CMP Algorithms, CMP Updates, Lightweight CMP Profile

draft-ietf-lamps-cmp-algorithms-15 publishes as RFC 9481
Hendrik Brockhaus, Hans Aschauer, Mike Ounsworth, John Gray

draft-ietf-lamps-cmp-updates-23 publishes as RFC 9480
Hendrik Brockhaus, David von Oheimb , John Gray

draft-ietf-lamps-lightweight-cmp-profile-21 publishes as RFC 9483
Hendrik Brockhaus, Steffen Fries, David von Oheimb

Hendrik Brockhaus

IETF 118 – LAMPS Working Group

Activities since IETF 117 on CMP Algorithms

Draft was published yesterday as RFC 9481.

AUTH48 changes:

- Correction of OIDs in Section 6.2.3
- Moving RFCs 8551 and 8692 from the Informative References section to the Normative References section.

Activities since IETF 117 on CMP Updates

Draft was published yesterday RFC 9482.

AUTH48 changes:

- Added info about the rfc4210bis and rfc6712bis activity to Section 1.
- Minor changes to comments in the ASN.1 modules updating outdated algorithms, e.g., replaced DES-MAC and Triple-DES-MAC with HMAC-SHA256 and AES-GMAC.

Activities since IETF 117 on Lightweight CMP Profile

Draft was published yesterday RFC 9483.

AUTH48 changes:

- The profile only utilizes signature-based proof-of-possession according to RFC 4211 Section 4.1 point 3. Some text was added/changed in Sections 3 to 5 clarifying the binding of proof-of-possession and proof-of-identity with this regard.
- Section 5.2.2.1 was updated to clarify the usage of nested messages to add additional message protection.