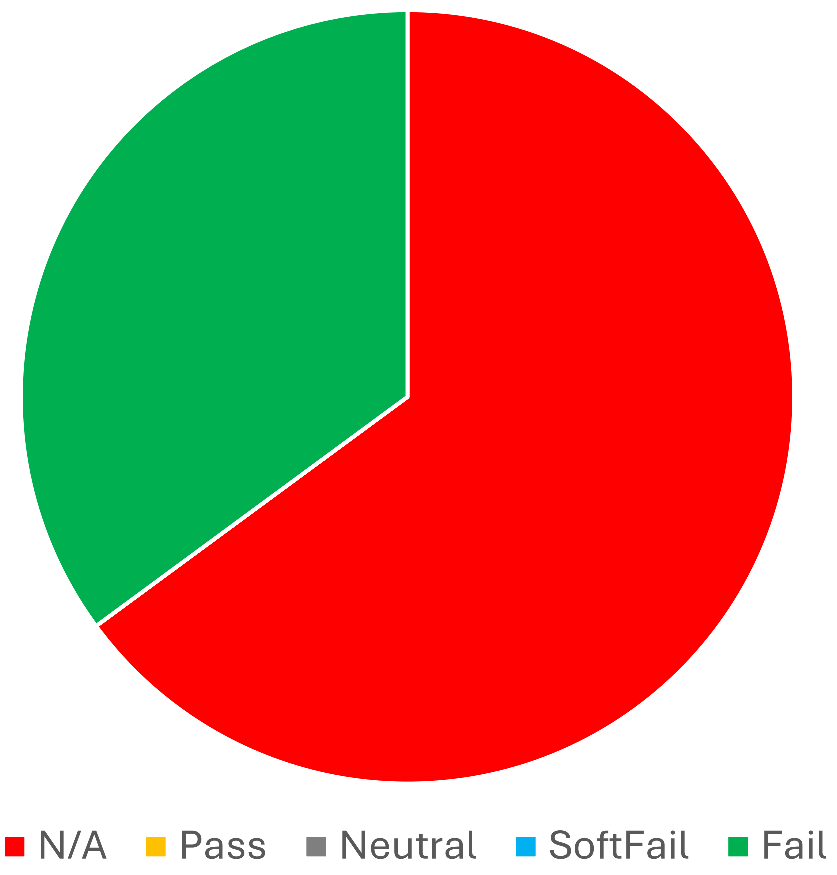




# A little bit of statistics from the Slovakia Republic: SPF

SPF records of known state domains within gov.sk

