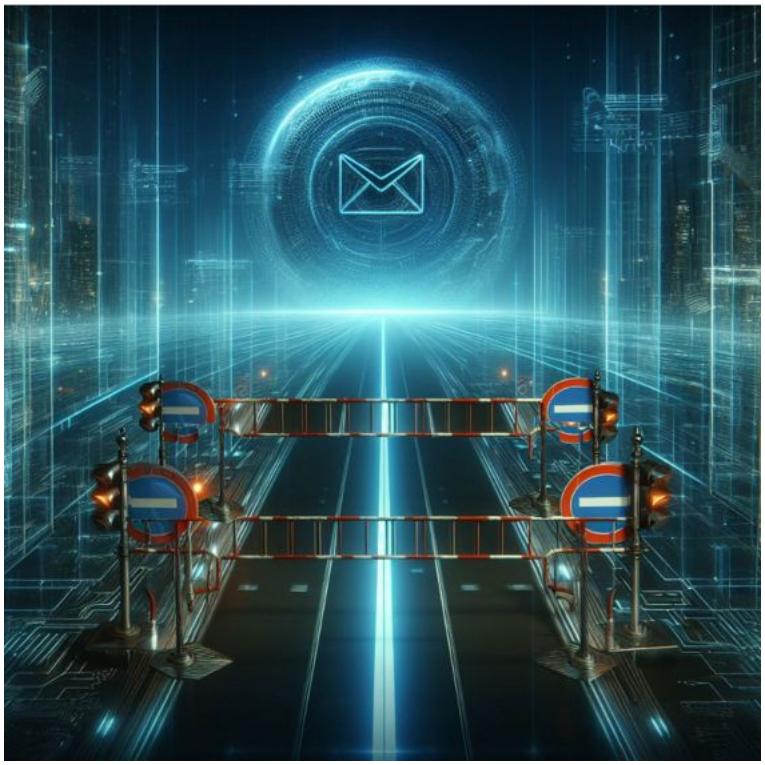


Combine the best of SPF and DKIM with DMARC

DMARC, *Domain-based Message Authentication, Reporting & Conformance*, is a protocol providing email authentication, policy and reporting capabilities. It builds on SPF and DKIM to improve monitoring and reporting of the protection of your email domain.

A DMARC policy allows a sender to indicate that their messages are protected by SPF and/or DKIM, and to tell the receiver what to do if these authentication methods give a negative result. It also provides a way for the receiver to report back to the sender about the handling of his messages.

DMARC is based on efforts by financial organizations (PayPal, Bank of America...) and Internet companies (Yahoo, Google...) to reduce the number of fraudulent domain spoofing mails.

How DMARC works

When the mail administrator of the *example.com* domain wants to use DMARC to allow the recipients to check mails sent under his domain name are authentic, he needs to take the following actions:

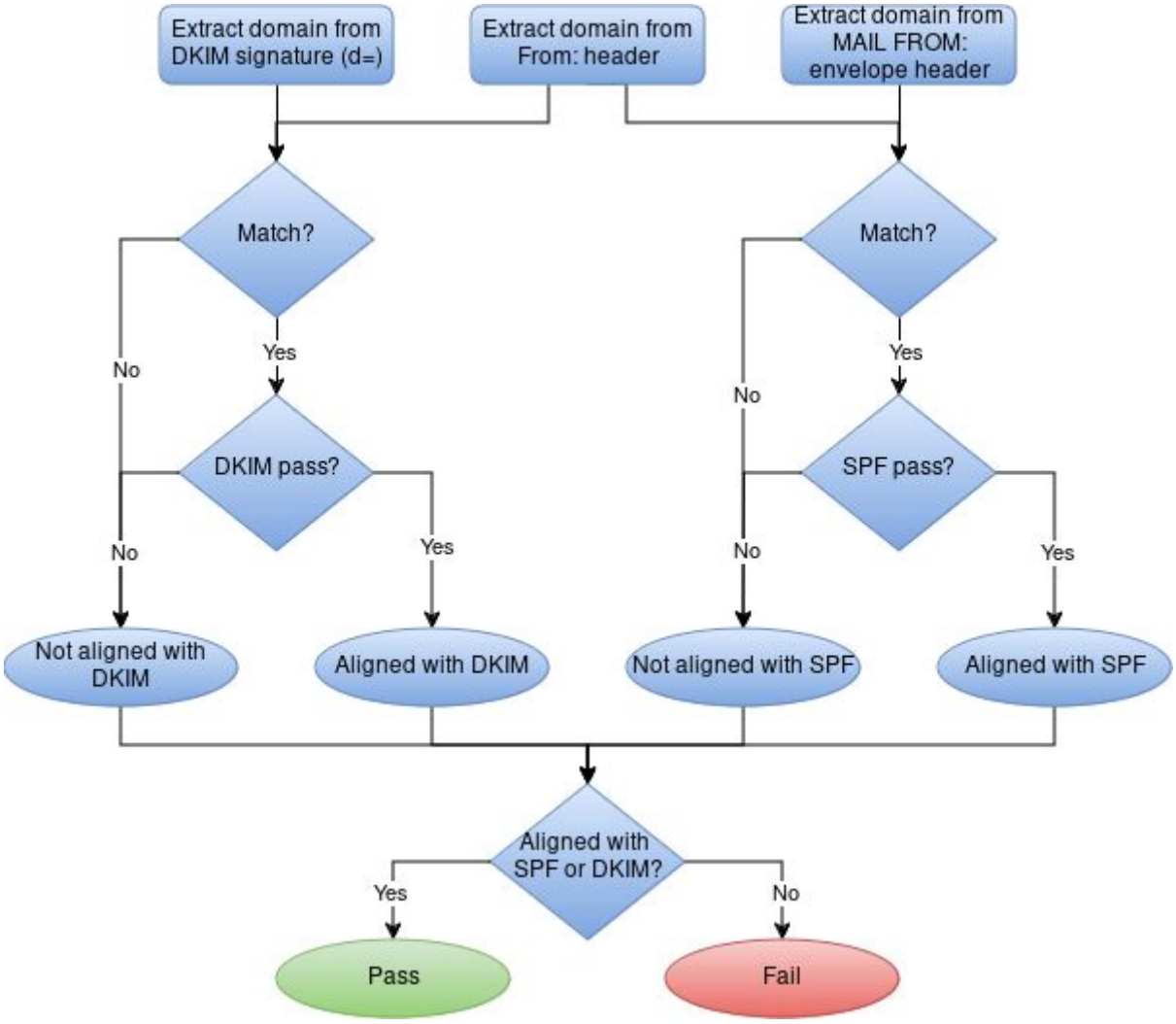
- Setup SPF and/or DKIM (preferably both);
- Publish a DNS TXT DMARC record;
- Setup a mailbox to receive reports.

Then, he and other mail administrators of domains receiving emails from the *example.com* domain need to enable DMARC so the email handling software can verify the emails and send feedback.

DMARC will perform the following steps:

- Extract the domain from the *From:* email header;
- Query DNS to retrieve the corresponding DMARC record;
- Extract the domain from the DKIM signature header (*d=*);
- If the 2 domains above do not match, the result is not aligned with DKIM, and the SPF check is performed
- If the 2 domains above match, the DKIM result is checked;
- If the DKIM result is pass, the DMARC result is aligned with DKIM;
- If the DKIM result is fail, the DMARC result is not aligned with DKIM;
- For the SPF check, the *From:* email header is compared with the *MAIL FROM:* envelope header;
- If they do not match, the result is not aligned with SPF;
- If they match, the SPF result is checked;
- If the SPF result is pass, the DMARC result is aligned with SPF;
- If the SPF result is not pass, the DMARC result is not aligned with SPF;
- In the end, if the DMARC result is aligned with DKIM or with SPF, the DMARC result is pass;
- Else, the DMARC result is fail.
- The resulting action will depend on the content of the DMARC record as described in one of the following paragraphs. DMARC can influence the email delivery and provide reporting to the sender. The ISPs and large Internet companies can send feedback to the senders if they indicate a mail address in their DNS DMARC record. Reports can be aggregated, summarizing activity during a certain period (by default, 24 hours), or individual, in case of DMARC alignment failure in a particular email.

