CMP Updates, CMP Algorithms, and Lightweight CMP Profile

draft-ietf-lamps-cmp-updates-18
Hendrik Brockhaus, David von Oheimb , John Gray

draft-ietf-lamps-cmp-algorithms-12
Hendrik Brockhaus, Hans Aschauer, Mike Ounsworth, John Gray

draft-ietf-lamps-lightweight-cmp-profile-11
Hendrik Brockhaus, Steffen Fries, David von Oheimb

Hendrik Brockhaus

IETF 113 – LAMPS Working Group

Activities since IETF 112 on CMP Updates

Changes since IETF 112:

- Removed the pre-RFC5378 work disclaimer after the RFC 4210 authors granted BCP78 rights to the IETF Trust
- Removed note on usage of language tags in `UTF8String` due to references to outdated/historic RFCs
- Clarified the usage of `CRLSource`
- Added further references regarding random number generation
- Extended `id-it-caCerts` support message to allow transporting to-be-trusted root CA certificates and added respective security consideration
- Rolled back changes made in previous version regarding root CA update to avoid registration of new OIDs

Remaining ToDos for CMP Updates

All comments from AD Review were addressed by the authors. Waiting for feedback from the AD.

Issues that may need further discussion:

- CMP Updates vs. RFC4210bis and RFC6712bis
- There is criticism to use a path segment not well-known but specific to the installation. Currently the `/.well-known` URI path is specified as in RFC7030. When offering certificate management for different CAs or certificate profiles, the `profileLabel` or `arbitraryLabel` can be used to specify the addressed CA or certificate profile.
  `https://www.example.com/.well-known/est/arbitraryLabel/simpleenroll`
  `http://www.example.com/.well-known/cmp/profileLabel/initialization`

Options for solving the URI path segment issue

Examples of the URI to use when enrolling an EE with an LDevID certificate (the local configuration the certificate profile to use `ldevid`):

1. To keep alignment with the EST approach in [RFC 7030], do not change anything:
   `example.com/.well-known/cmp/ldevid/initialization`
2. Use the query element in the URI for referencing the certificate profile:
   `example.com/.well-known/cmp/initialization?profile=ldevid`
3. Move the `profileLabel` giving the cert profile after the `operationLabel`:
   `example.com/.well-known/cmp/initialization/ldevid`
4. Give up using `.well-known` URIs (which could be combined with 2. or 3.):
   `example.com/cmp/ldevid/initialization`

Activities since IETF 112 on CMP Algorithms

Changes since IETF 112:

- Removed the pre-RFC5378 work disclaimer after the RFC 4210 authors granted BCP78 rights to the IETF Trust
- Implemented the improvements proposed by Quynh on usage of SHAKE and KMAC, the tables in Section 7, and the security considerations
- Fixing issues from WG and AD review
- Added two tables showing algorithms sorted by their strength to Section 7
- Updated the algorithm use profile in Section 7.1
- Updated and added security consideration on SHAKE, PasswordBasedMac, KMAC, and symmetric key-based MAC functions

→Next Steps: Waiting for feedback from the AD on the updated draft.

Activities since IETF 112 on Lightweight CMP Profile

Changes since IETF 112:

- Introduced implementation conformance requirements as new Section 7
- Recommended use of `implicitConfirm` for `ir`/`cr`/`p10cr`/`kur`
- Added some clarifications regarding validating the authorization of centrally generated keys and addressed some feedback from the CMP Algorithms review
- Clarified retrieval of CRL update in Section 4.3.4
- Rolled back part of the changes on root CA certificate updates in Section 4.3.2 to avoid registration of new OIDs

Remaining ToDos for Lightweight CMP Profile

Open points:

- Potentially change the structure of the `/.well-known` URIs
- Some clarifications on protection of error messages in Section 3
- Some clarifications on level of support of PKI management operations in Section 7.1

Waiting for AD review comments.