Number of domains and subdomains tested: 208

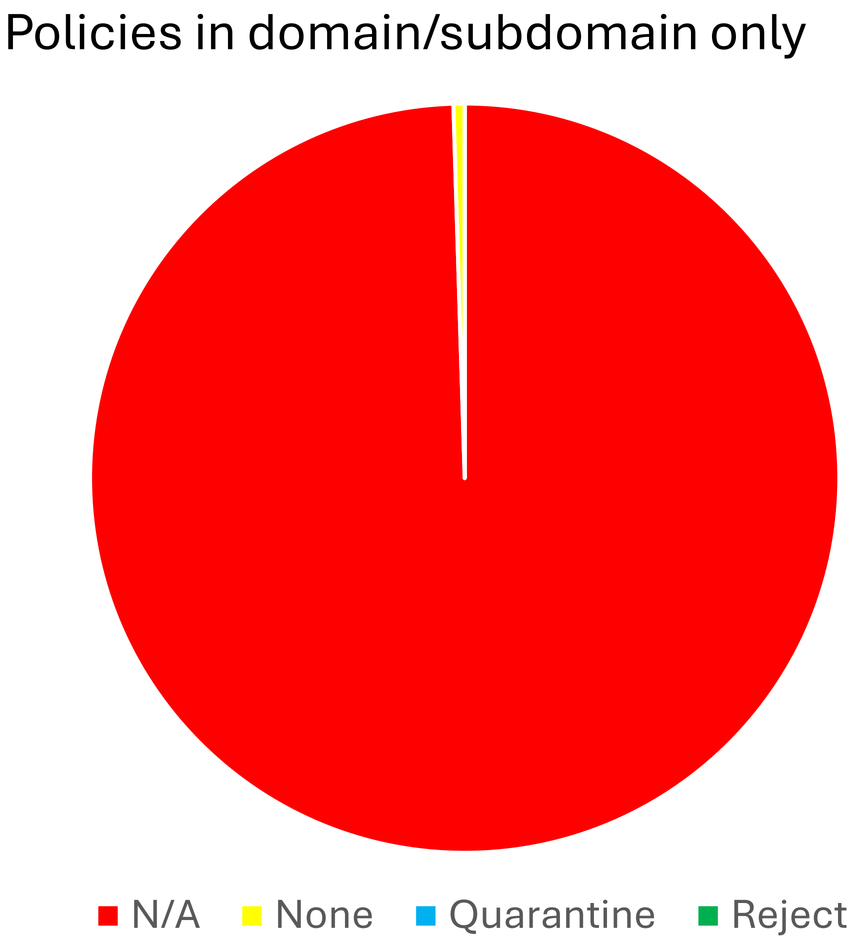


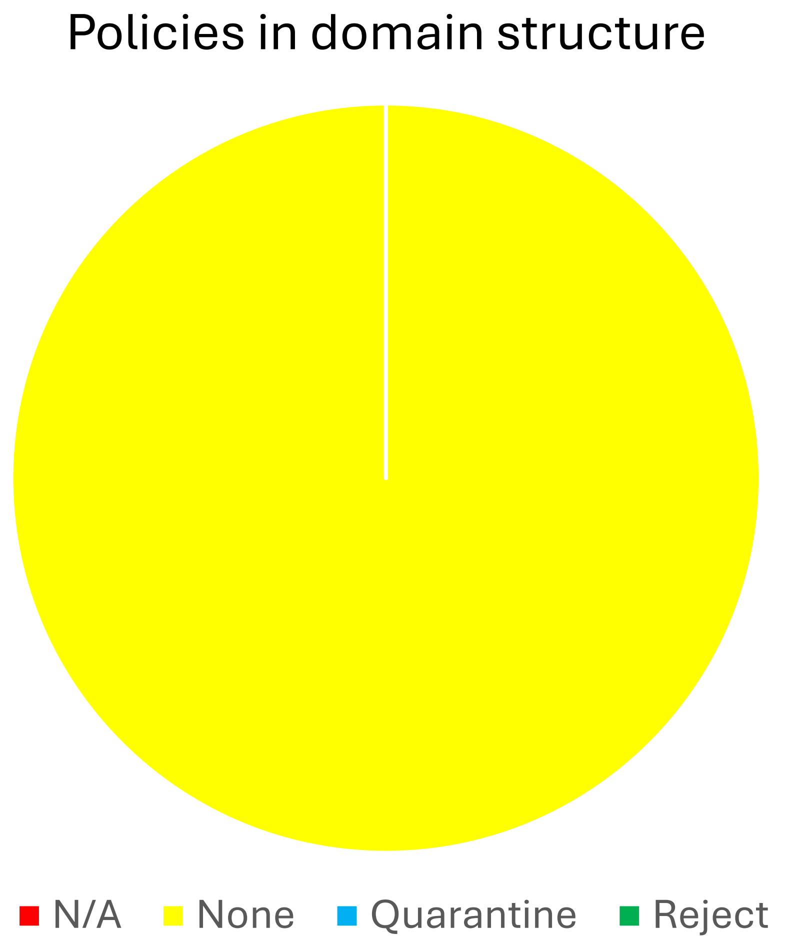
# A little bit of statistics from the Slovakia Republic: DMARC