The following figure summarizes the DMARC assessment process:



Setting up DMARK for a domain

A DMARC record is a DNS (Domain Name System) TXT record, generally containing 5 parts:

- The dmarc version;
- The action to take when the result is fail;
- The strictness to apply in the alignment checks;
- When to send reports;
- Where to send reports.

The general syntax of a DMARC record is the following:

```
_dmarc.<domain> TXT "v=DMARC1; p=<action>; <checking conditions>;
<reporting conditions>; <URIs for reports>"
```

- **action** can be *none*, *quarantine* or *reject*, depending on the action the sender wants the receiver to apply to mails that do not pass DMARC alignment check.
- **<checking conditions>** can be:
  - **pct=**<number> : percentage of the mails received from this sender to be subject to the action above. This allows a progressive rollout of the DMARC rules without disturbing the entire set of sent emails.

- **adkim=r** or **s**: relaxed or strict mode for DKIM alignment; default is r. In strict mode, the DKIM *d*= domain and the *From:* domain must be strictly equal. In relaxed mode, the *From:* domain can be a subdomain of the DKIM *d*= domain. For example, if the sender is *user@mail.example.com* and the *d*= domain is *example.com*, they are considered as aligned.
- **aspf=r** or **s**: relaxed or strict mode for the SPF alignment. The same rules apply as for adkim.
- **<reporting conditions>** is: **fo=<value>,<value>...** where <value>is **0** or **1** or **d** or **s**.
  - **0** is the default and generates a DMARC failure report when the DMARC result is not pass;
  - **1** generates a DMARC failure report when any of the SPF or DKIM alignment gives a result other then pass;
  - **d** generates a DMARC failure report when DKIM gives a fail result, regardless of its alignment;
  - **s** generates a DMARC failure report when SPF gives a fail result, regardless of its alignment.
- - **<URI for reports>** can be:
  - **rua=mailto:<mail address>**: address where to send the aggregated reports;
  - **ruf=mailto:<mail address>**: address where to send the message-specific failure reports.

Finding the DMARC record for a domain

As the DMARC record is a DNS TXT record, you can get it with the following commands:

```
dig -t txt _dmarc_.<domain>
nslookup -ty=txt _dmarc.<domain>
```

```
nslookup -ty=txt _dmarc.google.com
Server: 9.9.9.9
Address: 9.9.9.9#53

Non-authoritative answer:
_dmarc.google.com text = "v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com"
```

This means that Google wants the receiver to reject the mails that fail DMARC and wants to receive daily aggregated reports in their *mailauth-reports@google.com* mailbox.

You can also use the following free websites to find DMARC records:

- MXToolbox
- EasyDmarc

Checking DMARC results in email headers

DMARC adds its results to the *Authenticated-Results* headers in the emails it processes, generally after the SPF and DKIM results.

The general syntax is:

```
Authenticated-Results: <authenticating server> ....
    dmarc=<result> <dmarc policy summary> <checked header>
```

where <result> is pass or fail.

The format depends on the mail provider; Google, Microsoft and Yahoo have slghtly different formats.

