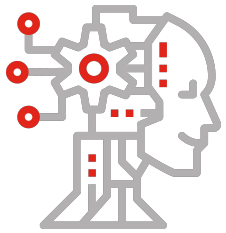
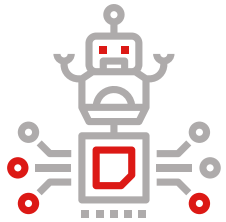
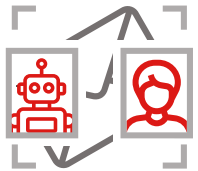






Email authorization and authentication

SPF/DKIM/DMARC

Jakub Olexa, Mailkit

what is
email authentication?

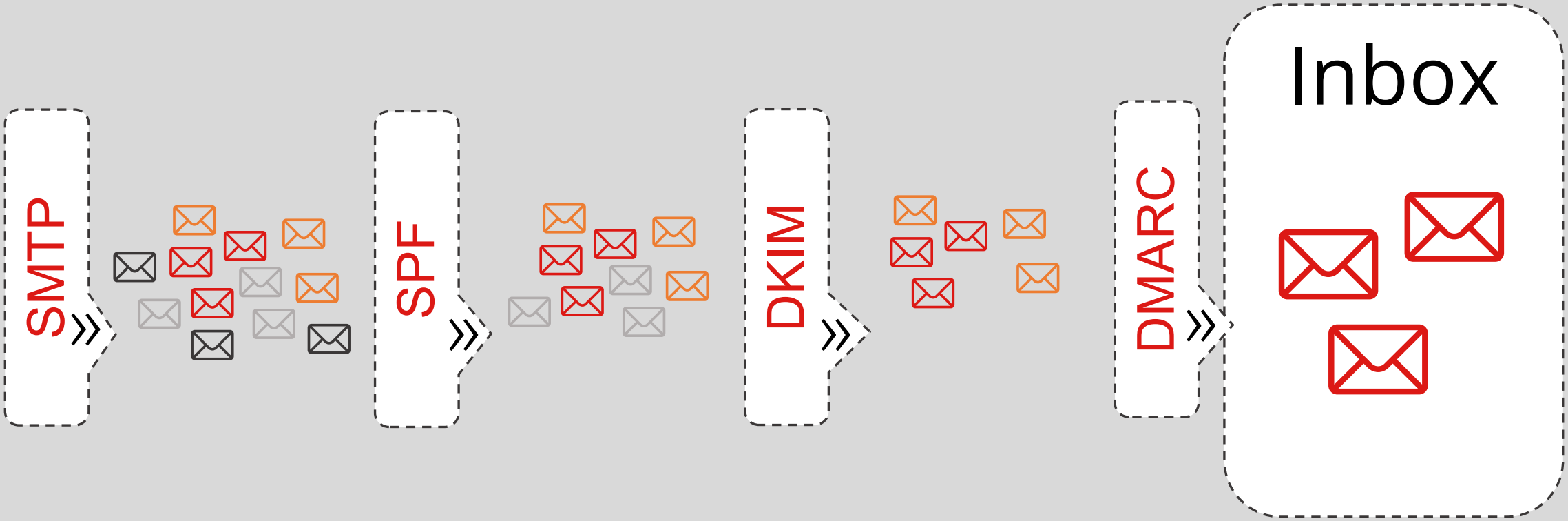
- Message sender and content authenticity validation

Why
and how?

» Email authentication at scale

Why
and how?

» Authentication at scale

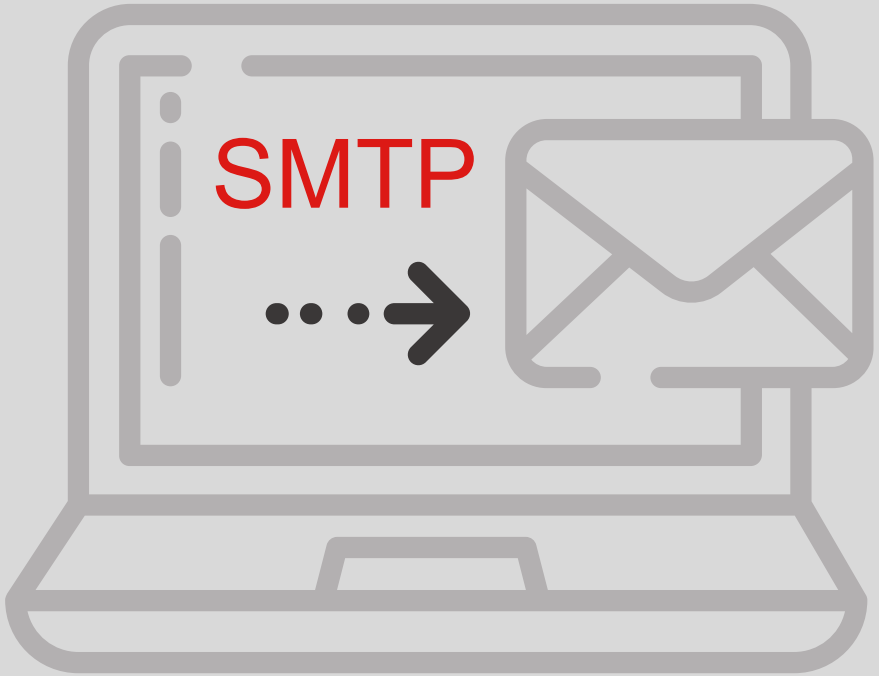


SMTP

Simple Mail Transfer Protocol

RFC5321

SMTP



- The main communication protocol for email message transfer
- Used for delivery of messages between servers as well as email clients to server
- Limited set of command and response codes
- No security or authentication of sender or message content

SMTP

- **EHLO/HELO**
- MAIL FROM
- RCPT TO
- DATA

```
Received: from mail040.prg201.mkt-synd.com (mail040.prg201.mkt-synd.com [185.136.201.40])
    by mail.mailkit.eu (Postfix) with ESMTPS id E40FA203A7
    for <jakub@mailkit.com>; Thu, 29 Oct 2020 14:41:46 +0100 (CET)
Authentication-Results: mail.mailkit.eu;
    dkim=pass (1024-bit key; unprotected) header.d=emaildemos.com header.i=mailkit@emaildemos.com header.b="U2yJ7WZ0";
    dkim=pass (1024-bit key; unprotected) header.d=mkt-synd.com header.i=@mkt-synd.com header.b="DeJZK6/q";
    dkim-atps=neutral
```

SMTP

- EHLO/HELO
- **MAIL FROM**
- RCPT TO
- DATA

```
Return-Path: <c7853-m5345333571-e680453539@mkt.emaildemos.com>
X-Original-To: jakub@mailkit.com
Delivered-To: jakub@mailkit.eu
Received: from localhost (localhost [127.0.0.1])
    by mail.mailkit.eu (Postfix) with ESMTP id 666CA2127A
    for <jakub@mailkit.com>; Thu, 29 Oct 2020 14:41:52 +0100 (CET)
```

```
mailkit.com>; Thu, 29 Oct 2020 14:41:45 +0100 (envelope-from <c7853-m5345333571-e680453539@mkt.emaildemos.com>)
```

```
Abuse-Reports-To: <abuse@mailkit.com>
From: "Mailkit Demo" <mailkit@emaildemos.com>
To: "=?UTF-8?Q?Felix=20Pokorn=C3=BD?=" <felix.pokorny@gmail.com>
Subject: [T]:testing stripo
Message-ID: <20201029144145.MKT5345333571@mailkit.eu>
Date: Thu, 29 Oct 2020 14:41:45 +0100
```

RFC5322

SMTP

- EHLO/HELO
- MAIL FROM
- **RCPT TO**
- DATA

```
Return-Path: <c7853-m5345333571-e680453539@mkt.emaildemos.com>
X-Original-To: jakub@mailkit.com
Delivered-To: jakub@mailkit.eu
Received: from localhost (localhost [127.0.0.1])
    by mail.mailkit.eu (Postfix) with ESMTP id 666CA2127A
    for <jakub@mailkit.com>; Thu, 29 Oct 2020 14:41:52 +0100 (CET)
```

```
Received: by mail040.prg201.mkt-synd.com id hjb39k2nttkm for <jakub@mailkit.com>; Thu, 29 Oct 2020 14:41:45 +010
X-CSA-Complaints: csa-complaints@eco.de
X-Auto-Response-Suppress: AutoReply, OOF, RN, NRN
Content-Type: multipart/alternative;
 boundary="----------=_1603978905-25721-7202"
MIME-Version: 1.0
```

```
Abuse-Reports-To: <abuse@mailkit.com>
From: "Mailkit Demo" <mailkit@emaildemos.com>
To: "=?UTF-8?Q?Felix=20Pokorn=C3=BD?=" <felix.pokorny@gmail.com>
Subject: [T]:testing stripo
Message-ID: <20201029144145.MKT5345333571@mailkit.eu>
Date: Thu, 29 Oct 2020 14:41:45 +0100
```

