CMP Updates and Lightweight CMP Profile

draft-ietf-lamps-cmp-updates-02

draft-ietf-lamps-lightweight-cmp-profile-02

Hendrik Brockhaus, Steffen Fries, David von Oheimb

IETF 108 – LAMPS Working Group

Activities since IETF 107 on CMP Updates

- Several issues and ToDos were addressed
  - Reuse id-kp-cmcCA and id-kp-cmcRA as proposed by Russ and Jim.
  - Changed from symmetric key-encryption to password-based key management technique for central key generation
  - Defined localKeyId to carry a key identifier of the revocation passphrase when using EnvelopedData
    > mailarchive.ietf.org/arch/msg/spasm/jBkcKuoKSiUasks1_rzHxiht3Us/
  - Moved the change history to the Appendix

Remaining ToDos for CMP Updates

- Define and register OID id-kp-cmKGA at IANA (pre-registration is requested)
- Update description of id-kp-cmcCA and id-kp-cmcRA at IANA
- Complete appendix with ASN.1 modules
- Polish wording and correct typos

Besides these ToDos, the text should be complete.

Any feedback is welcome!

Activities since IETF 107 on Lightweight CMP Profile - Part 1

- Several issues and ToDos were addressed
  - Changed delayed enrollment to OPTIONAL
  - Completed section ‘Request a certificate from a trusted PKI with signature protection’
  - Added an example for the certTemplate, see also Appendix B
  - Changed from symmetric key-encryption to password-based key management technique for central key generation
    > mailarchive.ietf.org/arch/msg/spasm/hOVFUSoH0ObCkBTFkR45h4pyA3E/
  - Defined new OID id-it-rootCaKeyUpdate
    > mailarchive.ietf.org/arch/msg/spasm/w4FSmmZsBMjqs651hVrup1-K7II/
  - Deleted sections ‘Get certificate management configuration’ and ‘Get enrollment voucher’

Activities since IETF 107 on Lightweight CMP Profile - Part 2

- Several issues and ToDos were addressed - continuation
  - Deleted ToDo on rsaKeyLength
    > mailarchive.ietf.org/arch/msg/spasm/wa4bjS05TXnwkAbZbyZ-7YWynOg/
  - Updated section on offline / file-based transport
  - Referred to new draft datatracker.ietf.org/doc/draft-msahni-ace-cmpv2-coap-transport/
  - Completed section ‘Adding protection’
  - Added section ‘Definition and discovery of HTTP URIs’ and section ‘HTTP transport’ on CMP endpoints
  - Moved the change history to the Appendix
  - Further minor changes, see the change history

Remaining ToDos for Lightweight CMP Profile

- Discuss content of SignedData for central key generation (separate slide)
- Define OID id-it-caCerts, id-it-rootCaKeyUpdate, and id-it-certReqTemplate and register them at IANA (pre-registration is requested)
- Add security considerations
- Complete appendix with ASN.1 modules
- Polish wording and correct typos

Besides these ToDos, the text should be complete.

Any feedback is welcome!

Change in section 4.1.6 of the SignedData content from OCTET STRING to id-ct-KP-aKeyPackage

Content of the SignedData as currently specified in section 4.1.6

```
            contentType             REQUIRED
-- MUST be id-data
            content                 REQUIRED
-- MUST be the privateKey as OCTET STRING
```

After discussion with Tomas, we think the encoding of the private key as OCTET STRING may course problems with specific algorithms.

Therefore, we propose to use the structure specified in RFC5958 as content of the SignedData.

Propose syntax using RFC5958 id-ct-KP-aKeyPackage

```
            contentType                 REQUIRED
-- MUST be id-ct-KP-aKeyPackage
            content                     REQUIRED
              AsymmetricKeyPackage      REQUIRED
                OneAsymmetricKey        REQUIRED
-- MUST be exactly one asymmetric key package
-- as specified in RFC5958
                  version               REQUIRED
-- The version MUST be v2
                  privateKeyAlgorithm REQUIRED
-- The privateKeyAlgorithm field MUST contain
-- the OID of the asymmetric key pair algorithm
                  privateKey            REQUIRED
-- The privateKey MUST be in the privateKey field
                  attributes            OPTIONAL
-- The attributes field SHOULD not be used
                  publicKey             REQUIRED
-- The publicKey MUST be in the publicKey field
```

WG support needed

- Please review the drafts!
  I am thankful for any suggestion and improvement!
- Support on completing the ASN.1 modules in the appendixes is appreciated
- Guidance regarding IANA interaction would be appreciated too
- Help me with polishing the grammar and spelling, as I am not a native speaker :-(

→ When is the right time for WG last call?