Let's check a real world mail header. This is an email sent from *pltrash2@outlook.com* to *pltrash2@gmail.com*. The DMARC *Authenticated-Results* is written by the *gmail.com* server (Google).

```
Delivered-To: pltrash2@gmail.com
Received: by 2002:a17:906:d294:b0:a4a:365b:20e4 with SMTP id
ay20csp1070802ejb;
Thu, 11 Apr 2024 07:40:27 -0700 (PDT)
X-Google-Smtp-Source:
AGHT+IG8Ug/mzFIi4XUZiyUuOHhLtnNJ6fGoGZvaZtp/3BC1KeNkNrCbgRVzWJR/on
Ew8po3ught
X-Received: by 2002:a05:6359:1581:b0:184:69c5:c088 with SMTP id
jv1-20020a056359158100b0018469c5c088mr8086931rwb.12.1712846426495;
Thu, 11 Apr 2024 07:40:26 -0700 (PDT)
ARC-Seal: i=2; a=rsa-sha256; t=1712846426; cv=pass;
d=google.com; s=arc-20160816;
b=yLQJJE6Qiznv95fE1PkudoTljBSl57xgJNtiESPiKv9yIIctOgSoPQINlDxcRpo+
1N
GTCMIT7wFb4MDOSGWjQOCyU4G4KCB7mU7cMliIJumByfMDnzjrrgOzeDQbjB79k3IC
sO
AvEcQOVOu2XLNON5i6gF3xmVRXWR3z8Oi8UnLaS+SJXCyr2+XIyOMJBoYKhvN89bua
36
Lz2Q5KbYggNDe1OBDV3ArRbmajt/zv1TsbjTzJL6+WWAcTDJj+
+i+GDNP+v1Nab75dwb
l2L4yAIyRPF3X3RcvKbkYI8arWWPtUiEDSYDwIjLcN9B8MaKM3H4leUP9daF51+HDu
ck
CASw==
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed;
d=google.com; s=arc-20160816;
h=mime-version:content-transfer-encoding:msip_labels:content-
language
:accept-language:message-id:date:thread-index:thread-topic:subject
```

```
:to:from:dkim-signature;
bh=nmuZdOMPqHHFa9pIGbO+I+SebjZShl563DjrzElH5JM=;
fh=H8fS/F1Xi7k6c76u5mat11UzewD7stRXC+xTg8ayz9I=;
b=jZYC1NhVVpwNhyOgFWM/
LHWOBZ3u9ljYk6DEqfBCtFHOHJuYhBpqdUOml2g+8U//Oc
MisUhmWXDObOH3EtyBRmSeQ3hZMZoSL4OoFKGVO7otms/
r6McJjUrEcWoshH3F6eFF/l
jOfGcYEsmVX85v5fHyjXOJfGPlBnVJcGtX7+I9v5QT5xJE6Vb2rlWPFy+z665grhAA
J7
SOQTWzeuIxBZ9LxIzEWS+2tktJziPw5J7xllrOW45VgrVPxqQeZAgqU4MHsCuGLwkc
Zx
DsblVAd6BgSHWEPH4D+YJK5olY7kAOgcIs9mGukYMl9cBhRwFU1H9MCheY4fqnnb6I
S+
j+/Q==;
dara=google.com
ARC-Authentication-Results: i=2; mx.google.com;
dkim=pass header.i=@outlook.com header.s=selector1
header.b=MvWEquRr;
arc=pass (i=1);
spf=pass (google.com: domain of pltrash2@outlook.com designates
2a01:111:f400:fe1f::810 as permitted sender)
smtp.mailfrom=pltrash2@outlook.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=outlook.com
Return-Path: <pltrash2@outlook.com>
Received: from EUR01-VE1-obe.outbound.protection.outlook.com
(mail-ve1eur01olkn0810.outbound.protection.outlook.com.
[2a01:111:f400:fe1f::810])
