CMCbis

IETF 118 - LAMPS WG
Joe Mandel & Sean Turner

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

Motivation & Changes & Question

Motivation: remove the SHA-1 & HMAC-SHA-1 defaults, process errata

Changes:

- -00 contents: 527*bis ⇒ 527*+6402+verified errata
- -01 contents: -00 + most of remaining editorial errata
- -02 contents: -01 + remaining errata + ‘08 ASN.1 (normative now)

Question:

- If we make SHA-1 a MUST NOT what’s the other algorithm SHA3 or SHAKE?