DMARC Training

Kurt Andersen

Based upon work done by Michael Adkins and Paul Midgen

Outline

Part 1

- Introduction to DMARC
  - Purpose and Goals
  - History
  - Roadmap
- DMARC Spec Overview
  - Identifier Alignment
  - DMARC Policy Records
  - Reporting
- Short Break

Part 2

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

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.

What does the audience want?

Who is in the audience?

- Mailbox providers?
- Domain owners?
- Domain owners who use 3rd party senders?
- 3rd party senders (ESPs, hosting providers, etc)?

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.
- Incent 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

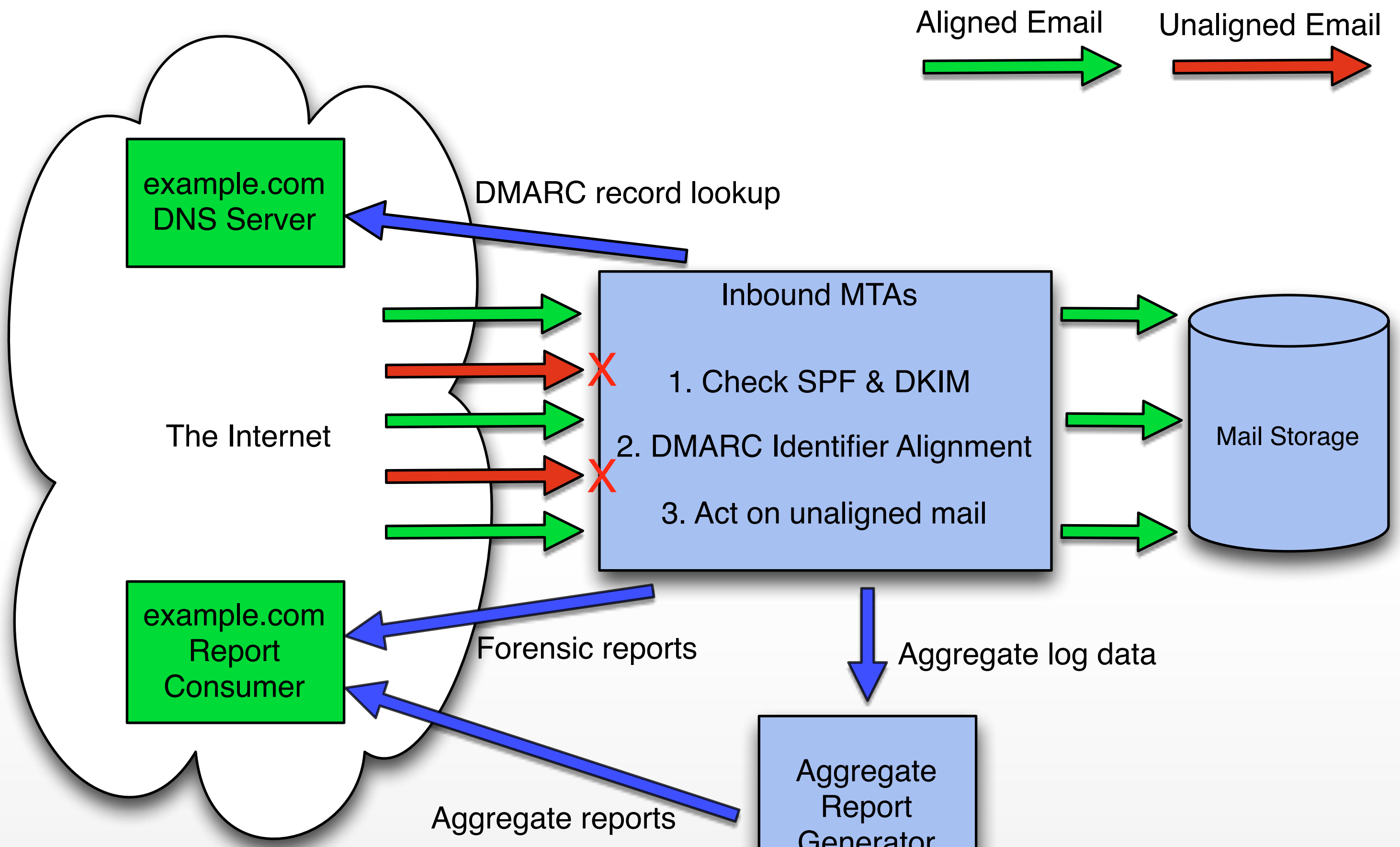
Intro to DMARC - History

- 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

Intro to DMARC - Roadmap

- Interop Event - July '12
- Produce a final draft
- Submit to the IETF

DMARC Spec Overview



DMARC Spec – Identifier Alignment

- DMARC tests and enforces Identifier Alignment
- Authenticated Identifiers are checked against Mail User Agent (MUA) visible "RFC5322.From" domain
- Only one Authenticated Identifier has to Align for the email to be considered in Alignment

DMARC Spec – Identifier Alignment

- Identifier Alignment can be strict (match exactly) or relaxed:
  - Relaxed SPF: The Organizational Domain of the SPF Authenticated RFC5321:Mail From and RFC5322:From must match.
  - Relaxed DKIM: The Organizational domain from 'd=' value of DKIM authenticated signature and RFC5322.From must match.

