

rfc6712bis and rfc4210bis

draft-ietf-lamps-rfc6712bis-03

Hendrik Brockhaus, David von Oheimb , Mike Ounsworth, John Gray

draft-ietf-lamps-rfc4210bis-07

Hendrik Brockhaus, David von Oheimb , Mike Ounsworth, John Gray

Hendrik Brockhaus

IETF 117 – LAMPS Working Group

Activities since IETF 116 on rfc6712bis

Changes since IETF 116:

- No updates since IETF116
- Draft on github.com/lamps-wg/cmp-updates/

Activities since IETF 116 on rfc4210bis

Changes since IETF 116:

- Updated **proposal for message protection using KEM keys and aligned it with draft-ietf-lamps-cms-kemri**
- **Each side of the communication uses its individual protection mechanism**
- Defined KEM-based MAC parameters **KemBMPParameter** as AlgorithmIdentifier, in line with PBMPParameter and DHBMPParameter already used in CMP
- Defined **KemCiphertextInfo** to deliver the KEM encapsulated ciphertext
- Defined **KemOtherInfo** as context input for the key derivation
- The draft is available on github.com/lamps-wg/cmp-updates/

New ASN.1 structures

```
id-KemBasedMac OBJECT IDENTIFIER ::= {1 2 840 113533 7 66 TBD4}
```

```
KemBMPParameter ::= SEQUENCE {  
    kdf          AlgorithmIdentifier{KEY-DERIVATION, {...}},  
    len          INTEGER (1..MAX),  
    mac          AlgorithmIdentifier{MAC-ALGORITHM, {...}}  
}
```

Algorithm identifier to be used in PKIHeader.protectionAlg when KEM-based MAC is used.

Entrust is willing to register the OID in the same branch like PBMPParameter.

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

```
KemCiphertextInfoValue ::= KemCiphertextInfo
```

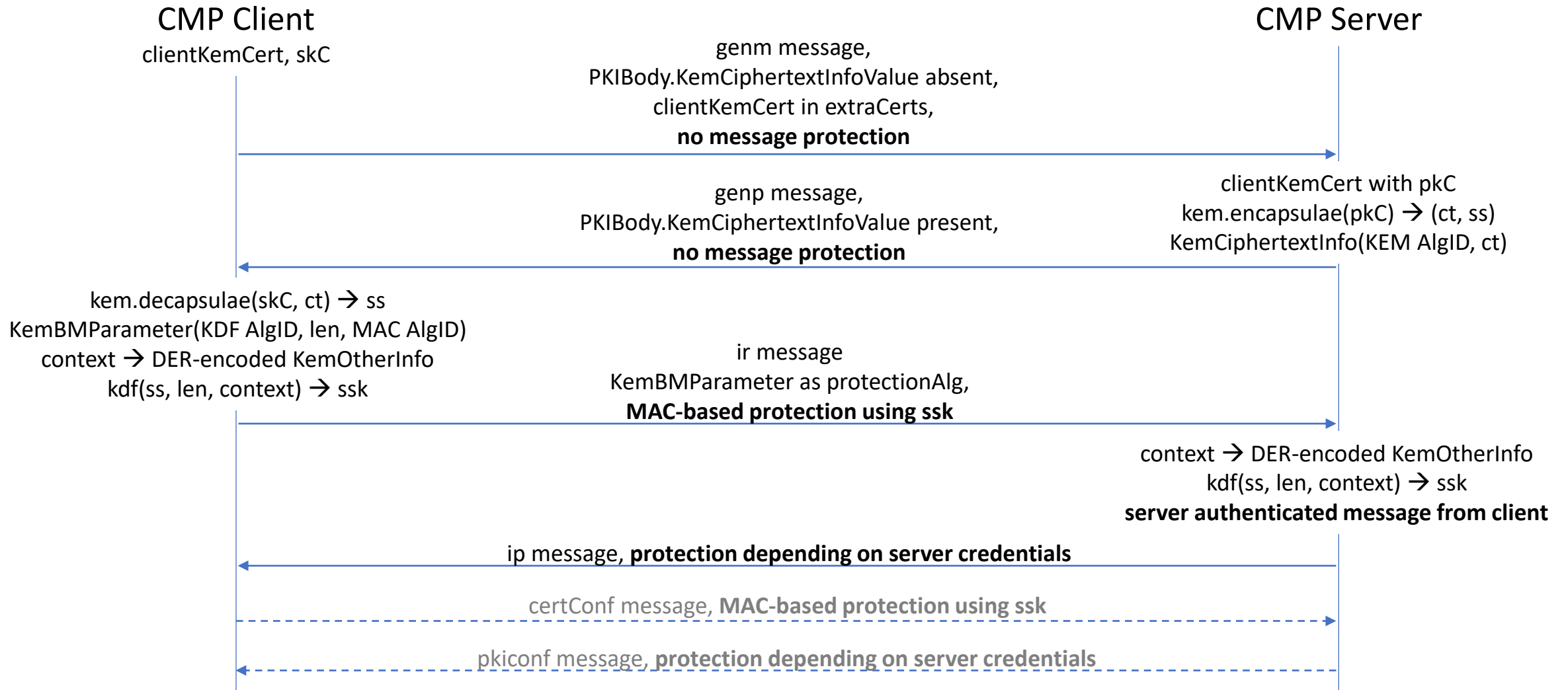
```
KemCiphertextInfo ::= SEQUENCE {  
    kem          AlgorithmIdentifier{KEM-ALGORITHM, {...}},  
    ct           OCTET STRING  
}
```

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

```
KemOtherInfo ::= SEQUENCE {  
    staticString PKIFreeText,  
    transactionID [0] OCTET STRING OPTIONAL,  
    senderNonce  [1] OCTET STRING OPTIONAL,  
    recipNonce   [2] OCTET STRING OPTIONAL,  
    len          INTEGER (1..MAX),  
    mac          AlgorithmIdentifier{MAC-ALGORITHM, {...}},  
    ct           OCTET STRING  
}
```

Context information as input to the KDF for domain separation and for ensuring uniqueness of MAC-keys. Uses transactionID, senderNonce, and recipNonce from the message containing the KemCiphertextInfoValue.ct, if present.

Client owns KEM key pair



Server owns KEM key pair