RFC5322

SMTP

- EHLO/HELO
- MAIL FROM
- RCPT TO
- **DATA**

```
Return-Path: <c7853-m5345333571-e680453539@mkt.emaildemos.com>
X-Original-To: jakub@mailkit.com
Delivered-To: jakub@mailkit.eu
Received: from localhost (localhost [127.0.0.1])
    by mail.mailkit.eu (Postfix) with ESMTP id 666CA2127A
    for <jakub@mailkit.com>; Thu, 29 Oct 2020 14:41:52 +0100 (CET)
X-Spam-Checker-Version: SpamAssassin 3.4.2 (2018-09-13) on mail.mailkit.eu
X-Virus-Scanned: Debian amavisd-new at mailkit.eu
X-Spam-Flag: NO
X-Spam-Score: 0.314
X-Spam-Level:
X-Spam-Status: No, score=0.314 tagged_above=-9999 required=5
    tests=[ALL_TRUSTED=-1, BAYES_50=1.5, DKIM_SIGNED=0.1, DKIM_VALID=-0.1,
    DKIM_VALID_AU=-0.1, DKIM_VALID_EF=-0.1, HTML_FONT_LOW_CONTRAST=0.001,
    HTML_MESSAGE=0.001, LOTS_OF_MONEY=0.001, SPF_HELO_NONE=0.001,
    T_KAM_HTML_FONT_INVALID=0.01] autolearn=no autolearn_force=no
Received: from mail.mailkit.eu ([127.0.0.1])
    by localhost (mail.mailkit.eu [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id RzHPK_4hVmJX for <jakub@mailkit.com>;
    Thu, 29 Oct 2020 14:41:47 +0100 (CET)
Received: from mail040.prg201.mkt-synd.com (mail040.prg201.mkt-synd.com [185.136.201.40])
    by mail.mailkit.eu (Postfix) with ESMTPS id E40FA203A7
    for <jakub@mailkit.com>; Thu, 29 Oct 2020 14:41:46 +0100 (CET)
Authentication-Results: mail.mailkit.eu;
    dkim=pass (1024-bit key; unprotected) header.d=emaildemos.com header.i=mailkit@emaildemos.com header.b="U2yJ7WZ0";
    dkim=pass (1024-bit key; unprotected) header.d=mkt-synd.com header.i=@mkt-synd.com header.b="DeJZK6/q";
    dkim-atps=neutral
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed; s=k1-7099; d=emaildemos.com;
 h=X-CSA-Complaints:Content-Type:MIME-Version:Feedback-ID:List-Unsubscribe:
 List-Unsubscribe-Post:List-Owner:From:To:Subject:Message-ID:Date;
 i=mailkit@emaildemos.com;
 bh=xy5NrnN5uummZeeVr1gAItR4Z5avgciwdAY8bBOn+XE=;
 b=U2yJ7WZ0/fPuTTZeBgG4DCxUnIcpialzJ7erUReDhSK04j5ExbjhqV9g2OHBtNlMi+b4rukWnFQQ
   bLteaamEp2gii71Ye74PHVG+rfEmaQxn7Gg9l/sPWRRkr/SUmPYyu1vBNYqLcWZpj8ij5iOJeIrY
   CoTUb0YIcmM68fQFbog=
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=mail-2016; d=mkt-synd.com;
 h=X-CSA-Complaints:Content-Type:MIME-Version:Feedback-ID:List-Unsubscribe:
 List-Unsubscribe-Post:List-Owner:From:To:Subject:Message-ID:Date;
 bh=wqWRxfulOeQcAnRpGbgoJBIyifhQXO2ssU5WN7zydic=;
 b=DeJZK6/qa1P6YWbsLvS7Zim/pbFU8dVOV26OoMf2rqU9+NnOd/ar8QApBIHD0ycC18ZDJlFZksBE
   yPnRNkOCTLQUCXjue6847JxdJBZ1SFsOo6K1nV8SUTjUMD4P/qetAr/xX3OyV877rDCp41JPkZxv
   lYz6PX7tuDIepWOTSJs=
Received: by mail040.prg201.mkt-synd.com id hjb39k2nttkm for <jakub@mailkit.com>; Thu, 29 Oct 2020 14:41:45 +0100 (envelope-from <c7853-m5345333571-e680453539@mkt.emaildemos.com>)
X-CSA-Complaints: csa-complaints@eco.de
X-Auto-Response-Suppress: AutoReply, OOF, RN, NRN
Content-Type: multipart/alternative;
 boundary="----------=_1603978905-25721-7202"
MIME-Version: 1.0
X-Mailer: Mailkit 2.8
X-Email-ID: 7853-0-107133-1843181-5345333571-680453539
X-MKT-Route: syndicate:c7853:a0
Feedback-ID: 107133:69607853:bulk:mailkit
List-Unsubscribe: <https://u.emaildemos.com/mc/VQCQVLVP/FFMUHOCPNCEQOIAXDH/LUELUUULIC>,
 <mailto:VQCQVLVP/FFMUHOCPNCEQOIAXDH/LUELUUULIC.owner@unsub.mailkit.eu>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
Precedence: bulk
X-Postmaster-Msgtype: 1843181
List-Owner: <mailto:helpdesk@mailkit.com>
X-Abuse-Info: <abuse@mailkit.com>
Abuse-Reports-To: <abuse@mailkit.com>
From: "Mailkit Demo" <mailkit@emaildemos.com>
To: "=?UTF-8?Q?Felix=20Pokorn=C3=BD?=" <felix.pokorny@gmail.com>
Subject: [T]:testing stripo
Message-ID: <20201029144145.MKT5345333571@mailkit.eu>
Date: Thu, 29 Oct 2020 14:41:45 +0100
```

RFC5322

SMTP

telnet mail.mailkit.eu 25	
220 Nobody reads this line - mail.mailkit.eu ESMTP ready	> Server welcome message
helo host.emaildemos.com	< helo identification of the sender (FQDN)
250 mail.mailkit.eu	> Command acknowledgement response
mail from: <>	**< RFC5321 from – this is what SPF is checked against**
250 2.1.0 Ok	> Sender acknowledgment response
rcpt to: <jakub@mailkit.com>	< RFC5321 to – who's the recipient of the message
250 2.1.5 Ok	> Recipient acknowledgement response
data	< Initiate data transfer
354 End data with <CR><LF>.<CR><LF>	> Data transfer acknowledgement response
From: "Jméno Příjmení" <email@domena.cz> Subject: Test Chytre povidani	**< Message content RFC5322** (this is where the headers used by DMARC are)
.	< End of transfer
250 2.0.0 Ok: queued as 42CAF202DD	> Message acknowledgment response
quit	< End connection
221 2.0.0 Bye	> Good bye message

SPF

Sender Policy Framework

RFC7208

SPF
what is it for?

- Authorizes message source at SMTP (5321) level
- Non-recursive TXT record in DNS
- Defines sources (IP)
  - IP addresses/networks
  - A/MX/PTR records
  - Redirect/Include of 3rd party SPF records
  - Macros
- Allows rules to be set
  - + - pass
  - ~ - softfail
  - - - fail
  - ? - neutral

SPF
DNS records

Host authorization | IPv4 authorization | IPv6 authorization | Everything else

@ IN TXT “v=spf1 a mx ip4:185.136.200.0/24 ip6:2a06:ffc0::/29 ~all”

@ IN TXT “v=spf1 a mx include:domain.com ~all”
@ IN TXT “v=spf1 a:host.com include:domain.com ~all”
@ IN TXT “v=spf1 +exists:%{i}._spf.domena.com -exists:%{i}.sbl.domena.com ~all”

- Must start with “v=spf1”
- TXT record in domain/subdomain
- Only ONE record allowed

Remove DNS records of type SPF! Only TXT type is valid

SPF
record evaluation

`telnet mail.mailkit.eu 25`	
`220 Nobody reads this line - mail.mailkit.eu ESMTP ready`	IP address of the connecting source
`helo host.emaildemos.com`	helo identification (FQDN) reverse DNS lookup
`250 mail.mailkit.eu`	
`mail from: <>`	Lookup SPF record for the domain part of the sender address
`250 2.1.0 Ok`	
`rcpt to: <jakub@mailkit.com>`	Evaluate exceptions and SPF record
`250 2.1.5 Ok`	Accept or reject
`data`	
`354 End data with <CR><LF>.<CR><LF>`	

