•17. November | ALAN DURIC, HAUKE GIEROW

Messaging Layer Security: How an IETF-Standard is made and what you can do with it

What is MLS?

Quick overview of the standard

MLS will impact billions of people and will further disrupt coms / telco industry

We will tell the story of how it came to pass

- **M**essaging **L**ayer **S**ecurity is the first global open standard for end-to-end encrypted real-time communication (RfC 9420)
- The IETF standard can freely be implemented by everyone
- MLS standardizes the end-to-end encryption part of messaging, audio- and video calling and will thus be an important part of interoperability
- Groups with up to 10k users
- The protocol is designed for ciphersuite agility – new ciphers can be plugged without touching the protocol itself
- Already multiple independent implementations underway

wire

Standards are essential for **sustainable** and **secure** communications' **ecosystem**!

How do you create an IETF-Standard?

What we learned from creating a new standard from scratch

Creation of the IETF Standard

MLS Story

Different phases and their timing

- probing the interest and gathering critical mass of relevant interested parties **- H1 2016**

- in-official face to face meeting (**Bar BoFs**) – **JULY 2016** during the IETF 96 meeting in Berlin at Cordobar

- **BoF preparations** - set of meetings (virtual and in person) to form the “WG scaffolding” (draft charter, initial drafts, WG members) – **H2016/2017**

- IETF BoF meeting – final Go/NoGo from IETF **– in MAR2018** at IETF London

- **Ratified Standard** - IETF RFC 9420 published – **JUL2023**

Who was involved?

TECH / GOOGLE / SECURITY

Google Messages signs onto cross-platform encrypted group chat standard

/ Google is adopting the Messaging Layer Security (MLS) protocol for its Messages app that aims to handle end-to-end encryption and support sending and receiving between supported messaging apps.

Google urges EU regulators to make Apple open up iMessage

Apple's iMessage should be regulated as a core service and made interoperable with other messaging platforms, argues Google and a group of European telcos.

Hell freezes over – Apple to support RCS messages from Android phones next year

News By Lance Ulanoff published about 6 hours ago

Breaking: Apple will support RCS - the green bubble shame set to end

DMA phases

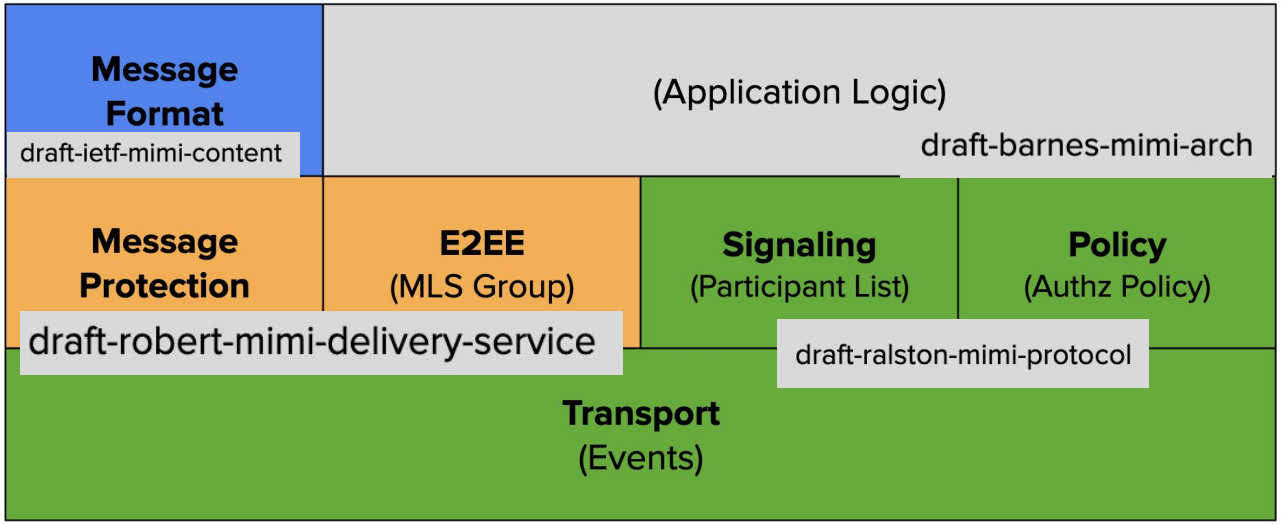
- 2024 (1-1 messages)
- 2025 (groups)
- 2026 (calling)

Sachin Tandon ✓
@cugwmui

In the last 3 years, the EU has pushed more innovation into Apple than Apple's own engineering team.

> **9to5Mac** ✓ @9to5mac · 5h
> Apple announces that RCS support is coming to iPhone next year
> 9to5mac.com/2023/11/16/app... by @ChanceHMiller

MIMI and more



- MIMI builds on MLS and will specify more areas necessary for interoperability between encrypted messaging providers

- current areas of interest are: transport protocol, discovery, group policies etc.

