LINE Encryption Report

2022.12.14

English

Dec 2022

Purpose of this Report

The purpose 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 layer encryption, which is used to protect traffic between LINE clients and servers, we also apply Letter Sealing encryption to supported message types and 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
■Letter sealing (End-to-end encryption)

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

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

If you want to see if the chat room is protected by Letter Sealing, you can check the room menu. Please refer to the guide **here**. Messages other than text and location messages, such as image, video, file, and audio messages, are encrypted only using transport layer encryption – either by LEGY*1 encryption or TLS. The chart below shows the transport layer encryption deployment status for each type of message for the period Aug 2021 - Aug 2022.

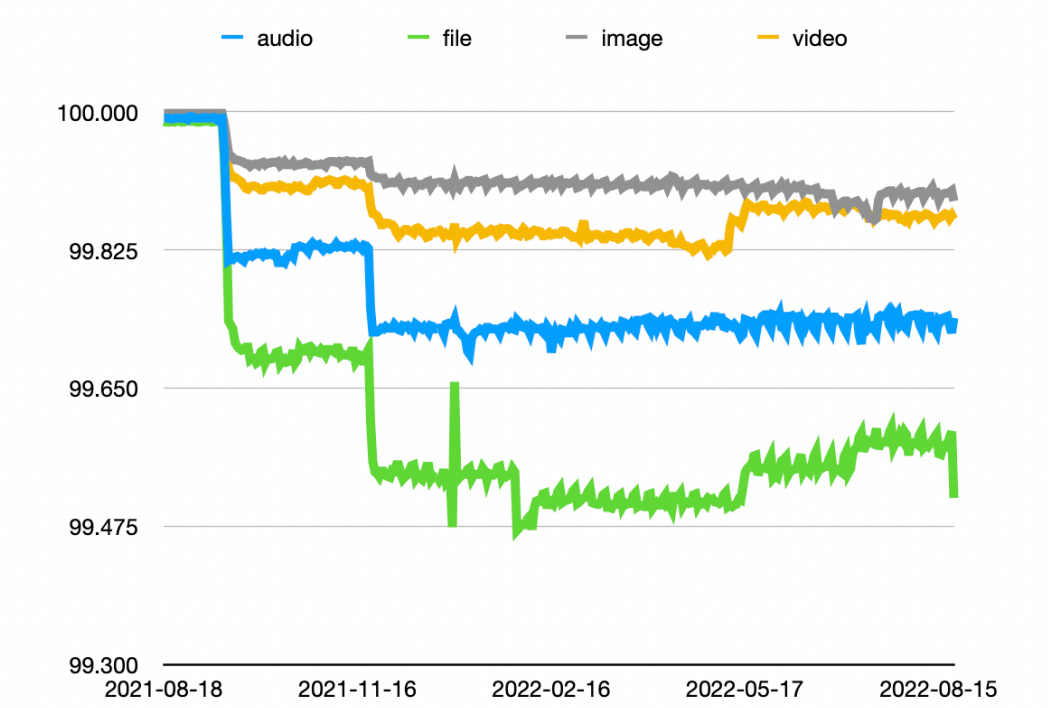

Figure 1: Transport encryption deployment status

*1 LEGY stands for Line Event-delivery GatewaY, and it's a custom-built API gateway server. LEGY uses standard cryptography algorithms for key exchange and encryption.

- For data before Aug 2021, please refer to the **last year's Encryption Report**.

■Transport layer encryption

The former default encryption was LEGY encryption. But we are migrating to TLS, and TLS is the default encryption protocol. Currently TLS 1.2 and 1.3 are supported.

We use either DHE or ECDHE for the key exchange to make sure forward secrecy.

Due to certain technical and environmental constraints, transport layer encryption was not sufficiently deployed for certain media types. However, starting from September 2017, we have maintained a transport layer 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, TLS) deployment status for each message and media type.

Message/media type	2015	2016	2017/9	2018/4	2019/10	2020/9	2021/9	2022/8
Text	○	○→◎	◎	◎	◎	◎	◎	◎
Location	○	○→◎	◎	◎	◎	◎	◎	◎
Stickers *2	△	△	○	○	○	○	○	○
Image files *3	△	△	○	○	○	○	○	○
Voice messages *4	X	X	○	○	○	○	○	○
Video files *4	X	X	○	○	○	○	○	○
Other files *3	△	△	○	○	○	○	○	○
Message reaction	-	-	-	-	-	-	○	○

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.

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

*3 △ 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.

*4 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 of 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, group video calls, and Line meeting are only protected with transport-level encryption.

Free call type	2015	2016	2017/9	2018/4	2019/10	2020/9	2021/9	2022/8
1-to-1 audio calls	○	○→◎	◎	◎	◎	◎	◎	◎
1-to-1 video calls	○	○→◎	◎	◎	◎	◎	◎	◎
Group audio calls	○	○	○	○	○	○	○	○
Group video calls	-	○	○	○	○	○	○	○
LINE Meeting	-	-	-	-	-	○	○	○

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 is enabled by default. And it cannot be turned off.

■ 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).

