

rfc4210bis, rfc6712bis

draft-ietf-lamps-rfc4210bis-02

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

Interim 09/22– LAMPS Working Group

Status of rfc4210bis and rfc6712bis drafts

- The authors of CMP Updates provided the following versions of the drafts
 - 00 versions containing the original RFC text
 - 01 versions merging the updates specified in CMP Updates
- Changes in rfc4210bis from version 01 -> 02:
 - 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
 - **Added ToDos on defining POP and message protection using KEM keys to some sections**
 - Added a ToDo to Appendix C to do a more detailed review
 - 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)
- Changes in rfc6712bis from version 01 -> 02:
 - Adding requirement to add the content-length field into the HTTP header to Section 3.4
 - Added a reference to TLS 1.3.
 - Updating references: RFC2616 -> RFC9112; RFC2818 -> RFC9110, and RFC5246 -> RFC8446