Inbox Co.

□ ☆ K. Knowles **SMTP: Security & History** - Email makes the world turn. But for all… **May 28**

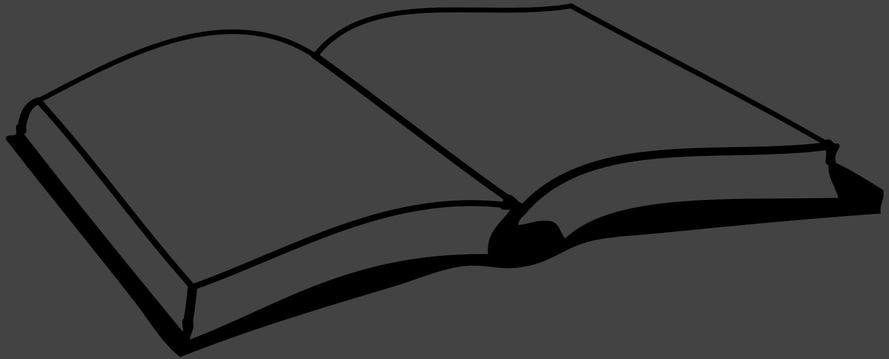
SMTP: Security & History

K. Knowles

to me (via LayerOne) ▾

May 28th, 2017

Email makes the world turn. But for all its glory flaws, contradictions, and bolt-on protocols haunt SMTP.
The security solutions we have are narrow and complicated.
How did it get this bad?



The tale these protocols offer is more than the story of SMTP security. This is the struggle of tragedies and triumphs that befall any generation of network practitioners.

@_sigil

Overview

- SMTP is Born
  - SMTP
  - SMTP AUTH
  - STARTTLS
- Verification Wars
  - SPF
  - SenderID
  - “The MARID Fiasco”
  - DKIM
- Unifying Standards
  - DMARC
- The Future
  - ARC
  - What’s next?

Who’s the Speaker?

Katie Knowles:

- Blue team warrior ☀
- Infosec explorer ☾
- Recovering Engineer (BSEE)
- Tortured-soul MTA administrator

