M³AAWG DMARC Training Series

Mike Adkins, Paul Midgen
DMARC.org
October 22, 2012
# M³AAWG DMARC Training Videos

(2.5 hours of training)

This is Segment 3 of 6
The complete series of DMARC training videos is available at: [https://www.m3aawg.org/activities/maawg-training-series-videos](https://www.m3aawg.org/activities/maawg-training-series-videos)

<table>
<thead>
<tr>
<th>Segment 1</th>
<th>Segment 2</th>
<th>Segment 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is DMARC? (about 20 minutes)</td>
<td>DMARC Identifier Alignment (about 20 minutes)</td>
<td>DMARC Policy Records (about 30 minutes)</td>
</tr>
<tr>
<td>Segment 4</td>
<td>Segment 5</td>
<td>Segment 6</td>
</tr>
<tr>
<td>DMARC Reporting (about 15 minutes)</td>
<td>DMARC Information for Mailbox Providers (about 20 minutes)</td>
<td>DMARC Information for Domain Owners and 3rd Parties (about 40 minutes)</td>
</tr>
</tbody>
</table>
DMARC Policy Records
DMARC Segment 3 – about 30 minutes

Mike Adkins, Paul Midgen, DMARC.org
October 22, 2012
DMARC Spec – Policy Records

- TXT records in DNS
  - _dmarc.example.com

- Check for a record at the exact RFC5322.From
  - If no record is found, check for a record at the Organizational domain of the RFC5322.From

- Policy options:
  - “none” – simply monitor and supply feedback
  - “quarantine” – process email with high degree of suspicion
  - “reject” – do not accept email that fails DMARC check
### DMARC Spec – Policy Records

<table>
<thead>
<tr>
<th>Tag</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>Protocol Version</td>
<td>v=DMARC1</td>
</tr>
<tr>
<td>p</td>
<td>Policy for the domain</td>
<td>p=quarantine</td>
</tr>
<tr>
<td>sp</td>
<td>Policy for subdomains</td>
<td>sp=reject</td>
</tr>
<tr>
<td>pct</td>
<td>% of messages subject to policy</td>
<td>pct=20</td>
</tr>
<tr>
<td>adkim</td>
<td>Alignment mode for DKIM</td>
<td>adkim=s</td>
</tr>
<tr>
<td>aspf</td>
<td>Alignment mode for SPF</td>
<td>aspf=r</td>
</tr>
<tr>
<td>rua</td>
<td>Reporting URI for aggregate reports</td>
<td>rua@<a href="mailto:aggrep@example.com">mailto:aggrep@example.com</a></td>
</tr>
<tr>
<td>ruf</td>
<td>Reporting URI of forensic reports</td>
<td>ruf@<a href="mailto:authfail@example.com">mailto:authfail@example.com</a></td>
</tr>
<tr>
<td>rf</td>
<td>Forensic reporting format</td>
<td>rf=afrf</td>
</tr>
<tr>
<td>ri</td>
<td>Aggregate reporting interval</td>
<td>ri=14400</td>
</tr>
</tbody>
</table>
DMARC Spec – Example Policy Records

Everyone’s first DMARC record

v=DMARC1; p=none; rua=mailto:aggregate@example.com;
DMARC Spec – Example Policy Records

Dipping a toe in the pool

v=DMARC1; p=quarantine; pct=10; rua=mailto:agg@ex.com; ruf=mailto:fail@ex.com;
DMARC Spec – Example Policy Records

Very aggressive. 100% reject.

dig -t TXT _dmarc.facebookmail.com

v=DMARC1; p=reject; pct=100;
   rua=mailto:postmaster@facebook.com,mailto:d@rua.agari.com;
   ruf=mailto:d@ruf.agari.com;
Exercise 1
Is this a valid record?

p=none; pct=50; rua=postmaster@example.com;
Exercise 1
Is this a valid record?

```
p=none; pct=50; rua=postmaster@example.com;
```

Answer: No. The v= tag is required.
Exercise 2
What DNS TXT record will be queried for mail from foo.example.com?
Exercise 2
What DNS TXT record will be queried for mail from foo.example.com?

Answer: _dmarc.foo.example.com

If no record is found, what will happen?
Exercise 2
What DNS TXT record will be queried for mail from foo.example.com?

Answer: _dmarc.foo.example.com

If no record is found, what will happen?

Answer: _dmarc.example.com will be queried.
Exercise 3
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com;

Is this email Aligned?

