CMP Updates and Lightweight CMP Profile

draft-ietf-lamps-cmp-updates-01
draft-ietf-lamps-lightweight-cmp-profile-01

Hendrik Brockhaus, Steffen Fries, David von Oheimb

IETF 107 – LAMPS Working Group

Activities since IETF 106 on CMP Updates

- Draft has been accepted as WG item
- Several issues and ToDos were addressed
  - Discuss and incorporate feedback from the WG and other reviewers
  - Clarification on multiple protection
  - Clarification on new extended key usage
  - Align wording with RFC 4210

Remaining ToDos for CMP Updates

- Clarify and align name and description of id-kp-cmcCA and id-kp-cmcRA at IANA to address the extended usage within CMP, if possible
- Define and register OID for id-kp-cmpKGA at IANA
- Decide which attribute structure (pkcs-9-at-friendlyName or pkcs-9-at-localKeyId) is to be used in the unprotectedAttr field to contain the passphrase identifier
- Add security and IANA considerations
- Complete appendix with ASN.1 modules
- Polish wording and correct typos

Change EKU name, description and information to be enrollment protocol agnostic

The goal is to **reuse the existing OIDs for id-kp-cmcRA and id-kp-cmcCA**. With these changes the OIDs will be enrollment protocol agnostic and can be used for different protocols like, e.g., CMC, CMP, and EST.

Existing OID: 1.3.6.1.5.5.7.3.27

Name: id-kp-cmcCA
→ **id-kp-cmCA**

Description : Certificate Management over Cryptographic message syntax (CMC) Certification Authorities (CA) Extended Key Usage (EKU)
→ **Certificate Management Certification Authorities (CA) Extended Key Usage (EKU)**

Information: See IETF RFC 6402
→ **See IETF RFC 6402 and 'Updates CMP'**

Existing OID: 1.3.6.1.5.5.7.3.28

Name: id-kp-cmcRA
→ **id-kp-cmRA**

Description: Certificate Management over Cryptographic message syntax (CMC) Registration Authorities (RA) Extended Key Usage (EKU)
→ **Certificate Management Registration Authorities (RA) Extended Key Usage (EKU)**

Information: See IETF RFC 6402
→ **See IETF RFC 6402 and 'Updates CMP'**

New OID: 1.3.6.1.5.5.7.3.x

Name: **id-kp-cmKGA**

Description: **Certificate Management Key-Generation Authorities (KGA) Extended Key Usage (EKU)**

Information: **See IETF 'Updates CMP'**

Existing OID: 1.3.6.1.5.5.7.3.29 **Proposed change to align the name and description?**

Name: id-kp-cmcArchive → **id-kp-cmArchive**

Description: Certificate Management over Cryptographic message syntax (CMC) archive servers Extended Key Usage (EKU) → **Certificate Management archive server Extended Key Usage (EKU)**

Information: See IETF RFC 6402

Password key identifier carried in pkcs-9-at-friendlyName vs. pkcs-9-at-localKeyId

- When using EnvelopedData the unprotectedAttrs and when using EncryptedValue the valueHint field MAY contain a key identifier (chosen by the entity, along with the passphrase itself) to assist in later retrieval of the correct passphrase (e.g., when the revocation request is constructed by the entity and received by the CA/RA).

The **attribute structure containing the password key identifier in the unprotectedAttr field could either be pkcs-9-at-friendlyName or pkcs-9-at-localKeyId** as specified in RFC 2985 section 5.5 [RFC2985]. I would tend to take pkcs-9-at-localKeyId. Are there further preferences for either one?

Activities since IETF 106 on Lightweight CMP Profile

- Draft has been accepted as WG item
- Several issues and ToDos were addressed
  - Discuss and incorporate feedback from the WG and other reviewers
  - Added endpoints for HTTP transport including labels to address multiple CAs or certificate profiles
  - Clarification on the required certificates for root CA certificate update
  - Decide on using PBMParameter for symmetric key-encryption key management technique
  - Align wording with RFC4210

Remaining ToDos for Lightweight CMP Profile Part 1

- Decide to either recommend support for delayed enrollment or to have it optional
- Add an optional operation for requesting a certificate from a trusted PKI
- Get feedback on using PBMParameter for keyEncryptionAlgorithm in KEKRecipientInfo
- Get feedback on the proposed changes to the caKeyUpdateInfo structure regarding which certificate must be present to streamline the content for machine-to-machine communication (proposal: newWithNew -> required, newWithOld -> recommended, oldWithNew -> optional; instead of all three required)
- Add an example on how to pre-fill the certTemplate in the get-certificate-parameters request message
- Decide if the rsaKeyLength should be an INTEGER or a SET OF INTEGER in the get-certificate-parameters request message
- Discuss if both support messages (get-certificate-parameters and get-certificate-management-configuration) are needed
- Discuss if the get-enrollment-voucher should be limited to the ANIMA-BRSKI specification or offer more flexibility