@_sigil

kknowl.es

The Beginning

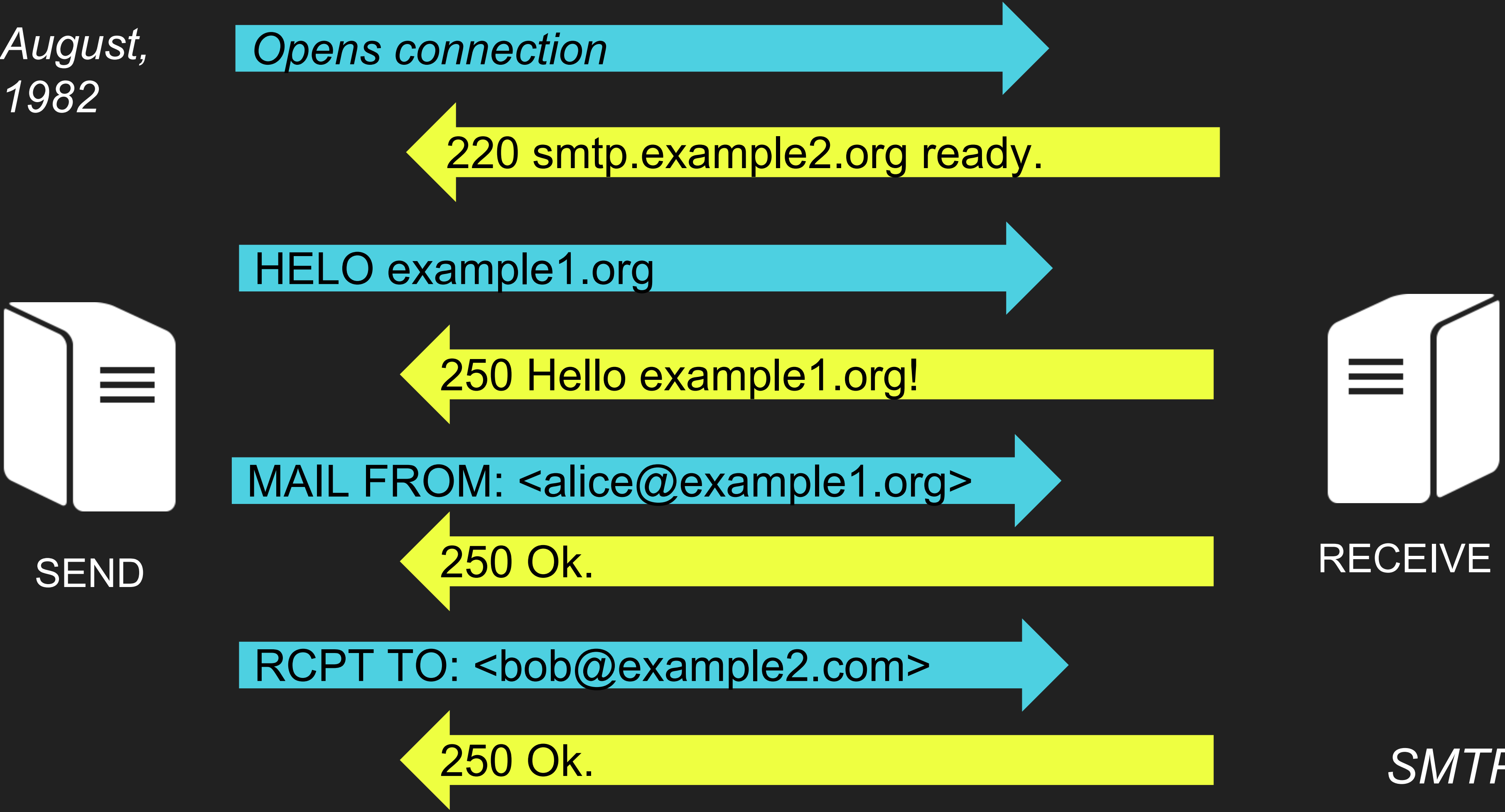
1981, Marina del Rey

“The objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently.”

A small, early internet means no considerations for security.

@_sigil

August, 1982



Opens connection

220 smtp.example2.org ready.

HELO example1.org

250 Hello example1.org!

MAIL FROM: <alice@example1.org>

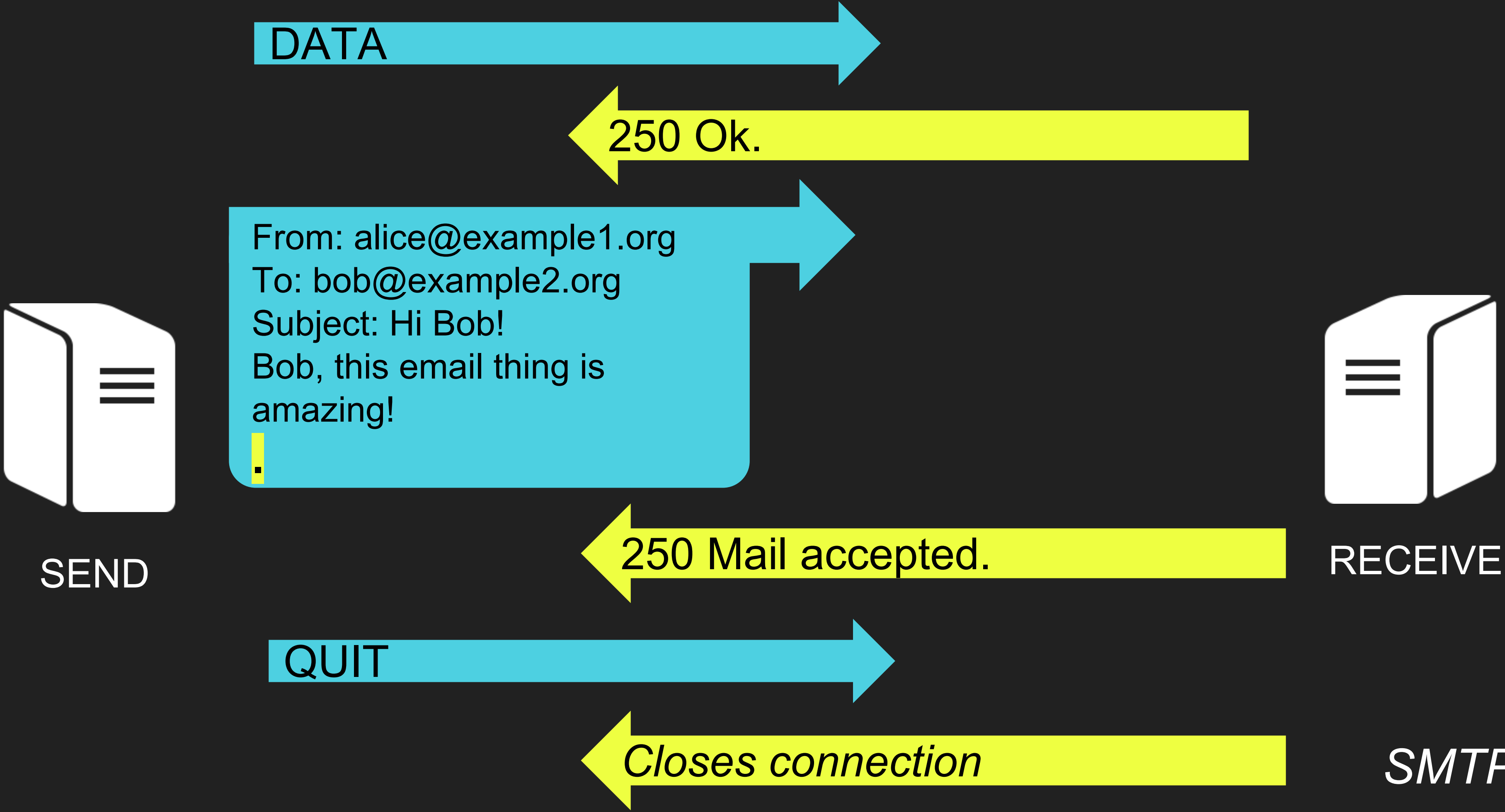
250 Ok.

RCPT TO: <bob@example2.com>

250 Ok.

SMTP

@_sigil



SEND

RECEIVE

DATA

250 Ok.

From: alice@example1.org
To: bob@example2.org
Subject: Hi Bob!
Bob, this email thing is amazing!
.

