MLS@JAN2019Interim

WG Info: https://datatracker.ietf.org/wg/mls/about/
Chairs: Nick Sullivan & Sean Turner

NOTE WELL

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a reminder:

- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process),
- BCP 25 (Working Group processes),
- BCP 25 (Anti-Harassment Procedures),
- BCP 54 (Code of Conduct),
- BCP 78 (Copyright),
- BCP 79 (Patents, Participation),
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Requests

Minute Taker(s)

Jabber Scribe(s)

Sign Blue Sheets

State your name @ the mic

Keep it professional @ the mic

Agenda

Administrivia (Chairs)

Recap of WG status (Chairs)

Review of open issues (Chairs)

Encryption of Welcome messages (Barnes)

Add-in-Place (Barnes)

Efficiency of the core protocol (Robert, Barnes)

Simplifying the key schedule? (Omara)

Lazy handshake messages (Robert)

Proxy re-encryption for server assist (Robert, Beurdouche)

User-initiated Add (Barnes)

Federation considerations (Omara)

ACK / NACK / State management / Re-init (Millican)

Analysis Updates (Bhargavan, Cremers, Beurdouche)

Implementation & Interop Updates (Robert, Beurdouche)

Brainstorm open items, review schedule

WG Status: Charter

The primary goal of this working group is to develop a standard messaging security protocol for human-to-human(s) communication with the following security and deployment properties so that applications can share code, and so that there can be shared validation of the protocol:

- Message Confidentiality - Messages can only be read by members of the group.
- Message Integrity and Authentication - Each message has been sent by an authenticated sender, and has not been tampered with.
- Membership Authentication - Each participant can verify the set of members in the group.
- Asynchronicity - Keys can be established without any two participants being online at the same time.
- Forward secrecy - Full compromise of a node at a point in time does not reveal past messages sent within the group.
- Post-compromise security - Full compromise of a node at a point in time does not reveal future messages sent within the group.
- Scalability - Resource requirements have good scaling in the size of the group (preferably sub-linear).

WG Status: Charter

Non goals include:

- Enabling interoperability/federation between messaging applications beyond the key establishment, authentication, and confidentiality services.
- Developing new authentication technologies.

WG Status

Info

GH repos:

- Meetings
- Architecture
- Protocol

IETF WG:

- Mailing List: mls@ietf.org
- Subscribe
- Architecture I-D
- Protocol I-D

WG Status

Brief Timeline

BOF @ IETF101 (2018-03)

WG chartered (2018-05)

1st meeting @ IETF102 (2018-07)

Architecture and Protocol I-Ds adopted by WG (2018-08)

Choose TreeKEM over ART @ 2018ParisInterim (2018-09)

Architecture I-D @ Informational Track

Contents include:

Architecture (see below)

Functional and Security Requirements

```
 ----------------      --------------
| Authentication |    | Delivery     |
| Service (AS)   |    | Service (DS) |
 ----------------      --------------
                    /        |        \             Group
*********************************************************
*                 /          |          \               *
*                /           |           \              *
*      ----------       ----------       ----------     *
*     | Client 0 |     | Client 1 |     | Client N |    *
*      ----------       ----------       ----------     *
*      ............................      ...........    *
*      Member 0                          Member 1       *
*                                                       *
*********************************************************
```

Protocol I-D @ Standards Track

- Protocol overview
- Ratchet Trees
    - Terminology, Credentials, Group State, Key Schedule, etc.
- Initialization Keys
- Handshake Messages
    - Init, Add, Update, Remove
- Message Protection

MLS@JAN2019Interim

WG Info: https://datatracker.ietf.org/wg/mls/about/
Chairs: Nick Sullivan & Sean Turner