DMARC Training – SANOGxxiv

Kurt Andersen
KurtA@linkedin.com
@DrKurtA

Based upon work done by Michael Adkins and Paul Midgen
with contributions from Tim Draegon, ReturnPath and Cloudmark
Information provided by
Tim Draegen, Principal, dmarcian.com

tim@dmarcian.com

EMAIL REPORT CARD
WHERE ARE WE?
Just How Big Is This Thing?

This is really big. Lots of people have been trying to fix this thing for a long time.

Email is the most used, most valuable and highly-priced real estate on the Internet. This is why everyone wants it.

and it's actually changing!

The total number of searches on Google, Yahoo, and Bing combined is just 0.3% of all email traffic.

WHAT DOES THIS ADD UP TO?

THE VALUE OF EMAIL

- 2.5 Billion users
- 3.5 Billion searches
- 1.5 Billion pageviews

Research by: SmartInsights
Cyclical Adoption Cycles

2003-2006: building blocks (SPF, DomainKeys, DKIM)
   “I’ve heard this helps”
   Nice to have as anti-spam input, not reliable

2007-2009: prototype authenticated email model
   PayPal innovates, Financial Services publishes recommendations
   Yahoo & Gmail reject fake PayPal email, other big providers take note

2010-2011: make it work at internet scale
   PayPal funds/organizes effort to standardize the model
   Big webmail providers commit to support and implement

2012-2013: early adopters
   Senders with fraud and clean infrastructures deploy
   Big consumer mailboxes and those that can roll their own deploy

DMARC Current Adoption

**BIG RECEIVERS:**

dmarcian automatically processes data for its users. The following table shows receivers that have supplied DMARC XML data to dmarcian.com, effectively showing the current DMARC receiver footprint.

<table>
<thead>
<tr>
<th>Provider</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>facebook.com</td>
<td>1.15 billion</td>
</tr>
<tr>
<td>NetEase (163.com, 126.com, 188.com, yeah.net)</td>
<td>570 million</td>
</tr>
<tr>
<td>google.com</td>
<td>425 million</td>
</tr>
<tr>
<td>Microsoft Corp. (outlook.com)</td>
<td>400 million</td>
</tr>
<tr>
<td>Mail.Ru</td>
<td>300 million</td>
</tr>
<tr>
<td>Yahoo! Inc.</td>
<td>298 million</td>
</tr>
<tr>
<td>linkedin.com</td>
<td>238 million</td>
</tr>
<tr>
<td>Comcast</td>
<td>?</td>
</tr>
<tr>
<td>AOL</td>
<td>?</td>
</tr>
<tr>
<td>xs4all.nl</td>
<td>1 million</td>
</tr>
<tr>
<td>dmarc.org</td>
<td>?</td>
</tr>
<tr>
<td>andreasschulze.de</td>
<td>19</td>
</tr>
<tr>
<td>...many other low volume providers</td>
<td>?</td>
</tr>
</tbody>
</table>

**Total: 3.382 billion**
(updated: 13 Sept 2013)

**“ORGANIC” RECEIVERS:**

horizonlinux.org
Ivenue.com
junc.org
gcsdns.net
The Art Farm
dmarc.org
inteligis.ro
padz.net
newsbox.ro
CommuniGate, Inc
sapienti-sat.org
rosenkeller.org
mvps.org
laussat.info
thesandiegos.com
harrison-salmon.co.uk
llamas.net
castlehoward.co.uk
manda.tagmail.eu
prosper-ifa.co.uk
ceotex.de
bordo.com.au
midrange.com
vande-walle.eu
feha-imo.de
visp.mx
farron.co.uk
darkblue.co.uk
thockar.com
lehibe.eu
amstenrade.net
applemooz.nl
[core.at]
postaro.com
croakingduck.com
pac-hs.co.uk
entourage.mvps.org
activesynergy.org
AGARI
middlestudlehurstdfarm.co.uk
de-verbinding.org
nopourriel.fr
cisco.com
blr-esx.com
kestral.com.au
jrschneider.com
m brown.co.uk
amfes.com
winstanleysbikes.com
MVPS.ORG
lists.mvps.org
score42.tagmail.eu
fdwebdesign.nl
telesiscomms.com
fcbank.com.ua
blackops.com
cuckoobag.com
knoors.nl
yaplik.cz
What DMARC Can (and Cannot) Do

DMARC fixes a fundamental flaw:
• Is this email really from where it says it’s from?

