CMP Algorithms, CMP Updates, and Lightweight CMP Profile

draft-ietf-lamps-cmp-algorithms-03
Hendrik Brockhaus, Hans Aschauer, Mike Ounsworth, Serge Mister

draft-ietf-lamps-cmp-updates-08
Hendrik Brockhaus, David von Oheimb

draft-ietf-lamps-lightweight-cmp-profile-05
Hendrik Brockhaus, Steffen Fries, David von Oheimb

Hendrik Brockhaus

IETF 110 – LAMPS Working Group

Activities since IETF 109 on CMP Algorithms

All issues from IETF 109 and subsequent discussion on the mailing list were addressed

- Added Hans Aschauer, Mike Ounsworth, and Serge Mister as co-author

Changes to Section 2

- Added SHAKE digest algorithm

Changes to Section 3

- Deleted DSA
- Added RSASSA-PSS with SHAKE
- Added SECP curves to section on ECDSA with SHA2, ECDSA with SHAKE, and EdDSA

Changes to Section 4

- Deleted static-static DH and ECDH
- Added ECDH OIDs and SECP curves, as well as ECDH with curve25519 and curve448
- Deleted RSA-OAEP, but re-added it after discussion on the mailing list
- Added a paragraph to explain that the algorithms and key length for content encryption and key wrapping must be aligned

Activities since IETF 109 on CMP Algorithms

Changes to Section 5

- Deleted AES-CCM and AES-GMC and added AES-CBC

Changes to Section 6

- Added PBMAC1 and restructured text to easier differentiate between password- and shared-key-based MAC
- Deleted Diffie-Hellmann based MAC
- Added AES-GMAC and SHAKE-based KMAC

Changes to Section 7

- Moved former Appendix A to new Section 7
- Added a draft of a generic algorithm selection guideline
- Added a column to Table 1 in Section 7.2 to reflect the changes to RFC 4210
- Added a proposal for mandatory algorithms for the Lightweight CMP Profile

Changes to Section 9

- Added a paragraph to discuss backward compatibility with RFC 4210

CMP Algorithms - Status and ToDos

Complete Section 7. Algorithm Use Profiles

- Section 7.1 on general guidance on selecting an appropriate set of algorithms need to be extended. I think something like the text of the Security Considerations of RFC 5480 with references to NIST SP800-57 Part 1 Revision 5 Section 5.6 and ECRYPT-CSA D5.4 2018 Section 4.6.
  → **Is there any guidance from the group?**
- Section 7.2 is complete. Any feedback from people maintaining existing implementation of this profile are welcome.
- Section 7.2 is complete. Any feedback from people planning to implement this profile are welcome.

Any further feedback is welcome!

Activities since IETF 109 on CMP Updates

All issues from IETF 109 and subsequent discussion on the mailing list were addressed

- Added David von Oheimb as co-author
- Added a ToDo to Section 2.2 to reflect a current discussion on the need of an additional CMP-CA role and EKU and differentiation from CMP-RA
- Added or updated Sections 2.3, 2.6, 2.15, 2.16, and 2.20 to introduce new protocol version cmp2021
- Added Section 2.4 to refer to I-D.ietf-lamps-crmf-update-algs
- Added ToDos to Section 2.12 and 2.13
- Update Section 2.14 to make the minimal changes to the respective section in CMP more explicit
- Updated Section 2.17 to add new OID-requests for id-regCtrl-algId and id-regCtrl-rsaKeyLen
- Added Section 2.21 to update the Algorithm Use Profile in Appendix D.2 with the reference to the new CMP Algorithms document
- Updated Section 3.1 to delete the description of a discovery mechanism

Questions regarding EKU for id-kp-cmcCA

2.2. New Section 4.5 - Extended Key Usage

Tomas Gustavsson asked the question if a specific EKU for a CMP CA is required. There are two cases:

1. The CA uses its own key for the CMP endpoint
2. The CA uses a different key for the CMP endpoint and whishes to indicate the delegation of its role to the holder of this key

Isn’t the role of the entity in case 2 holding the new key the role of an CMP RA and the EKU id-kp-cmcRA is sufficient?

RFC 6402 (CMC Updates) introduced the EKUs reused by CMP Updates. Is there anyone recalling the use case for CMC CA based on the question above?

Remaining ToDos for CMP Updates

- Update Section 2.12 to request an update from a specific Root CA
- Update Section 2.13 to request a specific certificate request template

Any further feedback is welcome!

Activities since IETF 109 on Lightweight CMP Profile

All issues from IETF 109 and subsequent discussion on the mailing list were addressed

- Added algorithm names introduced in CMP Algorithms Section 7.3
- Updates Syntax in Section 4.4.3 due to changes made in CMP Updates
- Deleted the text on HTTP-based discovery as discussed in Section 6.1
- Updates Appendix A due to changed syntax in Section 4.4.3

Proposal for PSK cipher suites

6.3. HTTPS transport using shared secrets

We would like to specify suitable TLS cipher suite for use with pre-shared secret information, e.g., passwords.

- Proposal for TLS 1.2:
  - TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 or
  - TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256
- Proposal for TLS 1.3:
  - handshake mode psk_dhe_ke and cipher TLS_AES_128_GCM_SHA256

Remaining ToDos for Lightweight CMP Profile

- Double check sections on ‘preconditions’ for PKI management operations in Section 4
- Decide on extending of flow charts in Section 4 and 5
- Decide on simplifying error reporting in Section 4.3 and 5.3
- Update Section 4.4.2 and 4.4.3 based on outcome of the previous discussion on new CMP support messages
- Decide on extending Section 5 to address processing of messages next to forwarding

Any further feedback is welcome!