`From: "First Last" <email@domena.cz>`
`Subject: Test`
`Something really smart here`	

`.`	
`250 2.0.0 Ok: queued as 42CAF202DD`	
`quit`	
`221 2.0.0 Bye`	

SPF
practical examples - parked domain

```
telnet mail.mailkit.eu 25
220 Nobody reads this line - mail.mailkit.eu
ESMTP ready
helo host.emaildemos.com
250 mail.mailkit.eu
mail from: <test@spfpark.cz>
250 2.1.0 Ok
rcpt to: <spftest@mailkit.com>
550 5.7.23 <spftest@mailkit.com>: Recipient
address rejected: Message rejected due to:
SPF fail - not authorized. Please see
http://www.openspf.net/Why?s=mfrom;id=test@s
pfpark.cz;ip=185.142.211.18;r=<UNKNOWN>
```

Domain spfpark.cz is a so call parked domain, e.g. it's not used to send or receive emails. It's not in use at the moment. SPF record doesn't allow any messages to originate from this domain:

spfpark.cz. IN TXT "v=spf1 -all"

Parked domains should always have an SPF record blocking any email use to prevent abuse by spammers. Every domain even used one without an SPF record is valuable for spammers.

SPF
practical examples – multiple domain management

v=spf1 redirect=_spf.domena.cz

- Redirect to an SPF record including its rules
- Great for large organizations with multiple domains using same policies
- Never use with domains that are not managed by a single entity!!
- SPF record MUST NOT contain any policy as the whole record would be ignored

VS

v=spf1 include:_spf.domena.cz ~all

- Settings apply only for the specific domain
- Necessary when loading authorizations from a 3rd party domain
- Inefficient for organizations with a large number of domains that should have the same policies

SPF
practical examples – common use

- Permits messages from IPs with A record in domain - e.g. domain.com not www.domain.com
- Permits messages from all IPs of domain's MX records
- Include of 2 SPF records from 3rd party domains
  - Use Include only for trusted 3rd parties
  - Avoid excessive authorizations
  - Watch out for the limit of 10 DNS lookups – use Ips whenever possible instead of A/MX/include
  - Watch out for MX lookup limits - max 10 A records

SPF
practical examples - macros

v=spf1 +exists:%{i}._spf.emaildemos.com -exists:%{i}.sbl.emaildemos.com ~all"

Permits IPs with a record in _spf.emaildemos.com

Denies IPs with a record in sbl.emaildemos.com

- Allows you to hide authorizations in SPF record
- Allows for centralized authorization management (e.g. %{i}.%{d}._spf.provider.cz)
- Can be used in include and break down using wildcard DNS records
- Allows passive-DNS monitoring
- Granular down to a sending address

s = <sender> (mail from), l = local-part of <sender> (mail from),
o = domain of <sender> (mail from), d = <domain> (mail from or helo),
i = <ip> (connecting client), h = HELO/EHLO domain, ir = reverse <ip> (client)

SPF
practical examples - macros

v=spf1 +exists:%{i}._spf.emaildemos.com -exists:%{i}.sbl.emaildemos.com ~all

dig +short 123.123.123.123._spf.emaildemos.com
-> no response, IP not authorized

dig +short 185.136.200.19._spf.emaildemos.com
-> returns 127.0.0.1, IP is authorized

dig +short 123.123.123.123.sbl.emaildemos.com
-> returns 127.0.0.1, IP is blocked

Tip – test your record before deployment
https://www.kitterman.com/spf/validate.html

SPF

Postfix configuration example

Setting up Postfix server to check SPF for incoming messages

/etc/postfix/main.cf:

```
policy-spf_time_limit = 3600s
smtpd_recipient_restrictions =
    ...
    permit_sasl_authenticated
    permit_mynetworks
    reject_unauth_destination
    check_policy_service unix:private/policy-spf
    ...
```

/etc/postfix/master.cf:

```
policy-spf  unix  -       n       n       -       -       spawn
user=nobody argv=/usr/bin/policyd-spf
```

/etc/postfix-policyd-spf-python/policyd-spf.conf

```
TestOnly = 0
HELO_reject = Fail
Mail_From_reject = Fail
PermError_reject = False
TempError_Defer = False
Header_Type = AR
Authserv_Id = server.name
```

SPF

check

Checking inbound SPF validation using headers:

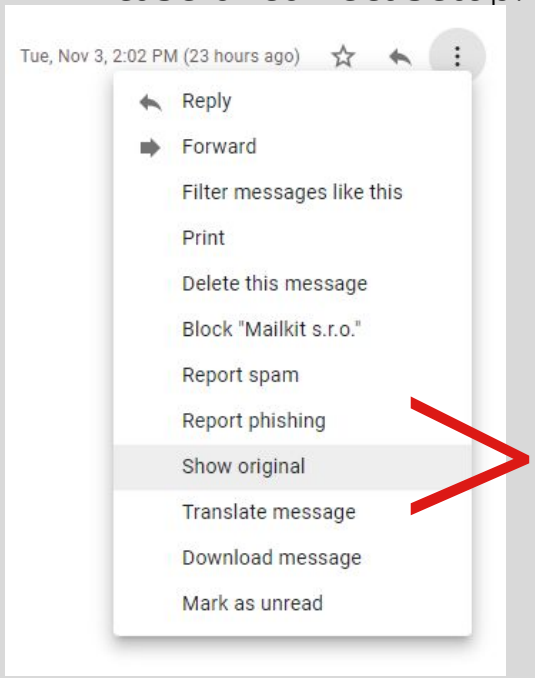
Authentication-Results: mail.mailkit.eu; spf=pass (mailfrom) smtp.mailfrom=domena.cz (client-ip=aaa.bbb.ccc.ddd; helo=server.domena.cz; envelope-from=email@domena.cz; receiver=<UNKNOWN>)

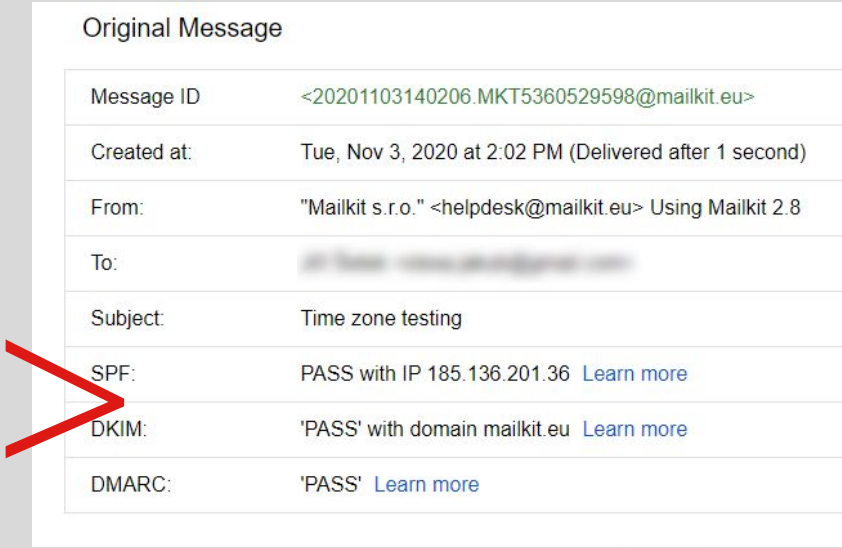
or

Received-SPF: pass (server: domain of email@domena.cz designates aaa.bbb.ccc.ddd as permitted sender) client-ip=aaa.bbb.ccc.ddd;

Checking outbound messages

Review the headers of the sent message for example in Gmail. In the Received-SPF and Authentication-Results header you will see “pass” in case of correct setup.





SPF

issues

- Easy to circumvent (authorizes MAIL FROM)
- Unrelated to From* (RFC5322)
- Limited to 10 DNS queries
- Incorrect use by administrators
- Misunderstanding of “-all”
  - Incompatible with DMARC
  - Important for parked domains in form or “v=spf1 -all”
- Often too generic (too many sources allowed)
- Often multiple records (only 1 record allowed!)
- Rarely used for monitoring

* Except few exceptions that violate RFC

Tip – try to test your records first
https://www.kitterman.com/spf/validate.html

SPF

facts and myth

- **SPF protects domain from abuse**
  SPF doesn't protect the sending address (RFC5322)
- **SPF increases security and protects from spam**
  SPF has no impact on security or inbound spam
- **SPF affect deliverability**
  Depends on message type, delivery method, reputation and other factors
- **SPF authorizes sender**
  SPF applies to email servers sending on behalf of the domain
- **Unauthorized messages will be rejected**
  In general the SPF record has little to no impact on message delivery
- **Policy -all is safer than ~all**
  -all has no security advantage but has negative deliverability impact
- **SPF is used only for domains sending emails**
  SPF is important for domains, subdomains as well as parked domains

DKIM

DomainKeys Identified Mail

RFC6376

DKIM
what is it for?

