DKIM Update

RIPE-53

Eliot Lear

RIPE & IETF: Perfect Together

From The RIPE Anti-Spam WG charter:

To develop a "Code of Conduct" to which ISPs might agree to adhere. It is foreseen that this document might be used as an indication that a signing party would make efforts to ensure that their customers are not responsible for abuse of the network resources of others or that they would be prepared to take actions to combat network abuse.

True or False?

We can eliminate SPAM through technical means.

False. But we can identify bad actors and reduce it.

True or False?

We can eliminate Phishing through technical means.

True. However, improved authentication is required.

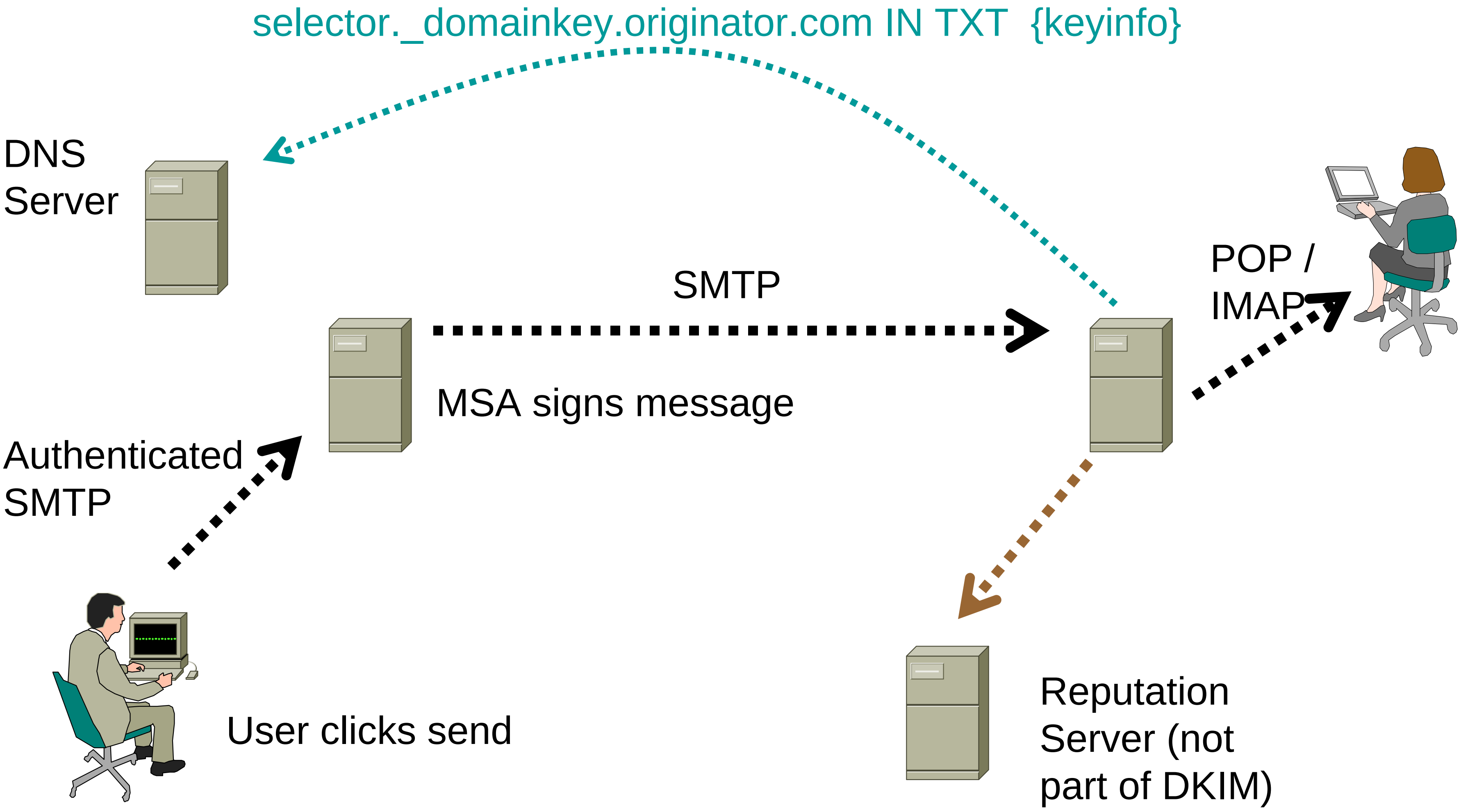
What DKIM is NOT

- DKIM is not a replacement for PGP or S/MIME
- DKIM is not a path-based authentication mechanism
- DKIM does not say whether a message is or is not Spam

What DKIM Is

- DomainKeys Identified Mail
- A signature-based approach that identifies a message as authorized by a domain administrator.
- Transparent to end users.
- Three key components:
  - Signature in message
  - Public key in DNS
  - Signing Practices in DNS

Where does DKIM Work?