SPF records of known state domains within gov.sk

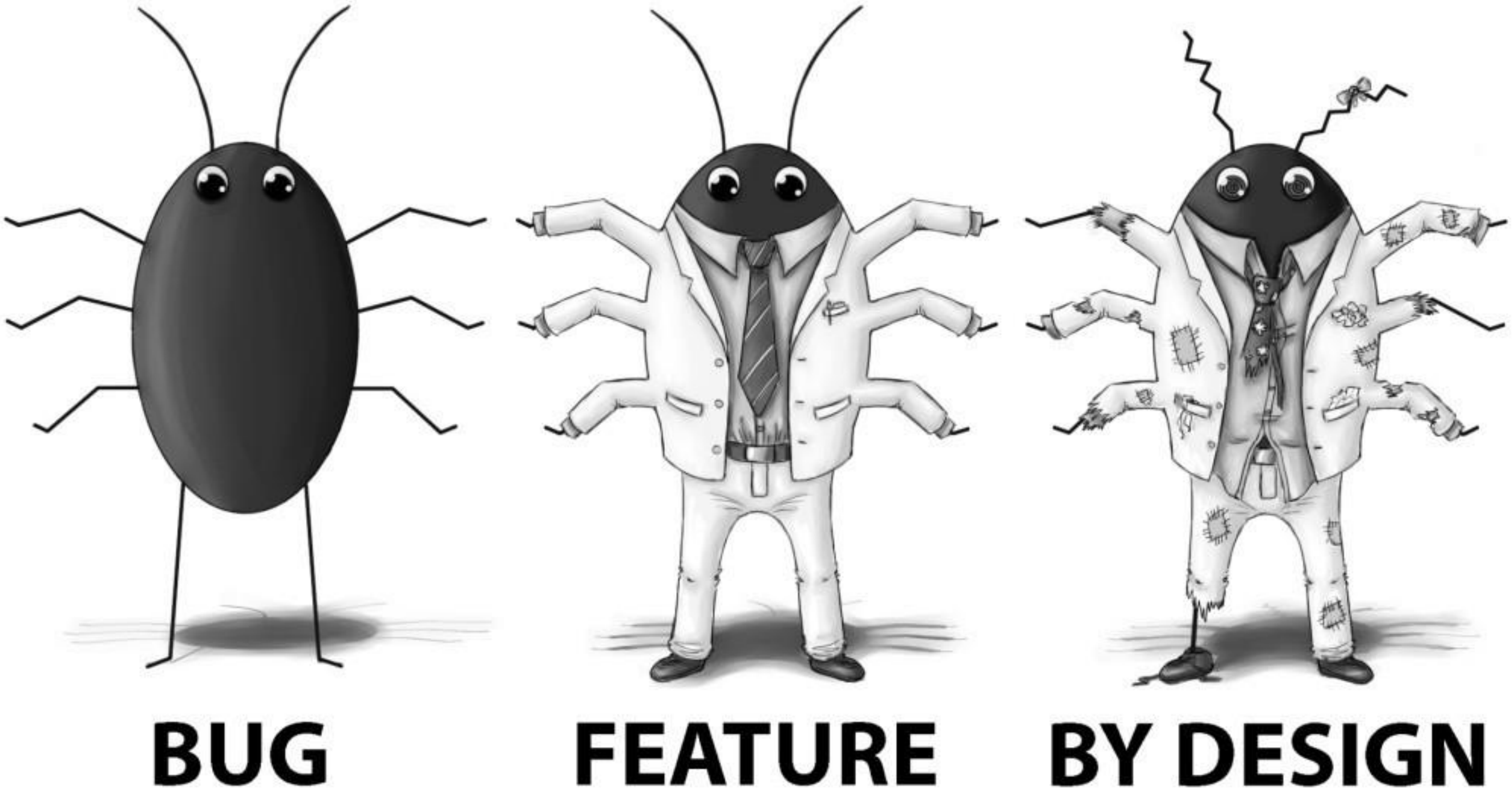
Number of domains and subdomains tested: 208

The gov.sk domain has DMARC configured, but the next-order domains do not have DMARC configured