DMARC Spec – Identifier Alignment

Organizational Domain

- TLD + 1 atom
  - groups.facebook.com = facebook.com
  - aol.co.uk = aol.co.uk
  - foo.bar.example.ne.jp = example.ne.jp

- Uses publicsuffix.org for TLD list

- More robust methods being considered

DMARC Spec – Alignment Examples

SPF and DKIM Strict Identifier Alignment

```
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=@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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

- SPF domain = example.com
- DKIM domain = example.com
- From domain = example.com

DMARC Spec – Alignment Examples

SPF Strict Identifier Alignment

```
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>
```

- SPF domain = example.com
- From domain = example.com

DMARC Spec – Alignment Examples

DKIM Strict Identifier 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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

- DKIM domain = example.com
- From domain = example.com

DMARC Spec – Alignment Examples

SPF and DKIM Strict Unaligned

```
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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

- SPF domain = phish.com
- From domain = example.com

DMARC Spec – Alignment Examples

SPF and DKIM Strict Unaligned

```
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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

- SPF domain = foo.example.com
- DKIM domain = bar.example.com
- From domain = example.com

DMARC Spec – Alignment Examples

SPF and DKIM Relaxed Alignment

```
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=@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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

- SPF domain = example.com
- SPF Organizational domain = example.com
- DKIM domain = example.com
- DKIM Organizational domain = example.com
- From domain = example.com
- From Organizational domain = example.com

DMARC Spec – Alignment Examples

SPF and DKIM 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@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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

- SPF domain = foo.example.com
- SPF Organizational domain = example.com
- DKIM domain = bar.example.com
- DKIM Organizational domain = example.com
- From domain = example.com
- From Organizational domain = example.com

DMARC Spec – Alignment Examples

SPF and DKIM Relaxed Alignment

```
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;
          h=From:Subject:Date:To:MIME-Version:Content-Type;
          bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=; b=T6m3ZvppP3OLGNQVoR/llW
          +RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy+svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/
          I8zlMKPmVOf/9cLIpTVbaWi/G2VBY LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@foo.example.com>
```

- SPF domain = bounce.example.com
- SPF Organizational domain = example.com
- DKIM domain = bounce.example.com
- DKIM Organizational domain = example.com
- From domain = foo.example.com
- From Organizational domain = example.com

DMARC Spec – Alignment Examples

SPF Relaxed Alignment

```
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>
```

- SPF domain = example.com
- SPF Organizational domain = example.com
- From domain = example.com
- From Organizational domain = example.com

DMARC Spec – Alignment Examples

SPF Relaxed Alignment

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

- SPF domain = bounce.example.com
- SPF Organizational domain = example.com
- From domain = foo.example.com
- From Organizational domain = example.com

DMARC Spec – Alignment Examples

DKIM Relaxed 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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

- DKIM domain = foo.example.com
- DKIM Organizational domain = example.com
- From domain = example.com
- From Organizational domain = example.com

DMARC Spec – Alignment Examples

SPF and DKIM Relaxed Unaligned

```
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=bar.example.com; s=s1024-2011-q2; c=relaxed/simple;
          q=dns/txt; i=@example.com; t=1337318096; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

- SPF domain = phish.com
- SPF Organizational domain = phish.com
- From domain = example.com
- From Organizational domain = example.com

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/1lW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

Answer: No, SPF did not pass.

Is the email Aligned anyway?

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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.

DMARC Spec – Alignment Exercises

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

DMARC Spec – Alignment Exercises

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/1lW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

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

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/1lW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

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

Under what conditions would the email be Aligned?

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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 considering 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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

DMARC Spec – Alignment Exercises

Exercise 4
Under what conditions would this email be considering 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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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 considered Aligned?

DMARC Spec – Alignment Exercises

Exercise 4
Under what conditions would this email be considering 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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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 considered Aligned?

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 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

Tag	Purpose	Example
v	Protocol Version	v=DMARC1
p	Policy for the domain	p=quarantine
sp	Policy for subdomains	sp=reject
pct	% of messages subject to policy	pct=20
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r
rua	Reporting URI for aggregate reports	rua=mailto:aggrep@example.com
ruf	Reporting URI of forensic reports	ruf=mailto:authfail@example.com
rf	Forensic reporting format	rf=afrf
ri	Aggregate reporting interval	ri=14400

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;
```

DMARC Spec –Policy Record Exercises

Exercise 1
Is this a valid record?

