DKIM

Patrik Fältström

Based on material produced by among others: Sanjay Pol, Ashok Ramaswami, Jim Fenton and Eric Allman

September 22, 2005

What is Domain Keys Identified Mail?

- Method of using cryptographic signatures for email authentication
- Signature is intended to protect sender from spoofing and recipients from phishing
- Mechanism designed to minimize impact on existing mail infrastructure:
  - Uses DNS for key management
  - Does not require certificate authorities
  - Does not require client changes
- DKIM is a hybrid of two prior message signature proposals
  - Identified Internet Mail (Cisco)
  - DomainKeys™ (Yahoo!)

Status of DKIM

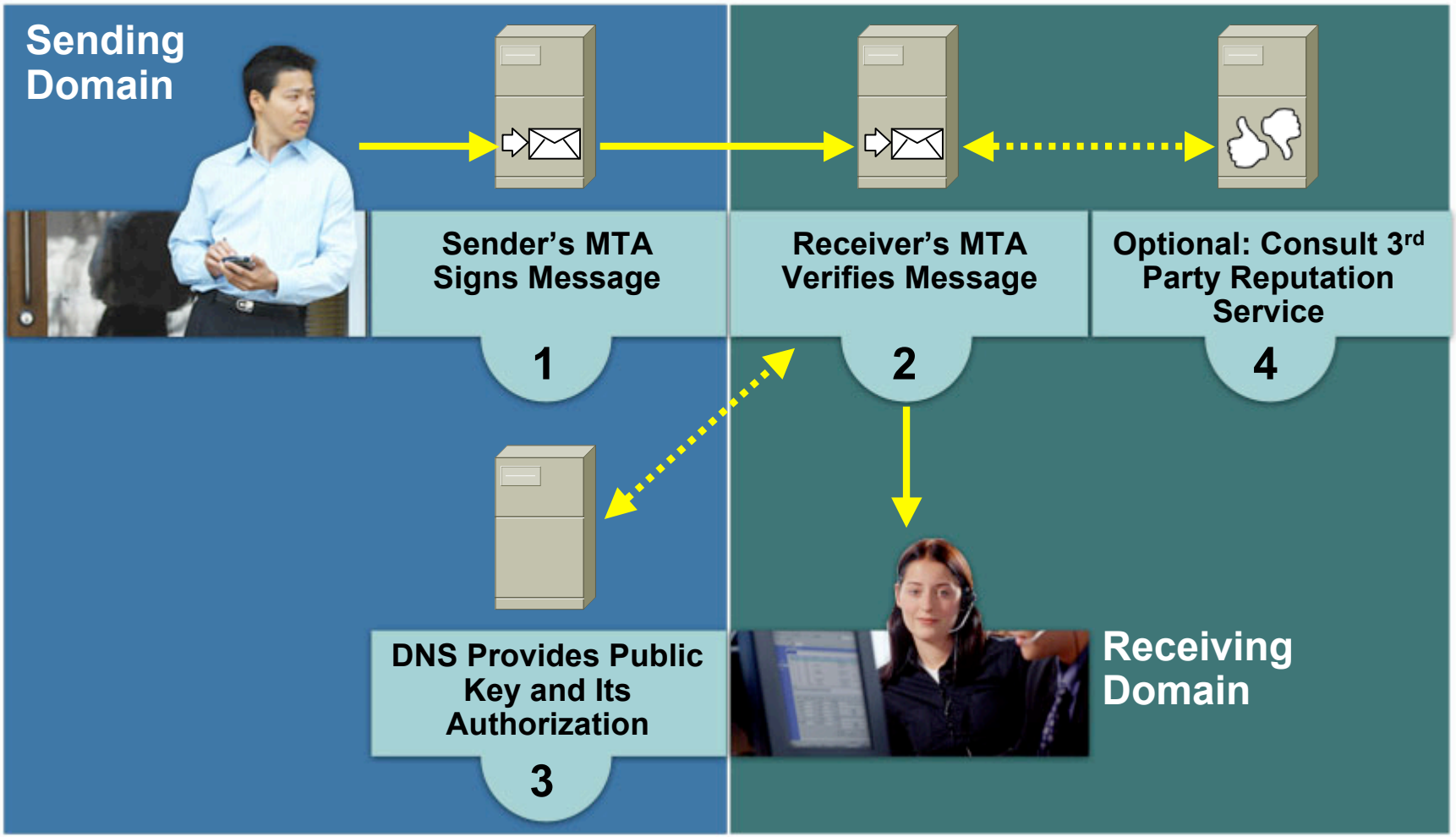
- Draft of base specification submitted to IETF
  - BOF held at IETF 63 – jabber log available at http://www.xmpp.org/ietf-logs/mass@ietf.xmpp.org/2005-08-04.html
  - Work in progress on signing policy
  - Work of new RR type for DNS is planned
- Standardization process will start with formation of working group at IETF (expected)
- At least four interoperating prototype implementations
- Tools and other information for deployment will be made available over the next 3-6 months