Return-Path:postmaster@foo.example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com designates 10.1.1.1 as permitted sender) smtp.mail=postmaster@foo.example.com;
  dkim=pass header.i=@bar.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=bar.example.com; s=s1024-2011-q2; c=relaxed/simple;
  q=dns/txt; i=@bar.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=015o8r4ftEPBr083MbUpe0mIrWKR5yT46DR6CGk/Mk=;
  b=T6m3ZvppP3OLGNQVoR/l1W+RxSbQiRlaCcwZpXTF/xjWk0xjY1/8S0UvttFPHZ1l 0cy
  +svp5ymrqBgnDEN/ZQEcfmzYE0g1BNL/18z1MKpmVOf/9cLIpTVbaWi/G2VBY
  LXONpLsSymtoeqTBYOJgoiNLzDN0p1pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
DMARC Spec – Policy Record Exercises

Exercise 3
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com;

Is this email Aligned?

Return-Path:postmaster@foo.example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com designates 10.1.1.1 as permitted sender) smtp.mail=postmaster@foo.example.com;
   dkim=pass header.i=@bar.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=bar.example.com; s=s1024-2011-q2; c=relaxed/simple;
   q= dns/txt; i=@bar.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=015o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
   b=T6m3ZvppP3OLGNQVoR/1lW+RxSbQiRlaCcwZpXTP/xjWk0xjYl/8S0UUvtFPHZ1l 0cy+syp5ymrqBgnDEN/ZQEcFmzYEOg1BNL/I8z1MKpVOf/9cLIpTVbaWi/G2VBY
   LXONpLsSymtoeqTBYOJgoiNlzDNp01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>

Answer: Yes. Alignment is Relaxed by default.
Exercise 4
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com; adkim=s; aspf=r;

Is this email Aligned?

Return-Path: postmaster@example.com
Authentication-Results: mx.mail.com; spf=neutral (mail.com: domain of postmaster@example.com does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com; dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple; q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=015o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
b=T6m3ZvppP3OLGQVoR/l1W+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UvFPHZ11 0cy+syp5ymrBgnDEN/ZQEcfmzYEOg1BNL/I8z1MKPmVOf/9cLIpTVbaWi/G2VBY LXONpLsSymtoeqTBYOOJgoiNLzDNP0lpVGfYunf8h90=;
From: "Postmaster" <postmaster@example.com>
Exercise 4
Given this record for _dmarc.example.com:

```
v=DMARC1; p=none; rua=postmaster@example.com; adkim=s; aspf=r;
```

Is this email Aligned?

Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=neutral (mail.com: domain of postmaster@example.com does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com; dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple; q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=015o8r4ftEPBr083Mbupe0mIrWKRs5yT46DR6CGk/Mk=; b=T6m3ZvppP3OLGNOVoR/11W+RxSbQiRlaCcwZpXTF/xjWk0xjY1/8S0UUvtFPHZ1l 0cy+svp5ymrqBgnDEN/ZQEcflmzYEQOg1BNL/I8z1MKPmVOf/9cLIpTVbaWi/G2VBY LXONpLsSymtoeqTBY00JqoiNLzDP01pVgZUnf8h90=;
From: "Postmaster" <postmaster@example.com>

Answer: No. SPF did not pass. DKIM passed, but DKIM Alignment is in strict mode and the DKIM domain does not exactly match the From domain.
DMARC Spec – Policy Record Exercises

Exercise 4
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com; adkim=s; aspf=r;

Is this email Aligned?

Return-Path: postmaster@example.com
Authentication-Results: mx.mail.com; spf=neutral (mail.com: domain of postmaster@example.com does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
dkim=pass header.i=@foo.example.com

DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
    q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=01508r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
b=T6m3ZvppP3OLGNQVoR/l1w+RxBbQiRlaCcwwZpXTF/xjWk0xjY1/8S0UuvtFPHZ11 0cy+svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8z1MKPmVOf/9cLIpTVbaWi/G2VBYLXONpLsSymtoeqTBY00JgoiNLzDNP01pVgZYunf8h90=;

From: "Postmaster" <postmaster@example.com>

Then what will happen to the email?
Exercise 4
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com; adkim=s; aspf=r;

Is this email Aligned?