- Authenticates the CONTENT of the message
- TXT record in “_domainkey.” space of domain
- Identifies responsible domains
- Authenticates messages
- Assigns domain reputation
- Prevents easy abuse
- Allows multiple keys
  - Secure key distribution
  - Easy identification
  - Key rotation

selector1._domainkey IN TXT “v=DKIM1;p=.... *public key* ...”
selector2._domainkey IN TXT “v=DKIM1;p=.... *public key* ...”
selector3._domainkey IN TXT “v=DKIM1;p=.... *public key* ...”
selector4._domainkey IN TXT “v=DKIM1;p=.... *public key* ...”

DKIM
DNS records

Selector | DKIM space | DKIM record

name1._domainkey IN TXT “v=DKIM1; p=public key….”

- TXT records in “_domainkey” space of domain
- Record name matches the selector
- Must start with “v=DKIM1”
- Key-length of min. 1024 bits, 2048 recommended (longer keys may cause problems)

DKIM
message header

SELECTOR DKIM domain

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed; s=**k1-7099**; d=**emaildemos.com**;

Signature header fields

h=**X-CSA-Complaints:Content-Type:MIME-Version:Feedback-ID:List-Owner:From:To:Subject:Message-ID:Date;**

Sender identifier Header signature Body signature

i=mailkit@emaildemos.com;bh=**7kjpqWoVqYLzO13eCYMpz247WgpuCbwpHxLxcEwlOaE**=;b=XVvcW0L+qxW1
VGZuVhqCfemEz+dlcd32bcn84VjLW8yXRY0m42QZHjYI9slkI2Xr3klSmz/KAd5tV18YrBDom64CYcj0oLUU1jw2MMT
1zD2TO//kxyboNWdam4Q2XgX0XVFkWfWNF7JEKp42+0nRM0sc7kbSzr2rTdttrzefotI=

Messages can have multiple signatures – usually signed by sending domain DKIM and sending service (ESP) DKIM, that allows the ESP to receive FBL reports from mailbox providers

DKIM
process

Sending mail server

\+

Private DKIM key

DKIM signed email sent
(DKIM signature in message header)

Mail received by destination mail server

d=domain.com
s=selname1

Extract DKIM signature from message header

domain.com
DNS

Query DKIM record selname1._domainkey.domain.com

Validate message using public key from DNS record

Is the signature valid?

Yes

DKIM Pass

No

DKIM Fail

DKIM

Postfix configuration example

/etc/opendkim.conf:

```
Syslog              yes
AutoRestart         yes
AutoRestartRate     10/1h
Background          yes
Socket              inet:12345@localhost
PidFile     /var/run/opendkim/opendkim.pid
Canonicalization    relaxed/simple
DNSTimeout          5
X-Header            no
Mode                sv
SignatureAlgorithm      rsa-sha256
KeyTable            etc/opendkim/dkim-keytable
AlwaysAddARHeader       yes
SigningTable        refile:/etc/opendkim/dkim-signingtable
ExternalIgnoreList  /etc/opendkim/TrustedHosts
InternalHosts       /etc/opendkim/TrustedHosts
UserID              opendkim:opendkim
```

/etc/opendkim/signingtable:

```
*@domain.com  domain_com
```

/etc/opendkim/dkim-keytable:

```
domain_com          domain.com:selector:/etc/
                    opendkim/private_key.rsa
```

/etc/postfix/main.cf:

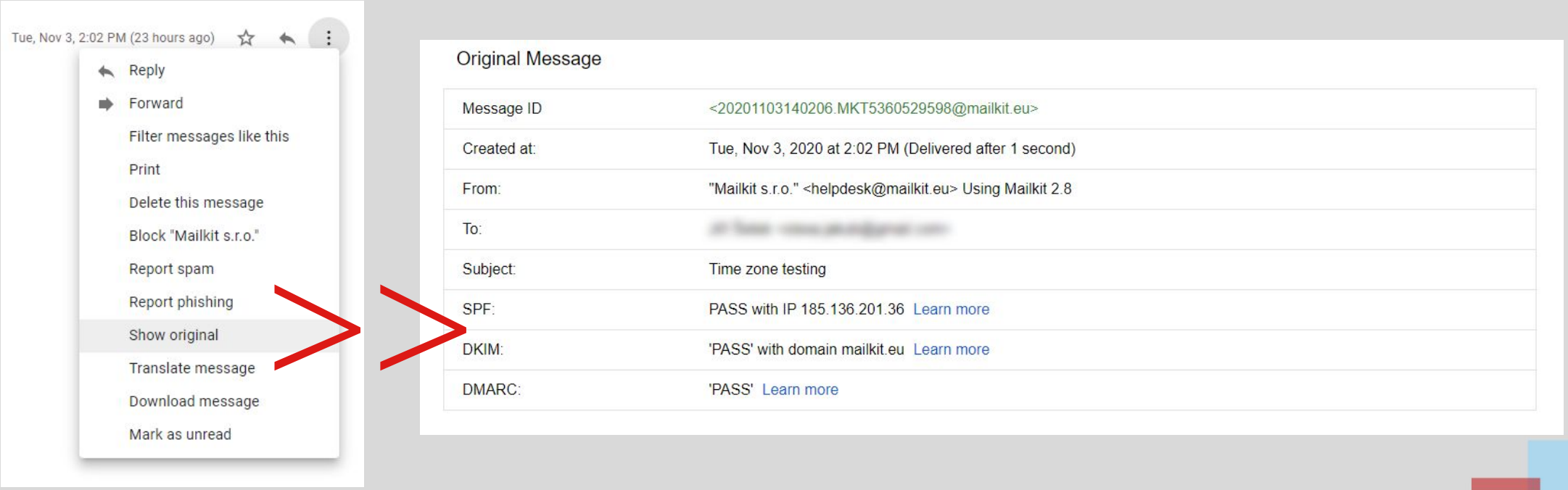
```
smtpd_milters = inet:localhost:12345
```

DKIM

check

“Authentication-Results” headers:

Authentication-Results: mx.google.com;
dkim=**pass** header.i=@mailkit.eu header.s=pmta header.b=WQlsSRfi;
dkim=**pass** header.i=@mkt-synd.com header.s=mail-2016 header.b=Z60qkzX5;
spf=**pass** (google.com: domain of c1234-m123456789-e123456789@mkt.mailkit.eu designates 185.136.201.36 as permitted sender)



DKIM
issues

- Anyone can sign (not related to mfrom 5321 nor From 5322)
- Forwarding can break signature
- Some DNS servers have record length issues
- Insufficient deployment (one server out of many)
- Insufficient key length
- Missing key rotation policies
- Difficult monitoring

DKIM

- facts and myths

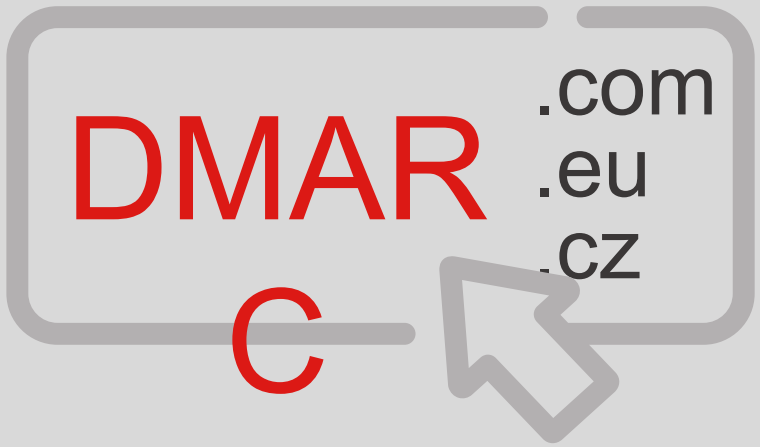
- **DKIM signature means it's not SPAM**
  Anyone can add a DKIM signature, including spammers
- **DKIM signature means headers are "legitimate"**
  No, it only means that the headers have been signed
- **DKIM doesn't work with mailing-lists**
  It depends on the mail-list configuration but the list system should sign the messages
- **DKIM prevents spam**
  No, DKIM only authenticates the content and allows receiving servers to assign reputation to the signing domain
- **DKIM encrypts emails**
  DKIM is not an encryption mechanism but a digital signature
- **Invalid DKIM = fake email**
  Invalid signatures are often caused by forwarding or incorrect settings
- **DKIM is only for bulk-mail**
  Message authentification is important for all types of messages no matter the content or audience size
- **There is no point in using DKIM**

DMARC

Domain-based Message Authentication, Reporting & Conformance

RFC6376

DMARC
what is it for?