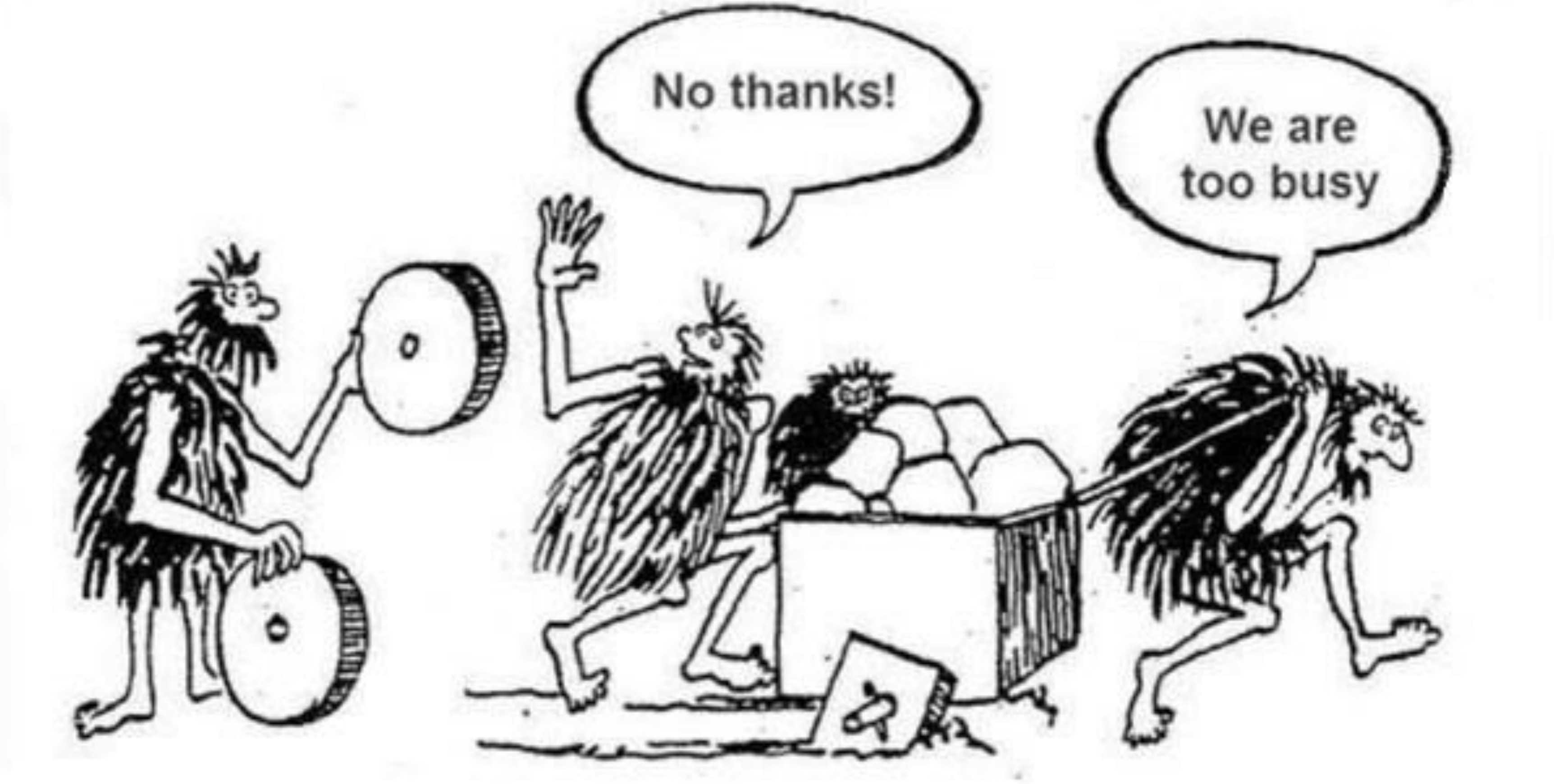
# Technology challenges



# Deviation from IETF-defined standards high risk

Is it really necessary to develop your own wheel and burn all the power to start a non-standard service?

- The service fails to ensure the necessary deliverability of mail messages, the reason being its own architecture design



# Use and abuse of dedicated account

medium risk

RFC 2142 (May 1997) defines standard system accounts:

- postmaster – mail server management
- hostmaster – DNS server management
- www, webmaster – HTTP server management
- abuse, trouble – system abuse, problem reporting
- news, usenet – NNTP protocol (news), now little used
- list – mailing list management

Other recommended addresses are e.g. info, sales, support, marketing, NOC, security, but their use depends on traffic requirements.

- Standard accounts, there should be at least a basic set of postmaster, hostmaster, webmaster and abuse
- It is used to inform about the technical state of the system, errors, outages and the like
- Sending non-operational communications (e.g. marketing) from these accounts is a violation of established practices

# Publications and liability for domains medium risk

Organisations can have part of their services provided by a third party. However, in terms of e.g. DMARC reports and DNSBL sheets, there is no difference between a third party service (even a poorly configured one) and a service running on a domain. This can lead to a situation where a third party postal service causes a DNSBL listing for the entire domain.

- Liability provided within domains of different levels is not fully transparent
- Insufficient liability publication (so far only draft for DBOUND – Domain Boundary)

A partial solution to operational problems is the use of the Zero Trust principle, where no application shares areas of responsibility and configuration data with another. A possible failure of one application does not affect another. However, even Zero Trust will not solve liability problems.

- Shared responsibility is evil
- Both a third party (and its possible misuse) and an application using a shared record can become a threat.

# Relay and OpenRelay

high risk

Mail forwarding was a method of protection to ensure deliverability. Relay is used by authenticated users, OpenRelay can be used by all internet users.

- Option to use different methods of address formatting and placeholders or address boundaries
- Historical forms of addressing, using UUCP, News and FTP (mutual data transfers with these protocols)
- Option to use "%" hack

Testing is limited by the number of requests within a single connection, usually 8 or 20

Best known testers:

| | |
|---|---|
| • Anonymous Relay Test | http://www.aupads.org/test-relay.html |
| • AppRiver Open Relay Test | https://tools.appriver.com/OpenRelay.aspx |
| • MXToolBox | https://mxtoolbox.com/diagnostic.aspx |

It is also possible to use NMAP, or directly Telnet on port 25

- Forwarding is easily abused by attackers
- This is probably the easiest way to abuse the system

# Structure of SPF policy

high risk

Common errors

- Exceeding 10 DNS queries (10 NS lookups)
- Infinite recursions (include from one domain contains the include of the other domain, but this contains the include on the first domain)
- Incorrect use of operators

Examples:

| | |
|---|---|
| - | Strict - valid/not valid evaluation |
| ~ | Softfail - if not valid, information is given for further processing (originally for testing purposes) |
| ? | Neutral - no matter whether valid or not |
| + | Pass - valid, default parameter allowing validity even if not specified ( +all = all, +mx = mx etc) |

Failure to understand SPF policy settings and corresponding operators can lead to domain security implications

- All clause means +all, i.e. the possibility of receiving from all other systems
- All clause and accepts all address records in the domain

# SPF and wide range of IP addresses

high risk

Too wide IP ranges in the cloud can be exploited by attackers. Any mail server in this range will allow you to send messages, authorized with SPF.