■ Letter Sealing Exception

In the following cases, a part of user communication can be sent to LINE servers

- Website preview(aka Pagepoker): To generate the website preview in the chat room, URLs will be sent to the Pagepoker server. Such URLs are processed solely for the purpose of preview generation. Users can opt-out of this function in the settings.(Settings → Chats → URL previews)
- Spam report: When a user wants to report a spam issue, the suspicious part of the chat message will be sent to the server for investigation. The message is sent to the server only if the reporter consents.
- Announced messages: You can "announce" things like messages you've sent and received, polls you created, and events so they permanently appear at the top of a chat. To make them available to newly joinned members, they are sent to the server.
- Sticker keyword: For LINE to be able to recommend an suitable sticker for the chat context, the LINE client will check the certain keywords in the messages. And if there's a match, it will be sent to the server anonymously.

Also, the messages will not be end-to-end encrypted when you use the cloud backup feature provided by a third party such as Apple and Google. In a such case the raw content will be stored on the cloud storage.

■ Deployment Status Summary by Features

Letter Sealing	Partial Letter Sealing	Transport layer encryption
		Media file messages
		Stickers
		Custom Sticker(non-plus)
		Open chat
		OA chat
		Group calls
Text and location messages		LINE meeting
1-to-1 calls	Custom Sticker Plus*5	LINE social plugin
Google Next-gen assistant		Message reaction
		Announce messages
		LINE Safety Check
		Imagemap message
		Template message
		Flex message
		Story message

*5 To generate a sticker with a custom wording of a user's choice, the user's client needs to talk to the rendering server. The text communication between the client and the rendering server is protected by E2EE. But the result image will be protected by transport layer encryption only.

■ 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 disable Letter Sealing, only transport-level encryption is applied.

■ Letter Sealing Versions

The original version of LINE messaging end-to-encryption protocol, released in 2015, 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

■ **E2EE v2 usage status**

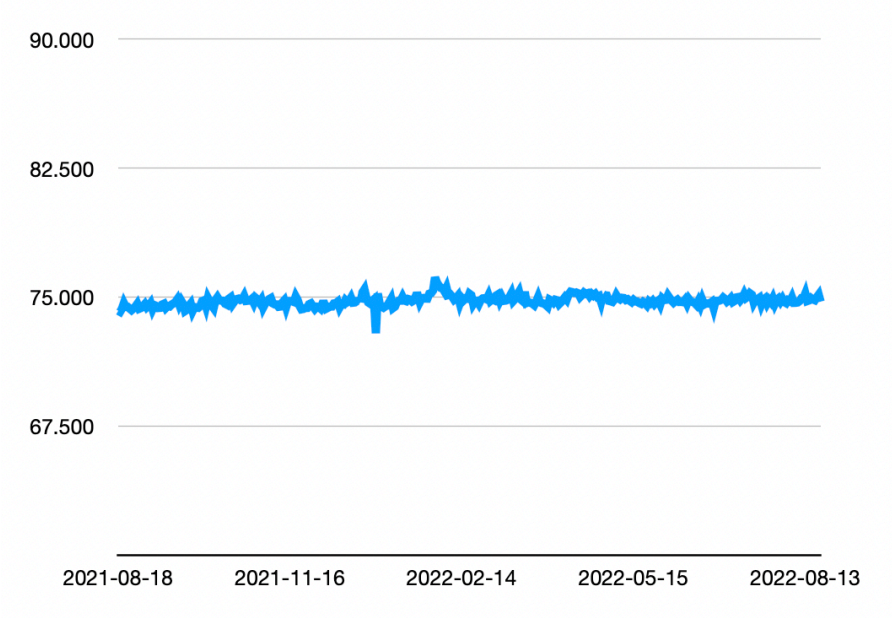

Figure 2: E2EE v2 ratio in the total E2EE traffic

E2EE v2 has been deployed since 2019. The graph above shows the ratio of E2EE v2 in the total E2EE traffic. For data before Aug 2021, please refer to the **last year's Encryption Report**.

■E2EE key migration

When you change your phone, you need to transfer the E2EE key in order to decrypt the previous messages.

In case you still have your old phone, you can transfer the E2EE key. For the details, please refer to **the official guide.**

For the safety, we provide an end-to-end encryption for the E2EE key. Each device generates an ephemeral ECDH key pair. And the old device's public key is sent via the QR code as an Out-Of-Band cryptographic data. Then the E2EE key is encrypted by AES256-GCM using the derived key.

■E2EE key backup

It is possible to do E2EE key backup to keep it safe. Then you can access the encrypted messages, even if you lost the phone. For the details enabling it, please refer to **the official guide**.

To keep the confidentiality, the E2EE key is encrypted using "client-side encryption"; the E2EE key is encrypted by the key generated from 6-digit PIN code. More over, the encrypted E2EE key is protected by our SGX server; the encrypted E2EE key is also end-to-end encrypted by our SGX server.

(4) Forward Secrecy Deployment Status

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

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

2021 Supporting cases reduced *6

2017/9 ○Supported for major clients *7

2016 △Partially supported *8

*6 TLS1.3 0-RTT(Zero Round Trip Time) has been enabled
*7 May not be supported depending on OS and LINE client version
*8 Supported for some regions and client versions

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

Not supported