CMP Updates, CMP Algorithms, and Lightweight CMP Profile

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

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

draft-ietf-lamps-lightweight-cmp-profile-13
Hendrik Brockhaus, Steffen Fries, David von Oheimb

Hendrik Brockhaus

IETF 114 – LAMPS Working Group
Activities since IETF 113 on CMP Algorithms

Changes since IETF 113:
• Addressed AD and IESG review comments

Draft is approved by IESG for publication
Activities since IETF 113 on CMP Updates

Changes since IETF 113:
• Updated Section 3.4 introducing the path segment 'p' to indicate the following arbitrary label according to the discussion during IETF 113
• Addressed AD and IESG review comments

Draft is approved by IESG for publication
Activities since IETF 113 on Lightweight CMP Profile

Changes since IETF 113:

• Clarifying the combination of central key generation with certificate update
• Clarification that only one CRL per round-trip is requested
• Define more clearly that signature-based protection is the default protection and the exception for not protecting error message
• Introducing new well-known path segment ‘p’ for profile labels
• Updated the requirements on supporting PKI management operations required for EEs, RAs, and CAs

Waiting for AD review.
IESG requests LAMPS to submit RFC4210bis and RFC6712bis drafts

- IESG requests LAMPS to submit RFC4210bis and RFC6712bis documents merging the updates specified in CMP Updates with the original text.
- The RFC4210bis activity may open a discussion about the entirety of RFC4210 (written in 2005) under the modern crypto protocol design philosophy, and the WG must be prepared to deal with it. Some ADs already announced a review of the complete text of the -bis drafts, including the unchanged text of the original RFCs.
- The authors of CMP Updates would provide:
  - 00 versions containing the original RFC text
  - 01 versions merging the updates specified in CMP Updates
  - 02 versions fixing reported issues from idnids
- To respond to comments on the original text of the RFCs help by the original authors and/or the WG is required.

Is any of the original authors or other volunteers willing to join as co-author of the -bis drafts?

27 July 2022
Hendrik Brockhaus - Siemens