Workgroup: dispatch
Internet-Draft:
draft-mahy-dispatch-immi-mls-mime-00
Published: 7 March 2022
Intended Status: Informational
Expires: 8 September 2022
Authors: R. Mahy
Wire

Inside MLS Message Interop (IMMI) MIME type extensions

Abstract

This document defines two new extensions to the MLS (Messaging Layer Security) Protocol to allow for negotiation of MIME types exchanged among members of an MLS group.

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/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 September 2022.

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2219].

The terms MLS client, MLS group, and KeyPackage have the same meanings as in the MLS protocol [I-D.ietf-mls-protocol].

2. Introduction

MLS is a group key establishment protocol motivated by the desire for group chat with efficient end-to-end encryption. While one of the motivations of MLS is interoperable standards-based secure messaging, the MLS protocol does not define or prescribe any format for the encrypted "application messages" encoded by MLS. This document describes two extensions to MLS which allow MLS clients to advertise their supported MIME types, and to specify which MIME types are required for a particular MLS group. These allow clients to discover MLS groups with an interoperable and extensible set of content types.

A companion document [I-D.mahy-dispatch-immi-content] describes a specific profile for interoperable instant messaging body types.

3. Extension Description

This document specifies two MLS extensions of type MimeTypeList: accepted_mime_types, and required_mime_types.

MimeType is the ASCII string encoded as a TLS vector type containing a single MIME type and any of its parameters.

MimeTypeList is an ordered list of MimeType objects.

```
// Text string representation of a single IANA registered MIME Type.
MimeType mime_type<V>

struct {
    MimeType mime_types<V>
} MimeTypeList
```

Example MIME Types:

```
image/png
text/plain;charset="UTF-8"
```

An MLS client which implements this specification SHOULD include the accepted_mime_types extensions in its KeyPackages, listing all the MIME types it can receive.

When creating a new MLS group, the group MAY include a required_mime_type extension in the group Extensions. When used in a group, the client MUST include the required_mime_types extension in the list of extensions in RequiredCapabilities.

MLS clients SHOULD NOT add an MLS client to an MLS group with required_mime_types unless the MLS client advertises it can support all of the required MIME Types. As an exception, a client could be preconfigured to know that certain clients support the mandatory types.

4. IANA Considerations

This document proposes registration of two MLS Extension Types.

4.1. accepted_mime_types MLS Extension Type

The accepted_mime_types MLS Extension Type is used inside KeyPackage objects. It contains a MimeTypeList representing all the MIME Types supported by the MLS client publishing the KeyPackage.

```
Template:
Value: 0x0005
Name: accepted_mime_types

Message(s): This extension may appear in KeyPackage objects
Recommended: Y
Reference: RFC XXXX
```

Description: list of MIME types supported by the MLS client advertising the KeyPackage

4.2. required_mime_types GroupContext extension

The required_mime_types MLS Extension Type is used inside GroupContext objects. It contains a MimeTypeList representing the MIME Types which are mandatory for all MLS members of the group to support.

Template:
Value: 0x0006
Name: required_mime_types

Message(s): This extension may appear in GroupContext objects
Recommended: Y
Reference: RFC XXXX

Description: list of MIME types which every member of the MLS group is required to support.

5. Security Considerations

The Security Considerations of MLS apply.

Use of the extensions in this document could leak some private information both in KeyPackages and inside an MLS group. They could be used to infer a specific implementation, platform, or even version. Clients should consider carefully the implications in their environment of making a list of acceptable MIME types available.

A client which can take over group administration could prevent members from joining or sending messages in an established group, by requiring a list of required MIME types which the attacker knows is unsupported. This attack is not especially helpful, as taking over group administration can have more disruptive effects.

6. Normative References

[I-D.ietf-mls-protocol] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", Work in Progress, Internet-Draft, draft-ietf-mls-protocol-12, 11 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-protocol-12>.

[RFC2219] Hamilton, M. and R. Wright, "Use of DNS Aliases for Network Services", BCP 17, RFC 2219, DOI 10.17487/RFC2219, October 1997, <https://www.rfc-editor.org/info/rfc2219>.

7. Informative References

[I-D.mahy-dispatch-immi-content]
Mahy, R., "Inside MLS Message Interop (IMMI) instant message content", Work in Progress, Internet-Draft, draft-mahy-dispatch-immi-content-00, 7 March 2022, <https://datatracker.ietf.org/doc/html/draft-mahy-dispatch-immi-content-00>.

Author's Address

Rohan Mahy
Wire

Email: rohan.mahy@wire.com