DMARC

Providing domain owners control of their brand in the email channel

January 2012

DMARC Defined

DMARC stands for:

Domain-based Message Authentication, Reporting & Conformance

(pronounced “dee-mark”)

DMARC.org is Formed

A loose collaboration of leading organizations working for 18 months to develop an Internet standard that enables senders and receivers to communicate email authentication information to thwart phishing.

Phishing continues to be a major pain point for the consumer Internet

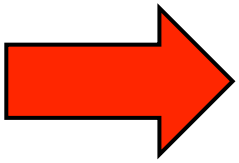
90% peak spoof rates[1]

10% average spoof rate of the Internet Retail 500[1]

30% average spoof rate for top federal government sites[1]

Incidence and costs related to spear phishing rising quickly

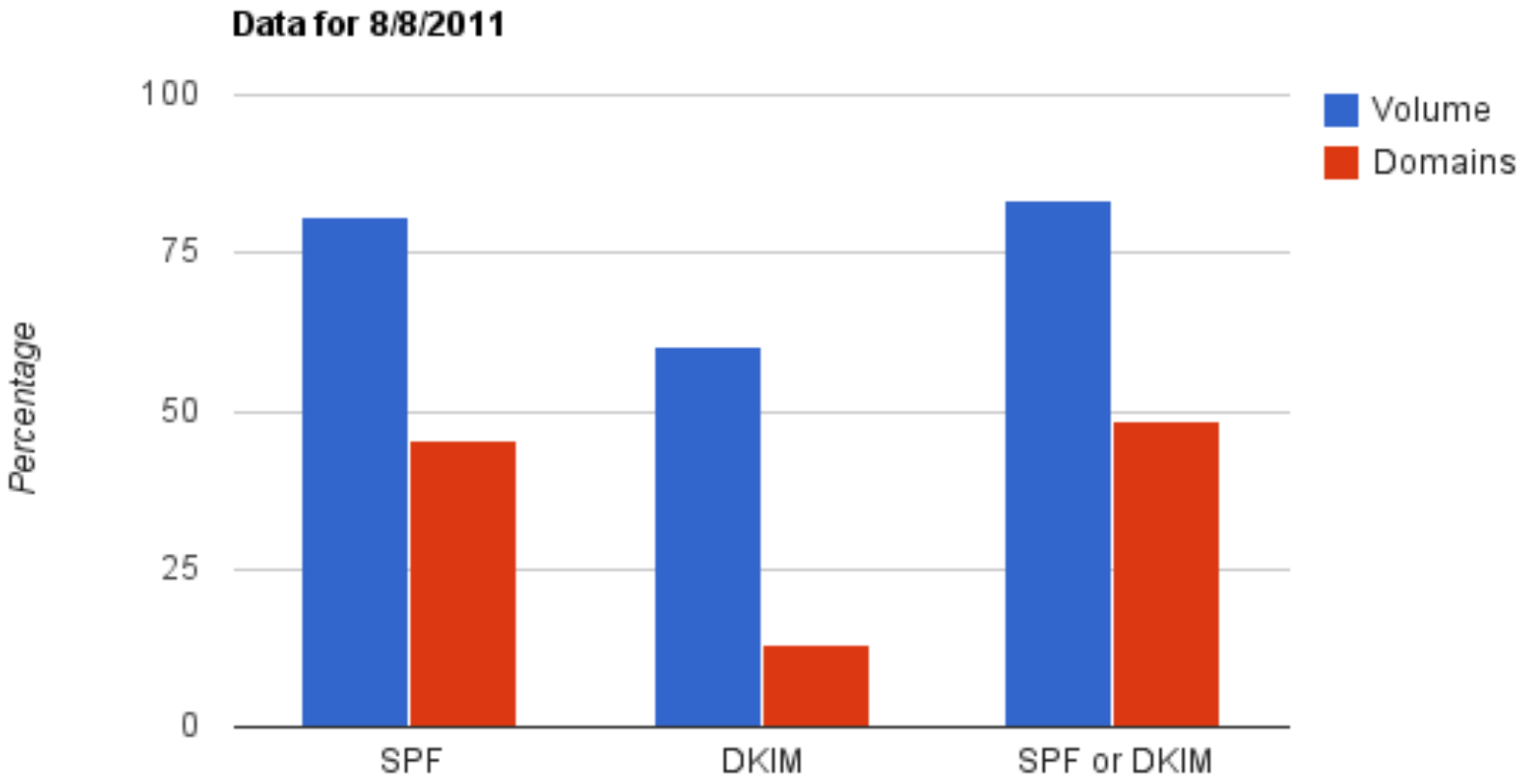
100k's account hijackings daily



Loss of trust in online resources
Decrease in future online activity

1 Source: Online Trust Alliance https://otalliance.org

SPF and DKIM adoption reaching the tipping point

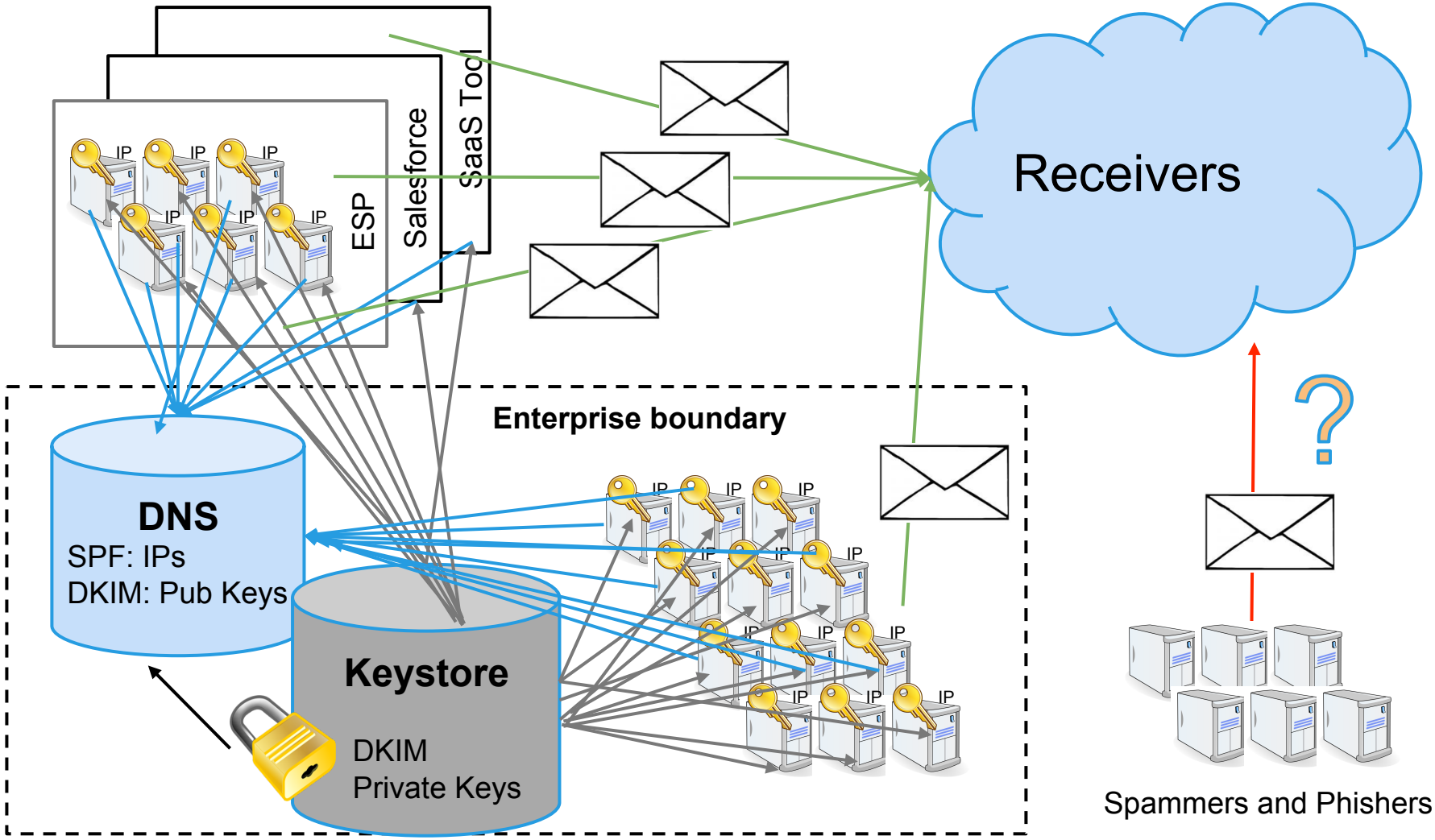


Majority of clean mail is authenticated[1]

