Workgroup: MLS
Internet-Draft:
draft-mahy-mls-group-anchors-00
Published: 13 March 2023
Intended Status: Informational
Expires: 14 September 2023
Authors: R. Mahy
Wire

Per-group Credential Anchors for Message Layer Security (MLS)

Abstract

This document describes a Message Layer Security (MLS) GroupContext extension to restrict the set of trust anchors used for identity validation in MLS groups. It is useful in federated or interoperability environments to allow a specific federated domain to assert identities for its own identifiers but not for the identifiers of other domains.

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 14 September 2023.

Copyright Notice

Table of Contents

1. Terminology
2. Introduction
3. Example Use
4. Extension Description
5. IANA Considerations
   5.1. group_trust_anchors MLS Extension Type
6. Security Considerations
7. Normative References
Author's Address

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, LeafNode, GroupContext, KeyPackage, GroupContextExtensions Proposal, Credential, CredentialType, and RequiredCapabilities have the same meanings as in the MLS protocol [I-D.ietf-mls-protocol].

2. Introduction

A typical desktop or mobile operating system may have hundreds of root certificates configured. Not all of these certificates are appropriate to make identity assertions about every domain which participates in a federated MLS group. The members of a federated group should be able to restrict the specific trust anchors expected, on a per-domain basis. The root of the trust anchor still needs to be among the operating system or application trusted root certificates.

In addition, this extension allows the domain validation to be restricted to an intermediary certificate which is anchored in one of the trusted root certificates. For example, the domain example.com might use the Certificate Authority "Large Commercial Certificate Authority LLC" as the root for its domain certificates, but only the intermediate certificate ca.messaging.example.com actually makes assertions about MLS identities for that domain.

While this extension initially only specifies behavior for X.509 certificates and the x509 credential type in MLS, other credential types with strong cryptographic verification, such as VerifiableCredentials, could extend this extension to include the relevant notion of trust anchors.

3. Example Use

Consider an MLS group containing MLS clients from three domains: alpha.example, beta.example, and charlie.example. All three use compatible MLS-based instant messaging services which are federated [I-D.ietf-mls-federation].

- alpha.example is a very large company or national government with their own root certificate authority which is already present in most operating systems.
- beta.example is a large company which uses certificate authority yankee.example.
- charlie.example is a small organization whose service is hosted by a cloud provider cirrus.example. Their certificates (both charlie and cirrus) are issued by the certificate authority zulu.example.

Alice is a user on alpha.example, and creates a private federated MLS group, inviting Andy (from alpha.example), Bob and Betty (from beta.example), and Cathy and Chuck (from charlie.example). Every client in the group would like to verify the identities of the other clients. If alpha.example is compromised, we don't want an attacker to be able to impersonate Bob, Betty, Cathy, or Chuck without detection. Likewise if yankee.example is compromised, we don't want an attacker to be able to impersonate Alice, Andy, Cathy, or Chuck without detection.

With this extension, the clients in an MLS group maintain a list of identity domains and each of their corresponding trust anchors. This does not replace the operating system or application trusted root certificates, it just associates a specific domain with a specific trust anchor.

4. Extension Description

This document specifies a GroupContext MLS extension group_trust_anchors of type PerDomainTrustAnchors. The syntax is described using the TLS Presentation Language [RFC8446].

Each PerDomainTrustAnchor represents a specific identity domain which is expected and authorized to participate in the MLS group. It contains the domain name and the specific trust anchor used to validate identities for members in that domain.

```
struct {
    opaque domain_name<V>;
    CredentialType credential_type;
    select (Credential.credential_type) {
        case x509:
            Certificate chain<V>;
    };
} PerDomainTrustAnchor;

struct {
    PerDomainTrustAnchor domain_anchors<V>;
} PerDomainTrustAnchors;

PerDomainTrustAnchors group_trust_anchors;
```

An MLS client which implements this specification SHOULD include the group_trust_achors extension in the extensions field in the GroupContext of groups it creates. It includes the per-domain trust anchors for all the domains expected and authorized to participate in the group. As new members of the group are added or removed, the member which Commits these membership changes is expected to maintain the list of trust roots up-to-date by also including an appropriate GroupContextExtensions Proposal any time the list of expected federated domains changes. Likewise, when any of the trust anchors used in a domain changes, an appropriate member needs to Commit a GroupContextExtensions Proposal updating the list of trust roots.

5. IANA Considerations

This document proposes registration of a new MLS Extension Type.

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

5.1. group_trust_anchors MLS Extension Type

The group_trust_anchors MLS Extension Type is used inside GroupContext objects. It contains a PerDomainTrustAnchors object representing the trust anchors which are expected for identity validation inside the MLS group.

Template:
Value: 0x000A
Name: group_trust_anchors
Message(s): This extension may appear in GroupContext objects
Recommended: Y
Reference: RFC XXXX

6. Security Considerations

The Security Considerations of MLS apply.

Improper use of the extension in this document could allow the creator of an MLS group or the sender of a GroupContextExtensions Proposal to maliciously add or remove authorized domains from a group, and to impersonate members from specific domains. Therefore it is vital that all clients which implement this extension validate that changes to their own domain trust anchors conform to their domain policies.

7. 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-18, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-protocol-18>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

Author's Address

Rohan Mahy
Wire

Email: rohan.mahy@wire.com