null
Since 119
- MTI KDF is now at least one of HKDF, KMAC, with justification for both
- Address Jonathan Hammell’s review
  - Remove section introducing KEMs, move relevant bits to ML-KEM section
  - Remove KEMRecipientInfo processing summary, move relevant bits elsewhere
  - Minor editorial changes
- ASN.1

Next
- Wait for NIST
- Examples
- Harmonize with draft-ietf-lamps-kyber-certificates
- Include PK and CT in the KDF? (next slide)
PK and/or CT in KDF?

  “Any protocol in which revealing a private key or accepting private keys from a third party is part of the protocol flow, should use the seed used to generate the private key...”

  “The binding situation of ML-KEM are actually quite good: As long as the private key is not mal-formed, it is robust against any misbinding” – Sophie Schmeig

- Do we need to do anything?
  - CMS private keys are self-generated or from a (hopefully) trusted key manager.

- If yes, what?
  - Hope that NIST allows private key seeds and update draft-ietf-lamps-kyber-certificates to require private keys to be stored as seed?
  - Add PK and/or CT to KDF in draft-ietf-lamps-cms-kyber?