rfc6712bis and rfc4210bis

draft-ietf-lamps-rfc6712bis-04
Hendrik Brockhaus, David von Oheimb , Mike Ounsworth, John Gray

draft-ietf-lamps-rfc4210bis-08
Hendrik Brockhaus, David von Oheimb , Mike Ounsworth, John Gray

Hendrik Brockhaus

IETF 119 – LAMPS Working Group

Activities since IETF 118 on rfc6712bis

Changes since IETF 118:

- Aligned content with changes done by RFC Editor before release of RFC 9480
- Draft on github.com/lamps-wg/cmp-updates/

Next Steps:

- Ready for WGLC, but waiting for completion of rfc4210bis

Activities since IETF 118 on rfc4210bis

Changes since IETF 118:
- Sections 5.1.1, 5.1.3.4, 5.3.19.18, and Appendix E: Require using transactionID with KEM-based message protection
- Section 5.1.3.1: Added some text explaining where key expansion is needed with PasswordBasedMac and that it is not needed with using HMAC as specified in RFC 4211
- Section 5.2.8: Added POP for KEM-keys, added use of CMS EnvelopedData for encrypted challenge, added specification on using raVerified, and restructured the section fixing some references
- Section 5.3.19.15: Clarified the use of RootCaCertValue introduced in RFC 9480
- Appendix B: Added support for KEM-based message protection and use of CMS EnvelopedData for transferring revocation passphrases in encrypted form
- Aligned content with changes done by RFC Editor before release of RFC 9480
- Draft on github.com/lamps-wg/cmp-updates/
- PoC implementation are ongoing during the hackathon

Next Steps:
- **Waiting for review feedback from the WG as requested by Russ during IETF 116 (“Russ: requests that the KEM section get a lot of review since this part is very new.”), specifically opinions on KemOtherInfo are welcome**
- Address remaining issues on github, see next slides. Guidance from the WG appreciated.
- Add AttestationNonceRequest/Response message syntax, if draft-tschofenig-lamps-nonce-cmp-est is adopted

New ASN.1 structures for KEM-based message protection

```
id-KemBasedMac OBJECT IDENTIFIER ::= {1 2 840 113533 7 66 16}

KemBMParameter ::= SEQUENCE {
  kdf               AlgorithmIdentifier{KEY-DERIVATION, {...}},
  kemContext    [0] OCTET STRING     OPTIONAL,
  len               INTEGER (1..MAX),
  mac               AlgorithmIdentifier{MAC-ALGORITHM, {...}}
}
```

Algorithm identifier to be used in PKIHeader.protectionAlg when KEM-based MAC is used.
Entrust registered the OID in the same branch as PBMParameter.
Optional kemContext if needed with the used KEM algorithm like ukm in cms-kemri.

```
id-it-KemCiphertextInfo OBJECT IDENTIFIER ::= { id-it TBD1 }
KemCiphertextInfoValue ::= KemCiphertextInfo

KemCiphertextInfo ::= SEQUENCE {
  kem               AlgorithmIdentifier{KEM-ALGORITHM, {...}},
  ct                OCTET STRING
}
```

InfoTypeAndValue to deliver the KEM ciphertext in body of general message or in generalInfo field of message header.

```
KemOtherInfo ::= SEQUENCE {
  staticString      PKIFreeText,
  transactionID     OCTET STRING,
  kemContext    [0] OCTET STRING     OPTIONAL
}
```

Context information as input to the KDF for domain separation and for ensuring uniqueness of MAC-keys.
Uses transactionID from the message containing the KemCiphertextInfoValue.ct.
Optional kemContext if needed with the used KEM algorithm like ukm in cms-kemri.

Remaining Open Issues on github – 1

- **Remove normative language from Section 4.2.2**: https://github.com/lamps-wg/cmp-updates/issues/43**, by Tomas Gustavsson**

  There are various profiles that specify initial registration and certification in much more detail, e.g., Appendix C and D, RFC 9483, 3GPP TS 33.310, UNISIG Subset 137. Therefore, today rfc4210bis is more of a framework and Section 4.2 is more a guidance.

  Option 1: Adapt headline of Section 4.2.2 to avoid confusion and keep text as of RFC 4210 retaining backward compatibility.

  Option 2: Adapt headline of Section 4.2.2 to avoid confusion and remove normative language.

  Option 3: Rework Section 3, 4, and 6 to modernize it and remove normative where not needed.

Remaining Open Issues on github – 2

- **Update Section 4.4**: https://github.com/lamps-wg/cmp-updates/issues/45**, by Tomas Gustavsson**

  The text is on root CA key update. The main method described in Section 4.4 is using an LDAP directory providing all four link certificates (OldWithOld, OldWithNew, NewWithOld, and NewWithNew). As Section 4.4 is referenced quite a lot in other documents (draft-ietf-anima-constrained-voucher, RFC 8994, RFC 8649, RFC 7030, RFC 6024, RFC 5280). Tomas requests the following updates:
  - Introduce the optionality of CMPv3
  - Add something more about assumptions and restrictions. For example that CA subject DN change it a common, that old and new CAs may be on different systems, and that different use cases for the same protocol may have different restrictions and capabilities.
  - Remove specification of an X.500 directory and assumption on X.509v1 only certs

  Option 1: Keep text as of RFC 4210.