250 Mail accepted.

QUIT

Closes connection

SMTP

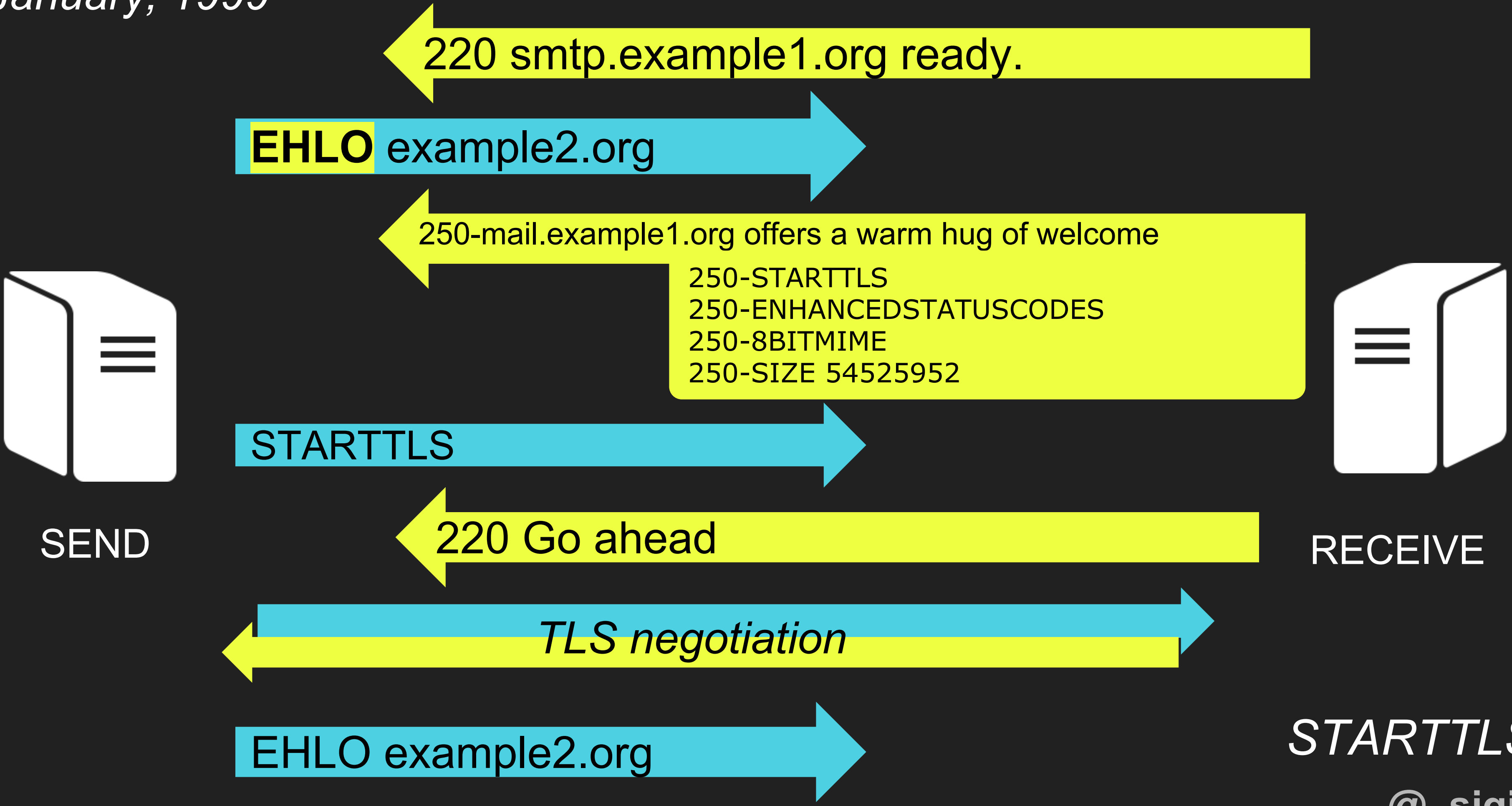
@_sigil

Securing the Basics

- “Service extensions” allow introduction of new SMTP functions, and encryption is high on the list.
- The STARTTLS extension is implemented for establishing a secure channel between servers.

@_sigil

January, 1999



220 smtp.example1.org ready.

EHLO example2.org

250-mail.example1.org offers a warm hug of welcome
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-SIZE 54525952

STARTTLS

220 Go ahead

TLS negotiation

EHLO example2.org

STARTTLS

@_sigil

We have:

Open Communications!

