CMCbis

IETF 120 - LAMPS WG

Joe Mandel & **Sean Turner**

Datatracker: draft-mandel-lamps-rfc5272bis & draft-mandel-lamps-rfc5273bis & draft-mandel-lamps-rfc5273bis
GitHub: CMCbis

Status / Queued PRs

Status: Out for WG adoption; please chime in!

Queued PRs: (waiting for WG adoption decision to merge)

- Document Full PKI Request KEM support
  - Direct supported, Indirect not; Indirect never was supported by CMC
  - Use existing “No Signature” algorithm and encrypted / decrypted POP controls
  - Client sends KEM cert request, CA returns encrypted POP, client returns decrypted POP, CA returns certificate
  - Thanks to Mike: found some bugs
    - Returned POP is not plaintext it is HMACed (text != example)
    - Need to say something about `SignedData.SignerInfos.SignerInfo.sid` set to 4 bytes of zeros

Queued PRs / To Do

Queued PRs: (waiting for WG adoption decision to merge)

- Update 6955 related text
- Add pre-5378 boilerplate
- Add requirement for BCP 195
- Use HMAC-256 not HMAC-SHA1 in examples
- Erratum 3943

To Do:

- Crypto requirements in -rfc5273bis (includes adding KEM)
- Erratum 8027