rfc4210bis, rfc6712bis

draft-ietf-lamps-rfc4210bis-03
Hendrik Brockhaus, David von Oheimb , Mike Ounsworth, John Gray

draft-ietf-lamps-rfc6712bis-02
Hendrik Brockhaus, David von Oheimb , Mike Ounsworth, John Gray

Hendrik Brockhaus

IETF 115 – LAMPS Working Group

Activities since IETF 114 on rfc4210bis

The following versions were provided since IETF 114

- -00 versions containing the original RFC text
- -01 versions merging the updates specified in CMP Updates
- -02 version containing the following changes:
  - Introduced the Key Generation Authority in new Section 3.1.1.4
  - Defined origPKIMessage in new Section 5.1.1.3 using content from Section 5.1.3.4
  - Removed listing of concrete algorithms and added reference to CMP Algorithms instead
  - Added references to Appendix D and E as well as the Lightweight CMP Profile for further information to message description in Section 5
  - Broaden the scope from human users also to devices and services
  - Updating reference from historic LDAP V2 to LDAP V3 (RFC4510)
- -03 version containing the following changes:
  - Updated definition on validity of „old with new“, „new with old“, and „new with new“ certificates in Section 4.4.1
  - Moved content from Appendix C to Sections 5.2.1, 5.2.8, and 5.2.8.1 where is belongs, updated references to Appendix C in the rest of the document and finally deleted Appendix C
  - Updated and added some ToDos on defining POP and message protection using KEM keys to some sections

Proposal on supporting KEM keys

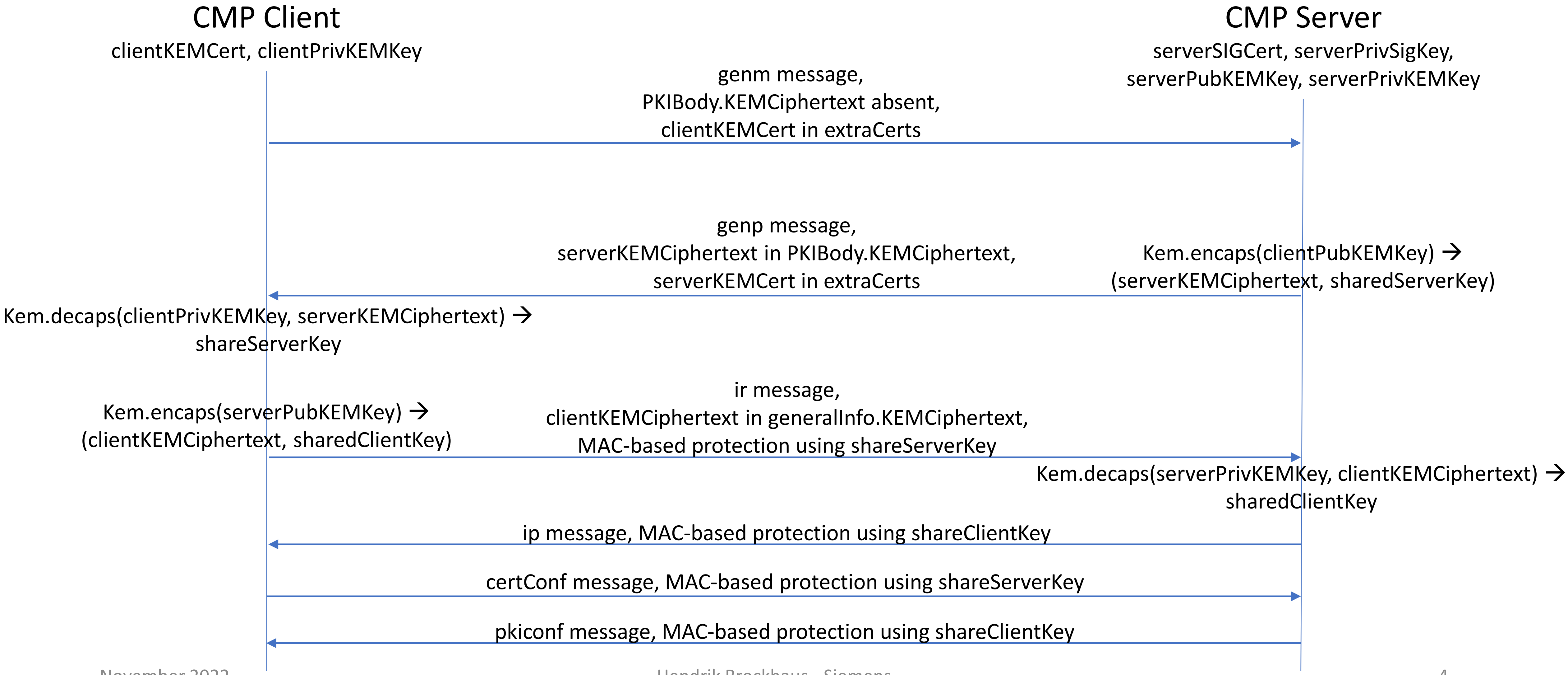
Proof-of-possession in certificate requests

- The authors will wait for a new I-D on POP for KEM keys.
- Currently an indirect POP could be used with certificate requests for KEM keys like for encryption-only keys. In CMP the newly issued certificate can be delivered in encrypted form and the recipient provides POP by sending a certHash in the CertConf message.

CMP message protection

- MAC-based message protection can be used at the cost of an additional roundtrip in advance to a PKI management operation establishing a authenticated shared key, see message flow on the next slide.

Client and server have KEM keys



CMP Client

clientKEMCert, clientPrivKEMKey

CMP Server

serverSIGCert, serverPrivSigKey,
serverPubKEMKey, serverPrivKEMKey

genm message,
PKIBody.KEMCiphertext absent,
clientKEMCert in extraCerts

Kem.encaps(clientPubKEMKey) →
(serverKEMCiphertext, sharedServerKey)

genp message,
serverKEMCiphertext in PKIBody.KEMCiphertext,
serverKEMCert in extraCerts

Kem.decaps(clientPrivKEMKey, serverKEMCiphertext) →
shareServerKey

Kem.encaps(serverPubKEMKey) →
(clientKEMCiphertext, sharedClientKey)

ir message,
clientKEMCiphertext in generalInfo.KEMCiphertext,
MAC-based protection using shareServerKey

Kem.decaps(serverPrivKEMKey, clientKEMCiphertext) →
sharedClientKey

ip message, MAC-based protection using shareClientKey

certConf message, MAC-based protection using shareServerKey

pkiconf message, MAC-based protection using shareClientKey

Activities since IETF 114 on rfc6712bis

The following versions were provided since IETF 114

- -00 versions containing the original RFC text
- -01 versions merging the updates specified in CMP Updates
- -02 version containing the following changes:
    - Updated Section 3.4 including the requirement to add the content-length filed into the HTTP header
    - Added a reference to TLS 1.3
    - Addressed idnits feedback, specifically changing RFC references: RFC2616 -> RFC9112, RFC2818 -> RFC9110, and RFC5246 -> RFC8446