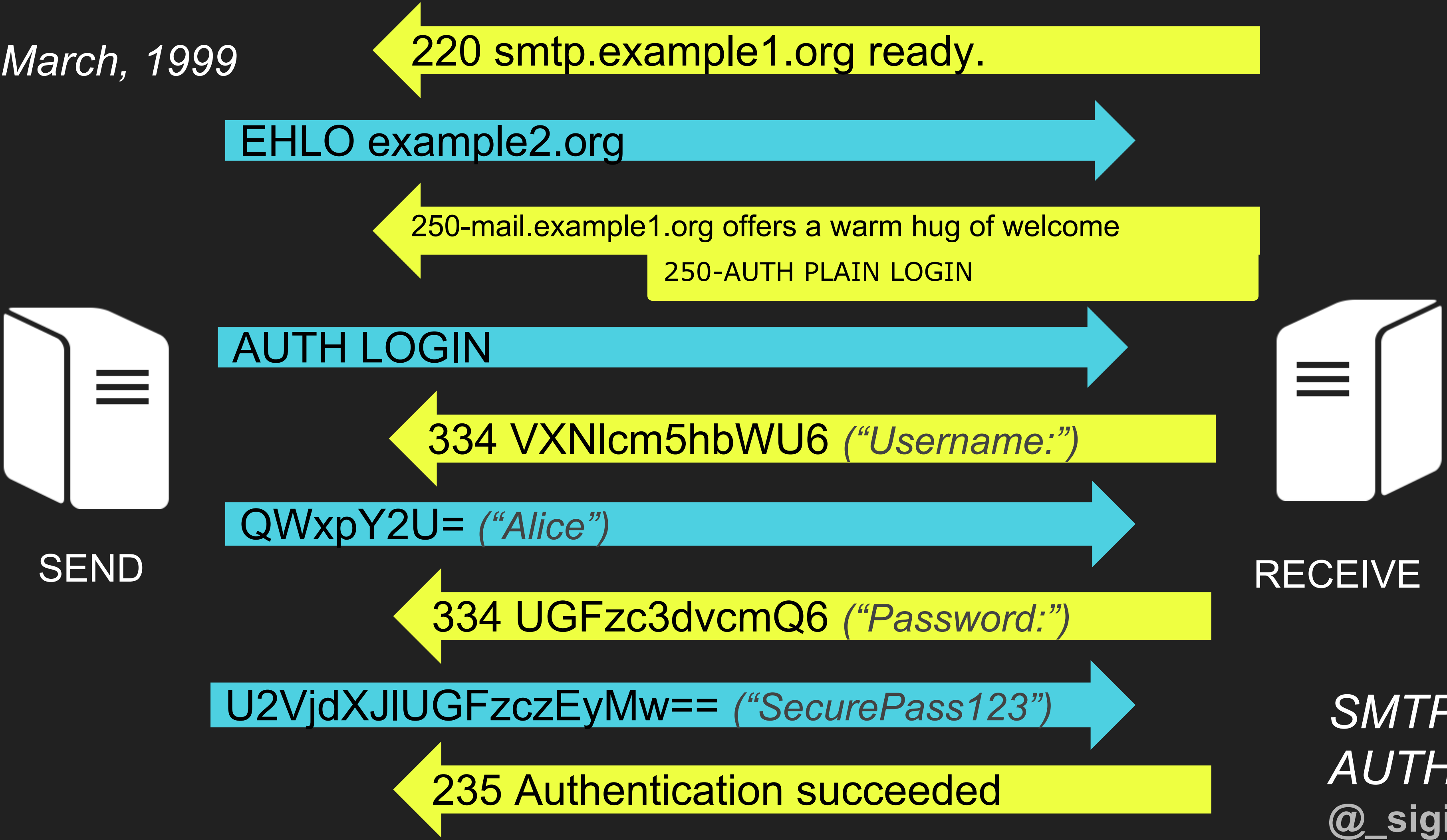
Adoption of SMTP leads to free and open email communication...

Open Spam!

...but growth of open relays allows the birth of mass junk mail. Closing open relays requires authentication.

@_sigil

March, 1999



220 smtp.example1.org ready.

