# CMP Algorithms, CMP Updates, Lightweight CMP Profile

draft-ietf-lamps-cmp-algorithms-15
Hendrik Brockhaus, Hans Aschauer, Mike Ounsworth, John Gray

draft-ietf-lamps-cmp-updates-23
Hendrik Brockhaus, David von Oheimb , John Gray

draft-ietf-lamps-lightweight-cmp-profile-15
Hendrik Brockhaus, Steffen Fries, David von Oheimb

**Hendrik Brockhaus**

IETF 115 – LAMPS Working Group

# Activities since IETF 114 on CMP Algorithms

Changes since IETF 114:

- -

Draft is approved by IESG for publication

One typo should be fixed before publication.

# Activities since IETF 114 on CMP Updates

Changes since IETF 114:

- -

Draft is approved by IESG for publication

Before publication a note to Section 1 may be added on rfc4210bis and rfc6712bis activity.

While drafting rfc4210bis it was identified that a change specified on Appendix C should be corrected before publication, if possible, see next slide.

# Correction to do on CMP Updates at AUTH48

## Syntax on POPOPrivKey in RFC 2511

```
POPOPrivKey ::= CHOICE {
  thisMessage       [0] BIT STRING,
  subsequentMessage [1] SubsequentMessage,
  dhMAC             [2] BIT STRING }
```

RFC 4210 Appendix C states that the content of "thisMessage" MUST be encoded as an EncryptedValue and then wrapped in a BIT STRING.

CMP Updates required to handle EnvelopedData in the same way and store it in “thisMessage”.

**Looking at RFC 4211 syntax, this is not the best way to transfer EnvelopedData!**

## Syntax on POPOPrivKey in RFC 4211

```
POPOPrivKey ::= CHOICE {
  thisMessage       [0] BIT STRING,   -- deprecated
  subsequentMessage [1] SubsequentMessage,
  dhMAC             [2] BIT STRING,   -- deprecated
  agreeMAC          [3] PKMACValue,
  encryptedKey      [4] EnvelopedData }
```

RFC 4210 Appendix C uses RFC 2511 syntax here and ignores CHOICE [3] and [4].

**CMP Updates should specify using CHOICE [4] when EnvelopedData is used.**

**Russ proposed doing this change at AUTH48 if Roman approves it.**

# Activities since IETF 114 on Lightweight CMP Profile

Changes since IETF 114:

- Addressed comments from AD Evaluation, genart and artart  review
- Added a note to Section 1 on rfc4210bis and rfc6712bis activity
- Added support for constrained PKI entities that can, e.g., only store a hash of a self-signed certificate as trust anchor and require the self-signed certificate to be provided in-line in extraCerts, see Section 3.3 and Section 9
- Addressed idnits feedback, specifically changing RFC3278 -> RFC5753

I-D is in IETF last call

I-D is on the agenda for the IESG telechat on December 01, 2022