DKIM Deployment Experiment

Document Status: Discussion Draft

A Proposed DKIM deployment experiment for the Higher Education community
RL "Bob" Morgan, University of Washington and Internet2

We propose an experiment to assess the value of a deployment of DKIM among a set of higher-education institutions in the US and in other countries. It is an experiment (rather than a pilot) because the utility and applicability of the technology is still the major question. The proposed plan has these steps:

1. Engage a number of institutions.
   Engagement would require participation from a skilled email technologist and, preferably, an analyst or architect. The email technologist should be familiar with modern email processing methods and should be responsible for technical decision-making for the institutional email system. Engagement would also imply willingness and ability to make changes to at least a portion of the production email service for the institution in support of the experiment. We will also attempt to take advantage of existing trust communities such as InCommon (in the US), Swamid (in Sweden), and the UK Access Management Federation.
2. Design the experiment.
   The experiment would consist of deployments of DKIM signing and verification services at the participant institutions, including key management and distribution, and modifications to spam processing. It would also include logging/monitoring components so statistics can be compiled on usage.
3. Conduct the experiment.
   It would run for a defined period of time, perhaps six months. Participants would communicate status and stats throughout, and modify operations as needed.
4. Report results.

Questions the experiment could address:

- Do signing domains need to state what their signing means, aka what their signing practices are?
- How does this relate to email outsourcing? Might institutions that have outsourced some or all of their email want their providers (e.g. Google, Microsoft) to sign/verify?
- Can all outgoing email be signed or just a subset? if a subset, how is it chosen?
- How does email signing integrate into outbound email processing? Does signing require massive CPU power or cause delivery delays?
- How does validation integrate into inbound mail processing and policy?
- Does DKIM provide benefits to email for the defined community that make it worth deploying? For example, does it solve problems like improving delivery success of mail to alumni and students using commodity email services?
- Is DKIM deployment useful prior to availability of standard signing-practices methods?
- What interoperability problems exist among differing implementations?
- What is the effect of failure cases (message validation failure due to modifications in transit, etc)?