Messaging Layer Security

The Future of Secure Communication

By Wire™ Swiss GmbH

This report provides an introduction to Messaging Layer Security (MLS) and describes the current ecosystem, the goals it sets to achieve, and Wire's vision as a driving force in developing a groundbreaking technology that has the potential to impact industry standards when it comes to secure group communication within organizations.

Leading a New Era of Collaboration

Messaging Layer Security, or MLS for short, is a new protocol designed to facilitate more secure enterprise messaging platforms.

In 2016, the lack of an open standard for end-to-end encryption lead Wire to open a discussion around its vision for secure messaging with others. What started as an informal conversation at a Berlin restaurant one evening during IETF 96' with peers from Mozilla and Cisco would later become a fully grown Internet Engineering Task Force (IETF) workgroup.

While the initial focus was on creating an open standard, other contributors including the University of Oxford, Facebook, INRIA, MIT, Google, and Twitter later joined the effort and brought more innovation to the table including Facebook and the University of Oxford's Asynchronous Ratcheting Trees concept publication. After a number of alternatives were considered, this concept became the base layer of discussions within the MLS group and finally lead to the analog TreeKEM concept, which is now at the core of the protocol. Academic research has also shown, that the security of group conversations can be improved. This extended the original scope of MLS to three major goals in the charter:

- Make secure messaging in (large) groups more efficient.
- Increase the security of groups with regards to membership, while maintaining security guarantees like Forward Secrecy and Post-Compromise Security.
- Make the protocol a standard that everyone can use freely and safely.

Bringing MLS to the Frontier of Secure Collaboration

While personal messaging systems are increasingly adopting end-to-end encryption, corporate messaging has failed to follow. A majority of organizations are still heavily relying on email communication, a tool that has proven an open door to cyber threats with odds showing that businesses are as unlikely to avoid a malware attack as they are to pull an Ace of Spades from a shuffled deck in one try. This comes to show that at a time when information is the most valuable asset to an organization, a substantial blind spot still remains in using email – and this is what MLS strives to tackle.

The Goals of MLS

MLS brings together some of the world's largest tech companies and renowned academics with a common vision of transforming enterprise communication, ensuring that now and in the future platforms can be interconnected seamlessly and in a standardized way.

The MLS protocol's most significant goal is to make end-to-end encrypted messaging in large groups efficient and more secure as well as to become an open standard for all industries. The MLS group messaging protocol aims to cover multiple industry use-cases including federation and web-browser support, to have sub-linear complexities allowing practical groups of thousands of clients, and to provide formal security guarantees.

Messaging applications are increasingly making use of end-to-end security mechanisms to ensure that messages are only accessible to the communicating endpoints, and not to any servers involved in delivering messages. A key factor of the MLS group protocol is that it provides efficient asynchronous group key establishment with Forward Secrecy and Post-Compromise Security for groups in size ranging from two to tens of thousands.

Why it is important for Wire

At Wire, we have a vision for secure messaging: federated environments based on open standards. Choosing open standards over proprietary technology is not an emotional decision. In the past we have been involved in similar efforts that made a deep impact on the industry:

- Standardizing the Internet Low Bitrate Codec (iLBC) at Global IP Sound paved the way for WebRTC.

- Skype disrupted the telecommunication world with free calls. SILK, the codec used for Skype calls, evolved and became an open standard known as Opus and now also an integral part of WebRTC.

Today WebRTC is built into most browsers (Chrome, Firefox, Safari, Edge, etc.) as well as into many communication products, making for an install base of billions of devices. We believe that in the next decade messaging will be shaped by the increasing awareness of users around subjects like privacy and security. People feel strongly about this and there is a large consensus that messages are something private and worth protecting from prying eyes.

We are convinced that the approach of pushing for open standards was valid in the past and that it is also valid for the future. The MLS workgroup benefits from work and assistance of the academic community, and the intent is to follow the pattern of TLS 1.3, with the specification, implementation, and formal verification proceeding in parallel.

A few implementations already exist, that now aim for perfect interoperability. By the time we arrive at the final version (RFC), we hope to have several interoperable implementations as well as a thorough security analysis. While more work needs to be

done on MLS, large hurdles have been overcome already and we believe the ongoing work is going in the right direction.

About Wire

Wire is the most secure collaboration platform, transforming the way businesses communicate in the same way and speed that its founders disrupted telephony with Skype. Headquartered in Switzerland with offices in Berlin and San Francisco, Wire launched its collaboration and communications platform for businesses in early 2018 and today counts over 700 enterprise customers, making Wire the fastest-growing collaboration platform. Wire offers messaging, voice, video, file-sharing, and search, all protected by end-to-end encryption. Wire's product suite has been recognized by both Forrester and Gartner as one of the most effective and secure communications platforms. Wire is consistently delivering ground-breaking innovation from a unique "message fortress" architecture to encrypted video conferencing, guest rooms and Messaging Layer Security. Built on the foundation of security and ease of use, Wire is receiving accolades in both categories, winning Cybersecurity Breakthrough's 2019 award for the *Most Secure Communication Solution* and Capterra's 2019 *Best Ease of Use* award.

Learn more about Messaging Layer Security

Architecture:	Github.com/mlswg/mls-architecture Protocol.messaginglayersecurity.rocks
Protocol:	Github.com/mlswg/mls-protocol Architecture.messaginglayersecurity.rocks
Code + Interop:	Github.com/mlswg/mls-implementations
Discussion:	mls@ietf.org (archives)