- further areas necessary to address related to E2EID and whole set of Application layer topics (like reactions, replies, etc.), which will be handled by EU Commission White Papers etc.

Benefits of MLS

MLS from within – encryption, architecture and protocol design,

IETF MLS versus Double Ratchet

PROS

-- **Scalability**: MLS is designed to be highly scalable, with thousands of group members. On the other hand, Double Ratchet is primarily designed for two-party communications

- **Group Management:** MLS provides built-in mechanisms for handling group changes (like adding or removing members) securely and efficiently. In contrast, Double Ratchet doesn't natively handle group dynamics.

-**Cryptographic Efficiency:** MLS uses a tree-based structure to manage group keys, which allows it to offer logarithmic complexity for group updates. This is more efficient than naive extensions of Double Ratchet to multi-party settings.

-- **Interoperability**: Because MLS is an IETF standard, it has the potential for wide adoption and interoperability between different messaging systems.

CONS

- **Protocol Complexity**: While MLS provides more features and better scalability, it is also more complex than Double Ratchet. This can make it harder to implement correctly and could potentially lead to more security issues if not handled properly.

Comparison

User Perspective

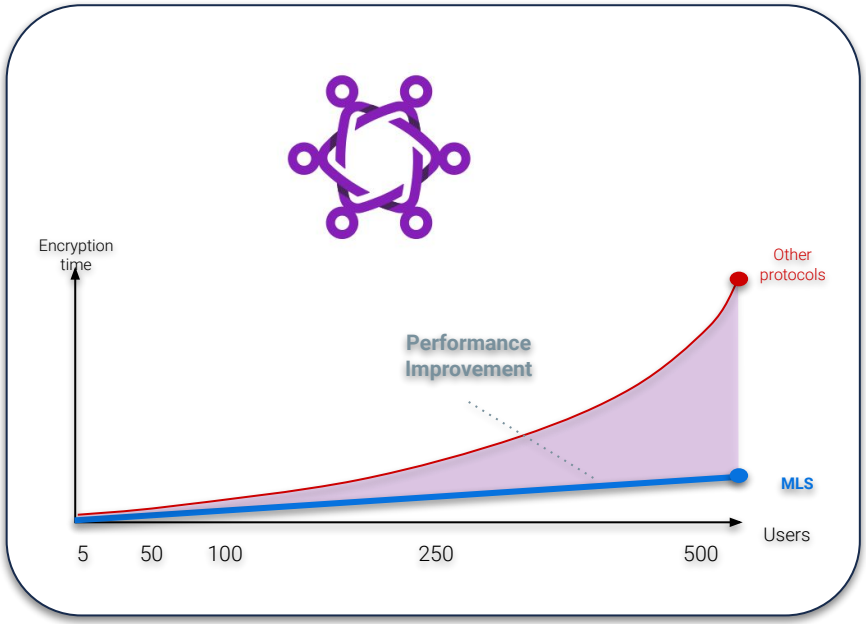
-- **Conversations verifications –** DR users can verify the authenticity of their encrypted sessions by scanning a QR code or reading aloud a string. Very cumbersome and set for failure for large groups and especially when App gets reinstalled or changed phone.

- **Group size** – DR group size is mostly in sizes of 250 or similar, while IETF MLS groups are designed for 10k users and more

High performance in large groups

- Unlike with double ratchet, compute time to encrypt group messages rises in a linear fashion with MLS, not exponentially