DMARC makes Domain Identifiers a reality:
• This email really does come from EXAMPLE.ORG!

So what:
• Strong exact-domain anti-phishing (“Reject the fakers”)
• Domain reputation, finally! (“Do my users want this?”)
• Easier decision making. Pull out the known good so that anti-spam can go crazy on the grey stuff.
• Build it once, tell senders exactly what hoops they need to jump through. And these are not special hoops!
Outline

Part 1

• Introduction to DMARC
  • Purpose and Goals
  • History
  • Roadmap

• DMARC Spec Overview
  • Identifier Alignment
  • DMARC Policy Records
  • Reporting

• Break

Part 2

• Information for Mailbox Providers
  • DMARC Policy Enforcement
  • Aggregate Reporting
  • Forensic Reporting

• Lessons Learned in Provider Deployments

• Time Permitting:
  • Information for Domain Owners
    • The Reporting and Compliance Process
      • Initial Record Publishing
      • 3rd Party Deployment Profiles
      • Report Processing and Analysis
      • Initial Policy Ramp-up
      • Ongoing Monitoring
Things we won’t cover

• Why phishing is a problem.

• How DKIM, SPF, DNS, SMTP, or XML work.

• How to combat abuse of cousin domains or the display name field.

• Phishing website investigation or takedown services.
Who is in the audience?

- Mailbox providers?
- Domain owners?
- Domain owners who use 3rd party senders?
- 3rd party senders (ESPs, hosting providers, etc)?
What does the audience want?
Intro to DMARC

DMARC = Domain-based Message Authentication, Reporting, and Conformance

• Authentication – Leverage existing technology (DKIM and SPF)

• Reporting – Gain visibility with aggregate and per-failure reports

• Conformance – Standardize identifiers, provide flexible policy actions
Intro to DMARC – Purpose and Goals

• Open version of existing private mechanisms for preventing domain spoofing.

• Standardize use of authenticated identifiers.

• Provide insight into and debugging aids for your authentication practices.

• Encourage wider adoption of SPF & DKIM.

• Encourage iteration toward aggressive authentication policy.
Intro to DMARC – Non-Goals

• Address cousin domain abuse
• Address display name abuse
• Provide MUA treatment advice
• An enterprise security solution
• An incident response tool
• Provide delivery reporting
Intro to DMARC – History

• Private Prototype between Paypal and Yahoo – 2007

• Vendors being offering similar functionality – 2009 to present

• First Prototype DMARC records published – Feb ’11

• Draft specification released – Jan 30th 2012, revised April ’12

• Significant adoption since that time

• Currently (Summer 2014) forming an IETF WG to make the standard official
DMARC – Success Numbers for Senders & Recipients

• Nearly **2 billion** email accounts worldwide are protected

• Greater than **80%** of typical users are protected worldwide
  – Microsoft: Hotmail/Outlook/Live/Office 365
  – AOL
  – Gmail
  – Yahoo
  – Netease: 163.com/126.com
  – Mail.ru

• Over **80,000** active domains have deployed DMARC records
DMARC – Success Numbers for Brands

• Paypal:
  – More than **25 million** spoofed email messages were rejected during the 2013 holiday buying season.