- Used to **PROTECT** domains
- TXT record in the "_dmarc" name-space of the domain (affecting subdomains)
- Puts SPF & DKIM in context with **From** (RFC 5322)
- Defines policies for handling unauthenticated messages
- Allows policy verification and escalation
- Provide aggregate and forensic reports
  - Receiving side point of view on mail-flows
  - Identify infrastructure and issues with SPF & DKIM
- More accurate email filtering by receiving servers

DMARC
record

policy | Subdomain policy | percentage | aggregate reports | forensic reports

v=DMARC1; p=quarantine; sp=reject; pct=50; rua=mailto:rua-email@domain.com; ruf=mailto:ruf-email@domain.com;

Tag	Default value	Description
v	DMARC1	DMARC record version – must be always set to DMARC1
p	none	Policy applied to messages that fail DMARC alignment
adkim	r	Required DKIM alignment - “r” for Relaxed, “s” for Strict
aspf	r	Required SPF alignment - “r” for Relaxed, “s” for Strict
sp	value of p	Policy applied to messages from subdomains that fail DMARC alignment
fo	0	Forensic report settings - “0”, “1”, “d”, “s”
		0 – only messages failing alignment 1 – all messages that are partially unaligned d – messages where DKIM alignment failed s – messages where SPF alignment failed
ruf	-	URI to send forensic reports to *
rua	-	URI to send aggregate reports to
pct	100	Percentage of messages to apply policy to
ri	86400	Reporting interval (reports will be sent 1 per day in most cases no matter what the setting)

** Forensic reports are sent only by a handful of receivers and by their nature can become a GDPR liability. DO NOT USE!!*

DMARC
alignment

domain.com

Retrieve domain from RFC5321 mfrom message header

Domain.com

Retrieve domain from RFC 5322 "From" message header

domain.com

Retrieve domain from the DKIM-signature messages header

Domains match?

Domains match?

Valid SPF?

Yes

SPF aligned

No

Unaligned SPF
Check DKIM DMARC alignment

Yes

No

Unaligned DKIM
Check SPF DMARC alignment

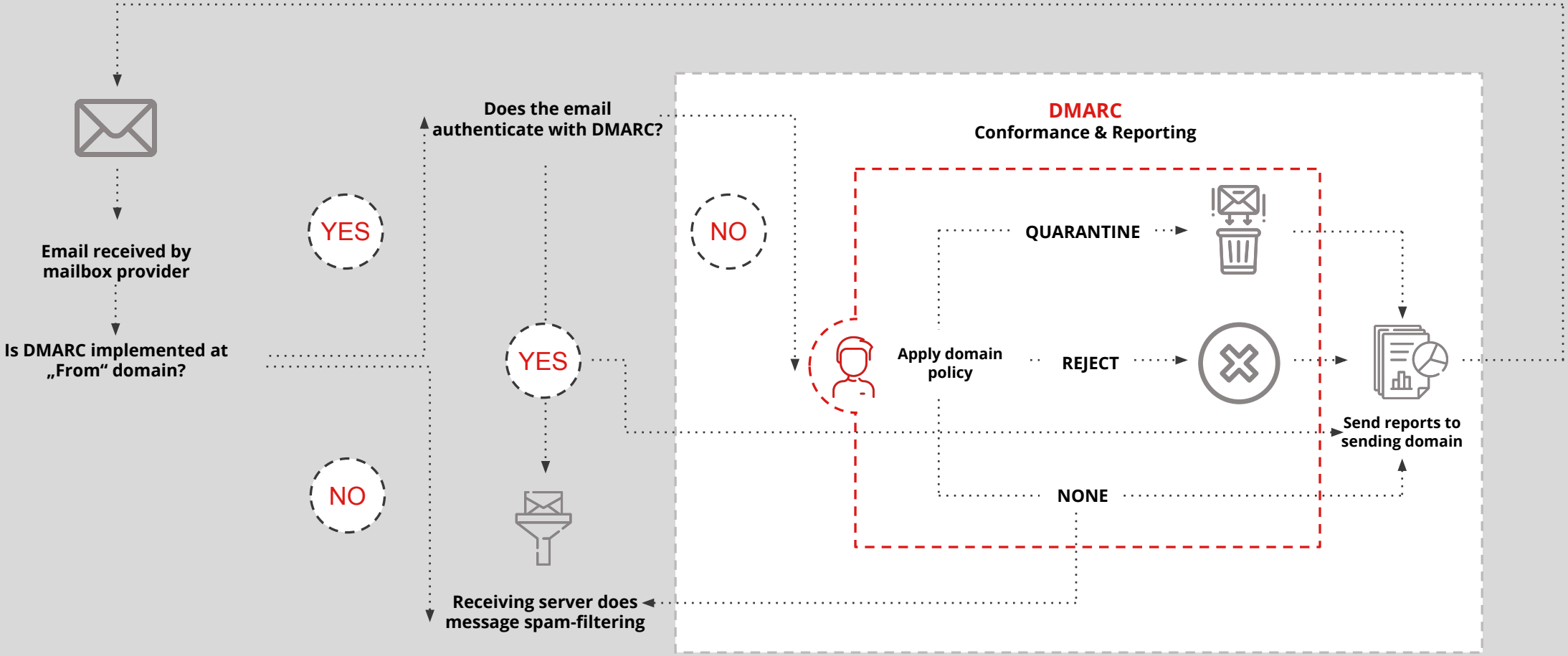
Yes

Valid DKIM?

Yes

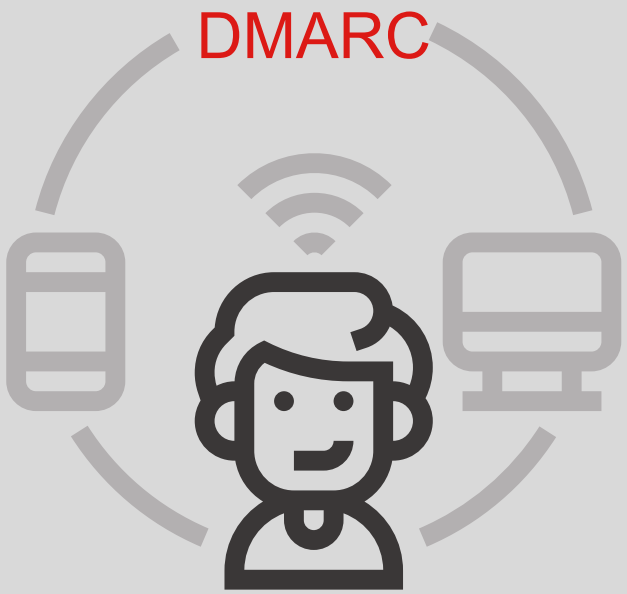
DKIM aligned

DMARC
record evaluation process



DMARC

settings for senders



Start (no protection, reporting only):

v=DMARC1; p=none; rua=mailto:reporting-email@domain.com

Goal (domain protection):

v=DMARC1; p=reject; rua=mailto:reporting-email@domain.com

DMARC

settings for receiving reports

Receiving reports on same domain:
_dmarc.domain.com IN TXT “v=DMARC1; p=none; rua=email@domain.com”

Receiving reports for 3rd party domains:
_dmarc.domain.com IN TXT “v=DMARC1; p=none; rua=email@otherdomain.com”

