Guidance for
End-to-end Cryptographic E-mail

LAMPS/IETF 111
Daniel Kahn Gillmor
draft-ietf-lamps-e2e-mail-guidance-00
draft-ietf-lamps-e2e-mail-guidance-00

• Just adopted by WG
• https://gitlab.com/dkg/e2e-mail-guidance
• Scope: Mail User Agents with end-to-end cryptographic protections
• Opinionated guidance on usability & security
• Opinions should come from experience
• No specific User Interface assumed
• Agnostic about PGP/MIME vs. S/MIME
Document Outline

- Expectations, shared definitions
- Reasonable types of protection (signed-only, signed+encrypted)
- Reasonable MIME structures (cryptographic envelope, cryptographic payload)
- Composition and Interpretation
- Certificate/Key management
- Common failures
Guidance needed!

• Classic IETF problem: mixed system with different security properties
• Lots of FIXMEs/TODOs
• You’ve run into trouble (as a user)
• You’ve run into trouble (as an implementer)
Optional elements

- Test vectors
- Example renderings of UI elements
- Implementer checklist
- ???
Lifecycle

- Dependency in Header Protection draft
- Living, ongoing document for community guidance
- RFC? Regularly-revised draft?