• Twitter:
  – During the first 45 days of initial monitoring, nearly **2.5 billion** spoof messages were seen
  – Before DMARC: ~**110 million** messages/day
  – After DMARC: **1,000/day** after publishing a "reject" policy

• Publishers Clearing House reports they used DMARC to block over **100,000** unauthenticated messages in a single 90 day period during 2013.
DMARC Spec Overview

1. Check SPF & DKIM
2. DMARC Identifier Alignment
3. Act on unaligned mail
DMARC Spec – Identifier Domain Alignment

- DMARC tests and enforces **Identifier Domain Alignment**

- Authenticated identifier domains are checked against Mail User Agent (MUA) visible “RFC5322.From” domain:

  - SPF: **RFC5321.From** domain
  - DKIM: “d=” domain

- Only one authenticated identifier domain has to align for the email to be considered “in alignment”
DMARC Spec – Identifier Alignment

- DMARC record publishers (domain owners) can require
  - strict identifier alignment (full domain matches exactly), or
  - permit relaxed alignment (organizational domain match)
DMARC Spec – Organizational Domains

- Delegation level + 1 atom
  - groups.facebook.com → facebook.com
  - aol.co.uk → aol.co.uk
  - foo.bar.example.ne.jp → example.ne.jp
  - a45.compute.amazonaws.cn → a45.compute.amazonaws.cn
  - a.b.example.co.in → example.co.in

- Uses publicsuffix.org for TLD list

- More robust methods being considered and discussed in the IETF appswg
Return-Path: postmaster@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@example.com; dkim=pass header.i=i@example.com
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=s1024-2011-q2; c=relaxed/simple; q=dns/txt; i=i@example.com; t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type; bh=015o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=; b=T6m3ZvppP3OLGNQVoR/11W+RxSbQiRlaCcwZpXTF/xjWk0xjY1/8S0UUvtFPHZ1l0cy+svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8z1MKPmVOf/9cLIpTVbaWi/G2VBYLXONpLsSymtoeqTBYO OJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>

- 5322. From domain = example.com
- SPF domain = example.com
- DKIM domain = example.com
Return-Path: postmaster@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@example.com
From: "Postmaster" <postmaster@example.com>

• 5322.From domain = example.com
• SPF domain = example.com
• DKIM domain → none
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=@example.com
DKIM-Signature: v=1; a=rsa-sha256; d=example.com;
s=s1024-2011-q2; c=relaxed/simple; q=dns/txt;
i=@example.com; t=1337318096; {. . .}
From: "Postmaster" <postmaster@example.com>

- 5322. From domain = example.com
- SPF domain → doesn’t matter, SPF did not pass
- DKIM domain = example.com
DMARC Spec – Alignment Examples – Failure

Return-Path: postmaster@phish.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@phish.com designates 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com; dkim=fail header.i=@example.com
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=s1024-2011-q2; c=relaxed/simple; q=dns/txt; i=@example.com; t=1337318096; {...}
From: "Postmaster" <postmaster@example.com>

- 5322. From domain = example.com
- SPF domain = phish.com → not aligned
- DKIM domain → doesn’t matter, DKIM authentication failed
DMARC Spec – Alignment Examples – Strict → Not 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@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=@facebookmail.com; t=1337318096; {. . .}
From: "Postmaster" <postmaster@example.com>

- 5322.From domain = example.com
- SPF domain = foo.example.com
- DKIM domain = bar.example.com
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; { . . . }
From: "Postmaster" <postmaster@example.com>

- 5322. From domain = example.com
- SPF domain = foo.example.com (org = example.com)
- DKIM domain = bar.example.com (org = example.com)
DMARC Spec – Alignment Examples – Relaxed

Return-Path: postmaster@bounce.example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@bounce.example.com designates 10.1.1.1 as permitted sender)
smtp.mail=postmaster@bounce.example.com; dkim=pass
header.i=@bounce.example.com
DKIM-Signature: v=1; a=rsa-sha256; d=bounce.example.com;
s=s1024-2011-q2; c=relaxed/simple; q=dns/txt;
i=@bounce.example.com; t=1337318096; {. . .} From: "Postmaster" <postmaster@foo.example.com>

• 5322. From domain = foo.example.com → org = example.com
• SPF domain = bounce.example.com → org = example.com
• DKIM domain = bounce.example.com → org = example.com
DMARC Spec – Alignment Examples – SPF Only

Return-Path: postmaster@bounce.example.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@bounce.example.com designates 10.1.1.1 as permitted sender)
smtplib.mail=postmaster@bounce.example.com
From: "Postmaster" <postmaster@foo.example.com>