PBMParameter usage for keyEncryptionAlgorithm in KEKRecipientInfo

```
          keyEncryptionAlgorithm
                              REQUIRED
-- MUST be id-PasswordBasedMac
            PBMParameter  REQUIRED
              salt        REQUIRED
-- MUST be the random value to salt the secret key
-- MUST be a different value than used in the PBMParameter
-- structure of the CMP message protection in the
-- header of this message
              owf         REQUIRED
-- MUST be the same value than used in the PBMParameter
-- data structure in the header of this message
              iterationCount
                          REQUIRED
-- MUST be a limited number of times the OWF is applied
-- To prevent brute force and dictionary attacks a reasonable
-- high number SHOULD be used
              mac         REQUIRED
-- MUST be the same as in the contentEncryptionAlgorithm field
```

To make **use of a different symmetric keys for encrypting the private key and for MAC-protection** of the CMP message, we, even though from the **derive another key using the same PBMParameter structure**perspective of field names, it is not intended to be used for deriving encryption keys.

Does anyone sees a better solution here?

caKeyUpdateInfo structure

```
    caKeyUpdateInfo       REQUIRED
-- MUST be present and be of type CAKeyUpdAnnContent
      oldWithNew          OPTIONAL
-- MAY be present if infoValue is present
-- MUST contain an X.509 certificate containing the old public
-- root CA key signed with the new private root CA key
      newWithOld          RECOMMENDED
-- SHOULD be present if infoValue is present
-- MUST contain an X.509 certificate containing the new public
-- root CA key signed with the old private root CA key
      newWithNew          REQUIRED
-- MUST be present if infoValue is present
-- MUST contain the new root CA certificate
```

To **reduce unnecessary overhead** by including not needed certificates, we intend to **require only to include the newWithNew** certificate in the caKeyUpdateInfo structure and optionally **omit the oldWithNew and newWithOld** certificates. **This is in conflict with [RFC4210] where also oldWithNew and newWithOld are required fields in caKeyUpdateInfo.** Is there any possibility to optionally leave these fields empty and still reuse the caKeyUpdateInfo structure as specified in [RFC4210]?

rsaKeyLength

```
    rsaKeyLen               OPTIONAL
-- This field is of type INTEGER. Any reasonable RSA key length
-- SHOULD be specified if the algorithm in the
-- subjectPublicKeyInfo field of the certTemplate is of type
-- rsaEncryption.
```

To offer a set of allowed RSA key lengths, the rsaKeyLen field **could also be specified as a SEQUENCE OF INTEGER**.

The **goal of this document is profiling and being more specific**. Therefore, I tend to stick to the current solution and **offer only one dedicated certTemplate and one RSA key length**. Otherwise the question comes up if we also want to offer a set of ECC curves or a set of some other attributed or extensions.

Finally the PKI management entity responding to the request, e.g., a management tool, may derive from the end entity's device type what specific content is required and feasible for the device.

get-certificate-parameters vs. get-certificate-management-configuration

5.4.4. Get certificate request parameters

This PKI management operation can be used by an EE to **request configuration parameters for a planned certificate request operation**.

general response

infoValue OPTIONAL

-- MUST be absent if no requirements are available

-- MUST be present if the PKI management entity has

-- any requirements on the content of the

-- certificates to be requested

certTemplate REQUIRED

-- MUST be present if infoValue is present

-- MUST contain the prefilled certTemplate structure

rsaKeyLen OPTIONAL

-- This field is of type INTEGER. Any reasonable RSA

-- key length

-- SHOULD be specified if the algorithm in the

-- subjectPublicKeyInfo field of the certTemplate is of

-- type rsaEncryption.

