Messaging Layer Security
Internet-Draft
Intended status: Informational
Expires: 3 September 2026

R. Mahy

2 March 2026

A more efficient FramedContentTBS structure in Messsaging Layer Security (MLS)

draft-mahy-mls-new-framed-content-tbs-01

Abstract

Most MLS signatures are signed over the relatively large GroupContext structure. This document defines a way to safely sign using a pre-hashed version of the GroupContext structure for better efficiency.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://rohanmahy.github.io/mls-new-framed-content-tbs/draft-mahy-mls-new-framed-content-tbs.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-mahy-mls-new-framed-content-tbs/.

Discussion of this document takes place on the Messaging Layer Security Working Group mailing list (mailto:mls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/mls/. Subscribe at https://www.ietf.org/mailman/listinfo/mls/.

Source for this draft and an issue tracker can be found at https://github.com/rohanmahy/mls-new-framed-content-tbs.

Status of This Memo

This Internet-Draft will expire on 3 September 2026.

Table of Contents

1. Introduction

In MLS [RFC9420] all in-member application, commit, and proposal messages (whether sent via a PublicMessage, PrivateMessage or SemiPrivateMessage [I-D.mahy-mls-semiprivatemessage]); and all external commits contain a signature of the FramedContentTBS structure. This structure contains the full GroupContext of the group, which can store a large amount of group state. (For example, in the MIMI protocol [I-D.ietf-mimi-protocol] it contains the participant list for the group, which could contain thousands of URIs.)

The GroupContext only changes once per epoch, therefore it is an excellent candidate to pre-hash and cache for efficiency reasons.

This document defines an a replacement for the FramedContentTBS structure that uses a pre-hashed GroupContext, and an MLS extension for safely negotiating the use of the new struct.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Mechanism

This document defines the new_framed_content_tbs extension. When present in a LeafNode.capabilities.extensions list, it indicates that the client supports this extension. When present in the required_capabilities.extension_types list in GroupContext.extensions it indicates that every member of the group MUST use the new FramedContentTBS structure.

The FramedContentTBS structure is replaced with the new structure below. The only change is that the GroupContext is replaced with context_hash: a hash (using the current hash function from the group’s MLS cipher suite) of the GroupContext.

Since the context_hash can be cached for an entire epoch, this can result in a substantial efficiency improvement for additional messages sent during the same epoch.

```
context_hash = RefHash(GroupContext);

struct {
    ProtocolVersion version = mls10;
    WireFormat wire_format;
    FramedContent content;
    select (FramedContentTBS.content.sender.sender_type) {
        case member:
        case new_member_commit:
            opaque context_hash<V>;
        case external:
        case new_member_proposal:
            struct{};
    };
} FramedContentTBS;
```

4. Security Considerations

This proposal replaces the GroupContext with the hash of the GroupContext.

The primary security consequence of this change is that if a non-member is aware of the context_hash, but not the entire GroupContext, it can still validate member signatures. This may have minor privacy implications.

5. IANA Considerations

This document requests the addition of a new MLS Extension Type value under the heading of "Messaging Layer Security".

RFC EDITOR: Please replace XXXX throughout with the RFC number assigned to this document.

The new_framed_content_tbs MLS Extension Type is used inside LeafNode and GroupContext objects. In a LeafNode it indicates support the the extension. In the required_capabilities of the GroupContext it indicates the extension is being used.

Value: 0x000b (suggested)

Name: new_framed_content_tbs

Message(s): GC,LN: This extension may appear in GroupContext and LeafNode objects

Recommended: Y

Reference: RFC XXXX

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/rfc/rfc9420>.

6.2. Informative References

[I-D.ietf-mimi-protocol]
Barnes, R., Hodgson, M., Kohbrok, K., Mahy, R., Ralston, T., and R. Robert, "More Instant Messaging Interoperability (MIMI) using HTTPS and MLS", Work in Progress, Internet-Draft, draft-ietf-mimi-protocol-05, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-mimi-protocol-05>.

[I-D.mahy-mls-semiprivatemessage]
Mahy, R., "Semi-Private Messages in the Messaging Layer Security (MLS) Protocol", Work in Progress, Internet-Draft, draft-mahy-mls-semiprivatemessage-06, 16 October 2025, <https://datatracker.ietf.org/doc/html/draft-mahy-mls-semiprivatemessage-06>.

Author’s Address

Rohan Mahy
Email: rohan.ietf@gmail.com