- 5322.From domain = foo.example.com → org = example.com
- SPF domain = bounce.example.com → org = example.com
DMARC Spec – Alignment Examples – DKIM only

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; {. . .}
From: "Postmaster" <postmaster@example.com>

• 5322. From domain = example.com
• DKIM domain = foo.example.com → org = example.com
Return-Path: postmaster@phish.com
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of postmaster@phish.com designates 10.1.1.1 as permitted sender) smtp.mail=postmaster@example.com.com; dkim=fail header.i=@example.com
DKIM-Signature: v=1; a=rsa-sha256; d=bar.example.com; s=s1024-2011-q2; c=relaxed/simple; q=dns/txt; i=@example.com; t=1337318096; {...}
From: "Postmaster" <postmaster@example.com>

• 5322. From domain = example.com
• SPF domain = phish.com
• DKIM n/a – failed
**DMARC Spec – Alignment Exercises**

**Exercise 1 – Is SPF in Strict Alignment?**

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=@example.com
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=s1024-2011-q2; c=relaxed/simple; q=dns/txt; i=@example.com; t=1337318096; {. . .}
From: "Postmaster" <postmaster@example.com>

---

Answer: No, SPF did not pass.

**Is the email Aligned anyway?**

Answer: Yes, DKIM is in Strict Alignment, so the email is Aligned regardless.
Exercise 2 – Is SPF in Relaxed Alignment?

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@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=@facebookmail.com; t=1337318096; {...}
From: "Postmaster" <postmaster@example.com>

Answer: Yes, foo.example.com shares the same Organizational domain as example.com.

Additional question: Is DKIM in alignment?

Answer: Yes, but only if relaxed alignment is allowed.
DMARC Spec – Alignment Exercises

Exercise 3 – Is DKIM in Strict Alignment?

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; {...}
From: "Postmaster" <postmaster@example.com>

Answer: No, foo.example.com does not exactly match example.com

Under what conditions would the email be Aligned?

Answer: Since SPF does not pass, the email would only be Aligned if Relaxed DKIM Alignment was allowed.
DMARC Spec – Alignment Exercises

Exercise 4 – Under what conditions would this email be considered in alignment?

Return-Path: postmaster@foo.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@foo.example.com; dkim=fail
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; {. . .}
From: "Postmaster" <postmaster@example.com>

Answer: None. Neither DKIM nor SPF are valid.

Assuming DKIM and SPF were actually valid, under what conditions would this email be consideredAligned?

Answer: If Relaxed Alignment was allowed for either DKIM or SPF, the email would be Aligned.
DMARC Spec – Policy Records

• TXT records in DNS
  • _dmarc.example.com

• Check for a record at the exact 5322.From
  • If no record is found, check for a record at the Organizational domain of the 5322.From

• Policy action 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 Record Components

<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>fo</td>
<td>Forensic reporting trigger</td>
<td>fo=1</td>
</tr>
<tr>
<td>ri</td>
<td>Aggregate reporting interval</td>
<td>ri=14400</td>
</tr>
</tbody>
</table>
## DMARC Spec – Policy Record Defaults

<table>
<thead>
<tr>
<th>Tag</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>Protocol Version</td>
<td><em>no default, this is must be explicit</em></td>
</tr>
<tr>
<td>p</td>
<td>Policy for the domain</td>
<td><em>no default, this is must be explicit</em></td>
</tr>
<tr>
<td>sp</td>
<td>Policy for subdomains</td>
<td><em>inherits p= setting</em></td>
</tr>
<tr>
<td>pct</td>
<td>% of messages subject to policy</td>
<td>100</td>
</tr>
<tr>
<td>adkim</td>
<td>Alignment mode for DKIM</td>
<td>r (relaxed)</td>
</tr>
<tr>
<td>aspf</td>
<td>Alignment mode for SPF</td>
<td>r (relaxed)</td>
</tr>
<tr>
<td>rua</td>
<td>Reporting URI for aggregate reports</td>
<td><em>none</em></td>
</tr>
<tr>
<td>ruf</td>
<td>Reporting URI of forensic reports</td>
<td><em>none</em></td>
</tr>
<tr>
<td>rf</td>
<td>Forensic reporting format</td>
<td>afrf</td>
</tr>
<tr>
<td>fo</td>
<td>Forensic reporting trigger</td>
<td>0 (all mechanisms failed)</td>
</tr>
<tr>
<td>ri</td>
<td>Aggregate reporting interval</td>
<td>86400 (24h)</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