by mx.google.com with ESMTPS id mi16-
20020a056214559000b0069b1f8b5ab0si1554535qvb.574.2024.04.11.07.40.
26
for <pltrash2@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256
bits=128/128);
Thu, 11 Apr 2024 07:40:26 -0700 (PDT)
Received-SPF: pass (google.com: domain of pltrash2@outlook.com
designates 2a01:111:f400:fe1f::810 as permitted sender) client-
ip=2a01:111:f400:fe1f::810;
Authentication-Results: mx.google.com;
dkim=pass header.i=@outlook.com header.s=selector1
header.b=MvWEquRr;
arc=pass (i=1);
```

```
spf=pass (google.com: domain of pltrash2@outlook.com designates
2a01:111:f400:fe1f::810 as permitted sender)
smtp.mailfrom=pltrash2@outlook.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=outlook.com
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com;
cv=none;
b=T8fKfYp1xtjbOqieQ31Y51ISZTrb9fTW9Zg8Cms2n8fk3D8fJ5LLeOHwayMMia2z
QOouohDRCiapcdyon9YNkOmburCbkVXAex/
raoCTzQciQAkZoxrWbK4uRN56Xt3XVcUNk4WcV6xz4xcOz+DEpUg4Ced6OcbVUQ3g4
u8GhGmDV3IOIQddNHU5SPpoBg2Oxy8lzshxy504fcNoPnHtWskMuXJiOzlec/
cvWXkq6P/
33d5ao4jeLvqpfiJQ5kfE4h6BTDbqKKfZBFcOOSia4qTwlseRd3jNxbi87gH3os/
3MwiJqU65hjG44kvHPtNddg9Uh928FVTwu4jPB+vVEw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed;
d=microsoft.com; s=arcselector9901; h=From:Date:Subject:Message-
ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-
ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-
AntiSpam-MessageData-1;
bh=nmuZdOMPqHHFa9pIGbO+I+SebjZShl563DjrzElH5JM=;
b=UvWIO8OhU698YsiJgODAkrVCQ5ywbtuYdDkh1LUMHeEh5CkA49VttSuIDaH6ipTW
lU/
ZR8aSmYUF2g5nSwxoJxnpxyyF71PKDaVkXyUu+y9i8gTTLIsDjTA6x9OTs3czGXq6K
3IddQp4mcjODImvb2jmQKXkJJBAnv5infAIeL3ZfmNsUMGaJao5fnJMN+gyZrioOjg
lgu3ga4Scdi8rsESfDKW82L7eOmrPTBGDQ53DNhdrw4JVBlhr8pvijuyNofPXXfyMB
gblHmgY/7zLuCNtE3FzNeGDadnYRi9sqPr2TCn8c+OEHYopwm9xbVyZft2eWn/
g7Hw9qkmD+1Meeg==
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=none;
dmarc=none; dkim=none; arc=none
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=outlook.com; s=selector1; h=From:Date:Subject:Message-
ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=nmuZdOMPqHHFa9pIGbO+I+SebjZShl563DjrzElH5JM=;
b=MvWEquRrP2D5ugmX4w/vutSLGDGXY/ew1uzQXW5LvhDkDUCDmvPox6ubAEbVd7gW
W2dluyDexiUFkZSFOrXMf41MVF9mnrJG2hNrAQYDS3n3vbRbuAl3AqBfCC2+ivIUUt
VhKvhnwbDd4eNV1rgBAoDIyvrhTSOVBnz7MEolrggeh1mR5nbOophNeSXYpVT4Old4