EHLO example2.org

250-mail.example1.org offers a warm hug of welcome
250-AUTH PLAIN LOGIN

AUTH LOGIN

334 VXNlcm5hbWU6 *(“Username:”)*

QWxpY2U= *(“Alice”)*

334 UGFzc3dvcmQ6 *(“Password:”)*

U2VjdXJlUGFzczEyMw== *(“SecurePass123”)*

235 Authentication succeeded

SMTP AUTH

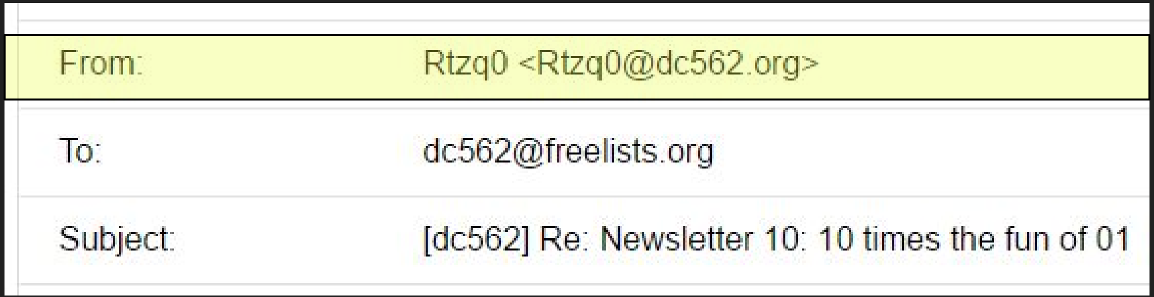
@_sigil

A Matter of Trust

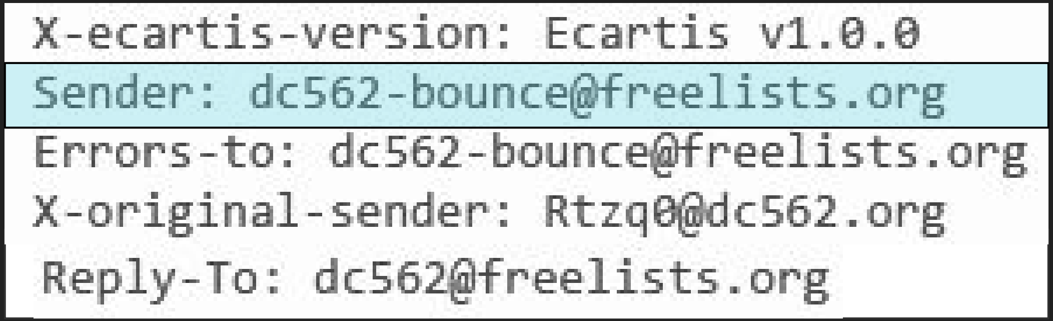
- Encrypted mail works! ...but third-party hosting and mailing lists prevent verification solely by certificate.
- Researchers get to work. Their most prominent ideas: SPF, SenderID, and DKIM.

PRA Identity

Displayed “From” sender shows in user’s inbox



```
From:      Rtzq0 <Rtzq0@dc562.org>
To:        dc562@freelists.org
Subject:   [dc562] Re: Newsletter 10: 10 times the fun of 01
```

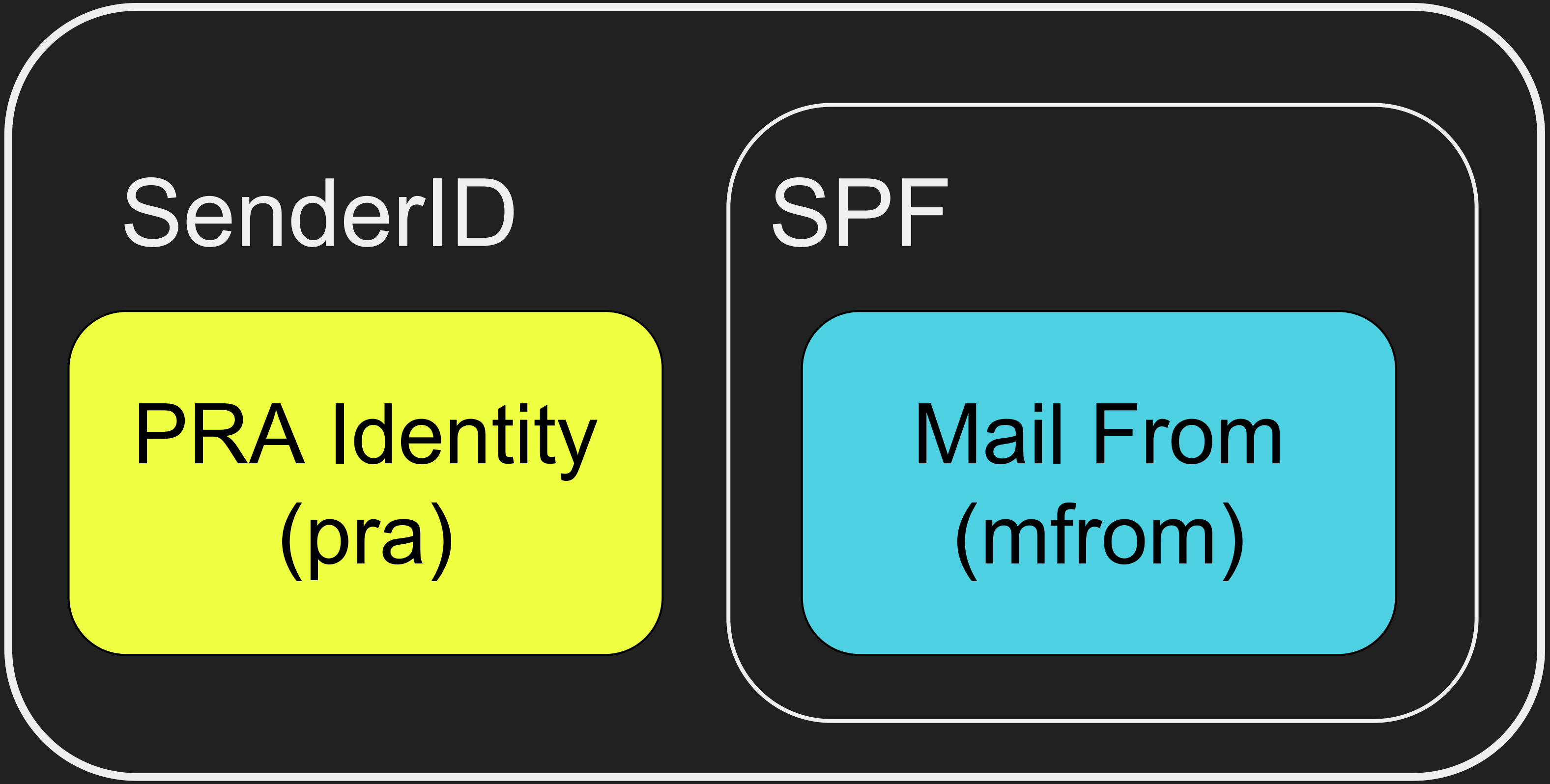


```
X-ecartis-version: Ecartis v1.0.0
Sender: dc562-bounce@freelists.org
Errors-to: dc562-bounce@freelists.org
X-original-sender: Rtzq0@dc562.org
Reply-To: dc562@freelists.org
```