Begin some enforcement... 

v=DMARC1; p=quarantine; pct=10; 
rua=mailto:agg@example.com;

or, with forensic reports:

v=DMARC1; p=quarantine; pct=10; 
rua=mailto:agg@example.com; 
ruf=mailto:fail@example.com;
Well controlled mail streams can do 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;
DMARC Spec – Policy Record Exercises

Exercise 1 – Is this a valid record?

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

Answer: No. The v= tag is required as the first component.
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.
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; {. . .}
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; {...}
From: "Postmaster" <postmaster@example.com>
```

Then what will happen to the email?

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.

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 designates 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; { . . .}
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.

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

Answer: No. Both SPF and DKIM are in Strict Alignment mode and neither exactly match the From domain.

Then, what will happen to the email? example.com, is this email aligned?

Answer: It will be rejected due to the subdomain policy action sp=reject. The answer will be the email is not compliant with the DMARC policy and is rejected.
Protecting Parked Domains

• No mail is sent from this domain
  – SPF: v=spf1 -all

• No mail is received by this domain
  – “Null” MX: “MX 0 .”

• But tell me about any attempts to abuse this domain
  – DMARC: v=DMARC1; p=reject; rua=report@example.com

• Example: gmail.co (Columbian TLD mis-spelling for gmail.com):
  – v=spf1 -all
  – v=DMARC1; p=reject; rua@mailto:mailauth-reports@google.com
DMARC Spec – Reporting

Aggregate Reports

• Each report covers one 5322. From domain.
• You should get one from each supporting mailbox provider that sees email with your From domain.
• Daily by default, adjustable with ri= tag.
  For instance: hourly : ri=3600

XML Format
• Organized by sending IP address
• Contains
  • Authentication Results (DKIM, SPF)
  • Alignment Results
  • Policy actions taken
  • Reasons for not taking policy actions

Just publish a record to see one
DMARC Spec – Reporting

XML Format

The policy they found.
<policy_published>
    <domain>facebookmail.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>none</sp>
    <pct>100</pct>
</policy_published>
DMARC Spec – Reporting

XML Format
An example record.
<record>
  <row>
    <source_ip>106.10.148.108</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>facebookmail.com</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>facebookmail.com</domain>
      <result>pass</result>
    </dkim>
    <spf>
      <domain>NULL</domain>
      <result>none</result>
    </spf>
  </auth_results>
</record>
DMARC Spec – Reporting

Forensic Reports

• One per DMARC failure
• AFRF or IODEF formats
• Should at least include ‘call-to-action’ URIs
• Throttling

• Privacy issues
  • Might be redacted
  • Might not be supported by all receivers that otherwise support DMARC
Verifying 3rd party report destinations

If the record for example.com contains reporting URIs at other domains:

    mailto:aggregate@foo.com

Report generators should verify that foo.com expects the reports by looking for:

    example.com._report._dmarc.foo.com

The 3rd party can change the URI to a different address in their domain:

    v=DMARC1; rua=mailto:reports@foo.com
Break
For Domain Owners (Brands)
Information for Domain Owners

- The Reporting and Compliance Process
  - Initial Record Publishing
  - 3rd Party Deployment Profiles
  - Report Processing and Analysis
  - Rolling out Policies
  - Long Term Monitoring
The Reporting and Compliance Process For Domain Owners

Phase 1: Initial Auditing
- Publish Initial Record
- Process Reports
- Fix Infrastructure Issues

Phase 2: Initial Policy Ramp-up
- Assess Initial Threat Level
  - Abuse Detected
  - No Abuse Detected
- Process Reports
- Make Policy Changes

Phase 3: Ongoing Monitoring
- Assess Current Threat Level
- Make Policy Changes / Other Response
Initial Record Publishing

