CMP Updates, CMP Algorithms, and Lightweight CMP Profile

draft-ietf-lamps-cmp-updates-12
Hendrik Brockhaus, David von Oheimb

draft-ietf-lamps-cmp-algorithms-06
Hendrik Brockhaus, Hans Aschauer, Mike Ounsworth, John Gray

draft-ietf-lamps-lightweight-cmp-profile-06
Hendrik Brockhaus, Steffen Fries, David von Oheimb

Hendrik Brockhaus

IETF 111 – LAMPS Working Group

Activities since IETF 110 on CMP Updates

All issues from IETF 110 and subsequent discussion on the mailing list were addressed

- Referred to RFC 6402 for definition of id-kp-cmcCA and id-kp-cmcRA
- Define id-it-rootCaCert and id-it-certProfile and allow a sequence of certificate profiles in CertProfileValue
- Add hashAlg field to the CertStatus type to support certificates signed with a signature algorithm not explicitly indicating a hash algorithm in the AlgorithmIdentifier
- Explicitly indicate the root CA for which an update is requested by using id-it-rootCaCert and the requested certificate request template by using id-it-certProfile
- Added localKeyId attribute to Appendix A.1
- Exchanged the import of CertificationRequest syntax from RFC 2986 to the definition from RFC 6402 Appendix A.1

Remaining ToDos for CMP Updates

Draft is stable and text looks mainly complete.

- Another update needs to be submitted after IETF 111 to address feedback from Sean (errata on RFC 4210), Russ, and Lijun
- Update ASN.1 modules addressing feedback from Russ
- Final internal review is ongoing, comments may require an updated version

Any further feedback is welcome!

The authors think, that the document could proceed to WGLC before IETF 112.

Activities since IETF 110 on CMP Algorithms

All issues from IETF 110 and subsequent discussion on the mailing list were addressed

- Added John Gray to the list of authors
- Added text to clearly specify the hash algorithm to use for certConf messages for certificates signed with EdDSA
- Added some clarification of the use AES-GMAC
- Extended the guidance on the use of algorithms in Section 7
- Deleted the algorithms mandatory to support in Section 7.2
- Extended the Security considerations

CMP Algorithms - Status and ToDos

Draft is stable and text looks complete.

- Some formatting nits need to be fixed (missing spaces before and after references)
- Final internal review is ongoing, comments may require an updated version

Any further feedback is welcome!

The authors think, that the document could proceed to WGLC before IETF 112.

Activities since IETF 110 on Lightweight CMP Profile – 1

All issues from IETF 110 and subsequent discussion on the mailing list were addressed

General

- Multiple language corrections, clarifications, and changes in wording
- Aligned with updated versions of CMP Algorithms and CMP Updates
- Updated new RFC numbers for I-D.ietf-lamps-crmf-update-algs

Section 2

- Changed the requirements on the support of two RA use cases: adding protection to a single message is now mandatory and replacing protection is now optional.

Section 3

- Added reference to using hashAlg
- Added sub-sections on generic prerequisites to PKI management operations, generic message validation, and generic error reporting.

Activities since IETF 110 on Lightweight CMP Profile – 2

Section 4

- Added EE side state machine
- The generic error handling in Section 3.6 replaces the former error handling section.

Section 5

- Added description of behavior of PKI management entities when responding to requests
- Reworked usage of nested messages
- Updates on performing PKI management operation on behalf of another entity
- The generic error handling in Section 3.6 replaces the former error handling section.

Section 6

- Merged HTTP and HTTPS and added CoAP endpoints

Section 8

- Added sub-sections on security considerations on usage of shared secret information

Appendix A

- Updated the example and added newly registered OIDs to the example in Appendix A

Supersede polling with generic resend of original request

Today polling is only available for certificate request messages to cover delays in request approval.

Message flow:

1. ir, cr, kur, or p10cr
2. ip, cp, or kup with status “waiting”
3. pollReq
4. pollRep with checkAfter
5. pollReq
6. ip, cp, or kup

For asynchronous transport and delayed delivery of all types of messages polling is not feasible.

Our proposal in cases of delayed delivery is to respond with an error message indicating when to resend the original request:

1. ir, cr, kur, or p10cr, certConf, rr, or genm
2. error with status “waiting” and resend wait time
3. ir, cr, kur, or p10cr, certConf, rr, or genm (identical to 1.)
4. ip, cp, kup, pkiConf, rp, or genp

This change would simplify the polling mechanism for certificate requests and enable asynchronous transport for all message types. No changes to the ASN.1 syntax is needed, only the interpretation of the error message needs to be extended.

Remaining ToDos for Lightweight CMP Profile

Draft is stable and text looks mainly complete.

- Possibly add a section on using the profile with BRSKI and SZTP
- Possibly replace delayed enrollment with delayed delivery, see previous slide
- Add further topics to the security considerations section on demand
- Final internal review is ongoing, comments may require an updated version

Any further feedback is welcome!

The authors think, that the document could proceed to WGLC before IETF 112.