[1]Courtesy, DMARC.org member company

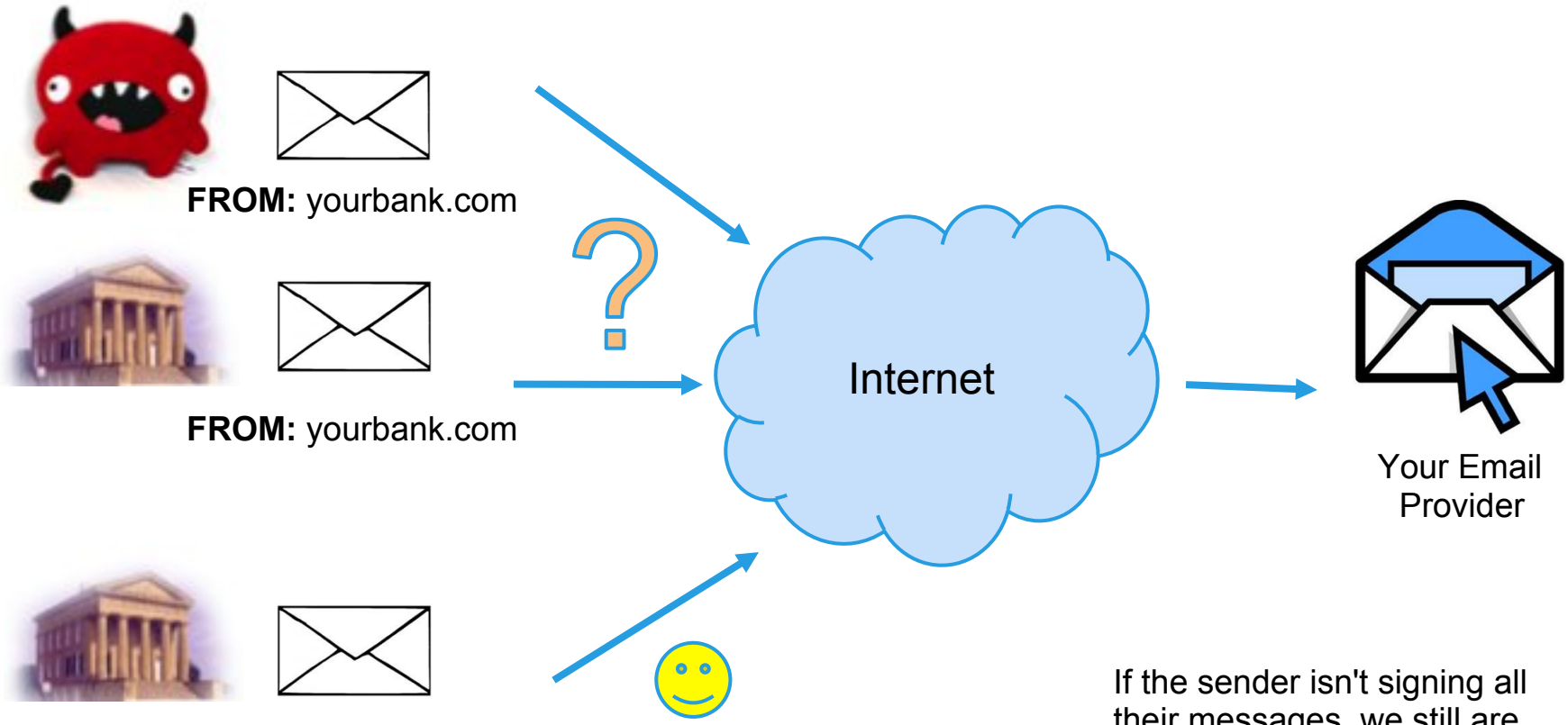
The Challenge for Senders

Mail Authentication is hard and with uncertain ROI



The Challenge for Receivers

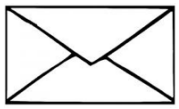
Senders adding some authentication helps only a little



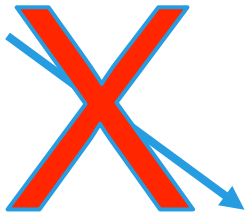
If the sender isn't signing all their messages, we still are forced to guess what's phishing and what's not