Examples:

`_spf.google.com`

| | |
|---|---|
| IPv4: | 328 918 |
| IPv6: | 412 316 860 404 |

`spf.protection.outlook.com`

| | |
|---|---|
| IPv4: | 491 512 |
| IPv6: | 9 851 624 184 872 950 |

- An attacker can create a custom server in the cloud covered by the scope and send the data according to their requirements
- These problems are behind a number of attacks

# SPF and (un)supported macros

low risk

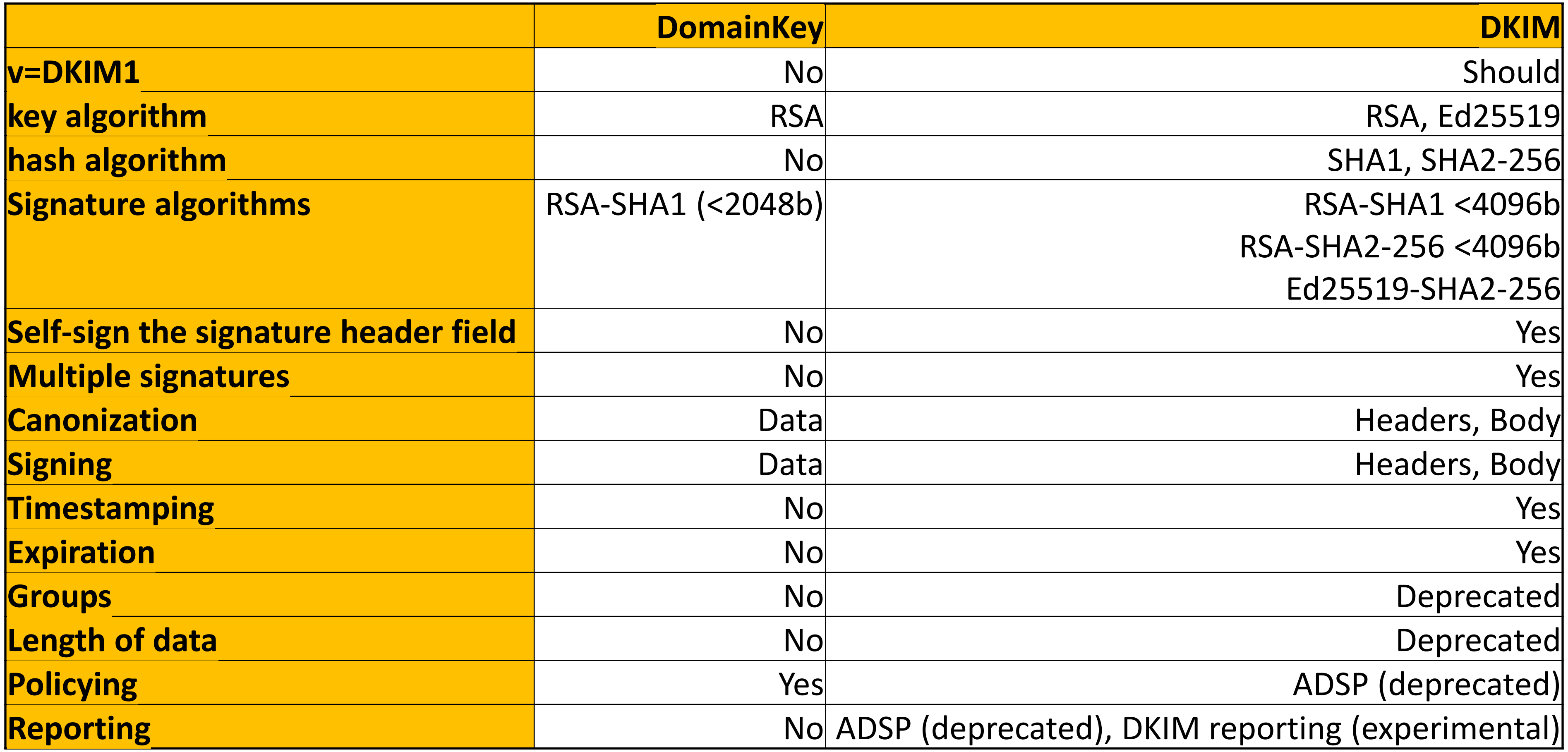
Despite the fact that macros in SPF are an old and standardized issue back in 2006 (RFC 4408), not all systems support macros.

