LINE Encryption Status Report

2017.09.13

English | Sep 2017

Purpose Statement

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.** The purpose of this report is to clarify the types and scope of encryption applied in each of LINE's features.

Main LINE Message Types and Their Encryption Status

	2015	2016	2017/9
Text messages	○	○ → ◎	◎
Location messages	○	○ → ◎	◎
Stickers *1	△	△	○
Images *2	△	△	○
Voice messages *3	x	X	○
Videos *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

Supplementary Information

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

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

*2 △ During the signified 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 the signified 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.

Encryption Status of Audio and Video Calls

	2015	2016	2017/9
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

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).

Additional Information about Letter Sealing

In order for messages to be encrypted with Letter Sealing, all parties' LINE clients (all group members' clients in the case of group chats) have to support Letter Sealing, and Letter Sealing needs to be enabled by all parties. If Letter Sealing is unsupported or disabled, only transport-level encryption is employed.

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 *1

2016 △ Partially supported *2

*1 May not be supported depending on OS and LINE client version *2 Supported for some regions and client versions

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

Not supported

Version history

2017/9/13 Initial release