Proposal for a Pilot Project: Using DKIM to Create a Email Trust Channel

Dave Crocker
Brandenburg InternetWorking
bbiw.net
Roadmap

- Trust with domain names: Why do DKIM?
- DKIM authentication basics
- Reputation layer above signature layer
- A modest publishing proposal
Reputation — Using IP vs. Domain

**IP**

**Pros**
- Can be at SMTP time
- Lots of existing practice
- High granularity

**Cons**
- Dynamic
- Not portable
- Shared among senders
- Tied to machine, not org.

**Domain Names**

**Pros**
- Aligns better with org
- Long-term stability
- Less long-term admin
- Can be delegated

**Cons**
- Must wait for message header to be transmitted
- More complex software
Mistrust and Trust are Different

- **Mistrust**
  - Actor is typically hidden and unaccountable
  - Look for bad behavior
  - Heuristic results – with false positives

- **Trust**
  - Actor is accountable and collaborative
  - Presumes good intent
  - Problems are “errors”, not abuse
Trust is a separate channel
DKIM – Identify a Responsible Party

Goals

- Compatible/transparent with existing infrastructure
- Minimal new infrastructure
- Implemented independently of MUA clients
- Deployed incrementally
- Permit delegation of signing to third parties (non-authors)

Non-Goals

- No assertions about behaviors of signing identity
- Not directions to receivers
- No protection after signature verification.
- No re-play protection
  - Transit intermediary or a recipient can re-post the message


© 2008, D. Crocker
**DKIM Core Technology – RFC 4871**

- **Authenticated identity**
  - DKIM-specific parameter
  - From:, Sender:, intermediary, mailing list, other…

- **Authentication mechanism**
  - Cryptographic signing
  - Signer chooses header fields to include [+ body]

- **DNS query mechanism**
  - Identity + selector defines query string
  - Produces public key

- **Effort to add to origination**
  - Private key
  - Signing module

- **Effort to add to reception**
  - Public key
  - Validation module

- **Limitations**
  - Minimal robustness against mailing lists
  - Relaying can break signature
Sample DKIM Signed Message

Received: from mercury.example.net (HELO mercury.example.net) ([192.168.1.1])
   by mail.example.com with ESMTP/TLS/DHE-RSA-AES256-SHA; 01 Oct 2008 17:11:15 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=example.net;
   s=dorrington; t=1222881075; bh=HOVyUZdDUFeesnM3UlaizGPhdeJQS6N061IKw
   7iUjZ4=; h=Message-ID:Date:From:MIME-Version:To:Subject:
   Content-Type:Content-Transfer-Encoding; b=kp3vRZo7CiYpOz8lQtlOTZ+W
     Gl+Cd+te3KPLzFVopncLnmfyNE0XToxOqSo9FZfz7an9B25gxfZpZ80LpXmaZmtxx
     tikwSp0gdDJOWHUtGD2zs1osjDbRKT6KyNYb7
Message-ID: <48E3AF2E.10108@example.net> Date: Wed, 01 Oct 2008 10:11:10 -0700 From: Alice Smith <alice@example.net> MIME-Version: 1.0
To: Bob Brown <bob@example.com>
Subject: Tomorrow's meeting
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
Authentication-Results: mail.example.com; header.From=alice@example.net; dkim=pass ( sig from example.net/dorrington verified; );
Status

- **dkim.org/#deployment**
- 20(!) at interop event
- 18 software; 5 service
  - Steady adoption rate
- Relatively minor early-stage rough edges
  - Some confusion about identity to evaluate —DKIM has two identity parameters (d= and I=)

Further work
- ADSP – publish signing practices to detect messages that should be signed
- Authentication-Results – header from signature validator to identity assessor
- …
Authentication is Useless...

* ... by itself
  * We all say this, but do we appreciate what it really means?
* We often say: *If you have a validated name, you can make simple decisions for folks you know.*
  * After all, you already know that I’m a great guy…
  * But this means really means you’ve gone beyond simple authentication… into reputation.
* This added layer is a barrier to adoption of authentication!
  * Must have a reputation step, before an adopter gets value.
  * Potential adopters of authentication are waiting for compelling and immediate utility *that is turnkey*.
Can a simple project help?

- Some utility, based on authentication
  - *Without prior sender/receiver arrangement*

- Goals
  - Simple, useful
  - Not compete with “reputation” services…
  - Possibly serve as a template for others

- Proposal
  - Published Member List (PML)
Published Member List (PML)

- **Pilot project**
  - Create an email trust domain among member institutions to permit streamlined email filter handling.
  - Demonstrate utility of validated membership lists

- **Publish a list of a group’s members**
  - Membership *can be* a meaningful “indication” of Goodness
  - Might publish related attributes, like type of institution
  - Assessor might interpret favorably, but not give message a free pass

- **Could be template for other organizations**
  - Banks, Airlines, Governments, Political Parties…
Project Details

- Write charter for project
- Define expected use by assessment engine
- Agree on list semantics
- Evaluate legal implications
- Document and publish it

- Obtain agreements to publish
- Define DNS/VBR* query format
- Begin operation
- Document the project
- Recruit spamassassin and other users of list

* VBR: Vouch by Reference
  <http://www.domain-assurance.org/protocol-overview.phtml>
Attributes in an Entry

- Domain name
- Associated name of institution
- Member attributes, such as
  - Type of institution
  - ...?
Audience Survey

**Interest?**
- Idea of membership lists
- Participation in pilot project

**Concerns?**