- As of 2019, macros are being used massively to flatten SPF records

- Because macros are subdomain records, without their names, the attacker's job is made more difficult
- They allow for a considerably more dynamic and complex structure, without the need to exceed the number of SPF records

# Comparison of DomainKey and DKIM algorithm

low risk



| | DomainKey | DKIM |
|---|---|---|
| **v=DKIM1** | No | Should |
| **key algorithm** | RSA | RSA, Ed25519 |
| **hash algorithm** | No | SHA1, SHA2-256 |
| **Signature algorithms** | RSA-SHA1 (<2048b) | RSA-SHA1 <4096b<br>RSA-SHA2-256 <4096b<br>Ed25519-SHA2-256 |
| **Self-sign the signature header field** | No | Yes |
| **Multiple signatures** | No | Yes |
| **Canonization** | Data | Headers, Body |
| **Signing** | Data | Headers, Body |
| **Timestamping** | No | Yes |
| **Expiration** | No | Yes |
| **Groups** | No | Deprecated |
| **Length of data** | No | Deprecated |
| **Policycing** | Yes | ADSP (deprecated) |
| **Reporting** | No | ADSP (deprecated), DKIM reporting (experimental) |

- Using outdated DomainKey technology can create security threats and give the attacker a chance to bypass the set mechanisms

# Important DomainKey, DKIM and ARC signature tags low risk

For both DomainKey (**DomainKey-Signature:**) and newer DKIM (**DKIM-Signature:**) and ARC (**ARC-Message-Signature:**) headers can be defined counting into the signature content. Non-existent headers are ignored (replaced by an empty set).

Header Signing List (h=headers list)

| | |
|---|---|
| `From, To, CC, Sender, Reply-To` | List of recipients, senders and reply addresses |
| `Subject` | Subject Name |
| `Message-Id, In-Reply-To, References` | Message Identification Number and References to This Number |
| `Date` | Date Sent |
| `MIME-Version` | MIME Version |
| `Content-Type, Content-ID, Content-Description` | Attachment Type, Attachment Identification and Attachment Description |
| `Content-Disposition, Content-Encoding` | Attachment Usage, Attachment Encoding |
| `Precedence` | Identification of the e-mail type (bulk, sheet, etc.) |
| `List-Unsubscribe, List-Unsubscribe-POST` | Definition and URL for single-click unsubscribe |

- An attacker can change or expand attachments, list of recipients, or change the URL for single-click unsubscribe to an address providing malignant content

# Important signature tags for DKIM and ARC

low risk

It is possible to define timestamps for both DKIM (**DKIM-Signature:**) and ARC (**ARC-Message-Signature:**) to determine the beginning and end of a signature's validity. For ARC, it is not mentioned in the standard, but refers to DKIM. In the case of ARC, therefore, I recommend, mainly at the end of the signature's validity, self-experimentation for the time being, some systems indicate this as an error. In all cases, the expiration time should be longer than the time of delivery of e-mails ("Maximum Deliveriability Time"), i.e. approximately 5 days. The practical setting of the limit should be a multiple of this value (e.g. 15 days).

Timestamps

| | |
|---|---|
| • Timestamp (**t=**timestamp) | Timestamp to create a signature |
| • Expiration (**x=**timestamp) | Timestamp to create a signature |

- If there is no SPF, an attacker with access to e-mails without timestamps can use these messages to create a DoS attack on the target server (connection, disk space)

# (Un)important DKIM and ARC signature tag high risk

It is possible to define the length of the signed part for both DKIM (DKIM-Signature:) and ARC (ARC-Message-Signature:). Indicates the length of the trusted part of the email, if the rest of the message changes, the message is still trusted!!! Since there is no link to the length of the message and the length of the email, it is correct to use it without defining the length. Otherwise, cryptographic protection provides a false sense of security and reduces overall security !!!

Length (**l=**length) Length of the trusted signed part !!! Do not use !!!