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

DMARC Spec –Policy Record Exercises

Exercise 2
What DNS TXT record will be queried for mail from foo.example.com?

DMARC Spec –Policy Record Exercises

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?

DMARC Spec –Policy Record Exercises

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; h=From:Subject:Date:To:MIME-
          Version:Content-Type; bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

Answer: Yes. Alignment is Relaxed by default.

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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@example.com>
```

Then what will happen to the email?

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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@bar.example.com>
```

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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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.

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;
```

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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/1lW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" postmaster@bar.example.com
```

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;
```

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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" postmaster@bar.example.com
```

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

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;
```

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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" postmaster@bar.example.com
```

Then what will happen to the email?

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;
```

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=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
          b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l 0cy
          +svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBY
          LXONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
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.

DMARC Spec –Reporting

Aggregate Reports

- Each report covers one RFC5322.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.

  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 include ‘call-to-action’ URIs
- Throttling
- Privacy issues
  - Might be redacted
  - Might not be supported

DMARC Spec –Reporting

DMARC URIs

Advertise the maximum report size a destination URI will accept

```
    mailto:aggregate@example.com!25M
```

Works for both report types.

DMARC Spec –Reporting

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:

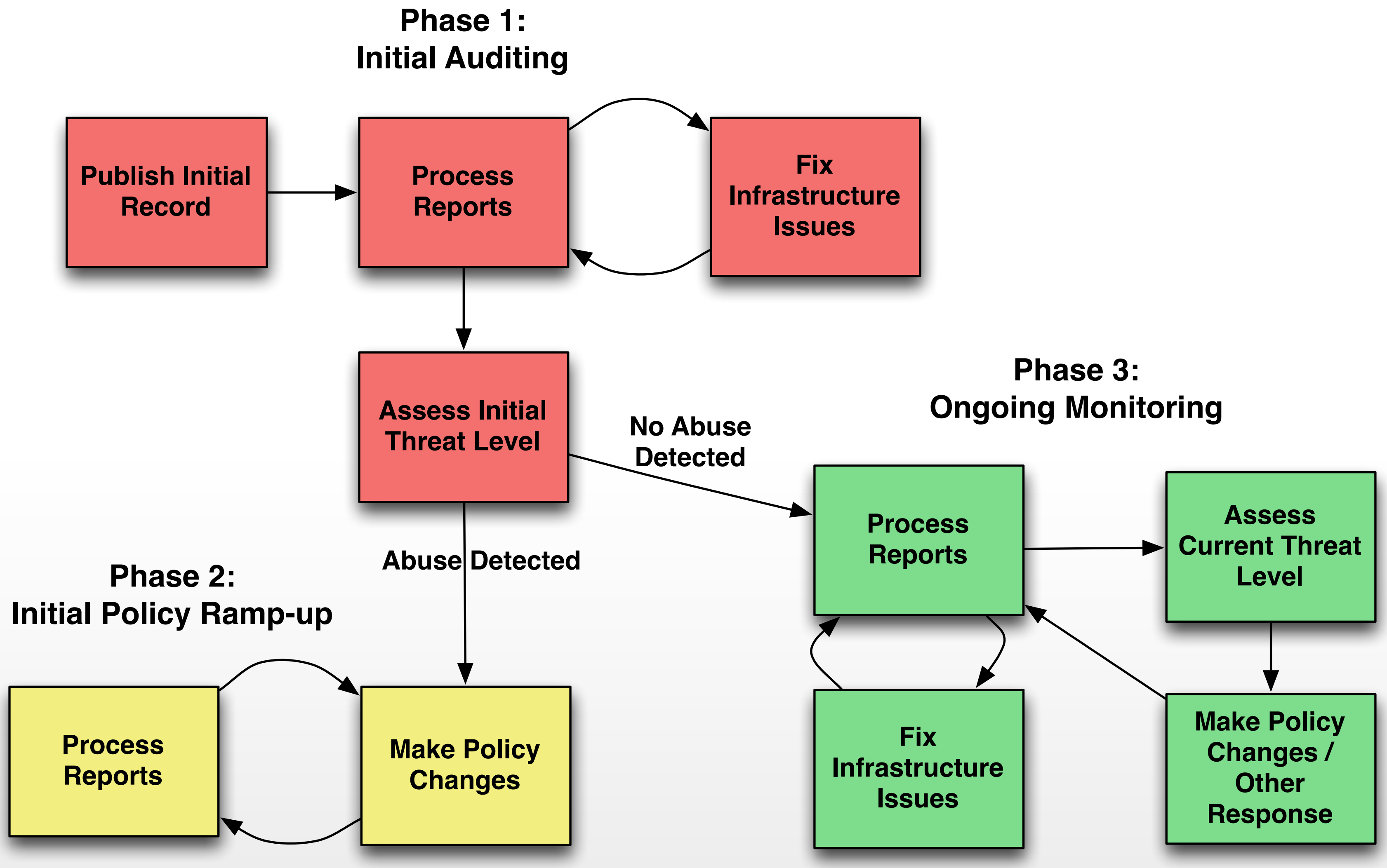
```
    v=DMARC1; rua=mailto:reports@foo.com
```

Break

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

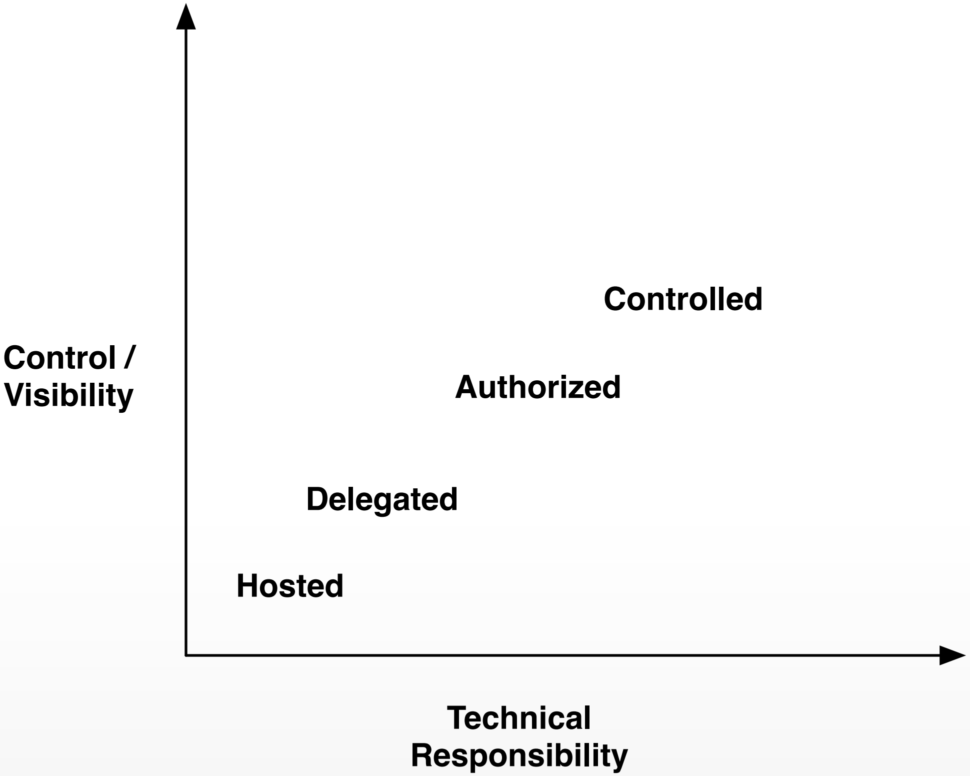


Initial Record Publishing

Everyone’s first DMARC record