The Solution

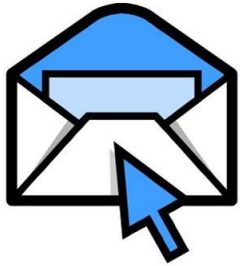
Senders authenticate ALL mail and tell that to receivers



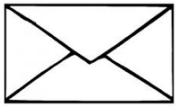
FROM: yourbank.com



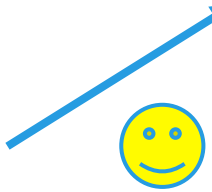
Internet



Your Email Provider



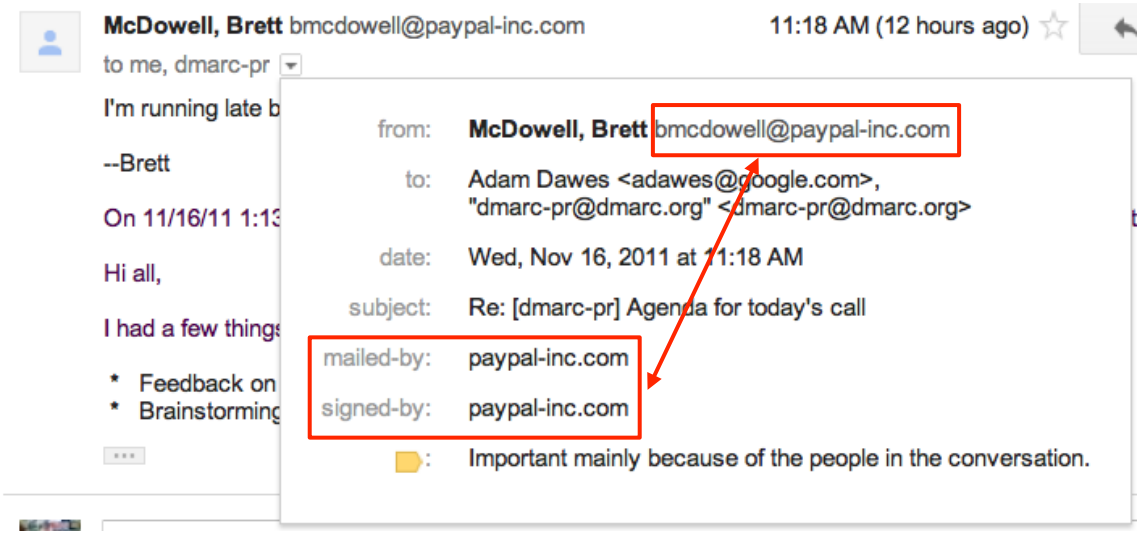
FROM: yourbank.com



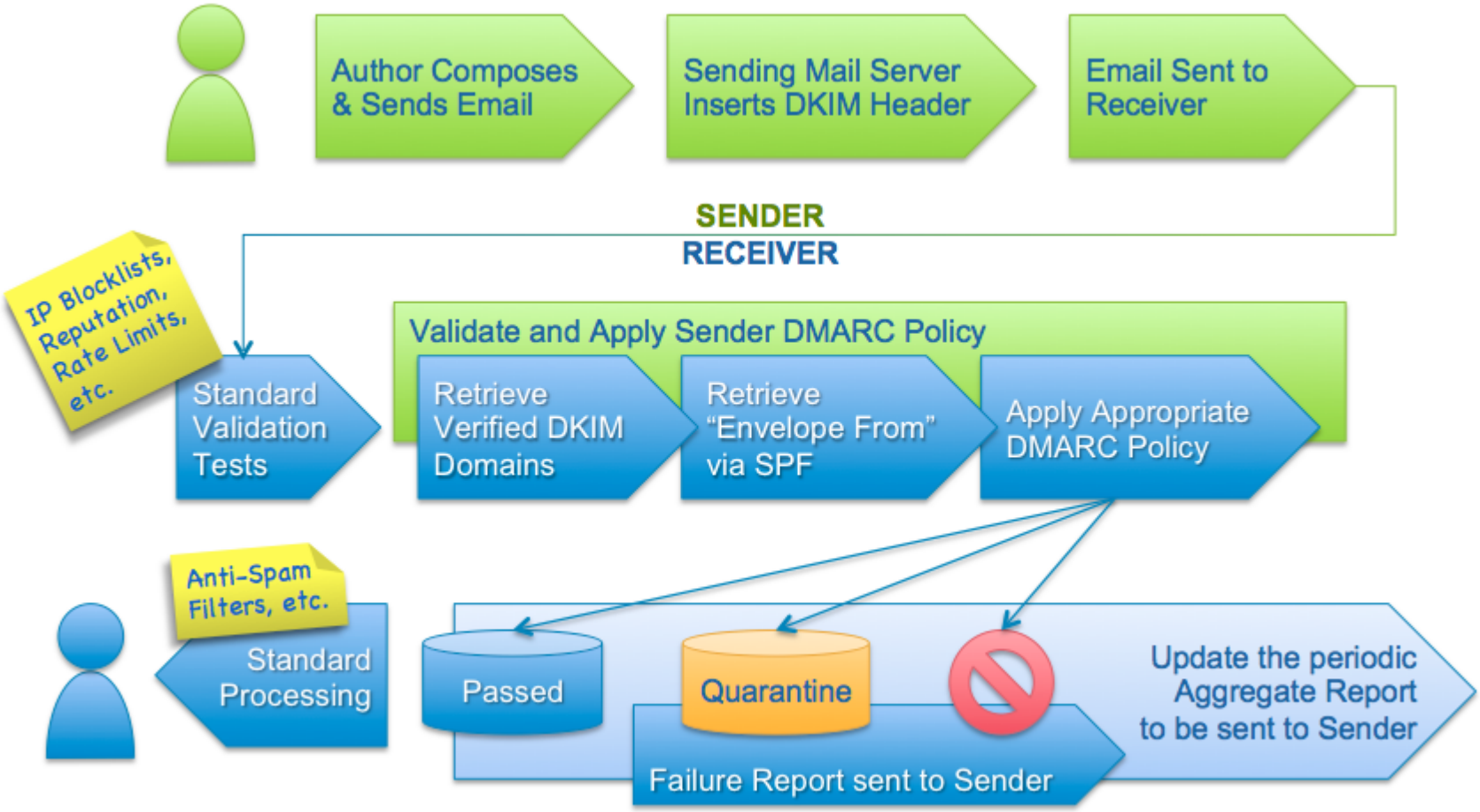
If the sender is signing all their messages, the receiver knows unsigned messages are phishing

DMARC Identifier Alignment

- DMARC combats phishing by tying Mail User Agent (MUA) visible "RFC5322.From" field to the DKIM or SPF authenticated domain
- Identifier alignment can be strict (match exactly) or relaxed:
  - Relaxed SPF: SPF Authenticated RFC5321:Mail From and RFC5322:From must share Organizational domain
  - Relaxed DKIM: Organizational domain from 'd=' value of DKIM authenticated signature must be equal or parent to RFC5322.From



DMARC from Author to Recipient



DMARC Defines:

- **DKIM & SPF Configuration Guidelines**
  - Designed to achieve identifier alignment
- **DNS Resource Record**
  - A new TXT RR of sender policies including:
  - alignment types: **Strict** | **Relaxed**
  - disposition: **Quarantine** | **Reject** | **Monitor**
  - reporting URIs: **Failure** & **Aggregate**
- **Aggregate Reporting Format**
  - Aggregate of email disposition data over time.
  - XML syntax format for aggregate reports

DMARC DNS Record Options

- Domain owners post policies in the DNS, just like with SPF or ADSP
- Policy record consists of a series of DKIM-style “tag=value” pairs

