End-to-End Cryptographic E-mail Guidance

Daniel Kahn Gillmor

IETF 109 / LAMPS
Useful concepts (Cryptographic Envelope, Cryptographic Payload, Cryptographic Layer)

Common user expectations

Guidance for composing messages

Guidance for interpreting messages

Common pitfalls and suggestions

Test Vectors
Example guidance

- Generate only simple, whole-message MIME structure
- Don’t render failed signatures (similar to DKIM)
- Don’t send encrypted-but-unsigned messages
- Avoiding cleartext leaks on replies to encrypted mail
- Enumerating ways that signatures can fail
- How to deal with an incoming message with bad MIME structure
- ...

How can you help?

- Review current draft
- Contribute suggestions
- Large to-do list already (§7) – pick one!

https://gitlab.com/dkg/e2e-mail-guidance
Call for adoption

• Willing to act as editor
• Happy to have interested co-editors
• Happy to be replaced as editor