Mail From

Message headers show who *actually* sent the message

@_sigil



SenderID

PRA Identity
(pra)

SPF

Mail From
(mfrom)

@_sigil

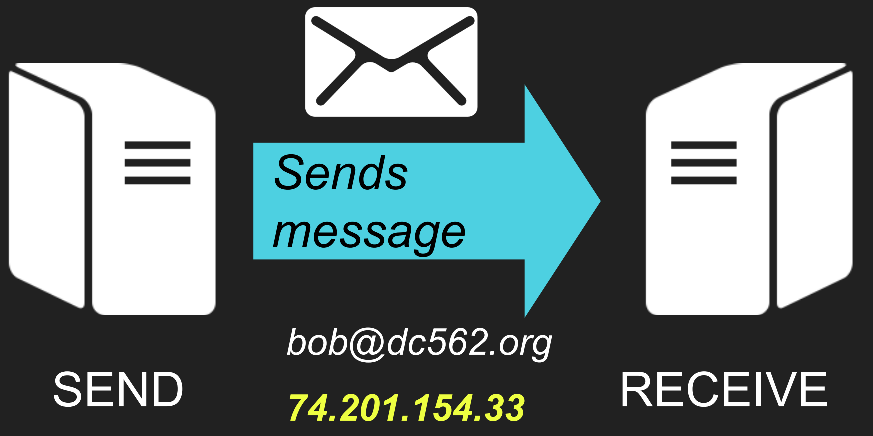
SPF: Sender Policy Framework

Syntax		Action
+	Pass	Accept
~	SoftFail	Accept but mark
-	Fail	Reject
?	Neutral	Accept

- Sending Domain:
  - Publishes TXT record of acceptable IPs
  - Defines action to take if IP fails check
- Receiving Server:
  - Verifies sending server IP is on the list
  - *(Generally)* Performs requested action

@_sigil

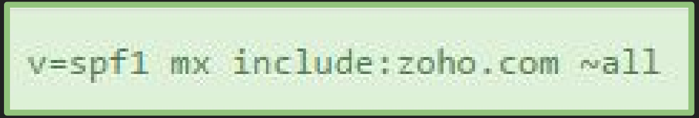
April, 2006



```
v=spf1 mx include:zoho.com
~all
```

```
v=spf1 include:spf.zoho.com
include:spf2.zoho.com
~all
```

```
v=spf1 ip4:74.201.154.0/24
ip4:74.201.84.0/24
ip4:135.84.80.192/26
ip4:135.84.80.0/25
ip4:165.254.168.0/24
ip4:8.45.169.0/24
ip4:204.141.32.0/23 ~all
```



```
v=spf1 mx include:zoho.com ~all
```

SPF

@_sigil

The MARID Fiasco

- MTA Authorization Records in DNS (MARID) is formed to refine proposals. *(2004)*
- Disbands after 7 months amidst IP battles and organizational struggles.
- SenderID is refined, but no RFCs are created.

SenderID

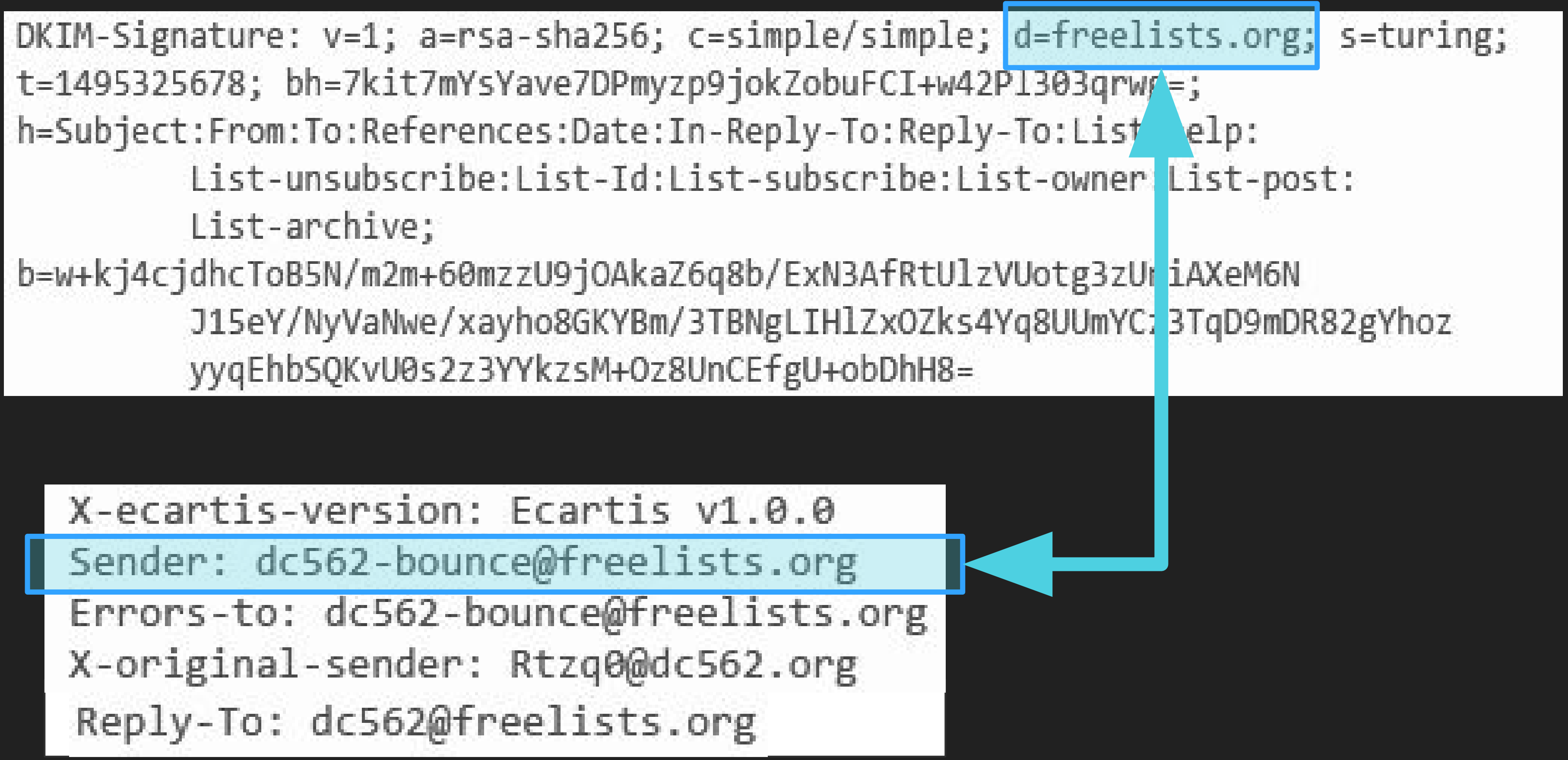
Creates SPF record options:

