LINE Encryption Report

2019.11.13

English

Nov 2019

Purpose of this Report

The propose of this report is to describe the type, scope, and deployment status of the encryption mechanisms integrated into each of LINE's main features.

Encryption in LINE

LINE employs various encryption technologies to protect user information. In addition to transport encryption, which is used to protect traffic between LINE clients and servers, we apply Letter Sealing encryption to supported message types and supported voice/video calls. Letter Sealing is the name of the end-to-end encryption (E2EE) protocol developed by LINE. For details about the encryption protocols and algorithms used in LINE, please refer to our **Encryption Whitepaper**.

Encryption Deployment Status

(1) LINE Messaging

Text and location messages sent and received using LINE's messaging feature are end-to-end encrypted with Letter Sealing if the following conditions are met.

Both users have Letter Sealing enabled in 1-to-1 chats

All users have Letter Sealing enabled in 1-to-n chats (chats with up to 50 members)

All users have Letter sealing enabled in group chats (groups with up to 50 members)

Message types and media other than text and location messages (image, video, file, and audio messages) are encrypted using transport-level encryption – either LEGY encryption or HTTPS. The chart below shows transport encryption deployment status for each message or media type for the period May 2018–October 2019.

- For data before May 2018, please refer to the **last year's Encryption Report**.

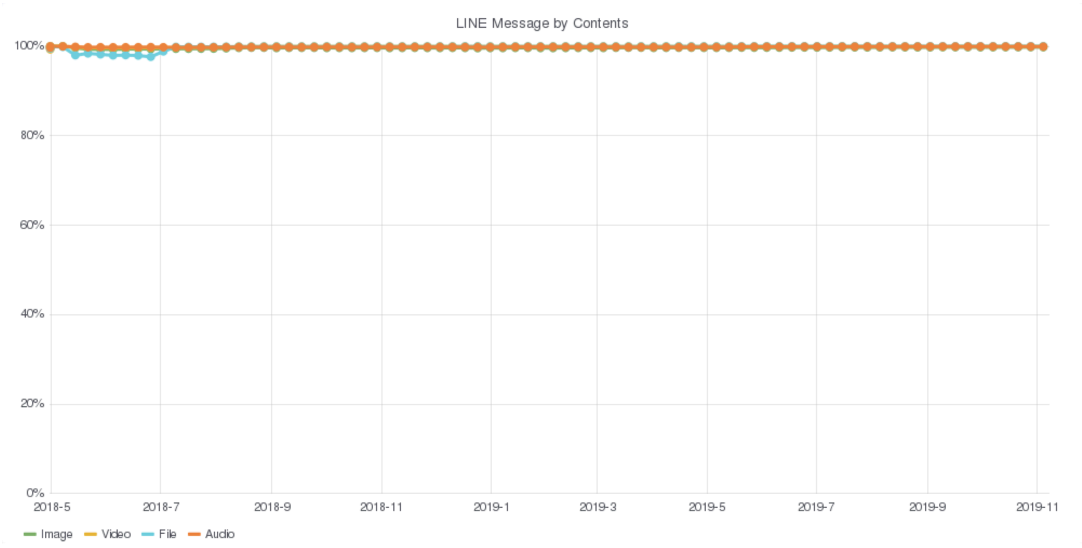

Figure 1: Transport encryption deployment status

Due to certain technical and environmental constraints, transport encryption was not sufficiently deployed for certain media types. However, starting from September 2017, we have maintained a transport-level encryption rate very close to 100%.

- Due to performance issues related to encryption, transport encryption deployment on certain platforms was delayed.
- In some countries, HTTPS could not be used on mobile networks for a certain period of time. Currently, transport encryption is deployed irrespective of network connectivity type.
- In July 2017, in order to resolve an issue with deploying transport encryption for audio files, transport encryption was scaled down for about two months. In September 2017, transport encryption scope was restored.

The following table summarizes the encryption (Letter Sealing, LEGY Encryption, HTTPS) deployment status for each message and media type.

Message/media type	2015	2016	2017/9	2018/4	2019/10
Text	○	○→◎	◎	◎	◎
Location	○	○→◎	◎	◎	◎
Stickers *1	△	△	○	○	○
Image files *2	△	△	○	○	○
Voice messages *3	X	X	○	○	○
Video files *3	X	X	○	○	○
Other files *2	△	△	○	○	○

Legend: ◎ Letter Sealing (end-to-end encryption)/ ○ Transport-level encryption / △ Partially protected / X Not encrypted or not sufficiently encrypted

■Notes

◎ Letter Sealing is enabled by default in major LINE clients.
○ sufficiently secure transport encryption, as evaluated at release time, is employed by major LINE clients.
△ that partial data protection was applied. The security level of the employed encryption was considered adequate both at release time, and at the time of writing of this report.
X the referenced message type or functionality did not have sufficient protection, as evaluated at the time of writing of this report.