- Allows the attacker to easily counterfeit the communication (attaching malware, extending text)
- If there are no other protections (headers, expiration), he can use the said signature according to his

# DomainKey, DKIM, ARC and digital signature attacks low risk

Domainkey (**DomainKey-Signature:**), DKIM **(DKIM-Signature:**) and ARC (**ARC-Message-Signature:**) support the RSA algorithm for the digital signature in the PKCS#1 v1.5 format:

- Bleichenbacher attack requires the existence of an oracle, controlling the query using a private key (1998)
- Attack using small exponents (3, 17, 65537 ... i.e. "small" Fermat primes)
- Håstad/Coppersmiths attack requires sending a message with the same signature and exponent, but with a different private key (not a problem with signatures)
- Multiplicative and deterministic properties (mainly problematic with encryption, not with signatures)

DKIM (**DKIM-Signature:**) and ARC (**ARC-Message-Signature:**) support the Ed25519 algorithm:

- The digital signature is not bound to random nonce as with NIST curves
- The nonce is generated by the hash of the signature key and open text
- A possible collision of two nonce leading to a private key cannot be exploited

Recommendation:

- As a precaution, do not use signatures for bounce messages
- Allow sending messages only to authenticated users (via MSA) and block any relays
- Use recommended security equivalent of 128b (RSA3072 and Ed25519, at worst at least RSA2048+)

# Signature public key and algorithm specification low risk

DKIM (**DKIM-Signature:**) and ARC (**ARC-Message-Signature:**) allow to specify the algorithms used during the signature. The custom key is specified in DER formats and transcoded to Base64, so the asymmetric algorithm is defined here and in the signature header. However, the hash algorithm is only specified in the signature header. Therefore, it is advisable to provide protection against misuse.

- The attacker has the possibility to change the hash algorithm (based on current knowledge, this should not be enough for an attack)
- To forge a signature, he must (based on current knowledge) know the private key

# DMARC records on next level domain

low risk

Records are evaluated on both the sender domain and the parent domain, unless a different SOA is found.

- Evaluation first in the given domain based on the domain name in the sender header (From:, Mailfrom:)
- Evaluation next on the parent domain (maximum 5 steps)
- Implementation of evaluation of parent domains is not always correct (Walking Tree Problem)

# DMARC with policy none and quarantine

medium risk

DMARC with the none policy only allows reporting of problems and does not set any rules for rejecting mail. It should only be used for testing purposes. Using BIMI requires at least a quarantine policy. Some companies reject this policy when crossing certain boundaries.

DMARC with the quarantine policy is implementation dependent. Some implementations move SPAM to system quarantine, others to user quarantines, others delete content. Due to unpredictability of behavior on target systems, this policy is unfortunate. For more predictable behavior, the reject policy is appropriate.

- The none policy can be used by the attacker, the sender system administrator learns about the abuse from regular reports (if it handles them)
- Practically, it is only suitable for testing purposes

# DMARC forensic reports and GDPR

medium risk

Forensic reports are used to send a detailed analysis of problems when receiving messages. The receiving server sends back information about the entire content of emails, so it is blocked by some organizations. The report may contain private information.

- From the GDPR perspective, forensic analysis is problematic and may have legal implications
- It should be considered whether forensic analysis should be supported

# ARC and (un) trusted first hop high risk

The use of ARC technology allows you to sign the entire path that the email has travelled. It requires that the first step of the path ensures the trustworthiness of the rest of the route. Therefore, the first step must be trustworthy and have a good reputation.

- If the first step of the path signs a chain of trust and has a good reputation, the path is trustworthy
- If the first step of the path does not sign a chain of trust, the path after the first signature of the trusted server is problematic to determine its trustworthiness
- The reputation of the signing servers is not mentioned anywhere

# BIMI a důvěra v logo odesílatele

medium risk

BIMI allows the sender logo to be displayed by the client, but what is displayed?

- The logo is displayed if the evaluation using DMARC is valid
- Problem with VMC support (Verifier Mark Certificate - refers to the list of registered certificates)
- No protection against copying image data

Partial or full support: Apple, AT Mail, British Telecom, Cloudmark, Comcast, GMX, Google Gmail, Fastmail, Microsoft Dynamics 365 Customer Insights – Journeys, Mozilla Thunderbird with DKIM extension Verifier, Qualitia, List, Yahoo, Zone, Zoner ...

