One e-mail message,
Recipients with different capabilities

- Carol writes to Alice and Bob
- Alice has a key, Bob does not (see draft-ietf-lamps-e2e-guidance §9.6):
  1. Carl can send encrypted to both; Bob can’t read the message ☹
  2. Carol can send in the clear to both ✓
  3. Carol can send encrypted to Alice, dropping Bob from the recipient list ✓
  4. Carol can send an encrypted copy to Alice, and a cleartext copy to Bob
- If Carol chooses (4), does Alice’s client represent the message as encrypted?
- If Alice wants to “reply all”, and replies to encrypted messages should be encrypted...
draft-dkg-mail-cleartext-copy
Problem Statement

• When recipients receive such an encrypted message:
  – How should the MUA describe it to the user?
  – How should the MUA behave when replying?
History

- IETF 116: secdispatch, marked as AD followup
- April 2023: discussion on LAMPS, some agreement to adopt, no objections
- draft-ietf-lamps-e2e-mail-guidance says this is probably not the most understandable approach, but some implementations do it.
- Related to e2e-mail-guidance “Future Work” §A.8 “expectations of cryptographic protections”
Possible design space

• How to signal? (*message header*)

• Signal in detail (which specific recipients did I not encrypt to?) vs. *boolean* (encrypted to all recipients?)

• How to interpret messages with no signal (what is the default)?
Updates from -01 to -02

• Add Daniel Huigens of Proton to authors
• New header: \texttt{E2EE-To-All} (values 0 and 1)
• Simple boolean (no detail to produce or parse)
• Focus on “visible recipients”
• Encourage removing this header from cleartext headers (see draft-ietf-lamps-header-protection)
• Default: vary based on how widespread use of the header is? (needs more clarity)
WG requests

• Please call for adoption
• Daniels Gillmor and Huigens willing to serve as editors if the WG desires
• Also willing to give up change control to the WG
• Review and give feedback!
• https://gitlab.com/dkg/cleartext-copy