*1 △ During this period, HTTP was used to download sticker packages, but messages that include stickers were themselves encrypted.

*2 △ During this period, both HTTP and HTTPS were used. Depending on usage environment (OS, region, connection type, etc.) transport encryption may not have been applied.

*3 X During this period, transport encryption was employed only for uploads, when connected via WiFi.

For users running older versions of the LINE client, or using an older or unsupported OS version, the encryption methods described above may not be applicable, and an older encryption method or algorithm may be used instead. In such cases, LINE communication may not be sufficiently protected.

(2) LINE Free Calls (Audio and Video Calls)

LINE supports several types free calls. Of those, 1-to-1 audio calls and 1-to-1 video calls are end-to-end encrypted using Letter Sealing as detailed in the table below. Group calls and group video calls are only protected with transport-level encryption.

Free call type	2015	2016	2017/9	2018/4	2019/10
1-to-1 audio calls	○	○→◎	◎	◎	◎
1-to-1 video calls	○	○→◎	◎	◎	◎
Group audio calls	○	○	○	○	○
Group video calls	-	○	○	○	○

Legend: ◎ Letter Sealing (end-to-end encryption) / ○ Transport-level encryption / - Not implemented

(3) Letter Sealing (end-to-end encryption) Deployment Status

Letter Sealing is LINE's end-to-end encryption protocol. Message types that support Letter Sealing are encrypted on the LINE client before being sent, and cannot be decrypted by LINE's servers. Letter Sealing was initially released as an optional feature in 2015/8, and was enabled by default in major clients in 2016. Currently the number of message types that support Letter Sealing is limited.

■ Letter Sealing Protection Scope

Text messages (in 1-to-1 chats, and in group chats with up to 50 members)
Location messages (in 1-to-1 chats, and in group chats with up to 50 members)
Audio calls (1-to-1 calls)
Video calls (1-to-1 calls)

* Letter Sealing is currently not applied to video and audio data sent as downloadable files (attachments).

■ Requirements for using Letter Sealing

For Letter Sealing to be applied to supported message types, all communicating users (all group members for LINE groups) need to have Letter Sealing enabled. If any of the communicating users disables Letter Sealing, only transport-level encryption is applied.

■ Letter Sealing Versions

The original version of LINE messaging end-to-encryption protocol, released in 2016, is referred to as Letter Sealing v1. While v1 provides end-to-end encryption for both 1-to-1 and group chats, several protocol-level attacks that could potentially lead to message forgery and user impersonation were reported via our Bug Bounty Program by Takanori Isobe (University of Hyogo, Japan) and Kazuhiko Minematsu (NEC Corporation, Japan). We verified that the attacks are not practically feasible due to additional server-side checks and restrictions implemented in LINE's messaging servers. In order to improve the security of our users and avoid potential future attacks against Letter Sealing, we developed Letter Sealing v2 in collaboration with the researchers. Details about Letter Sealing v2 can be found in our **Encryption Whitepaper**.

Letter Sealing v2 was deployed in October 2019 to all major LINE clients. The table below shows the minimum version of each LINE client required to support Letter Sealing v2.

Client type	Version
LINE for iOS/iPad OS	8.15.0
LINE for Android	8.17.0
LINE for Mac/Windows	5.12.0
LINE Chrome Extension/ChromeOS	2.2.0
LINE Lite for Android	2.6.0

(4) Forward Secrecy Deployment Status

Forward secrecy is enabled in some LINE usage environments. If forward secrecy is supported for a communication channel, even if one of the parties' long-term private key is leaked or compromised, messages encrypted before the time of compromise are still protected. Currently only some of LINE's communication channels support forward secrecy.

■ Forward Secrecy for LINE Client-Server Communication (forward-secure in case of LINE server key compromise)

2017/9 ○ Supported for major clients *4

2016 △ Partially supported *5

*4 May not be supported depending on OS and LINE client version / *5 Supported for some regions and client versions

■ Forward Secrecy in Letter Sealing (forward-secure in case of per-device private key compromise)

Not supported