Must be authorized by DNS record:
domain.com._report._dmarc.otherdomain.com

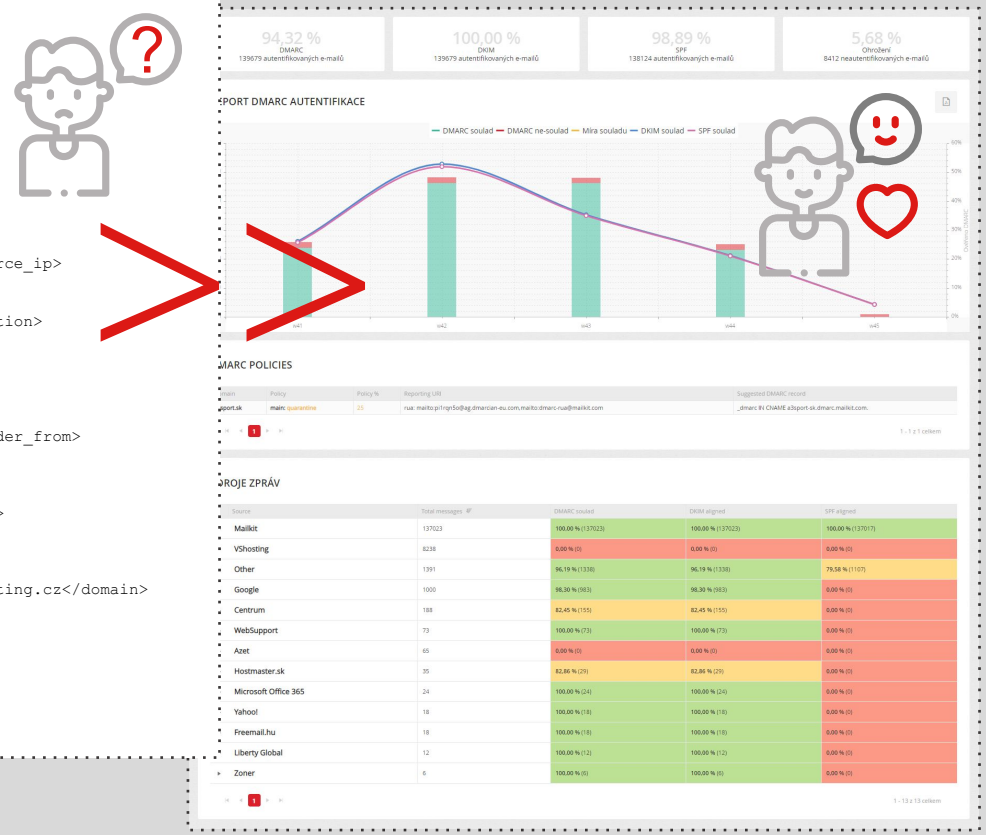
- Many servers send reports to unauthorized receiving domains
- Administrators often forget to setup authorization to receive reports

