CMP Algorithms, CMP Updates, Lightweight CMP Profile

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

draft-ietf-lamps-cmp-updates-23
Hendrik Brockhaus, David von Oheimb, John Gray

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

Hendrik Brockhaus

IETF 117 – LAMPS Working Group
Activities since IETF 116 on CMP Algorithms

Changes since IETF 117:
• -

Draft is approved by IESG for publication and waiting in RFC Editor queue. Document is in state REF.

ToDos in AUTH48:
• Contact information need to be updated.
• A typo is to be fixed.
Activities since IETF 116 on CMP Updates

Changes since IETF 116:
• -

Draft is approved by IESG for publication and waiting in RFC Editor queue. Document is in state REF.

ToDos in AUTH48:
• Section 1 should inform about the rfc4210bis and rfc6712bis activity.
• Section 2.7 needs an update of the guidance which CMS key management technique to use with encrypted values, see email thread "CMS: selection of key management technique to use for EnvelopedData".
• Section 2.27 requires a correction on the usage of EnvelopedData in POPPrivKey, see email thread "draft-ietf-lamps-cmp-updates Section 2.27 - Alignment with RFC4211 syntax".
Activities since IETF 116 on Lightweight CMP Profile

Changes since IETF 116:
- 

Draft is approved by IESG for publication and waiting in RFC Editor queue. Document is in state EDIT.

ToDos in AUTH48:
- A typo is to be fixed.
- Introduce LCMPP as abbreviation for “Lightweight CMP Profile” to be used in BRSKI-AE and potentially 3GPP.

Note that in the same batch of documents in RFC Editor queue, also the CoAP transfer for CMP is contained, which also references CMP Updates and LCMPP.