lPEEoVnHVW5+cNDGyQuDiDoLfnnHKzFADSoNA2u/
NdByeL8cjEcpmzQuT1tORS4Rk9kEqr9YVKQuAflhIWHTr7Ihg96Jtlp/
NdeTpmncNGXcqC/tiXazZKjYRN5kwGSzYnLuuqX/gJk1ykXwxQ==
Received: from AS8P189MB1621.EURP189.PROD.OUTLOOK.COM
(2603:10a6:20b:393::12) by AS8P189MB1176.EURP189.PROD.OUTLOOK.COM
(2603:10a6:20b:2aa::20) with Microsoft SMTP Server
(version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.7409.55; Thu, 11 Apr 2024 14:40:24 +0000
```

```
Received: from AS8P189MB1621.EURP189.PROD.OUTLOOK.COM
([fe80::c7fb:d192:40d8:2f36]) by
AS8P189MB1621.EURP189.PROD.OUTLOOK.COM
([fe80::c7fb:d192:40d8:2f36%3]) with mapi id 15.20.7409.053; Thu,
11 Apr 2024 14:40:24 +0000
From: PL Trash2 <pltrash2@outlook.com>
To: pl_trash <pltrash2@gmail.com>
Subject: DMARC test
Thread-Topic: DMARC test
Thread-Index: AQHajB4wmPTgUx5MKkyyBDK0ux2iFg==
Date: Thu, 11 Apr 2024 14:40:24 +0000
Message-ID:
<AS8P189MB1621F4DB3BE74F9B01145B2C8E052@AS8P189MB1621.EURP189.PROD
.OUTLOOK.COM>
Accept-Language: en-GB, en-US
Content-Language: en-GB
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
msip_labels:
x-ms-exchange-messagesentrepresentingtype: 1
x-tmn:
[qDT4Feh/8uxkRKMs4obZNyBSXqjQGgxEP3Nq6ghUfI3jSTFgier6/QQapWBw+sks]
x-ms-publictraffictype: Email
x-ms-traffictypediagnostic: AS8P189MB1621:EE_|AS8P189MB1176:EE_
x-ms-office365-filtering-correlation-id: 5d6abbf9-9b86-4e33-3f67-
08dc5a3552c3
x-ms-exchange-slblob-mailprops:
2xtDbzDEsjJ+6YSxtzQdlotZqtDO7vInfnrSL6pS9kKKX9cpt5q+D/W/Z/vd6hiIpc
Jzhm1qqMElxlVGJgmodMT7vr1lVL1jXT/
HHQWtj0rqHtZVXK8utDgbi+vwtUj1NWOYXAB9BSuulDRtwJm16amzIfl1O7c2abWQt
ienb86+6ue2YOVXt/
0j4183oplD4+bsBiF4fnPIALWwoGb9KcJe9HkzVV+dhPUKoyitZq7ZSiGSvaas2RlR
E/
9tl7ezuAgS84n4xdV8AAL1balAIuCu29bysHUM5MHVpfWX8pch+65rWHZ0kBn1bG5x
SLSm1gbCgdMQ96v88BN5QP1p+o3uuCUeqYGLIuIqx79bd0ciE9vlNrsStKdUY2NV2Q
9LZurSQ/0E7BPfUUss+Qggo2Hr5ryKsipQDTYshk63HaEt/
7JW32pBcIXUoojtRL44lu4o7qbu0fTm07/
pRapd2r9ldcpKf+ADb+n0rHFnhGXFvlf6mo13cfcE2frUtNQWa+dUBvIQorAFQ3urd
8nk3VXv0asc1KGCZ0GpvA4MBmEOYXxOQEFQgwjyWKLXwa/rBGh+G/
TpqCPtnSLQkfiAGA==
x-microsoft-antispam: BCL:0;
x-microsoft-antispam-message-info:
tZ3uQ5ZpAJAKQJTEklFMYMz/bVvjjWoTYW9OBDwRb6alguvNDmbmlwCXYOBJzYEuFi
```

```
KU8fQdcYeLOOxJNVyxwSOXC32vMuEuZ+1rQp2jG37W4RYng4JqHJRO7N8Aj0MxZXPM
n6SLtfUr9f9dVH5rOzcfM4si4EhmDHyhFzWsUSuVfmLarJRJHcA2VWtRrTfzL5F+SB
