Messaging Layer Security
Internet-Draft
Intended status: Informational
Expires: 23 April 2026

R. Mahy
Rohan Mahy Consulting Services

20 October 2025

Messaging Layer Security Credentials using Selective Disclosure JSON and CBOR Web Tokens

draft-mahy-mls-sd-cwt-credential-01

Abstract

The Messaging Layer Security (MLS) protocol contains Credentials used to authenticate an MLS client with a signature key pair. Selective Disclosure CBOR Web Tokens (SD-CWT) and Selective Disclosure JSON Web Tokens (SD-JWT) define token formats where the holder can selectively reveal claims about itself with strong integrity protection and cryptographic binding to the holder's key. This document defines MLS credentials for both these token types.

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-sd-cwt-credential/draft-mahy-mls-sd-cwt-credential.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-mahy-mls-sd-cwt-credential/.

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-sd-cwt-credential.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

This document defines new MLS [RFC9420] credential types for SD-CWT [I-D.ietf-spice-sd-cwt] and SD-JWT [I-D.ietf-oauth-selective-disclosure-jwt] tokens respectively. The SD-CWT Credential contains a Selective Disclosure Key Binding Token (SD-KBT). The SD-JWT Credential contains SD-JWT with Key Binding (SD-JWT+KB), which could be represented in the traditional data format, or in a more compact binary encoding.

The "holder" of one of these tokens could be the MLS client including the token in its Credential in its LeafNode (in a group or in a KeyPackage) or in an ExternalSender structure.

> Note: It is not necessary for an AS to selectively disclose any claims. In other words, an Identity Provider that normally generates JWT or CWT web tokens could generate the same claim set, as long as the confirmation key is included and verified by the issuer.

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.

The term Credential is used as defined in Section 5.3 of [RFC9420]. The terms MLS Distribution Service (DS) and MLS Authentication Service (AS) are used as defined in [RFC9750]. The terms MLS client, MLS group, LeafNode, KeyPackage, PublicMessage, PrivateMessage, ratchet tree, and GroupInfo are likewise common MLS terms defined in [RFC9420].

3. New MLS Credential types

This document extends the list of defined CredentialTypes in MLS to include sd_cwt and sd_jwt types. Additional syntax and semantics are defined in the following subsections.

```
struct {
    CredentialType credential_type;
    select (Credential.credential_type) {
        case basic:
            opaque identity<V>;
        case x509:
            Certificate certificates<V>;
        ...
        case sd_cwt:
            opaque sd_kbt<V>;
        case sd_jwt:
            SdJwt sd_jwt;
    };
} Credential;
```

The MLS architecture [RFC9750] describes the Authentication Services as having the following three services (i.e. requirements):

1. Issue credentials to clients that attest to bindings between identities and signature key pairs

2. Enable a client to verify that a credential presented by another client is valid with respect to a reference identifier

3. Enable a group member to verify that a credential represents the same client as another credential

The consequence of this is that the consumer of the SD-CWT or SD-JWT needs to be able to determine both the MLS client and the application identity referred to in a token in a Credential.

3.1. MLS SD-CWT Credential

An MLS SD-CWT Credential contains a single SD-KBT, containing an SD-CWT in the KBT protected header. The SD-CWT contains zero of more disclosures (in the sd_claims header field).

Any party that can view the credential can read the disclosed claims. For example if LeafNodes are visible to the MLS DS, because MLS handshake messages are conveyed in PublicMessage, the disclosed claims would also be visible to the DS.

The SD-CWT inside the credential MAY include zero or more encrypted disclosures (in the sd_encrypted_claims header field). Each encrypted disclosure is separately AEAD encrypted with a per-disclosure unique ephemeral key and salt. The per-disclosure encryption key allows the holder/MLS client to disclose an element to a specific subset of members, or (in the common case when the DS is privy to the ratchet tree) only to members of the group. A proof of concept to decrypt encrypted disclosures only for members of the group is described in [I-D.mahy-mls-member-secrets].