DMARC

aggregated reports

```
<?xml version="1.0"?>
<feedback>
  <report_metadata>
    <org_name>Yahoo! Inc.</org_name>
    <email>postmaster@dmarc.yahoo.com</email>
    <report_id>1604538164.934982</report_id>
    <date_range>
      <begin>1604448000</begin>
      <end>1604534399</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>a3sport.sk</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>quarantine</p>
    <pct>25</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>185.59.208.6</source_ip>
      <count>1</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>fail</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>a3sport.sk</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>a3sport.cz</domain>
        <result>pass</result>
      </dkim>
      <spf>
        <domain>a3sport-www2.vshosting.cz</domain>

        <result>none</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```



- Generated by receiving server
- Uncovers infrastructure and incorrect settings
- Provides information about messages and alignment results
  - Who (mfrom, From)
  - Source (IP)
  - Authentication (SPF, DKIM)
  - Policy
  - Policy applied

DMARC

aggregated reports

ZDROJE ZPRÁV

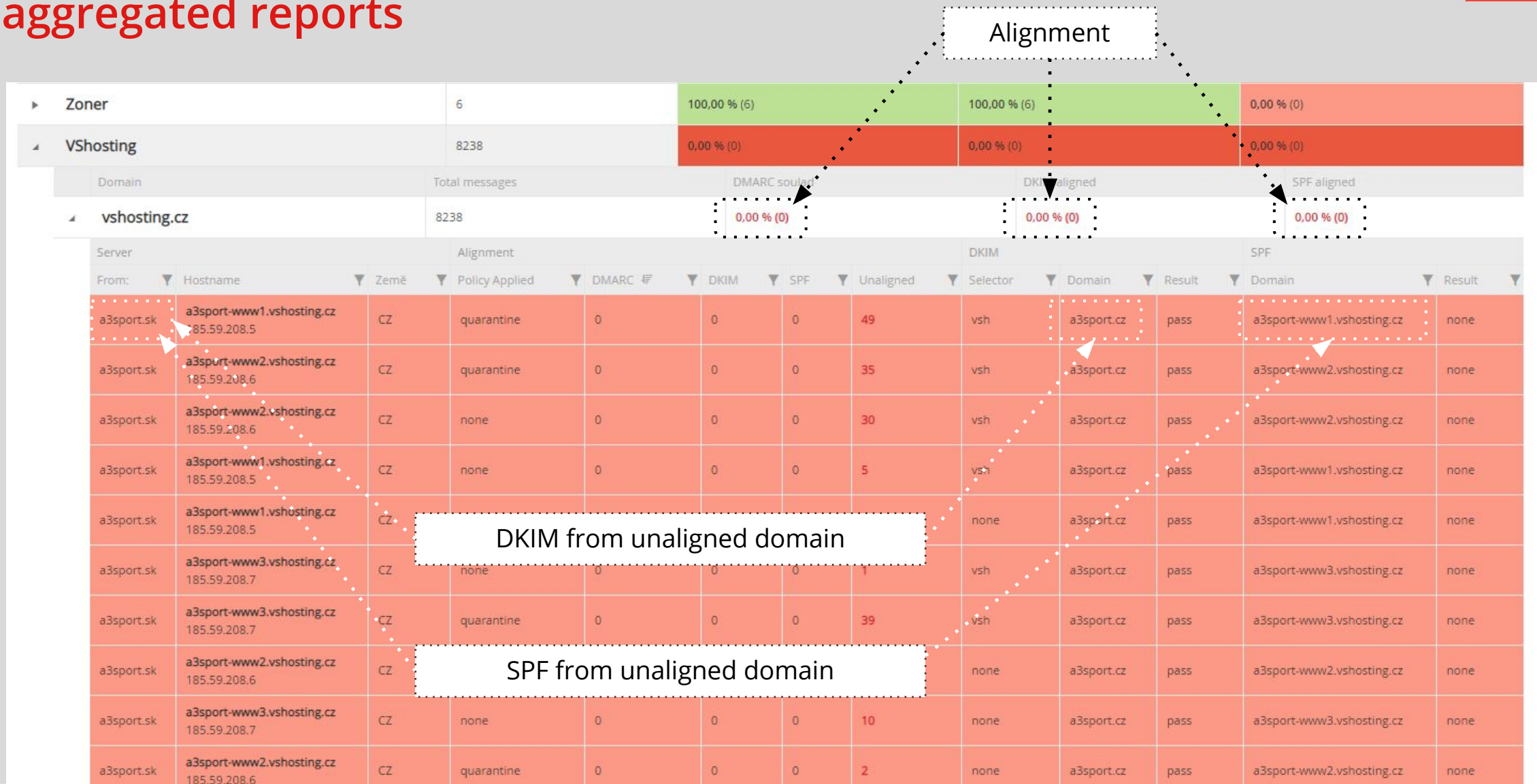
Source	Total messages	DMARC soulad	DKIM aligned	SPF aligned
Mailkit	137023	100,00 % (137023)	100,00 % (137023)	100,00 % (137017)
VShosting	8238	0,00 % (0)	0,00 % (0)	0,00 % (0)
Other	1391	96,19 % (1338)	96,19 % (1338)	79,58 % (1107)
Google	1000	98,30 % (983)	98,30 % (983)	0,00 % (0)
Centrum	188	82,45 % (155)	82,45 % (155)	0,00 % (0)
WebSupport	73	100,00 % (73)	100,00 % (73)	0,00 % (0)
Azet	65	0,00 % (0)	0,00 % (0)	0,00 % (0)
Hostmaster.sk	35	82,86 % (29)	82,86 % (29)	0,00 % (0)
Microsoft Office 365	24	100,00 % (24)	100,00 % (24)	0,00 % (0)
Yahoo!	18	100,00 % (18)	100,00 % (18)	0,00 % (0)
Freemail.hu	18	100,00 % (18)	100,00 % (18)	0,00 % (0)
Liberty Global	12	100,00 % (12)	100,00 % (12)	0,00 % (0)
Zoner	6	100,00 % (6)	100,00 % (6)	0,00 % (0)

1

1 - 13 z 13 celkem

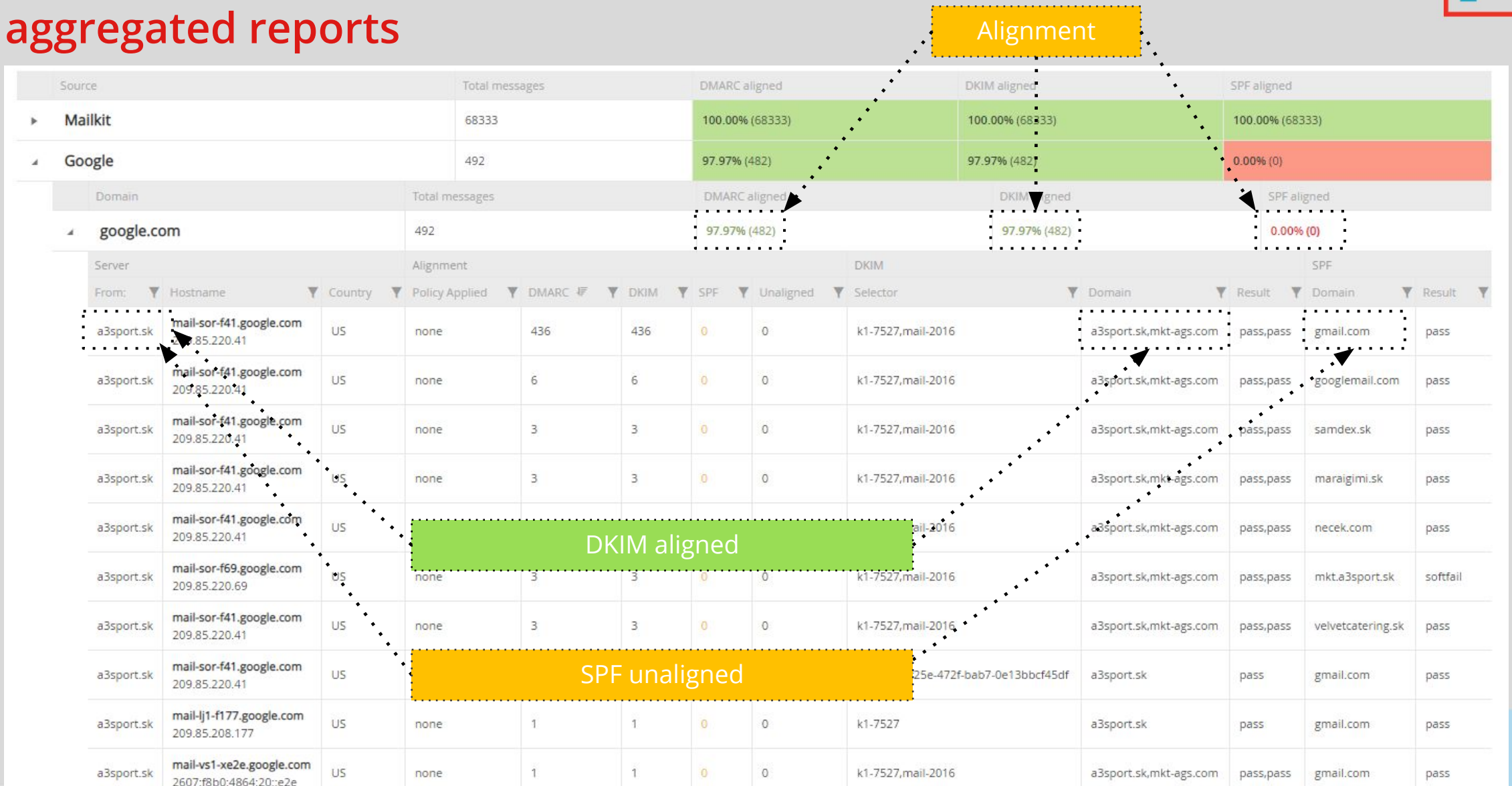
DMARC

aggregated reports



DMARC

aggregated reports



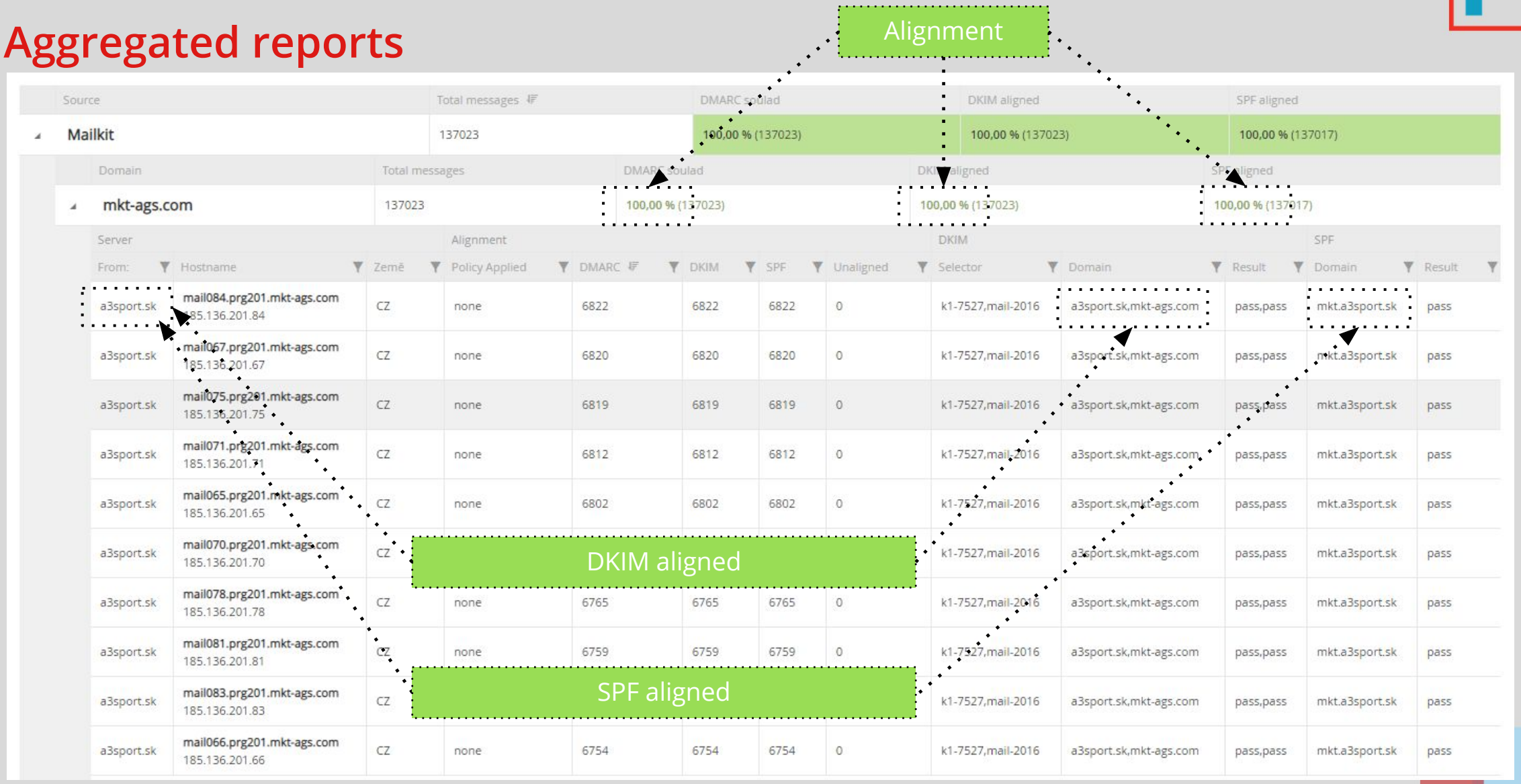
Source	Total messages	DMARC aligned	DKIM aligned	SPF aligned
Mailkit	68333	100.00% (68333)	100.00% (68333)	100.00% (68333)
Google	492	97.97% (482)	97.97% (482)	0.00% (0)

Domain	Total messages	DMARC aligned	DKIM aligned	SPF aligned
google.com	492	97.97% (482)	97.97% (482)	0.00% (0)

Server			Alignment					DKIM			SPF	
From:	Hostname	Country	Policy Applied	DMARC	DKIM	SPF	Unaligned	Selector	Domain	Result	Domain	Result
a3sport.sk	mail-sor-f41.google.com 209.85.220.41	US	none	436	436	0	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	gmail.com	pass
a3sport.sk	mail-sor-f41.google.com 209.85.220.41	US	none	6	6	0	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	googlemail.com	pass
a3sport.sk	mail-sor-f41.google.com 209.85.220.41	US	none	3	3	0	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	samdex.sk	pass
a3sport.sk	mail-sor-f41.google.com 209.85.220.41	US	none	3	3	0	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	maraigimi.sk	pass
a3sport.sk	mail-sor-f41.google.com 209.85.220.41	US							a3sport.sk,mkt-ags.com	pass,pass	necek.com	pass
a3sport.sk	mail-sor-f69.google.com 209.85.220.69	US	none	3	3	0	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	softfail
a3sport.sk	mail-sor-f41.google.com 209.85.220.41	US	none	3	3	0	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	velvetcatering.sk	pass
a3sport.sk	mail-sor-f41.google.com 209.85.220.41	US						25e-472f-bab7-0e13bbcf45df	a3sport.sk	pass	gmail.com	pass
a3sport.sk	mail-lj1-f177.google.com 209.85.208.177	US	none	1	1	0	0	k1-7527	a3sport.sk	pass	gmail.com	pass
a3sport.sk	mail-vs1-xe2e.google.com 2607:f8b0:4864:20::e2e	US	none	1	1	0	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	gmail.com	pass

DMARC

Aggregated reports



Source	Total messages	DMARC soulad	DKIM aligned	SPF aligned
Mailkit	137023	100,00 % (137023)	100,00 % (137023)	100,00 % (137017)

Domain	Total messages	DMARC soulad	DKIM aligned	SPF aligned
mkt-ags.com	137023	100,00 % (137023)	100,00 % (137023)	100,00 % (137017)

Server			Alignment					DKIM			SPF	
From:	Hostname	Země	Policy Applied	DMARC	DKIM	SPF	Unaligned	Selector	Domain	Result	Domain	Result
a3sport.sk	mail084.prg201.mkt-ags.com 185.136.201.84	CZ	none	6822	6822	6822	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail067.prg201.mkt-ags.com 185.136.201.67	CZ	none	6820	6820	6820	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail075.prg201.mkt-ags.com 185.136.201.75	CZ	none	6819	6819	6819	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail071.prg201.mkt-ags.com 185.136.201.71	CZ	none	6812	6812	6812	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail065.prg201.mkt-ags.com 185.136.201.65	CZ	none	6802	6802	6802	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail070.prg201.mkt-ags.com 185.136.201.70	CZ	none	6765	6765	6765	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail078.prg201.mkt-ags.com 185.136.201.78	CZ	none	6765	6765	6765	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail081.prg201.mkt-ags.com 185.136.201.81	CZ	none	6759	6759	6759	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail083.prg201.mkt-ags.com 185.136.201.83	CZ	none	6754	6754	6754	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass
a3sport.sk	mail066.prg201.mkt-ags.com 185.136.201.66	CZ	none	6754	6754	6754	0	k1-7527,mail-2016	a3sport.sk,mkt-ags.com	pass,pass	mkt.a3sport.sk	pass

DMARC

forensic reports

- Full message headers
- GDPR liability
- Not worth the risk

- Do not enable on your domains!
- Do not generate on mail servers!

DMARC

server side

- Easy to implement
- Applies policies set by domain owners
- Provides domain owners reports
- Protects recipients
- Save computing time

Try OpenDMARC:
https://github.com/trusteddomainproject/OpenDMARC

DMARC
sample Postfix configuration

/etc/postfix/main.cf: openDKIM openDMARC
smtpd_milters = inet:localhost:12345, **inet:localhost:54321**

/etc/opendmarc.conf:
RejectFailures true
Syslog true
Socket inet:54321@localhost
HistoryFile /var/run/opendmarc/opendmarc.dat
UserID opendmarc:opendmarc
SoftwareHeader false
IgnoreAuthenticatedClients true
RequiredHeaders true
SPFSelfValidate true

Generating reports:

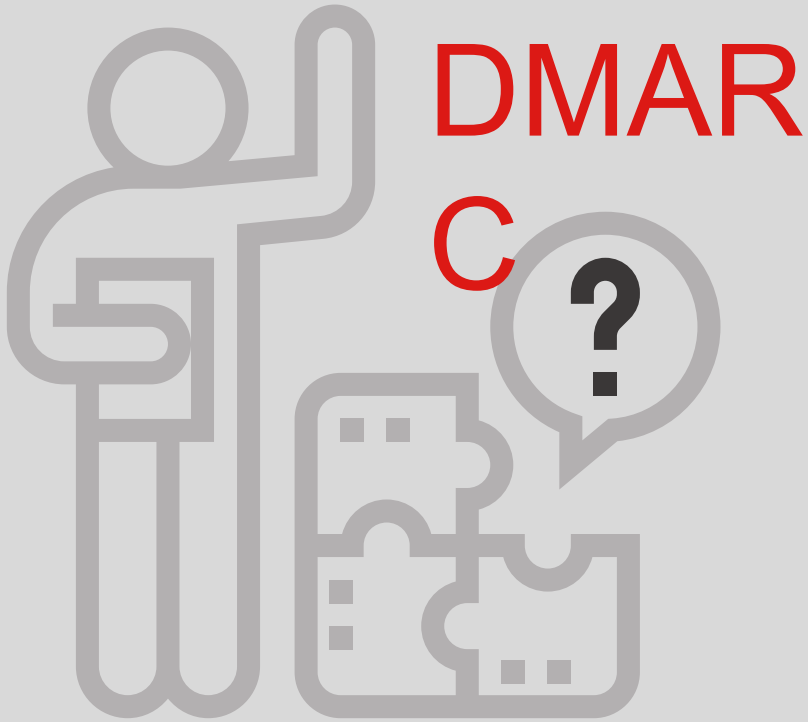
```
#!/bin/bash
DB_SERVER='192.168.222.117'
DB_USER='opendmarc'
DB_PASS='heslo'
DB_NAME='opendmarc'
WORK_DIR='/var/run/opendmarc'
REPORT_EMAIL='dmarc-reporter@domena.cz'
REPORT_ORG='Moje firma'
mv ${WORK_DIR}/opendmarc.dat
${WORK_DIR}/opendmarc_import.dat -f
cat /dev/null > ${WORK_DIR}/opendmarc.dat
/usr/sbin/opendmarc-import --dbhost=${DB_SERVER}
--dbuser=${DB_USER} --dbpasswd=${DB_PASS}
--dbname=${DB_NAME} --verbose <
${WORK_DIR}/opendmarc_import.dat