RuTeZY8bHa2Jy0YJN2x2iF0Rl5c7k3C3z9i2bShznaV8pe321Jtz1a9EAkmqAKnWT9
r7ba08jmBzO/GBv66H5YcEuMAGl45IY9jcc=
x-ms-exchange-antispam-messagedata-chunkcount: 1
x-ms-exchange-antispam-messagedata-0:
SWztyGh0+xzwMjhhddodI9svPCkRH0zqRj/QEE59LAjgna7Q7xznA8oC63KYq8qzL3
+WMl0UXvBG3lkRS2X7CQJEFnaiC2fapN3f9eSgTozyf90ZoUwQzIZtXfBLAMLIV06O
YVc0RvTcdpg0Mu67AnuIfTgdHnuBCXNBwY+AHLQVT3iCxNlXw9EsfD1rpXrMXTxofS
GW6tifBQgE9aaDxdVqWY0Q3KsD0BxAB/Eo0Pw67NZCqvX1tDhaWvoJv/
nJf+bugtyuEhU9dXCMAgeYlEWSBHQT+pCOgJ6hAsgmMML2Fhua3uHao7Nvr79LrrcM
sgALz7qRQ3D1JTljLaZxNJDin+o/
wibvzKRPOwTp51BwiigRJdp0qd9PsnW4DFcOnfGnMOOVQKUjE9Z72V1xBiVkRJ3OyW
eRXZINVM8Mcv28zZ3Q4rhWEz65MdjvGX5ubIcWS6ngG/ViRO/
UtgKrnu908RvelS0jrk14Xeb8jq+jPWK7KnAociomdKaoCUKApKYRdPfbD6o6Rd+m5
oO50FcG9VjsH95BQn0wvq6AgG+2cZEb7AH//
gPBPlks8HthIgIw0VufrTJmVlU1y3K8yom7GwQ1ZjFXKbLq3xaeUQk4ECW8w6uGZQ8
BSSqCmKzwhK0OnaJ1tZhWolZL1ZFD0ilOOt+s0r+htnQxYbqt6ebOcWisKdBhONrCv
TwvuEOmeqkPenhx4ubi6HYUMqO6LwVSJ5cFlKdn0InKpTHtJwSDD2nskHvJNIJPFht
K9LCeYKncGOWtowXF4/kFuoVOYUIXhvlgMDdomL1Dz/
f4gj5AV81zydZ+i2YSt4mkiVfLcqsaGRXN0aX0aK66U1grOOq5THPu1u9RyOhxQdPI
D49ta5WsoEzDxQkX6VfG71OAIz7WLcCB9GK+KqCnSKq5WLKXHgC+swmJONH0MVqt7t
e77Z1cohCQp5GcnxClaGU09tpZS/mGwxDiHbIZqdPRSnnHHD69cnmekf3Y/
v6dG0VhNLJOHWzHon9GS78DNo2FLT61BcIeAnqMHhpyhA4+tQ7ivRztTFN+OoETtCq
bAGsIjYVjWC2wROnsrVhNkAlJkuLqO7GTgbbspciXM6VN2YF2LYWGMHq8Lx9wPD7mn
+1Kl349zSyXEG/5lc0KwkWLL6pEEozD/ZKYbzkPlRK0VFmvoPE146RNIpEEbY66/
avf5AF7gexwJ+oMb0BgpPFsyS7iXIa4BtaupL/
1T6n+aN8UPozeGMgZecvcaKJkW3ki+pE5/5SGRA8lNNBRg0DUunWs1vp8f1s4HhI1d
HONOQ==
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0
X-OriginatorOrg: outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Internal
X-MS-Exchange-CrossTenant-AuthSource:
AS8P189MB1621.EURP189.PROD.OUTLOOK.COM
X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg: 00000000-0000-
0000-0000-000000000000
X-MS-Exchange-CrossTenant-Network-Message-Id: 5d6abbf9-9b86-4e33-
3f67-08dc5a3552c3
X-MS-Exchange-CrossTenant-rms-persistedconsumerorg: 00000000-0000-
0000-0000-000000000000
```

```
X-MS-Exchange-CrossTenant-originalarrivaltime: 11 Apr 2024
14:40:24.7590 (UTC)
X-MS-Exchange-CrossTenant-fromentityheader: Hosted
X-MS-Exchange-CrossTenant-id: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
X-MS-Exchange-Transport-CrossTenantHeadersStamped: AS8P189MB1176

DMARC test.
```