The audience in the SD-KBT is either a representation of the MLS group, or a higher-level application structure associated with an MLS group or tightly-coupled collection of groups (for example, a chat room which maintains one MLS group for the main discussion and another for moderators to discuss the moderation of the room) such that being in one group without the collection would be nonsensical.

The subject in the SD-CWT represents a specific MLS client (for example a COSE key thumbprint, or a client ID URI). It should not use an identifier which represents multiple signature key pairs of the same type, or represents the same "user" on multiple devices.

3.2. MLS SD-JWT Credential

The SD-JWT Credential can be represented in the classic SD-JWT+KB data format defined in Section 4 of [I-D.ietf-oauth-selective-disclosure-jwt] (shown below), or in a more compact binary representation. MLS SD-JWT Credentials MUST include the Key Binding.

TODO: Discuss if the LeafNode signature over the Credential is sufficient

The classic format uses only characters from the unpadded base64url character set (Section 5 of [RFC4648]) plus the period (.) character to separate the three parts of the Issuer-signed JWT, and the tilde (~) character to separate disclosures from the other components.

```
<Issuer-signed JWT>~<Disclosure 1>~<Disclosure 2>~...~<Disclosure N>~<KB-JWT>
```

Figure 1: SD-JWT+KB in classic format

This document also defines a "compacted" format where each of the components of the Issuer-signed JWT, every Disclosure, and the KB-JWT are base64url decoded and stored in individual fields in the SdJwt struct.

```
struct {
    Bool compacted;
    select (compacted) {
        case true:
            opaque protected<V>;
            opaque payload<V>;
            opaque signature<V>;
            SdJwtDisclosure disclosures<V>;
            opaque sd_jwt_key_binding<V>;
        case false:
            opaque sd_jwt_kb<V>;
    };
} SdJwt;

enum {
  false(0),
  true(1)
} Bool;
```

The compacted variant allows implementations to tradeoff reduced size for the extra processing cost of base64url encoding and decoding the Credential.

4. Security Considerations

The privacy considerations in SD-CWT, SD-JWT, and MLS apply. TODO more security.

5. Privacy Considerations

The privacy considerations in SD-CWT and SD-JWT apply. The privacy considerations of MLS are largely discussed in [RFC9750]. TODO more privacy.

6. IANA Considerations

This document requests IANA to add the following entries to the MLS Credential Types registry. Please replace RFCXXXX with the RFC of this document.

6.1. SD-CWT Credential

* Value: 0x0005 (suggested)
* Name: sd_cwt
* Recommended: Y
* Reference: RFCXXXX

6.2. SD-JWT Credential

* Value: 0x0006 (suggested)
* Name: sd_jwt
* Recommended: Y
* Reference: RFCXXXX

7. References

7.1. Normative References

[I-D.ietf-oauth-selective-disclosure-jwt]
Fett, D., Yasuda, K., and B. Campbell, "Selective Disclosure for JWTs (SD-JWT)", Work in Progress, Internet-Draft, draft-ietf-oauth-selective-disclosure-jwt-22, 29 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-selective-disclosure-jwt-22>.

[I-D.ietf-spice-sd-cwt]
Prorock, M., Steele, O., Birkholz, H., and R. Mahy, "SPICE SD-CWT", Work in Progress, Internet-Draft, draft-ietf-spice-sd-cwt-04, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spice-sd-cwt-04>.

[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>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/rfc/rfc4648>.

[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>.

[RFC9750] Beurdouche, B., Rescorla, E., Omara, E., Inguva, S., and A. Duric, "The Messaging Layer Security (MLS) Architecture", RFC 9750, DOI 10.17487/RFC9750, April 2025, <https://www.rfc-editor.org/rfc/rfc9750>.

7.2. Informative References

[I-D.mahy-mls-member-secrets]
"*** BROKEN REFERENCE ***".

Acknowledgments

Thanks to Richard Barnes for his comment.

Author’s Address

Rohan Mahy
Rohan Mahy Consulting Services
Email: rohan.ietf@gmail.com