/usr/sbin/opendmarc-reports --keepfiles --dbhost=${DB_SERVER}
--dbuser=${DB_USER} --dbpasswd=${DB_PASS}
--dbname=${DB_NAME} --verbose --interval=86400 --report-email
$REPORT_EMAIL --report-org $REPORT_ORG

/usr/sbin/opendmarc-expire --dbhost=${DB_SERVER}
--dbuser=${DB_USER} --dbpasswd=${DB_PASS}
--dbname=${DB_NAME} --verbose --expire=30
```

DMARC

common mistakes



- DMARC record outside _dmarc name-space
- DMARC record on subdomain only
- “v=DMARC1” a “v=DMARC1; p=none” - useless records
- Inexistent or insufficient report analysis
- Misunderstanding of reports

Tools

https://dmarcian.com
https://dmarcanalyzer.com
https://easydmarc.com
https://redsift.com

https://github.com/domainaware/parsedmarc
- Open-source DMARC parser

DMARC

facts & myths

- **DMARC only prevents domain abuse**
  Although DMARC's primary goal is to protect domain from abuse, proper DMARC setup opens up the door to new standards like AMP and BIMI
- **DMARC is only for banks**
  Not only banks but companies of all sizes are subject of phishing attacks.
- **DMARC record is all we need**
  DMARC record alone without strict policy enforcement has no effect except to receive reports
- **Work is done with strict policy enforcement**
  Strict DMARC policy enforcement is the goal, the reports remain monitored and relevant changes to authentication deployed
- **DMARC is only for sending domains**
  Any domain can be abused and it's important that all domains are protected

- **DMARC has privacy implications (GDPR)**
  GDPR liability is related only to forensic reports and that's why we recommend not enabling them at all
- **DMARC is simple**
  DMARC record itself is no rocket-science but the work starts with the report analysis and proper implementation of authentication
- **DMARC has negative deliverability impact**
  DMARC has positive impact on deliverability when properly setup. According to Yahoo! DMARC enforcement bring 10% increase in

Authentication

recap

Why SPF?

- Provides receivers with signal for more efficient filtering
- Allows domain owners to authorize message sources and prevent direct abuse

Why DKIM?

- Allows receivers to filter messages with higher accuracy by assigning domain reputation
- Provides senders with access to FBL data and act on complaints

Why DMARC?

- Most efficient message filtering based on SPF and DKIM authentication
- Provides senders with information necessary to improve authentication and disclose sending infrastructure
- Required by latest email technologies
  - 1click Unsubscribe
  - AMP4mail
  - BIMI

Contact Us

For additional questions, please email: jakub@mailkit.com

Such a shame, he was THIS close to emptying his inbox