- spf2.0/pra
- spf2.0/mfrom → Equivalent to “spf1” record
- spf2.0/mfrom,pra

> *“The [spf2.0] tag name is a historical accident and was assigned by the failed MARID IETF working group.”*
>
> -openspf.org

DKIM: DomainKeys Identified Mail

- Public key published to a “selector” as TXT record
  - Ex. *“mail2017._domainkey.example1.org”*
- Private key used to hash content of outgoing messages
- Message headers define:
  - Where to find selector with public key
  - What message headers to include in hash of content
- Cannot specify action for failed DKIM



```
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=freelists.org; s=turing;
t=1495325678; bh=7kit7mYsYave7DPmyzp9jokZobuFCI+w42Pl303qrwg=;
h=Subject:From:To:References:Date:In-Reply-To:Reply-To:List-help:
         List-unsubscribe:List-Id:List-subscribe:List-owner:List-post:
         List-archive;
b=w+kj4cjdhcToB5N/m2m+60mzzU9jOAkaZ6q8b/ExN3AfRtUlzVUotg3zUniAXeM6N
         J15eY/NyVaNwe/xayho8GKYBm/3TBNgLIHlZxOZks4Yq8UUmYCz3TqD9mDR82gYhoz
         yyqEhbSQKvU0s2z3YYkzsM+Oz8UnCEfgU+obDhH8=
```

```
X-ecartis-version: Ecartis v1.0.0
Sender: dc562-bounce@freelists.org
Errors-to: dc562-bounce@freelists.org
X-original-sender: Rtzq0@dc562.org
Reply-To: dc562@freelists.org
```

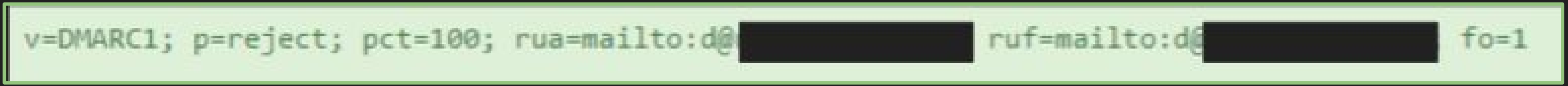
@_sigil

Time Passes

- IETF quietly releases RFCs for SPF, SenderID, and DKIM. *(2006)*
- Servers still have no way to evaluate DKIM failures.
- No way to notify servers of SPF/DKIM failures makes for a difficult deployment.
- DMARC is created to help.