DKIM Goals

- Low-cost (avoid large PKI, new Internet services)
- No trusted third parties required
- No client User Agent upgrades required
- Minimal changes for (naïve) end users
- Validate message itself (not just path)
- Allow sender delegation (e.g., outsourcing)
- Extensible (key service, hash, public key)
- Structure usable for per-user signing

DomainKeys Identified Mail Explained

Cisco.com



Authentication/Authorization Model

Messages Must Pass Two Tests Before They Are Authenticated

AUTHENTICATE THE MESSAGE

Receiving Domain Authenticates the Message—i.e. Verifies that the Message Was Not Altered in any Consequential Manner Prior to Reaching the Receiving Domain

AUTHORIZE THE SENDER

Receiving Domain Asks Sending Domain to Confirm that Whoever Signed the Message Was Authorized to Do So (Without Having to Identify the Sender)

Technical Overview

- Signs body and selected header fields
- Signature transmitted in DKIM-Signature header field
  - DKIM-Signature is self-signed
  - Signature includes the signing identity (not inherently tied to From:, Sender:, or even header)
- Initially, public key stored in DNS (new RR type, fall back to TXT) in `_domainkey` subdomain
- Namespace divided using *selectors*, allowing multiple keys for aging, delegation, etc.
- Sender Signing Policy lookup for unsigned, improperly signed, or third-party signed mail

Example of DKIM Signed Message


```
Subject: Sample message
From: John Doe <jdoe@example.com>
To: Mary Smith <msmith@example.net>
Content-Type: text/plain
Message-Id: <1098727240.13184.0.camel@lucid.example.com>
Mime-Version: 1.0
X-Mailer: Ximian Evolution 1.4.6 (1.4.6-2)
Date: Wed, 25 May 2005 11:00:40 -0700
Content-Transfer-Encoding: 7bit
DKIM-Signature: a=rsa-sha1; d=example.com; s=may2005;
  i=jdoe@example.com; c=nowsp; q=dns; t:1098727241; x:10988893641;
  h=Subject:From:Date;
  b=QQgUTUMvDA1BPxxIpSrAiAUXB5rtOt4tJT1BcN3zB01pUARhybDLGF7KLU7ens
  Wie1Zcm7+h51fOhYvuy3DUTQ==;

Did you receive today's sales orders yet?

-John
```

DKIM-Signature header

- Example:

```
DKIM-Signature: a=rsa-sha1; q=dns;
  d=example.com;
  i=user@eng.example.com;
  s=jun2005.eng; c=nowsp;
  t=1117574938; x=1118006938;
  h=from:to:subject:date;
  b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb
    av+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

- DNS query will be made to:

