DKIM Overview Document

IETF 66

Tony Hansen

Dave Crocker

Phillip Hallam-Baker

Outline

1. Introduction
   - About This Document, A Quick Overview of DKIM, Outline Potential DKIM Applications
2. DKIM Within Existing Internet Email
   - Review of Internet Mail Service Architecture, Where to Place DKIM Functions, Impact on Email Activities, Migrating from DomainKeys
3. DKIM Service Architecture
4. Relationship to Previous Message Signature Technologies
   - Transparent Signature, Treat verification failure as if unsigned, Legacy Client Semantics, Key Centric PKI, Domain Level Assurance, Security Policy
5. Implementation Considerations
   - Development, Deployment, Operations
6. Outline Future Extensions
   - Introducing a new signing algorithm, Possible future signature algorithm choices, Transition strategy, Linkage to Other PKIs, Trusted Third Party Assertions, Linkage to X.509 Certificates, XKMS, Verification in the Client, Per user signature, Encryption, Reuse of Key Record, Use of Policy Record

Issues

- Only a few posted so far
  - Various suggestions we concur with
  - Issues about describing I/O vs. CPU boundness
  - Wording issues around failure situations
  - Wording issues around trust, reputation

What's missing?

- Mail list administrators
  - Good practices (How *should* a mailing list play well with DKIM?)
- ???? (Send your cards and letters!)

Q&A