CMCbis

IETF 119 - LAMPS WG
Joe Mandel & Sean Turner

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

Motivation & Changes

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)

Motivation & Changes & Question

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

Changes:

- 5272-02: Added module to support new HMAC algorithms in PBKDF2
- 5273-02 contents: Replaced TLS 1.0 with TLS 1.2
- 5274-02: Updated intro + updated section naming and numbering to match intro

To-do:

- 5272-03: Address management of KEM certificate
- 5273-03: Add support for AuthEnvelopedData
- 5274-03: Update Cryptographic Algorithm Requirements

Question:

If we make SHA-1 a MUST NOT,
and SHA-256 is the MUST do we need a SHOULD algorithm: Nothing, SHA3, or SHAKE?