5.4.5. Get certificate management configuration

This PKI management operation can be used by an EE to **request the current certificate management configuration information** in advance to a planned PKI management operation, e.g., in case no out-of-band transport is available. Such certificate management configuration **can consist of** all information the EE needs to know to generate and deliver a proper certificate request, such as

- **algorithm, curve, and key length for key generation**
- **various certificate attributes and extensions** to be used for the certificate request
- **specific host name, port and path on the RA/LRA** to send this CMP request to
- **Infrastructure Root CA Certificate**, e.g., the root of the (L)RA TLS and CMP signer certificates.

general response

infoValue OPTIONAL

-- MUST be absent if no certificate management

-- configuration is available

-- MUST be present if the PKI management entity

-- provides any certificate management configuration

certMgtConfig REQUIRED

-- MUST be present if infoValue is present

-- MUST contain the **certificate management**

-- configuration as OCTET STRING

Focusing on profiling, I would suggest to keep Section 5.4.4 and delete Section 5.4.5. If there is anyone volunteering to specify the content of certMgtConfig, I am happy to also keep Section 5.4.5. Please let me know.

get-enrollment-voucher

5.4.6. Get enrollment voucher

This PKI management operation can be used by an EE to **request an enrollment voucher containing the root certificate of a new, additional, or alternative PKI** to establish trust in this PKI, e.g., in case no out-of-band transport is available. Such an enrollment voucher can be used in advance to an enrollment to this new environment.

```
general message
   infoValue                    OPTIONAL
 -- MUST be absent if no voucher request
 -- is available
 -- MUST be present if the EE provides
 -- the voucher request
     voucherRequest             REQUIRED
 -- MUST be present if infoValue is present
 -- MUST contain the voucher request as
 -- OCTET STRING
```

```
general response
   infoValue                    OPTIONAL
 -- MUST be absent if no enrollment
 -- voucher is available
 -- MUST be present if the PKI
 -- management entity provides the
 -- enrollment voucher
     enrollmentVoucher          REQUIRED
 -- MUST be present if infoValue is present
 -- MUST contain the enrollment voucher
 -- as OCTET STRING
```

Do we want to explicitly limit this operation to the exchange of RFC 8366 voucher request and response?
Focusing on profiling, I would say yes.

Remaining ToDos for Lightweight CMP Profile Part 2

- Decide on the different usage of multiple protection to be specified in this document as optional operations (see next slide)
- Discuss if http endpoints for RA-to-RA communication should be defined
- Complete the section on file-based transport of CMP messages
- Decide on adding a profile for CoAP-based message transport. @Michael Richardson, would you like to contribute that?
- Add usage of new EKUs in the profile
- Define additional OIDs in the tree 1.3.6.1.5.5.7.4 (id-it) and register them at IANA (id-it-getCaCerts , id-it-getCSRParam, id-it-getCertMgtConfig)
- Add security considerations
- Polish wording and correct typos

Adding an additional RA signature by using multiple protection

- The **RA** confirms the validation and authorization of a message **and forwards** the original message unchanged.
- The **RA collects several messages and forwards them in a batch**. This can for instance be used to bridge an off-line connection between two PKI management entities. In communication to the CA request messages and in communication from the CA response or announcement messages will be collected in such batch.
- The **RA modifies the message(s)** in some way (e.g., add or modify particular field values or add new extensions) **before forwarding them**, then it MAY create its own desired PKIBody. In case the changes made by the RA to PKIMessage breaks the POP, the RA MUST either set the POP RAVerified or include the original PKIMessage from the EE in the generalInfo field of PKIHeader of the nested message (to force the CA to check POP on the original message). The infoType to be used in this situation is {id-it 15} (see Section 5.3.19 for the value of id-it) and the infoValue is PKIMessages (contents MUST be in the same order as the requests in PKIBody). For simplicity reasons, if batching is used in combination with inclusion of the original PKIMessage in the generalInfo field, all messages in the batch MUST be of the same type (e.g., ir).

http endpoints for RA-to-RA communication

A valid full operational path can look like this:

```
 1  http://www.example.com/.well-known/cmp
 2  http://www.example.com/.well-known/cmp/keyupdate
 3  http://www.example.com/.well-known/cmp/arbitraryLabel1
 4  http://www.example.com/.well-known/cmp/arbitraryLabel1/keyupdate
```

PKI management operations SHOULD use the following URI path:

PKI management operation	Path	Details
Enroll client to new PKI (REQUIRED)	/initialization	Section 5.1.1
Enroll client to existing PKI (OPTIONAL)	/certification	Section 5.1.2

[...]

Should we also specify path values for communication among PKI management entities as specified in section 6 are needed, e.g., **'forward' or 'nested'**?

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 needed
- Help me with polishing the grammar and spelling, as I am not a native speaker :-(
- If the WG wants to have a section on the CoAP message transport as suggested by Michael, I need support on that