Return-Path: postmaster@example.com
Authentication-Results: mx.mail.com; spf=neutral (mail.com: domain of postmaster@example.com does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com; dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
  q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=01508r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
b=76m3ZvppP30LGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjY1/8S0UUvFPHZ11 0cy+svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8z1MKPmVOf/9cLIpTVbaWi/G2VBYLXONpLsSymtoeqTBYOOJgoiNLzDNP01pVgZYunf8h90=

From: "Postmaster" <postmaster@example.com>

Then what will happen to the email?

Answer: No policy action will be taken. The results will be included in the requested aggregate report and the message will be processed as normal.
DMARC Spec – Policy Record Exercises

Exercise 5
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
  adkim=s; aspf=s; sp=reject;

Is this email Aligned?

Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
  q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=015o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
b=T6m3ZvppP3OLGNQVoR/11W+RxBqRl1cCcwZpXTF/xjWk0xjYl/8S0UUVtFPHZ11 0cy+syp5ymrBgnDEN/ZQEcYmzYE0g1BNL/I8zJMnPmVOf/9cLIpTVbaWi/G2VBY
LXONpLsSymtoeqTBY0OJgo1NLzZDP01pVgZYnu8h90=;
From: "Postmaster" <postmaster@bar.example.com>
Exercise 5
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
   adkim=s; aspf=s; sp=reject;

Is this email Aligned?

Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
   q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=01508r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiR1aCcwwZwUy jo/sXjWk0xjY1/8S0UUvtEPHZ1l_0cy
   +svp5ymrqBgnDEN/ZQEcWdzgYEOg1BNL/18z1MKPmVOf/9cLiPTVbaWi/G2VBY
   LXONpLsSsymteqTBVY0OJgoiNLzDNF01lVgZYunf8h90=
From: "Postmaster" <postmaster@bar.example.com>

Answer: Trick question! It depends on whether or not there is a DMARC record at _dmarc.bar.example.com.
Exercise 5
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
  adkim=s; aspf=s; sp=reject;

If there is no record at _dmarc.bar.example.com, is this email Aligned?

Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
  q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type;
  bh=0l5o8r4ftEPBr083MbUpe0mIrWKR5yT46DR6CGk/Mk=;
b=T6m3ZvppP3OLGNQVoR/llW+RxBQ1R1aCcwZpXTF/xjWk0xjY1/8S0UUvtFPHZ1l 0cy
  +svp5ymrqBgnDEN/ZQEcfmzYEo1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
  LXONpLsSymtoeqTBYY0Jgo1NLzDNp01pVgZunf8h90=;
From: "Postmaster" postmaster@bar.example.com
Exercise 5
Given this record for _dmarc.example.com:

\[v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com\]
\[\text{adkim=s; aspf=s; sp=reject};\]

If there is no record at _dmarc.bar.example.com, is this email Aligned?

Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
g=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=015o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ11 0cy+svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8z1MKPmVOf/9cLIpTVbaWi/G2VBY
LXONpLsSyntoeqTBYOOJgoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" postmaster@bar.example.com

Answer: No. Both SPF and DKIM are in Strict Alignment mode and neither exactly match the From domain.
Exercise 5
Given this record for _dmarc.example.com:

v=DMARC1; p=none; rua=postmaster@example.com; ruf=postmaster@example.com
  adkim=s; aspf=s; sp=reject;

If there is no record at _dmarc.bar.example.com, is this email Aligned?

Return-Path:postmaster@example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@example.com
does not designate 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com;
dkim=pass header.i=@foo.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=foo.example.com; s=s1024-2011-q2; c=relaxed/simple;
  q=dns/txt; i=@foo.example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type;
bh=01508r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRilaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHHZ1l 0cy
  +svp5ymrBgnDEN/ZQEcfmzyEOg1BNL/I8z1MKPmVOf/9cLIpTVbaWi/G2VBY
  LXONpLsSymtoeqTBvOJgoiNLzDNF01pVgZYunf8h90=;
From: "Postmaster" postmaster@bar.example.com

Then what will happen to the email?
Answer: It will be rejected due to the subdomain policy action sp=reject. The results will be
included in the requested aggregate report, and a forensic report will be sent.
This has been the third of six DMARC video segments

View the entire

**M³AAWG DMARC Training Series**

from the public training video pages on the M³AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Michael Adkins, Paul Midgen and DMARC.org
for developing the material in this series
and allowing M³AAWG to videotape it for professionals worldwide.

This video is presented by the
Messaging, Malware and Mobile Anti-Abuse Working Group
For information about M³AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form