Lightweight CMP Profile and CMP Updates

draft-brockhaus-lamps-cmp-profile-01

draft-brockhaus-lamps-cmp-updates-01

Hendrik Brockhaus, Steffen Fries, David von Oheimb

IETF 106 – LAMPS Working Group

Results of IETF 104 and 105

- Split of the contents into two documents
- Changes to CMP needs a standard track RFC
- Exchange of EncryptedValue with EncryptedKey is the best way to enable the usage of EnvelopedData
- Re-charter of WG LAMPS covers work on CMP Profile and Updates CMP
- CMP Profile and Updates CMP will both be covered by the updated charter, CMP Profile should be aligned with LWIG
- Add milestones for WG adaption for December 2019 and November 2020 for submission to IESG

Lightweight CMP Profile

draft-brockhaus-lamps-lightweight-cmp-profile-01

Changes since -00

- Complete specification of requesting a certificate from a legacy PKI using a **PKCS#10 request** in Section 5.1.5.
- Complete specification of adding **central generation of a key pair** to a certificate request in Section 5.1.6.
- Complete specification of handling **delayed enrollment** due to asynchronous message delivery in Section 5.1.7.
- Complete specification of **additional support messages** in Section 5.4 to
  - get CA certificates,
  - update a Root CA certificate,
  - get certificate request parameters,
  - get certificate management configuration, and
  - request an enrollment voucher.

Next Steps for Lightweight CMP Profile

- Discuss and incorporate feedback from the WG and others
- Decide on adding section on requesting additional certificates from a trusted PKI
- Decide on using PBMParameter for symmetric key-encryption key management technique as described in -01 to use a different symmetric key for encrypting the private key and for MAC-based protection of the CMP Message
- Complete the section on file-based transport of CMP messages
- Add usage of new EKUs in the profile
- Define additional OIDs and register them at IANA
- Add security considerations
- Polish wording and correct typos

CMP Updates

draft-brockhaus-lamps-cmp-updates-01

Changes since -00:

- Add a section describing the **new extended key usages** for
  - CMP Certification Authority
  - CMP Registration Authority
  - CMP Key Generation Authority
- Complete the section on changes to the specification of **encrypted values**
- Add a section on some clarifications to Appendix D.4
- Minor generalization in sections 5.1.3.4 and 5.3.22
  - Delete the stipulation that all PKI messages contained in a nested message must be of the same type
  - Extend the polling mechanism also to outstanding p10cr transactions

Next Steps for CMP Updates

- Discuss and incorporate feedback from the WG and others
- Add usage of new EKUs in the profile
- Define additional OIDs and register them at IANA
- Add security considerations
- Complete appendix with ASN.1 modules
- Polish wording and correct typos