LINE Encryption Report

2018.04.24

English

Apr 2018

Purpose

The purpose of this report is to disclose information on three topics: the types of encryption methods applied to LINE's individual features, the scope of data protection, and the current encryption application status.

How LINE is Encrypted

LINE uses various encryption methods to protect the privacy of its user information. Not only is the communication pathway that protects communication between client (LINE) and server encrypted (with LINE Event Delivery Gateway ("LEGY") and HTTPS), certain message types and call types that are supported are also encrypted using what is called "Letter Sealing." Letter Sealing is an end to end encryption protocol (commonly known as end-to-end encryption or E2EE) developed by LINE.

For more details regarding encryption methods and algorithms that LINE uses, please refer to our **encryption white paper**.

Encryption Implementation Status

(1)Messaging feature

Text and location data sent and received with LINE’s messaging feature is end-to-end encrypted with Letter Sealing under the following circumstances:

Both sender and receiver have Letter Sealing enabled in a 1-on-1 chat.

All users have Letter Sealing enabled in a 1-to-N chat with up to 50 users.

All users have Letter Sealing enabled in a Group chat with up to 50 users.

Other content that is exchanged, such as images, videos, files, and audio data, is encrypted with LEGY or HTTPS. The timeline below shows how encryption was applied from April 2016 to the end of March 2018.

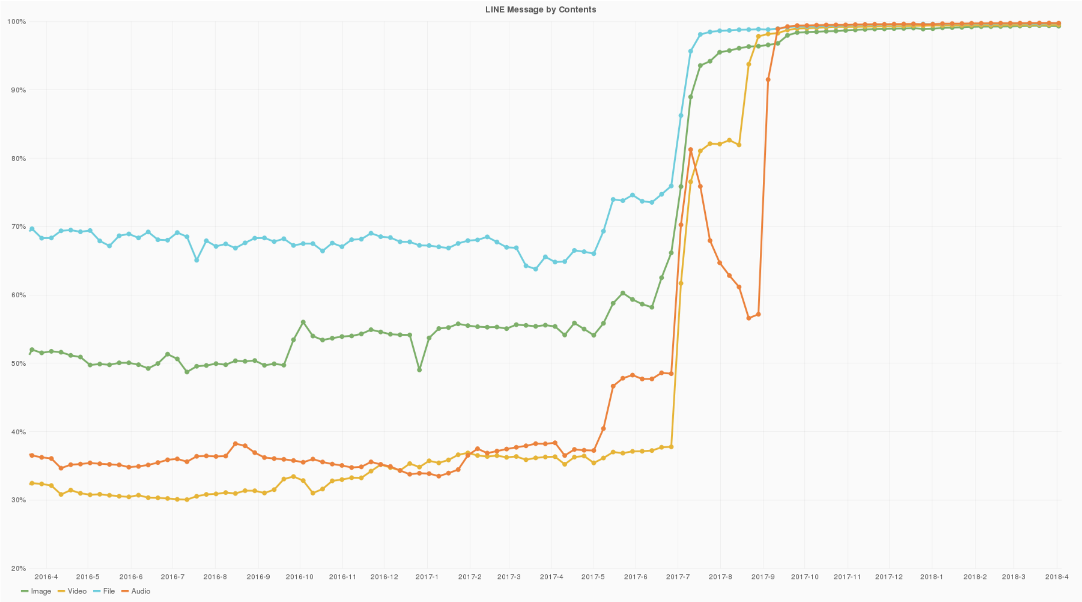

Figure 1: Time series transition of Encryption application status

Although encryption could not be fully applied to certain content in the past due to circumstances described below, the application rate has been maintained at roughly 100% since September 2017.

- Applying encryption caused performance issues.
- There was a time when some of the state's mobile networks could not access HTTPS. This has been resolved since, and all connections are currently being encrypted regardless of environment
- The encryption application scope was reduced for two months starting July 2017 in order to fix a bug that began to occur after applying encryption to more sound files. The scope was re-expanded in September 2017

Below is a summary of each content type's encryption status (Letter Sealing, LEGY, and HTTPS)

	2015	2016	2017 Sep.	2018 April
Text Message	○	○→◎	◎	◎
Location	○	○→◎	◎	◎
Sticker (*1)	△	△	○	○
Image File (*2)	△	△	○	○
Voice Message (*3)	x	X	○	○
Video File (*3)	x	X	○	○
Others (*2)	△	△	○	○

Notes: ◎ Encryption with Letter Sealing / ○ Any encryption applied in the network / △ Partially applied/ X Not implemented /

■Note

◎: Letter Sealing encryption was enabled by default for the main operating environments
○: Communication pathways were encrypted for the main operating environments at a level determined to be sufficient at the time
△: While data was only being partially protected, the encryption level was determined to be largely sufficient at the time as well as at the time of publication of this document
X: The protection level was determined to be insufficient at the time of publication of this document

*1 For the periods marked △, encryption was only being applied to the actual sticker transmissions in chats, and sticker packages were being downloaded via HTTP.

*2 For the periods marked △, HTTP and HTTPS were being used in combination. Depending on the operating environment (e.g. OS, region, network type), encryption was not being applied.

*3 For the periods marked X, only uploads via Wi-Fi were encrypted.

Sufficient protection is not guaranteed for old OS and LINE client versions, as encryption may not be applied as described above, or, communication may be taking place using an old encryption method.

(2)LINE calls (voice calls, video calls)

For LINE's call features, 1-on-1 voice calls and video calls are end-to-end encrypted with Letter Sealing under the circumstances listed below. For group voice calls and group video calls, encryption is applied to the communication pathway.

	2015	2016	2017 Sep.	2018 April
1-to-1 Voice Calls	○	○→◎	◎	◎
1-to-1 Video Calls	○	○→◎	◎	◎
Group Voice Calls	○	○	○	○
Group Video Calls	-	○	○	○

Notes: ◎ Encryption with Letter Sealing / ○ Any encryption applied in the network / - Not implemented

(3)Letter Sealing (end-to-end encryption) application status

Letter Sealing is an implementation of end to end encryption by LINE. When Letter Sealing is enabled, messages are encrypted on the client side before they are sent, and the content cannot be decrypted, even on LINE's servers. After Letter Sealing first became available in August 2015 as an optional feature, it was enabled by default in 2016 for the main operating environments. Presently, a limited number of message types are encrypted with Letter Sealing.

■Letter Sealing protection scope

Messages containing text (1-to-1 chats, group chats with up to 50 users)
Messages containing location information (1-to-1 chats, group chats with up to 50 users)
1-to-1 Voice Calls
1-to-1 Video Calls

※Currently, videos and sound clips transmitted as files are not being encrypted with Letter Sealing.

■Notes regarding Letter Sealing

To encrypt messages with Letter Sealing, the client of both sender and receiver (or all participants for group chats) must support Letter Sealing and have it enabled. If Letter Sealing is disabled, only the communication pathway is encrypted.

(4)Current support for Forward Secrecy

LINE supports forward secrecy in certain operating environments. In the event that a private key is leaked, messages that were encrypted before the leak are protected if the communication supports forward secrecy. Currently, only certain encrypted communication supports forward secrecy.

■Using forward secrecy to encrypt communication with the LINE server (if the LINE server's secret key is leaked)

September 2017: ○ Supported main operating environments (*4)

2016年: △ Partially supported (*5)

*4 Certain OS and LINE client versions were not supported
*5: Only certain regions and clients were supported

■Forward secrecy in Letter Sealing (if a user's device's secret key is leaked)

Not supported