selector._domainkey.originator.com IN TXT {keyinfo}

DNS Server

SMTP

POP / IMAP

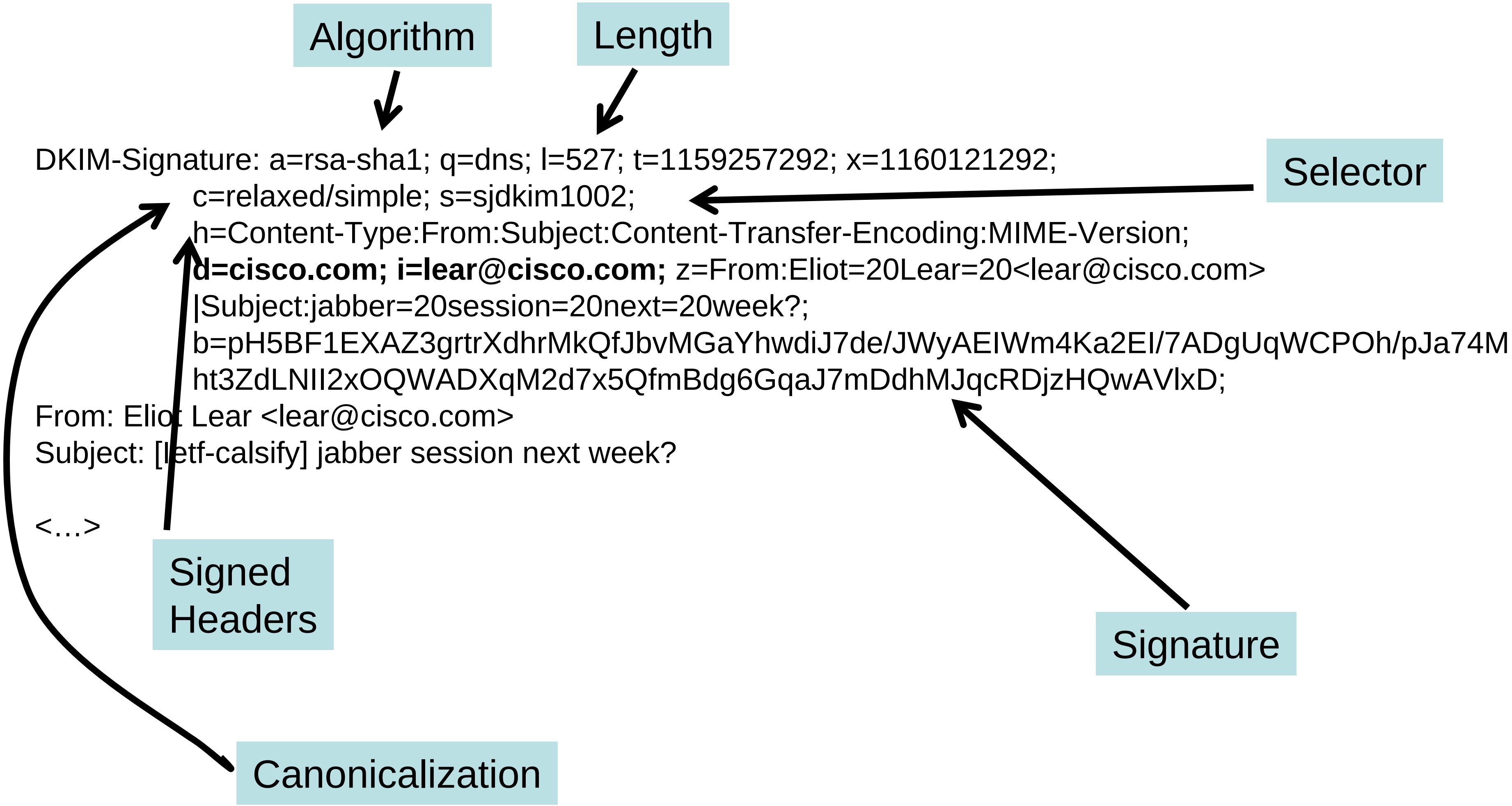
MSA signs message

Authenticated SMTP

User clicks send

Reputation Server (not part of DKIM)

How does it look?



```
DKIM-Signature: a=rsa-sha1; q=dns; l=527; t=1159257292; x=1160121292;
        c=relaxed/simple; s=sjdkim1002;
        h=Content-Type:From:Subject:Content-Transfer-Encoding:MIME-Version;
        d=cisco.com; i=lear@cisco.com; z=From:Eliot=20Lear=20<lear@cisco.com>
        |Subject:jabber=20session=20next=20week?;
        b=pH5BF1EXAZ3grtrXdhrMkQfJbvMGaYhwdiJ7de/JWyAEIWm4Ka2EI/7ADgUqWCPOh/pJa74M
        ht3ZdLNII2xOQWADXqM2d7x5QfmBdg6GqaJ7mDdhMJqcRDjzHQwAVlxD;
From: Eliot Lear <lear@cisco.com>
Subject: [ietf-calsify] jabber session next week?

<…>
```

In DNS…

Selector

```
sjdkim1002._domainkey.cisco.com text “v=DKIM1\; h=sha1\;
    k=rsa\; g=*\; s=email\; t=y\;”
   “p=MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhALhyyicVGqF5lObI
      l4ZyPVEJAmexX3tgxrgGe3SDT0sqAdGtrVRtA8vfhRHpHBIY
      +5qS3ibSMY/+xotoU4NBlDwq1rn/lul/lEi8szfUGgJ8T1Ht
      qiAIo2iUEZZ4RFbtJQIDAQAB”
```

Public Key

Currently TXT records. Maybe a new record later, depending on key sizes.

What’s Done

- Draft approved by IETF WG, awaiting IETF-wide “Last Call”
- Implementation done for sendmail.
- DKIM Consortium now building products.
- Many already using earlier verison “Domain Keys” (Yahoo!, Google)

What’s Not Done

- Sender Signing Practices (SSP) – in progress.
- Many will need to cut over to new version.
- Many more should implement and deploy DKIM (you can help)
- Reputation services need to make use of the identities
- We need to continue to improve authentication and security practices.

Thanks for your time

Questions? Discussion?