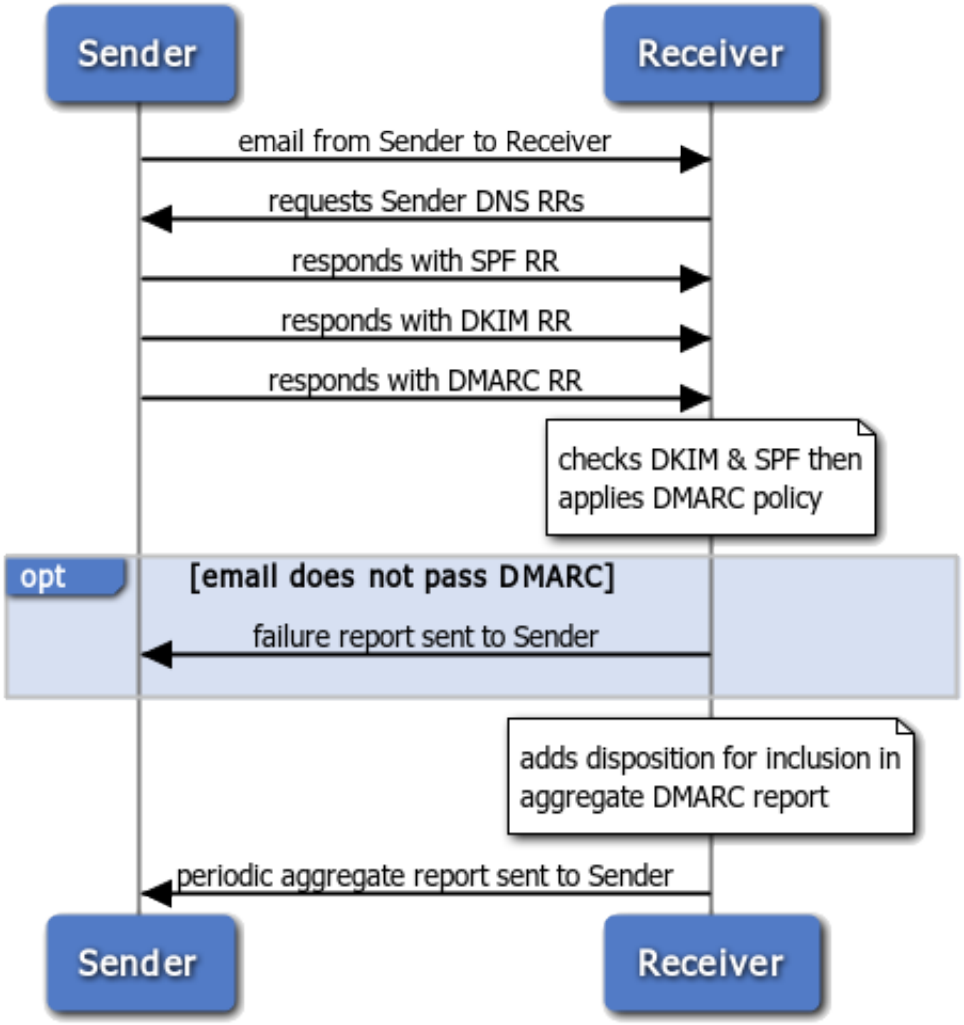
Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
pct	% of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=authfail@example.com
rua	Reporting URI of aggregate reports	rua=aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=strict
aspf	Alignment mode for SPF	aspf=relaxed

DMARC Reporting Specification

- Reporting is redacted for privacy
- Daily Aggregate reports, per From: domain
  - Does NOT contain delivery disposition
  - Does NOT contain individual email addresses
- Aggregate statistics by IP address
  - Authentication results for DKIM and SPF
  - DMARC identitifier alignment results
  - Policy actions requested and taken

```
<record>
  <row source_ip="173.0.84.226" count="1963" policy_domain="paypal.com" policy="reject" action_taken="none" />
  <identities envelope_from="intl.paypal.com" header_from="intl.paypal.com" />
  <auth_results>
    <dkim result="pass" human_result="" d="intl.paypal.com" />
    <spf domain="intl.paypal.com" identity="spf_envelope_from" result="pass" />
  </auth_results>
</record>
```

Swimlane: *Sender to Receiver*



DMARC Steps for Outbound Authentication

1. Deploy DKIM & SPF
2. Ensure identifier alignment
3. Publish a “monitor” record and ask for data reports (you will need the capability to process this data… build or buy)
4. Learn from the data, gain confidence in your mail streams
5. Slow roll actionable policies, from "monitor" to “quarantine” to “reject”

The Value of DMARC

Senders

- Improves resiliency of email authentication infrastructure
- Provides control over brand in email channel
- Lowers risk of hijacking
- Enables new forms of communication over email

Receivers

- Decreases spam
- Lowers risk of hijacking
- Enables new forms of communications over email

DMARC

Domain-based Message Authentication, Reporting & Conformance

Read the specification, and join the discussion at **dmarc.org**