```
v=DMARC1; p=none; rua=mailto:aggregate@example.com;
```

3rd Party Deployment Profiles



Control / Visibility

Controlled

Authorized

Delegated

Hosted

Technical Responsibility

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.

3rd 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
- (Quarterly) 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.

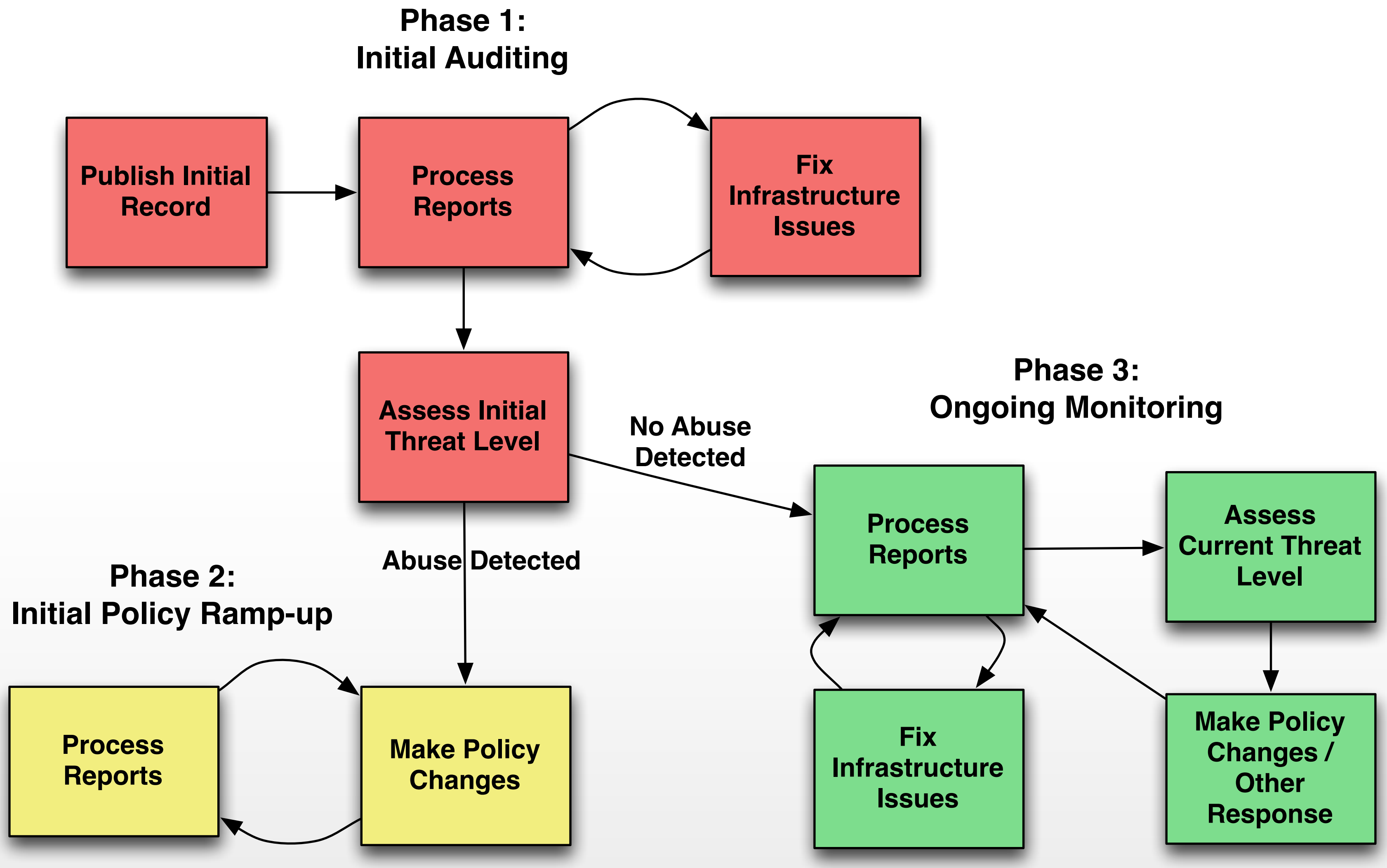
Con
- The domain owner is significantly more dependent on the 3rd party.

3rd Party Deployment Profiles

3rd Party responsibilities

