CMP Updates, and Lightweight CMP Profile

draft-ietf-lamps-cmp-updates-13
Hendrik Brockhaus, David von Oheimb , John Gray

draft-ietf-lamps-lightweight-cmp-profile-07
Hendrik Brockhaus, Steffen Fries, David von Oheimb

Hendrik Brockhaus

IETF 112 – LAMPS Working Group

Activities since IETF 111 on CMP Updates

Changes since IETF 111:

- Added John Gray to the list of authors
- Fixed errata no. 2615, 2616, 3949, 4078, and 5201
- Moved the hashAlg field in certConf to the end of the structure
- Changed rootCaCert from generalInfo to genm body and generalized to oldTrustAnchor
- Added genm use case: CRL update retrieval
- Extended polling to all kinds of CMP request messages, called delayed delivery; initiation by the server was extended by sending an error message with status "waiting“ for non-enrollment messages
- Updated CMP version handling
- Moved some security considerations from Lightweight CMP Profile to CMP Updates
- Updated the introduction of RFC 6712 regarding extended polling
- Fixed some nits in the ASN.1 modules
- Replaced the term "transport" by "transfer“ where appropriate

Remaining ToDos for CMP Updates

Draft is stable and text is complete.

Remaining ToDos:

- Register OIDs for CRL update retrieval
- Reorder some existing OIDs regarding root CA cert update, if possible

The authors believe that the document can proceed to WGLC.

Activities since IETF 111 on Lightweight CMP Profile

Changes since IETF 111:

- Added references to SZTP-CSR and BRSKI-AE (and BRSKI-PRM)
- Removed "rootCaCert" from generalInfo and updated the structure of the genm request body for root CA certificate updates
- Simplified handling of sender and recipient nonces in case of delayed delivery
- Added section on CRL update retrieval
- Generalized delayed enrollment to delayed delivery and updated the EE state machine
- Updated section 6 regarding delayed message transfer
- Changed file name extension from ".PKI" to ".pki", deleted operational path for central key generation, and added an operational path for CRL update retrieval
- Moved many security considerations to CMP Updates
- Replaced the term "transport" by "transfer" where appropriate

Extended the polling mechanism from enrollment messages to all kinds of PKIMessages

After extensive discussion of various option among the authors, we decided to present a proposal that extends the existing mechanism to all PKI management messages. This proposal will be using CMP V2 messages only, with no need to not change the existing polling, and therefore is backward compatible.

Today, polling is only available for certificate request messages, covering delays in request approval.

1. ir, cr, or kur
2. ip, cp, or kup with status “waiting”
3. pollReq (certReqId ≥ 0 referring to certResponse)
4. pollRep with certReqId from initial pollReq and checkAfter value
5. pollReq with certReqId from initial pollReq
6. ip, cp, kup, or error

Use existing polling mechanism for ir, cr, p10cr, and kur (enrollment) and use error message with status “waiting” for certConf, rr, and genm:

1. ir, cr, kur, p10cr, certConf, rr, or genm
2. ip, cp, or kup with “waiting” for enrollment and error with status “waiting” for all other requests
3. pollReq (certReqId ≥ 0 referring to certResponse, -1 when referring to the complete request)
4. pollRep with certReqId from initial pollReq and checkAfter value
5. pollReq with certReqId from initial pollReq
6. ip, cp, kup, pkiConf, rp, genp, or error

Added general messages for updating of most recent CRLs

GenMsg: {id-it TBD1}, SEQUENCE SIZE (1..MAX) OF CRLStatus
GenRep: {id-it TBD2}, SEQUENCE SIZE (1..MAX) OF CertificateList | < absent >

```
CRLSource ::= CHOICE {
    dpn         [0] DistributionPointName,
    issuer      [1] GeneralNames }
CRLStatus ::= SEQUENCE {
    source      CRLSource,
    thisUpdate  Time OPTIONAL }

id-it-crlStatusList   OBJECT IDENTIFIER ::= {id-it TBD1}
CRLStatusListValue        ::= SEQUENCE SIZE (1..MAX) OF CRLStatus
id-it-crls                OBJECT IDENTIFIER ::= {id-it TBD2}
CRLsValue                 ::= SEQUENCE SIZE (1..MAX) OF CertificateList
```

Remaining ToDos for Lightweight CMP Profile

Draft is stable and text is complete.

Remaining ToDo:

- Update section 4.1.6.1 regarding AD feedback on CMP Algorithms

The authors believe that the document can proceed to WGLC.