```
jun2005.eng._domainkey.example.com
```

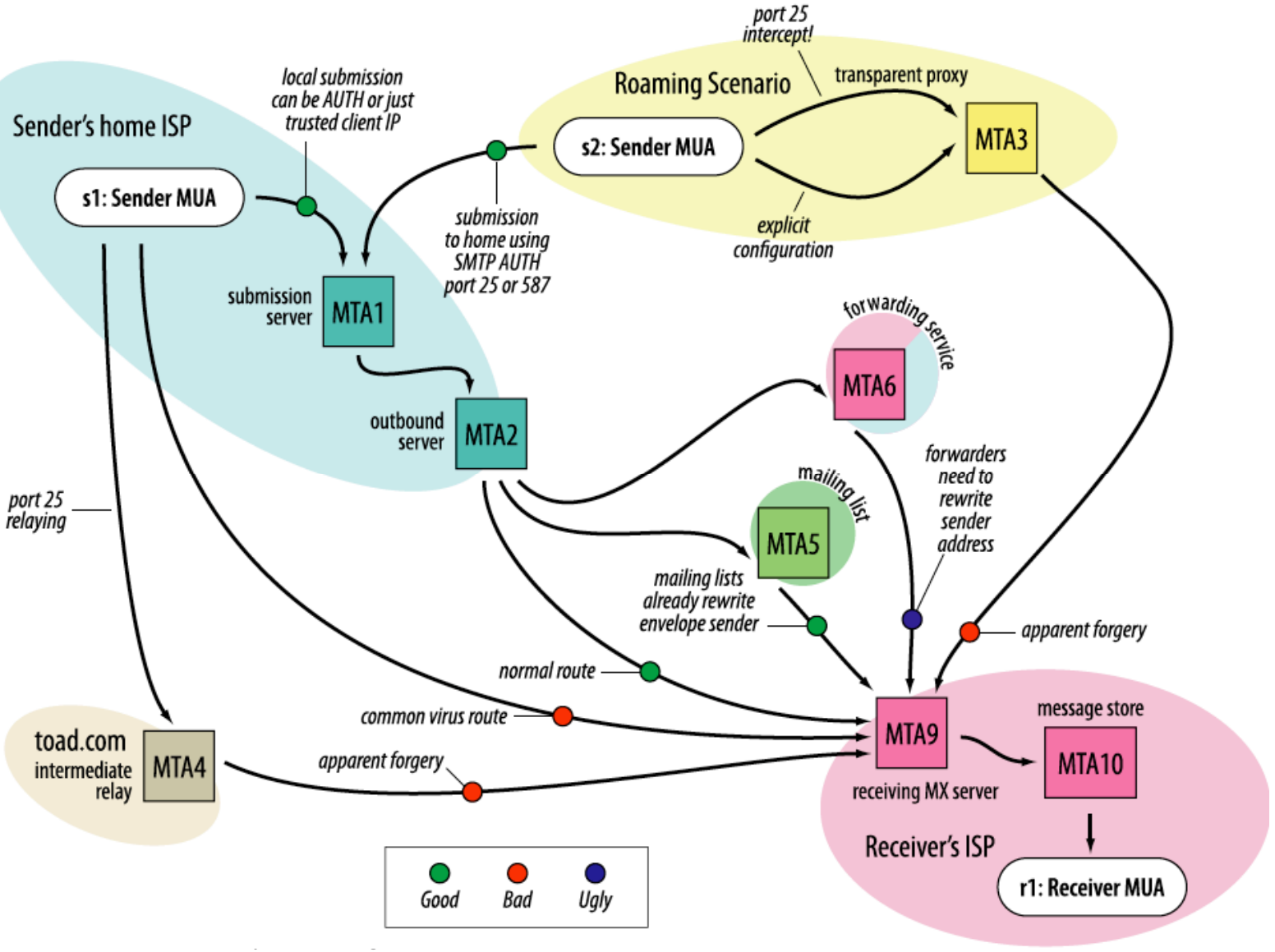
Controversial Points

- Not using S/MIME, PGP, PEM, …
  - Different goals, not intended to displace
- Use of i= & g=
  - Not redundant, e.g., g=marketing-*
- Body length counts (l=)
- Extensive per-user keys in DNS may hurt DNS
  - Should extend query mechanisms for this
- “Replay attacks”
  - Not a bug, any more than in S/MIME
- Canonicalization algorithms

Further Work Needed

- Resolve bullets from previous slide
- New DNS RRs undefined
- Sender Signing Policy document needs work
  - Notably binding of signature to header fields
- Threats document
  - Discussed in Security Considerations; separate document in process

Email delivery….



Deploying Message Signing

- **Deploy a signature-capable MTA**
  - Major MTA appliance vendors are adding signature support
  - “Milter” API software available for sendmail
  - DomainKeys toolkit for other MTAs (e.g., qmail)
- **Generate and publish message signing keys**
  - Published in DNS records in a separate subdomain
  - May delegate key subdomain to mail administrators
  - Optional: publish a message signing policy
- **Tell users how to handle message verification results**

Deployment - Enterprise perspective

- Key record in DNS
  - Typically different groups manage DNS and email infrastructure
  - Delegating key server to email group is one way to mitigate
- Expertise of email group to create DNS entries
  - Mitigate by providing comprehensive toolkit
- Need to audit email flows to determine what to sign
  - Multiple domains
  - Traveling users
  - Handheld devices
  - Outsourced service providers (ex; benefits)
- Signing requirements of smaller domains that use outsourced email services
  - Is DNS managed by the service provider?
  - Is DNS delegated for key records?
- Broad MTA support
  - Interoperability

Limitations to consider

- Handling mailing lists/ forwarders
  - Emails sent through a mailing list of forwarding address may be modified
  - Canonicalization methods define acceptable changes
  - Message signing policy can be used to define intermediate signing
- Roaming users who need to send email messages from handheld devices
  - Need to ensure email flows are architected for signing
- Exposure to replay attacks
  - Sender ID / SPF along with reputation services will help mitigate

Industry wide cooperation

… and several other partners