# DANE TLSA

low risk

DNS provides an additional source of trust, this trust provision depends on DNSSEC

- DANE TLSA requires information recovery automation using a secure API, often these are just ignored customer requests
- Non-standard "DNS-enabled" implementations threaten TLSA's credibility
- Self-Sign certificates may be used, but incorrect
- If there is no DNSSEC on the domain, the implementation of TLSA is nonsense

# DNSBL (Blacklists)

high risk

The provider of the blacklist to the DNS query (reverse IP.DNSBL) returns a value that determines whether the given IP address is blacklisted and, if so, for what issue. These lists should meet RFC 5782, but the values are not standardized. Therefore, it is necessary to know the implementation details and sensitively select DNSBL services. The most famous tools for testing include:

| | |
|---|---|
| **Blacklist Scan** | https://blacklistscan.com/ |
| **DNSBL Info** | https://www.dnsbl.info/ |
| **IP Blacklist Check** | https://www.ipvoid.com/ip-blacklist-check/ |

- Automatic blacklists check their lists and remove registered addresses if necessary
- Semiautomatic blacklists require user activity to perform tests for removal
- Manual blacklists require to contact the operator:
  - contacting the operator can be problematic
  - removal is free of charge or against payment according to the system

# Reputation score and status verification

high risk

Reputation scores indicate the degree of trust of the sending server or system. Reputation schemes exist for IP addresses and domains. The most well-known reputational systems include:

| | |
|---|---|
| **Baracuda Central** | https://www.barracudacentral.org/lookups |
| **CISCO TALOS** | https://talosintelligence.com/ |
| **SenderScore** | https://senderscore.org/ |
| **SpamHaus** | https://www.spamhaus.org/domain-reputation/<br>https://www.spamhaus.org/ip-reputation/ |
| **VirusTotal** | https://www.virustotal.com/gui/home/url |

- Sending server reputation is affected by evaluating it to recipient
- Low score points to difficult verification and frequent rule breaches
- Too loose rules allow an attacker to send unacceptable communications and reduce domain reputation

# Heating up the domains

high risk

In the case of reputational problems and in the case of new domains, it is necessary to "warm up" the domain before using it. The aim is to correct the reputational rating, or to move it from a Neutral rating to a Trusted rating. In the case of new domains, it is necessary to ensure that they "mature" for several weeks. New domains as senders are untrustworthy after creation.

- Creating a reputational score is time consuming, it is easy to lose a good score due to silly errors

Approximate time for safe warming of domains (indicative time, may vary according to other conditions):

| Days | Rate |
|---:|---:|
| 2 | 10 |
| 5 | 25 |
| 8 | 50 |
| 13 | 100 |
| 28 | 250 |
| 50 | 500 |
| 91 | 1000 |
| 193 | 2500 |
| 358 | 5000 |
| 667 | 10000 |

# FBL (Feedback Loop) and ARF (Automatic Reporting Format) low risk

ARF (RFC 3462) standardizes the AutoReply format and allows system tools to send user-reported spam (Feedback Loop, RFC 6449, RFC 6591, RFC 6692 and RFC 9477) to the sender's domain address (user abuse or postmaster). There should be regular evaluation on the sender's side.

- An attacker for fully automatic mode may misuse the Feedback loop to block one of the accounts
- Large providers (e.g. Google) do not use FBLs, although their accounts are often used to send out SPAMs

# Delivery Measurement and Log Analysis

high risk

E-mail services enable internal communication of the company and at the same time communication with customers. Despite the fact that this is an important part of the operation, unlike traditional communication, the efficiency (deliverability) is not usually evaluated. Unlike registered letters, communication by data mailbox, tracing parcel deliveries and evaluation of user satisfaction of these services, this service is underestimated.

- The biggest threat to the availability of the postal system service becomes its administrator, who does not evaluate the communication.

| **Technical reports** | **Description** | **Priority** |
|---|---|---|
| System logs | Technical reports informing about the operation of the system. Their collection and analysis can identify what happened to the message during and after receipt, or before and during sending. | High |
| Bounces | Technical reports informing about undeliverable. Bounces must be collected on the mail server side using mail server services, extensions or custom tools. | High |
| DMARC Report | Reports on results of SPF/DKIM compliance checks, defined by DMARC. | Medium |
| TLS Report | Reports of problems with establishing TLS connections, defined using TLSRPT. | Low |
| DKIM Report | Reports of problems with DKIM keys, definable by DKIM extensions. | Low |

# SMTP Server Settings Properties

medium risk

The SMTP server supports several extended features within the ESMTP (following an EHLO call), which may be a risk in themselves. Access to information beyond what is strictly necessary is considered a risk. One of these examples is the information provided by the server, which needs to be "purged" accordingly.

**VRFY**

- Verifying the existence of a user or group name
- Allows an attacker to verify the existence of a user

**EXPN**

- Expansion (breakup) of a group into user names
- Allows an attacker to get a list of names in a given group

**AUTH**

- Authentication mechanisms list
- Use on port 25/tcp is debatable, should be part of the architecture definition
- This list is for client software and user logins only
- Allows an attacker to get a list of algorithms that can be attacked

https://cryptosession.cz/download/LinuxDays2024en.pdf