Everyone’s first DMARC record

v=DMARC1; p=none; rua=mailto:aggregate@example.com;
3rd Party Deployment Profiles

Controlled – The Domain Owner fully controls their own DNS, and wants as much control over their email as possible.

Authorized – The Domain Owner lets the 3rd party dictate the content of some DNS records, while still retaining some operational control.

Delegated – The Domain Owner delegates control of their DNS to the 3rd party, and wants to be mostly hands-off with their email.

Hosted – The Domain Owner allows the 3rd party to handle everything, and has little control.
3rd Party Deployment Profiles

Controlled

The Domain Owner retains control of the domain or subdomain, provides a DKIM signing key to 3rd party and publishes the public key, and includes the appropriate information in their SPF record.

Pro
- This scenario allows 3rd parties to send as the organizational domain if desired.
- The Domain Owner retains operational control.

Cons
- Coordination between the domain owner and the 3rd party mailer is required to ensure proper DKIM key rotation, accurate SPF records, etc.
- Risk of coordination overhead/issues increases as the number of bilateral relationships increase for domain owners and vendors.
3rd Party Deployment Profiles

Controlled

Contractual points

• Process for DKIM key rotation. Obligations of each party, including testing.

• SPF record requirements and process for adding new hosts.
3rd Party Deployment Profiles

Authorized

Similar to Controlled Profile, except the 3rd party creates the DKIM key pair and generally takes a more active role in dictating record content. This approach is useful for Domain Owners where a different 3rd party is providing DNS and other services for the domain.

Pros
• Can streamline provisioning for the 3rd party.
• One less task for the Domain Owner.

Cons
• Can create additional management issues for Domain Owners who use multiple 3rd parties.
• Possible additional contractual point for key strength requirements.
3\textsuperscript{rd} Party Deployment Profiles

Delegated

The Domain Owner delegates a subdomain to 3rd party mailer and relies on contractual relationship to ensure appropriate SPF records, DKIM signing, and DMARC records.

Pros

• Reduces Domain Owner implementation issues to mostly contractual.
• The 3rd party is responsible for SPF records, DKIM signing and publishing, etc.
• Domain owner may still be responsible for ensuring Identifier Alignment.

Con

• The Domain Owner potentially gives up day to day control and visibility into operations and conformance.
3rd Party Deployment Profiles

Delegated

Contractual points
• Creation and maintenance of SPF, DKIM and DMARC records
• (At least every 6 months) Rotation of DKIM keys and minimum length of key (1024 recommended)
• Investigation of DMARC rejections
• Handling of DMARC Reports
• Requirements for reporting back to the Domain Owner
• Indemnification (if any) for mail lost due to improper records or signatures.
3rd Party Deployment Profiles

Hosted

The 3rd party is also providing DNS, webhosting, etc for the Domain Owner and makes the process mostly transparent to the domain owner.

Pro
• Very easy for less sophisticated Domain Owners.
• Can be mostly automated by the 3rd party.

Con
• The domain owner is significantly more dependent on the 3rd party.
### 3rd Party Deployment Profiles

#### 3rd Party responsibilities

<table>
<thead>
<tr>
<th></th>
<th>Controlled</th>
<th>Authorized</th>
<th>Delegated</th>
<th>Hosted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide SPF record content</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Maintain SPF records</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Maintain DKIM records</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Create DKIM Keys</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Rotate DKIM Keys</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Maintain DMARC Records</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Process DMARC reports</td>
<td>N</td>
<td>?</td>
<td>?</td>
<td>Y</td>
</tr>
</tbody>
</table>
Report Processing and Analysis

Phase 1: Initial Auditing
- Publish Initial Record
- Process Reports
