Guidance on End-to-end E-mail Security and Header Protection

Daniel Kahn Gillmor <dkg@fifthhorseman.net>

IETF 117

LAMPS session

2023-07-27

draft-ietf-lamps-header-protection-15

- Changes since IETF 116 (draft -14):
  - Clean up minor nits received during WGLC
  - Now in MISREF state, waiting on **`e2e-mail-guidance`**

draft-ietf-lamps-e2e-mail-guidance-10

- Changes since IETF 116 (draft -05):
  - Add Bernie Hoeneisen and Alexey Melnikov as editors
  - Added guidance on:
    - Draft messages
    - Local certificates
    - “Intervening” MUAs (forwarders)
    - External subresources in `text/html` parts
  - **Move remaining TODOs into substantial “Future Work” appendix**
  - WGLC
  - Responded to WGLC reviews (Thanks everyone, especially Russ, Eliot, and Stephen)

“Future Work” in e2e-mail-guidance

- Maintenance of secret keys and user’s certificates
- Retreival, selection, and maintenance of peer certificates
- Syncing MUAs that use the same mailbox
- Indexing and Search
- Expectations of cryptographic protection
- Secure deletion
- Cached signature verification
- Cryptographic status in aggregate
- Interaction with opportunistically-encrypted messages

Requests to WG

Wrap up WGLC on **`e2e-mail-guidance`**?
Interest in tackling any part of “Future Work”?