Identified Internet Mail
draft-fenton-identified-mail-00

Jim Fenton <fenton@cisco.com>

Identified Internet Mail Characteristics

- Header-based message signature
- Public key typically included in message
- Explicit support for user and domain-level signatures
- Specific headers signed at originator's option
  - Copies of signed headers in signature
- Key verification via query to originating domain
- Signing/verification typically in MTA, possible in MUA
- Header defined for conveying verification result to MUA, if desired
- Ability to query originating domain to determine outgoing mail policy
  - How to treat unsigned mail; should it be discarded?

Why user-level keying is needed

- Users who need to sign their own messages
  - People with “affinity addresses” (e.g., ieee.org) where that domain doesn’t operate an outgoing MTA
  - Users that are restricted to particular outgoing MTAs (some hotels, enterprises)
- Outsourced business functions like benefits providers and advertising partners want to send email as their client
- Without user-level keying, email signing does not solve the usage limitations of Sender ID and similar approaches
- We expect:
  - Many domains will use only domain-level keys
  - Many domains will use primarily domain-level and a few user-level keys
  - A few domains will key entirely at the user level

Changes in progress since -00 draft

- “Body Counts”
  - Sender can specify a subset of the body to sign
  - Permits messages to be appended to without breakage
  - Further canonicalization improvements being considered
- Responsible address based on Sender or From headers rather than Envelope-from
- DNS or KRS (HTTP)-based key verification