- Fix Infrastructure Issues
- Assess Initial Threat Level
  - Abuse Detected
  - No Abuse Detected

Phase 2: Initial Policy Ramp-up
- Process Reports
- Make Policy Changes
- Fix Infrastructure Issues

Phase 3: Ongoing Monitoring
- Process Reports
- Assess Current Threat Level
- Make Policy Changes / Other Response
- Fix Infrastructure Issues
Report Processing and Analysis

Report Parsing Tools

http://dmarc.org/resources.html

If you develop report parsing tools you are willing to share, please send a note to the dmarc-discuss list and let us know.
Report Processing and Analysis

Step 1: Categorize the IPs in the Aggregate Report

- Your Infrastructure
- Authorized 3rd Parties
- Unauthorized 3rd Parties *

* - You should consider everything an Unauthorized 3rd Party by default.
Step 2: Infrastructure Auditing

For both your Infrastructure and Authorized 3rd Parties

- Identify owners
- LOE for Deploying Domain Authentication
- LOE for Identifier Alignment
- Business case / Justification
Step 3: Identify Malicious Email

Research Unauthorized 3\textsuperscript{rd} Parties and label the Abusers

- Use public data sources
- Vendor services
- Look for known failure cases
- Forensic reports
Step 4: Perform Threat Assessment

Categories
- Your Infrastructure
- Authorized 3rd parties
- Unauthorized 3rd parties
- Abusers

Calculate the Sum of Unaligned Email from each Category
Report Processing and Analysis

Step 4: Perform Threat Assessment

**Phish** = Unaligned Email From Abusers

**Definite False Positives** = Unaligned Email from Your Infrastructure + Unaligned Email from Authorized 3rd parties

**Potential False Positives** = Unaligned Email from Unauthorized 3rd parties

**Consider:**
- Phish vs. False Positives
- Phish vs. Total Aligned Email

If there is no Phish, you don’t have a Domain Spoofing problem and don’t need to move forward with DMARC policies.
**Initial Policy Ramp-up**

**Phase 1: Initial Auditing**
- Publish Initial Record
- Process Reports
- Fix Infrastructure Issues

**Assess Initial Threat Level**
- Abuse Detected
- No Abuse Detected

**Phase 2: Initial Policy Ramp-up**
- Process Reports
- Make Policy Changes

**Phase 3: Ongoing Monitoring**
- Process Reports
- Fix Infrastructure Issues
- Make Policy Changes / Other Response
- Assess Current Threat Level
Initial Policy Ramp-up

Step 1: Verify Authentication and Alignment for all of your Infrastructure and all Authorized 3rd Parties.

Step 2: Update your record to:

p=quarantine; pct=10;

Do not:
• Skip ‘quarantine’ and go straight to ‘reject’
• Change the policy action from ‘none’ without setting a ‘pct’
Initial Policy Ramp-up

Step 3: Monitor your reports for issues and address them. Make a ‘go forward / go back’ decision.

Step 4: Update your record to increase the ‘pct’.

Rinse and repeat until you get to ‘pct=100’.
Initial Policy Ramp-up

Step 5: If needed, update your record to:

\[ p=\text{reject} \]
Ongoing Monitoring

Phase 1: Initial Auditing
- Publish Initial Record
- Process Reports
- Fix Infrastructure Issues

Phase 2: Initial Policy Ramp-up
- Process Reports
- Make Policy Changes

Phase 3: Ongoing Monitoring
- Assess Current Threat Level
- Assess Initial Threat Level
  - No Abuse Detected
  - Abuse Detected
- Process Reports
- Fix Infrastructure Issues
- Make Policy Changes / Other Response
Ongoing Monitoring

- Categorize new IPs in Aggregate reports
  - Your Infrastructure
  - Authorized 3rd Parties
  - Unauthorized 3rd Parties
  - Abusers

- Reassess the Threat Level
  - Increases in phish
  - Changes in unaligned email volume
  - Make changes accordingly
  - Takedowns or other phish responses
Ongoing Monitoring

Be on the look out for:
• Infrastructure changes
• New products / new subdomains
• New authorized 3rd parties
• Mergers and acquisitions
For Mailbox Providers
Information for Mailbox Providers

Are you ready for DMARC?

• Do you need DMARC?
  • Understand what DMARC does for the messaging ecosystem.
  • Who are you receiving mail from?

• Review your SPF and DKIM practices.
  • Why validate both?

• Develop a local-policy strategy.
  • Special cases
  • Trusted domains

• Commit to Reporting

• Outbound?
Information for Mailbox Providers