DMARC

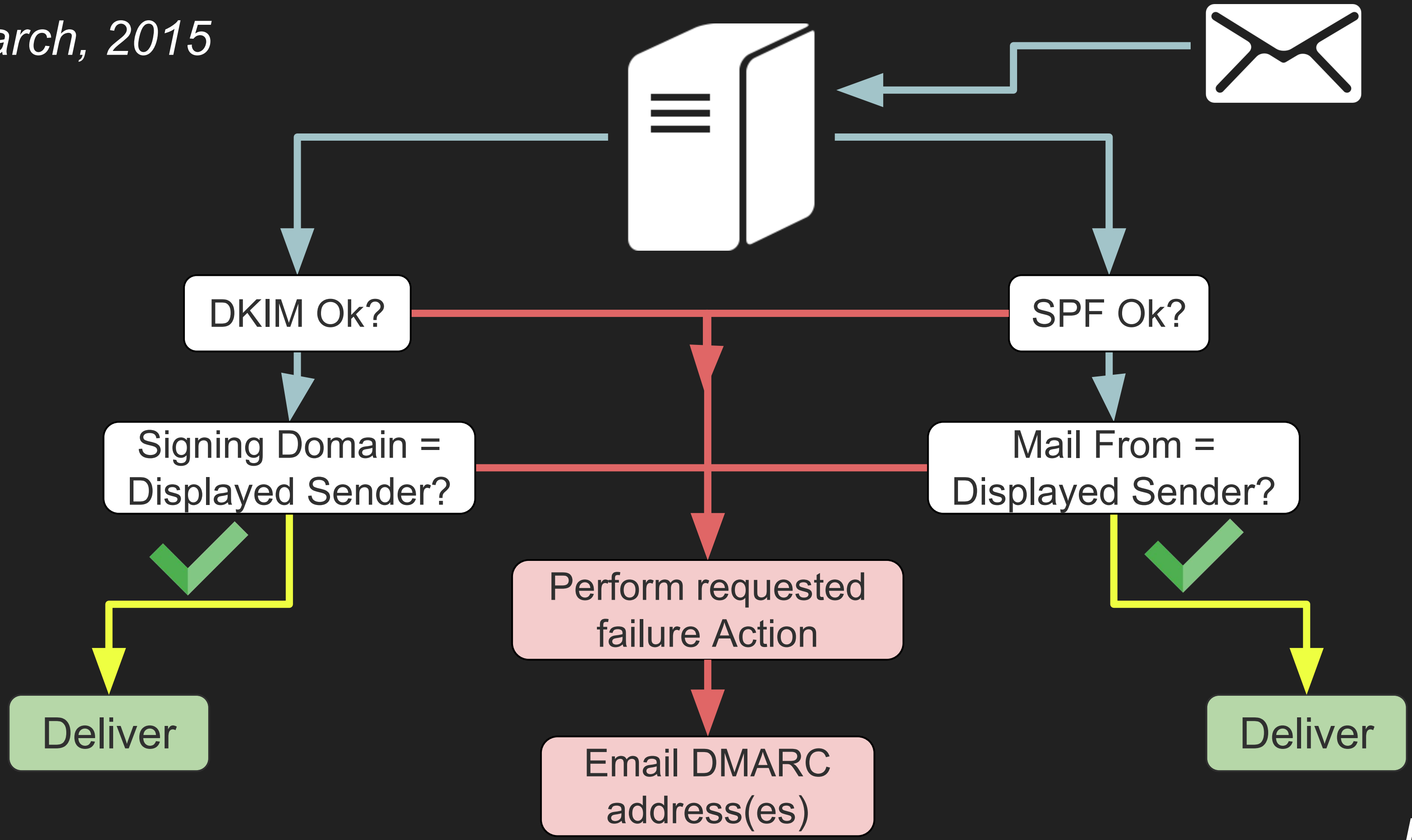
Domain publishes TXT record to _dmarc.example.org with...



```
v=DMARC1; p=reject; pct=100; rua=mailto:d@[redacted] ruf=mailto:d@[redacted] fo=1
```

- Email addresses to send feedback
  - Aggregate *(rua)*: Basic pass/fail data
  - Forensic *(ruf)*: Specific headers of failed messages
- Action for SPF/DKIM failed mail
- Percentage of mail to apply failure action to

March, 2015


DKIM Ok?
SPF Ok?
Signing Domain = Displayed Sender?
Mail From = Displayed Sender?
Perform requested failure Action
Email DMARC address(es)
Deliver
Deliver

DMARC

@_sigil

The Aftermath

“SMTP mail is inherently insecure in that it is feasible for even fairly casual users to negotiate directly with receiving and relaying SMTP servers and create messages that will trick a naive recipient into believing that they came from somewhere else. [...]

As knowledge of Internet mail increases, so does the knowledge that SMTP mail inherently cannot be authenticated, or integrity checks provided, at the transport level. Real mail security lies only in end-to-end methods involving the message bodies[.]”

-RFC 5321, October 2008

“MARID failed because a simple, non-controversial, and all-encompassing solution to Internet Mail Authentication does not seem to exist.”

-IETF Mailing List, March 2005

What Can We Do?

- Administrators:
  - Configure SPF! Audit SPF.
  - Publish DMARC with action “None” for feedback
- Technologists:
  - DMARC provides active mailing lists & working group
- Dreamers:
  - Don’t be scared to rebuild from scratch
  - Think outside the (in)box ✉

Qs?

Reach out at:

🐦 @_sigil

✉ katie(at)kknowl.es

Acronyms

Acronym	Expansion
SMTP	Simple Mail Transfer Protocol
SPF	Sender Policy Framework
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, & Conformance
ARC	Authenticated Received Chain

RFCs

RFC Number	Protocol
RFC 788, 821, 5321	SMTP
RFC 3207	STARTTLS
RFC 4954	SMTP AUTH
RFC 4408, 7208	SPF
RFC 4405	SenderID
RFC 4871, 6376	DKIM
RFC 7489	DMARC

Additional Resources

- http://www.openspf.org/
- http://dkim.org/
- https://dmarc.org/
- http://arc-spec.org/
- https://postmarkapp.com/guides/spf
- https://postmarkapp.com/guides/dkim
- https://postmarkapp.com/guides/dmarc
- https://mxtoolbox.com/
- https://openclipart.org