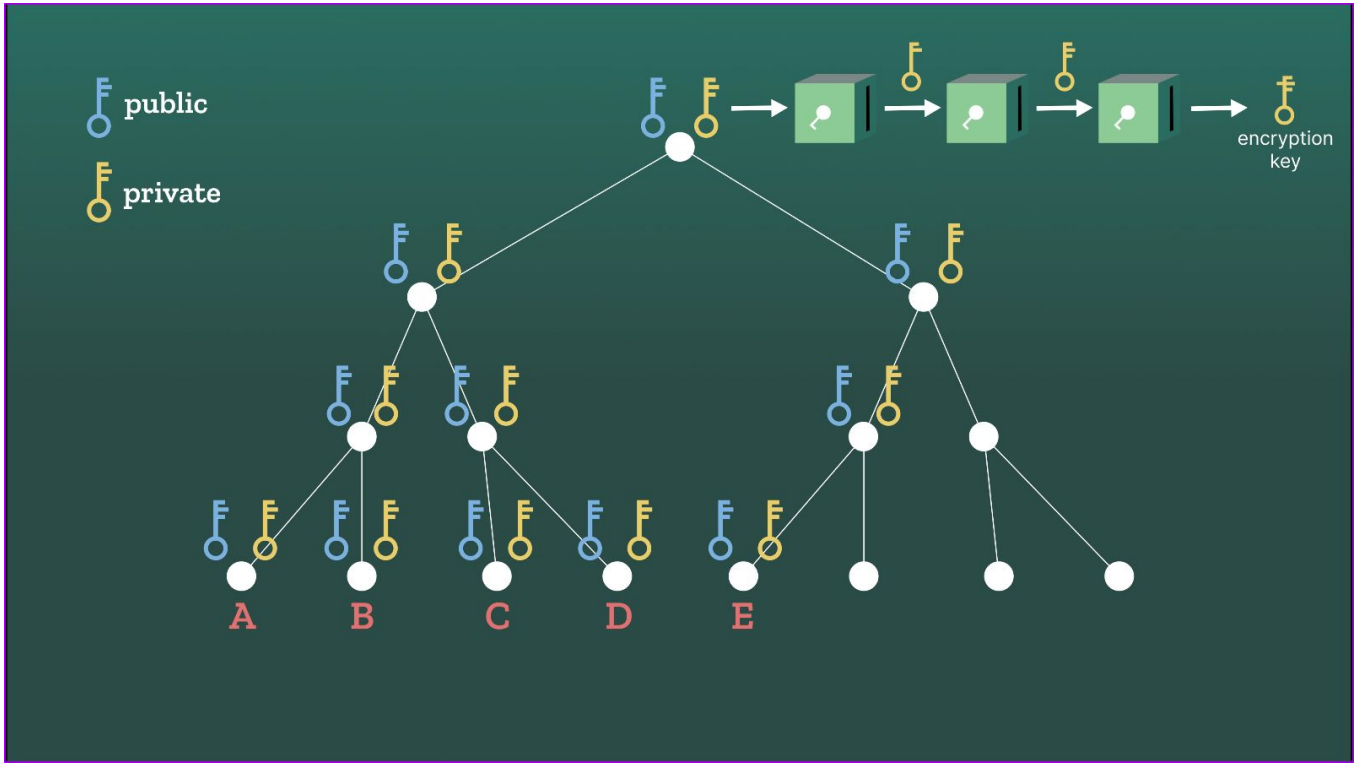
- With MLS, every group agrees on one group-key, that is valid for a specific instance and time of the group, removing expensive calculations of encrypted messages to every individual member of the group



How MLS Works

MLS Ratchet Tree:

- Maintained by every group member;
- Every leaf contains a DH-key pair for one device
- Root contains main group key
- Inner nodes contain subgroup keys



Source: https://www.youtube.com/watch?v=FESp2LHd42U

Ciphersuite agility

- MLS allows for the exchange of ciphersuites used in the protocol, without touching the protocol itself

- If one of the ciphers used in the current draft of the protocol is deemed insecure or insufficient it can be replaced

- Future use cases: the integration of quantum-safe cyphers, once the standard is finished

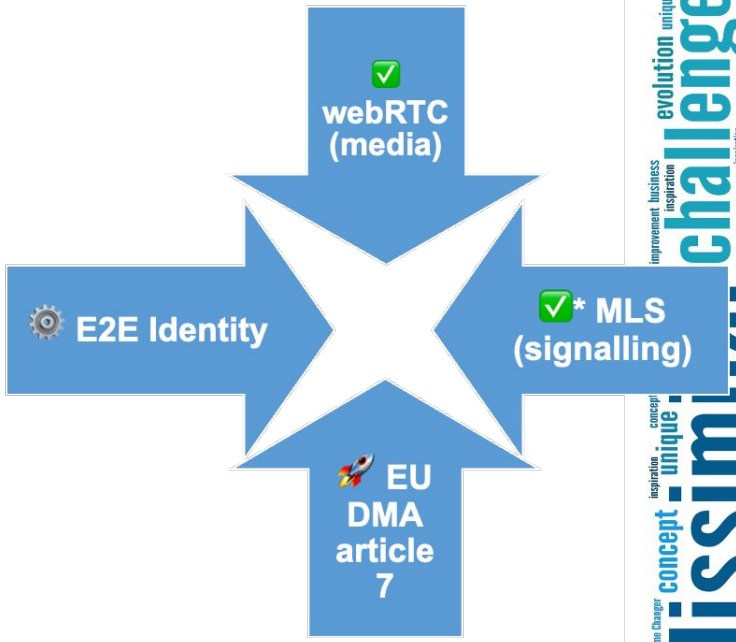
- We can even build **hybrid schemes** for post-quantum key exchange tunnelled through eg. ED25519; this way the system is safe as long as *either* of the two schemes is safe.

- Another use case: Use of different ciphersuites mandated by local laws, e.g. in government environments, like US requiring NIST EC

Whats ahead?

Using MLS to foster interoperability and reshape the telco industry

What is happening
The Big Shift!



Email and Telecom Calls as we know them are dead!

(or not much relevant)


Disruptions ahead!
NEW
NORMAL

Let’s make secure communication ubiquitous

Alan Duric

Hauke Gierow