  Option 2: Modernize text in Section 4.4. Tomas could provide an updated proposal in his pull request. See also my pull request, https://github.com/lamps-wg/cmp-updates/pull/54.

Remaining Open Issues on github – 3

- **Clear up incompatibility issue of RFC 4210 Section 5.1.3.1 with RFC 4211 Section 4.4**: https://github.com/lamps-wg/cmp-updates/issues/48**, by John Gray**

  When the output length of the hash algorithm used is smaller than the required key length of the MAC algorithms, a key expansion is required. RFC 4210 specifies such mechanism in contrast to RFC 4211 which focusses on using HMAC, where key expansion is provided within the HMAC. There was explanatory text added with -V08 to Section 5.1.3.1. There was no request for an Erratum regarding RFC 4211.

Remaining Open Issues on github – 4

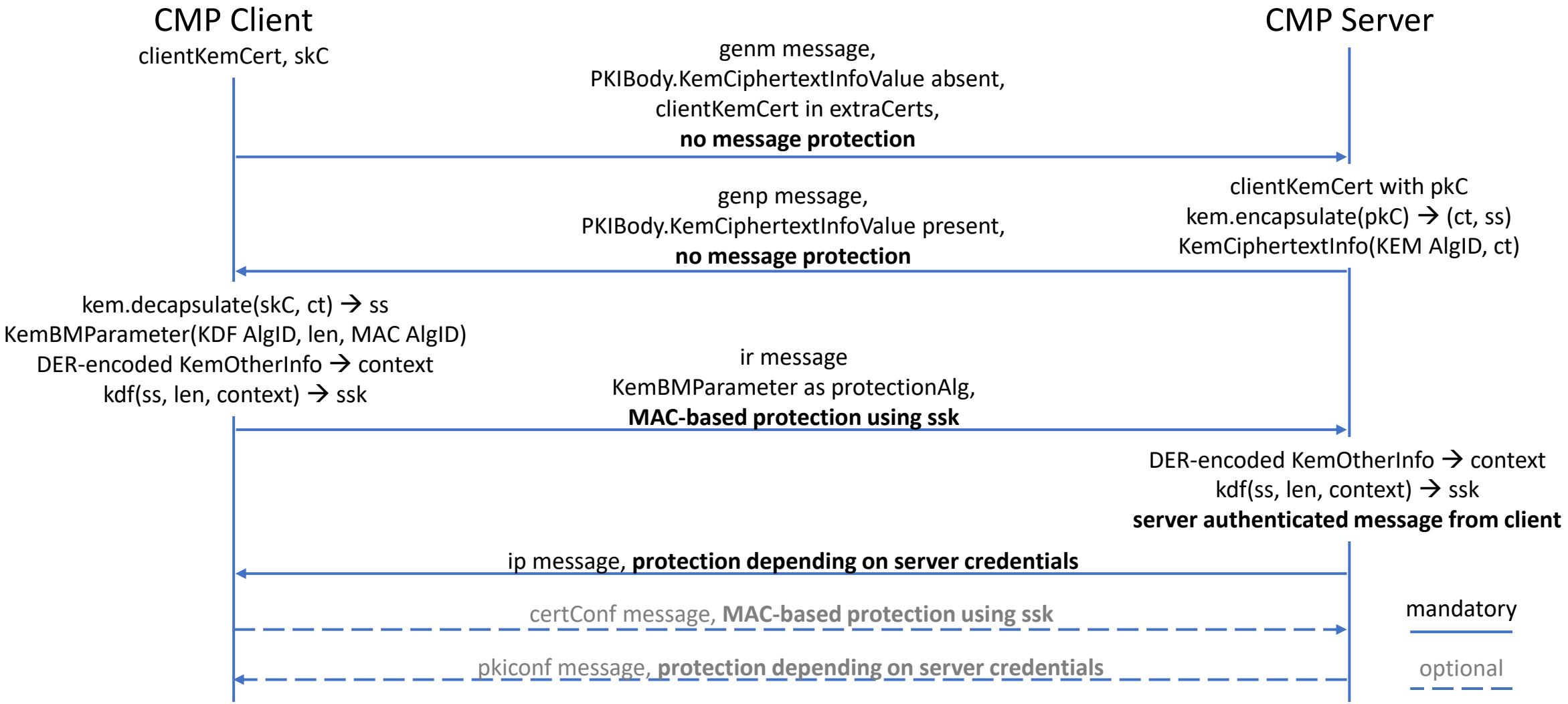
- **Update ckuann to use RootCaKeyUpdateContent**: https://github.com/lamps-wg/cmp-updates/issues/50**, by Tomas Gustavsson**

  The new ASN.1 type CAKeyUpdContent will be introduced to offer ckuann messages using RootCaKeyUpdateContent with CMP V3, see https://github.com/lamps-wg/cmp-updates/pull/52.

```
CAKeyUpdContent ::= CHOICE {
  cAKeyUpdAnnV2       CAKeyUpdAnnContent, -- deprecated
  cAKeyUpdAnnV3  [0] RootCaKeyUpdateContent }
```

BAK

Client owns KEM key pair



Server owns KEM key pair