The Authenticated-Results header is:

```
Authentication-Results: mx.google.com;
        dkim=pass header.i=@outlook.com header.s=selector1
header.b=MvWEquRr;
        arc=pass (i=1);
        spf=pass (google.com: domain of pltrash2@outlook.com
designates 2a01:111:f400:fe1f::810 as permitted sender)
smtp.mailfrom=pltrash2@outlook.com;
        dmarc=pass (p=NONE sp=QUARANTINE dis=NONE)
header.from=outlook.com
```

The verifier is *mx.google.com*, the Gmail mail server.

The DMARC result is pass since the SPF and DKIM results are both pass. The DMARC policy coming from *outlook.com* is: no action on DMARC fail, quarantine if it is coming from a subdomain, action taken on the current email is none. The *From:* header is *outlook.com*.

Let's check the *_dmarc.outlook.com* TXT record:

```
nslookup -ty=txt _dmarc.outlook.com
Server: 9.9.9.9
Address: 9.9.9.9#53

Non-authoritative answer:
_dmarc.outlook.com text = "v=DMARC1; p=none; sp=quarantine;
pct=100; rua=mailto:rua@dmarc.microsoft;
ruf=mailto:ruf@dmarc.microsoft; fo=1"
```

It corresponds to the *p=NONE sp=QUARANTINE* part of the header.

DMARC reports

If the sender indicates an email address to receive DMARC reports and he sends mails to well known ISPs or large Internet companies, he will receive reports. These reports come in a *.zip* file attached to a mail.

Once you unzip them, unfortunately, these reports are not very sexy; they are written in XML.

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>google.com</org_name>
    <email>noreply-dmarc-support@google.com</email>

<extra_contact_info>https://support.google.com/a/answer/2466580</e
xtra_contact_info>
    <report_id>3858404806197327731</report_id>
    <date_range>
      <begin>1712707200</begin>
      <end>1712793599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>quarantine</p>
    <sp>quarantine</sp>
    <pct>100</pct>
    <np>quarantine</np>
  </policy_published>
  <record>
    <row>
      <source_ip>XXX.XXX.XXX.XXX</source_ip>
      <count>1</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
        <result>pass</result>
        <selector>dkim</selector>
      </dkim>
      <spf>
```

```
        <domain>example.com</domain>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

We can still decode some information:

- **<org_name>** tag: the report was sent by *google.com*.
- **<policy_published>** tag: the DMARC policy for the sender domain
- Each **<record>...</record>** tag pair delimits one record containing the following data:
  - Source IP of the sender (**<source_ip>** tag)
  - Number of mails sent by this sender in this report (**<count>** tag)
  - The evaluated policies (SPF, DKIM) (**<policy_evaluated>** tag)
  - The From: header (**<header_from>** tag)
  - The DKIM and SPF results (**<dkim>** and **<spf>** tags)

We could summarize the report like follows:

Reporting organization			**Report for domain**		
google.com			example.com		
Domain policy	**Subdomain policy**	**Percentage**	**DKIM alignment**	**SPF alignment**	
quarantine	quarantine	100%	relaxed	relaxed	
Mail received					
Sending IP address	**#**	**Policy evaluation**	**Header From:**	**DKIM**	**SPF**
XXX.XXX.XXX.XXX	1	DKIM: pass, SPF: pass, Disposition: none	example.com	pass. domain:example.com, selector: dkim	pass. domain: example.com

Fortunately, there are some free sites that make these data readable:

- MXToolbox
- EasyDmarc
- Dmarcian