	Controlled	Authorized	Delegated	Hosted
Provide SPF record content	Y	Y	Y	Y
Maintain SPF records	N	N	Y	Y
Maintain DKIM records	N	N	Y	Y
Create DKIM Keys	N	Y	Y	Y
Rotate DKIM Keys	Y	Y	Y	Y
Maintain DMARC Records	N	N	Y	Y
Process DMARC reports	N	?	?	Y

Report Processing and Analysis



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.

Report Processing and Analysis – Infrastructure Auditing

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

Report Processing and Analysis

Step 3: Identify Malicious Email

Research Unauthorized 3rd Parties and label the Abusers

- Use public data sources
- Vendor services
- Look for known failure cases
- Forensic reports

Report Processing and Analysis

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

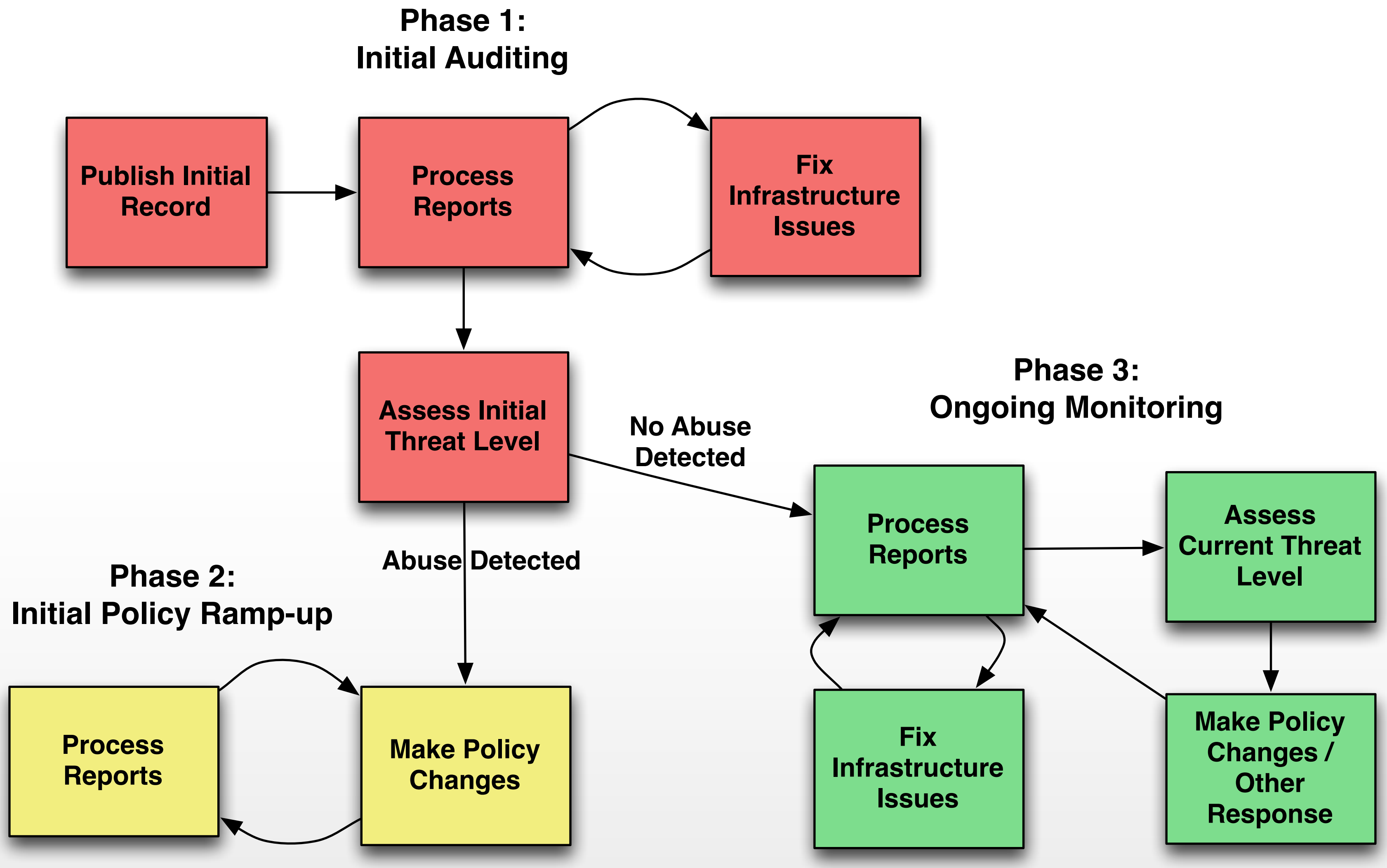
Potential False Positives = Unaligned Email from Unauthorized 3rd parties

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



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’.

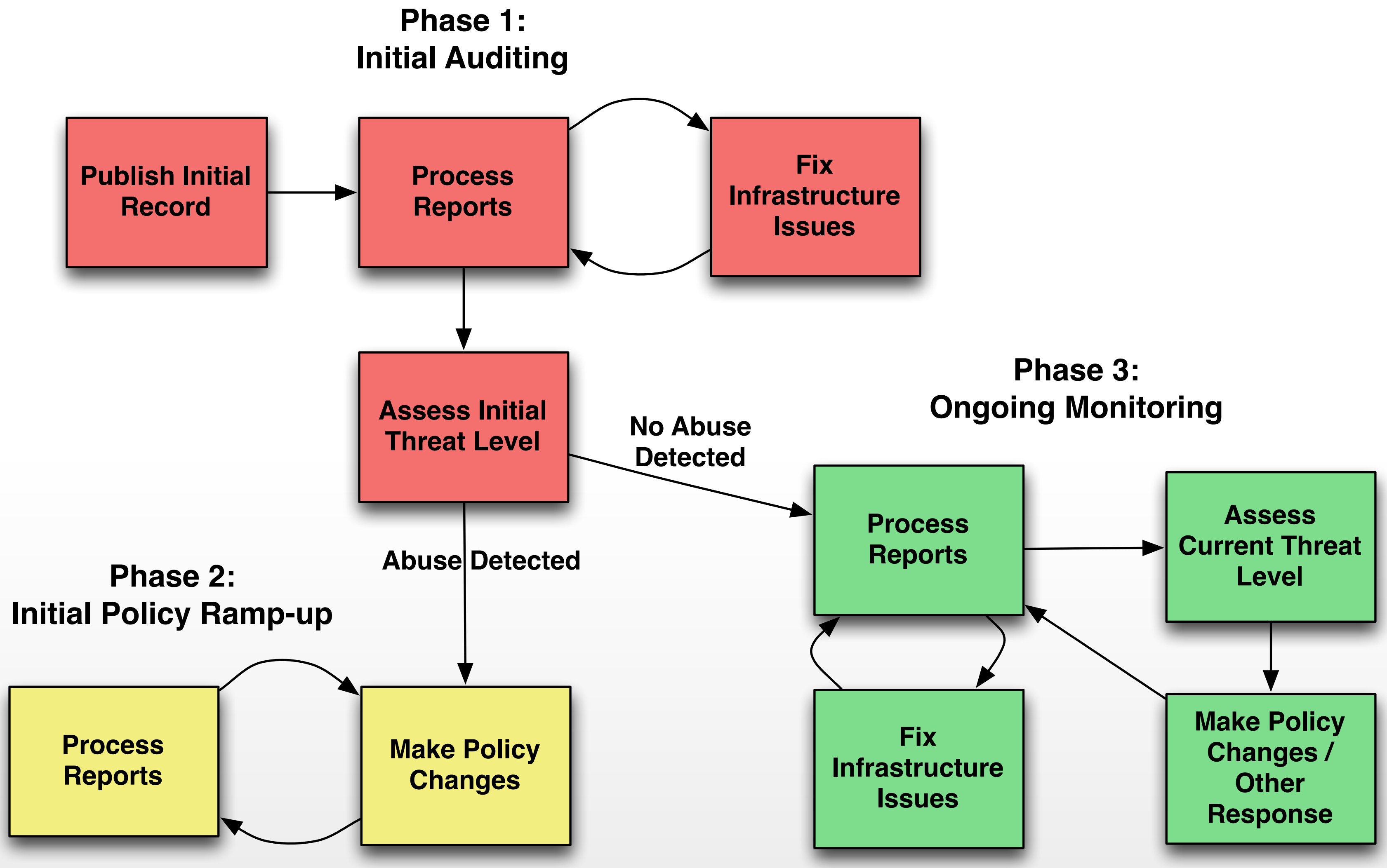
Rinse and repeat until you get to ‘pct=100’.

Initial Policy Ramp-up

Step 5: If needed, update your record to:

```
p=reject
```

Ongoing Monitoring



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

Break?

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?

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.

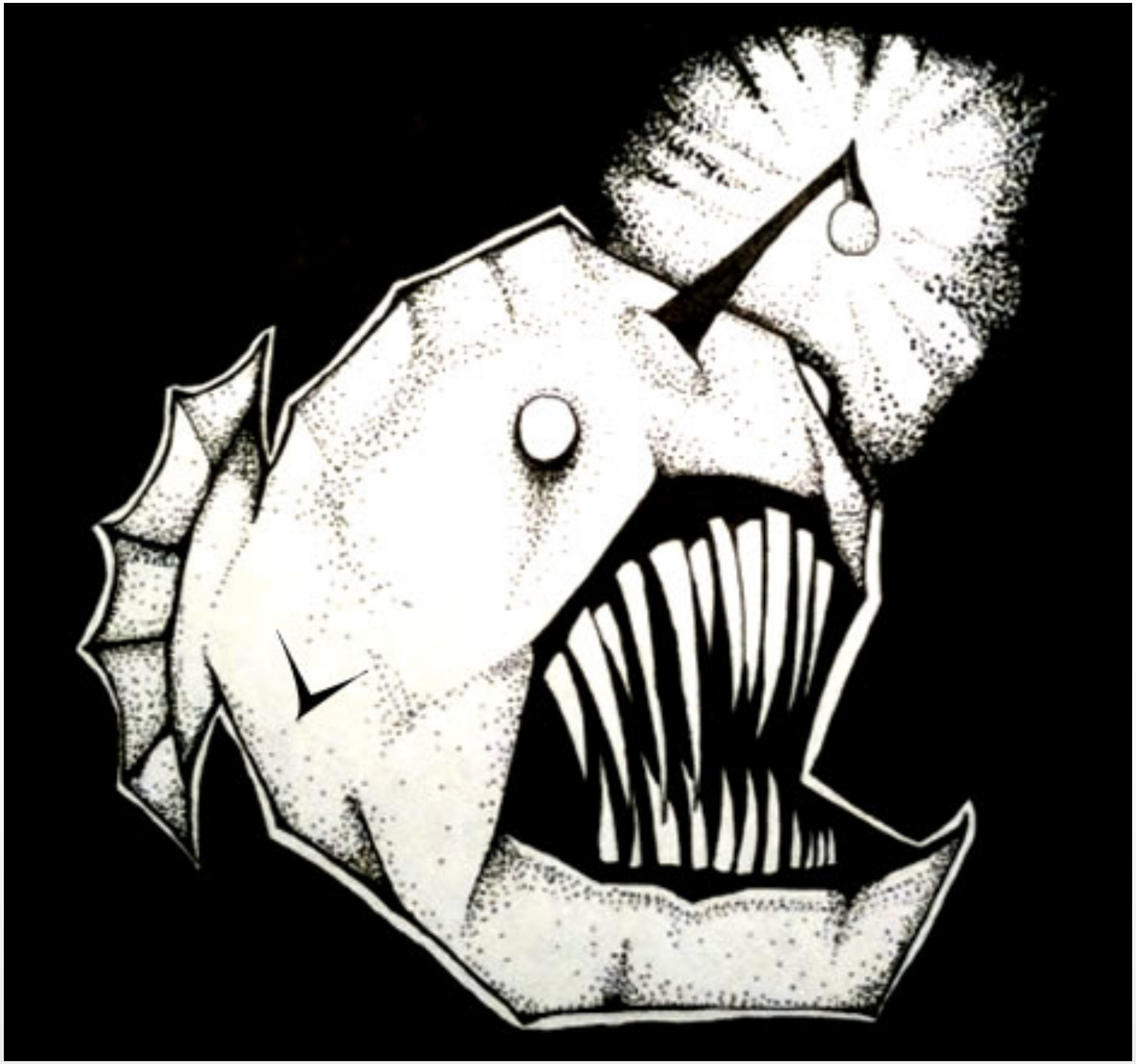
- Don’t queue. Sending as close to receipt as possible maximizes value.

Information for Mailbox Providers

Operational Considerations

- DMARC policy is the sender's policy and usually 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

Operational Considerations

- DMARC policy is the sender's policy and usually 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.
- Aggregate reporting interval is bounded by aggregation frequency.
- Failure Reports can offset impact of longer aggregate intervals.
- Beware of bad guys attempting to use your infrastructure to aim large report volumes at reporting addresses.
  - Latest draft addresses this issue.

Information for Mailbox Providers

Reporting and Privacy

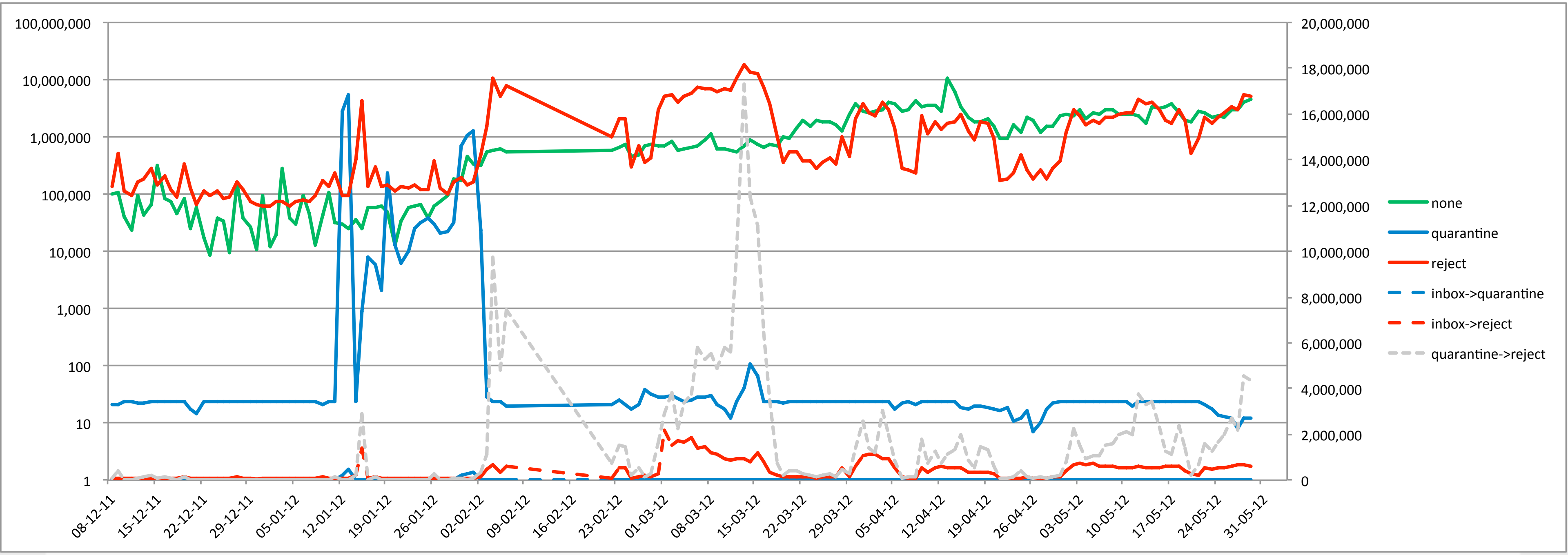
Forensic reports can send an unaltered message to someone other than the intended recipient.

It may not be from a bad actor.

- Do a privacy review!
- Understand applicable privacy regimes before sending reports.
  - Corporate
  - Federal/Legal
  - Only one US-based MBP is sending failure reports

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
Participate page for list sign up

Feedback

Please fill out the surveys!