Policy Enforcement in Review

• Evaluate SPF & DKIM according to the RFC.
  • Bonus points: use Authentication-Results

• Select applicable authentication results using alignment.
  • This only determines whether the results are used.

• No aligned and passing results? DMARC validation has failed – time to enforce!
  • None: message disposition is unchanged; “report only”
  • Quarantine: don’t deliver to the inbox.
  • Reject: don’t deliver at all.
Information for Mailbox Providers

Reporting in Review

Aggregate Reporting
• XML data correlating IPs, domains, and authentication results.

• Requires ability to aggregate & store data extracted from inbound messages. This can require a lot of storage.

• Specification is currently least-documented part of DMARC, join dmarc-discuss and ask questions.

Failure Reporting
• Copies of messages failing DMARC validation sent to the sender or their agent.

• Don’t queue. Sending as close to receipt as possible maximizes value.
Operational Considerations

- DMARC policy is the sender’s policy and should have higher priority than local and other policy.

- Consider ways to mitigate the impact of MLMs, forwarders, and so on.
  - These waters are deep. Fish with large teeth. Be deliberate, researched, and iterative.
Information for Mailbox Providers

Reporting and Privacy

*Forensic reports can send an unaltered message to someone other than the intended recipient.*

*It may not be from a bad actor.*

- A privacy analysis pertaining to the EU has been done and can be privately shared. Contact me if you are interested.

- Understand applicable privacy regimes before sending reports.
  - Corporate
  - Federal/Legal
Information for Mailbox Providers

Effect on Inbound Email @ Hotmail

- Based on private-channel policy.
- Policies move from quarantine to reject based on comfort.
- Steady growth in reject rate is good, wish magnitude were bigger.
Resources

Dmarc.org

Resources page for tools: dmarc.org/resources.html
LESSONS LEARNED & KNOWN ISSUES/PITFALLS

Courtesy of Cloudmark
Rollout Considerations – Overview

- DMARC has many moving parts
  - Both in protocol and technically
  - Plan rollout carefully
  - Partial controlled rollouts to gain experience
    - Find & work with sender partners (banks!)
    - Get vendor support if available
- Many benefits even with partial implementations
- ISPs: you are a *receiver*, not a *sender*
Rollout Planning – Infrastructure

• Most platforms have sufficient headroom, but
• Strong Requirements:
  – MTA support for DKIM, SPF, DMARC
  – MTA can reject in-line after DATA
  – Log storage
    • Aggregate: efficient custom logs only few % extra for typical MTA.
      Archive?
    • Forensic: archive full messages?
  – Will actually save a few % message storage
Rollout Considerations – Technical

- Performance impact: not a major issue
  - Apply DMARC (DKIM/SPF) only on relevant traffic
  - No benefit in authenticating obvious spam, so
  - Use DNSBLs / IP reputation to reject really bad stuff
  - DKIM crypto impact dwarfed by content scans etc
  - Consider implementing reporting out-of-band
  - But: potentially measurable extra DNS traffic
Rollout Considerations – Technical

• Allow for exceptions
  – SPF and DKIM don’t always play well with forwarded traffic & mailing lists
  – Use IP-reputation data to (de) select candidates
    • But keep in mind that ISP outbounds are a favorite for phishers to use
• Controlled rollout
  – Apply only to select domains at first
  – Allow overriding pct & p= value locally
Rollout Considerations – Policy

- Pro arguments
  - Supports ISP and sender “duty of care”
- Receiver has final control over how DMARC is applied
- Protection measures that balance security & privacy
- When in doubt, partial implementation is better than no implementation at all
Rollout Considerations – Policy

• Privacy issues – general
  – DMARC does not consider *content* or *recipient*
  – Senders participate *voluntarily* and *have authority on* how their domain is used

• Privacy issues – reporting
  – Aggregate reporting generally acceptable
  – Forensic reporting risky under EU rules
  – When in doubt, DO implement but DON’T report