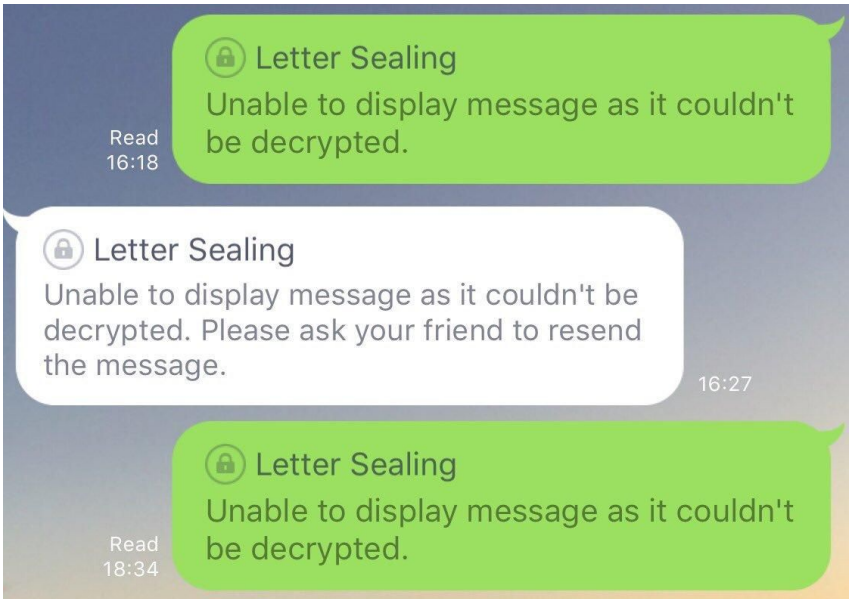
# Letter Sealing LINE Untuk Pengiriman Pesan




(Sumber: https://twitter.com/collinjackson)

## Apa itu *Letter Sealing* pada LINE?

Pesan pada gambar diatas mungkin pernah muncul pada beberapa pengguna aplikasi LINE. Biasanya, hal ini terjadi saat pengguna baru saja *log* in dari sebuah perangkat baru. Sebagian besar pengguna saat mengalami hal ini mungkin hanya mengikuti instruksi untuk meminta pengirim mengirimkan kembali pesan sebelumnya, tanpa mengetahui hal apa yang terjadi pada kondisi diatas. Sebenarnya, hal apa yang terjadi dibalik pesan tersebut?

Pada tahun 2016, LINE mengenalkan sebuah fitur yang menjamin keamanan komunikasi antar pengguna. Fitur ini dikenal dengan nama *Letter Sealing. Letter Sealing* berfungsi untuk menjamin keamanan dengan melindungi pesan para pengguna dari pihak tidak bertanggung jawab yang ingin mengakses pesan tersebut saat proses pengiriman pesan ke pengguna lain melalui server LINE. Secara garis besar, *Letter Sealing* ini menggunakan enkripsi *end-to-end* yang akan 'merubah' isi dari pesan yang dikirim oleh pengguna dan isi pesan tersebut hanya dapat disusun kembali dengan menggunakan *key* yang ada di masing-masing perangkat, bukan server. Sehingga jika pihak lain ingin mengambil isi dari pesan melalu server LINE, hal itu tidak dapat dilakukan karena server tidak memiliki *key* untuk menyusun ulang isi pesan yang sudah kacau tersebut.

## Apa itu Enkripsi *End-to-end*?

Enkripsi *end-to-end* adalah sebuah sistem komunikasi digital yang dirancang agar orang yang menerima pesan atau konten hanyalah pihak-pihak yang berhak menerimanya. Dalam kata lain, tidak ada penyadap yang dapat mengakses kunci kriptografi yang digunakan untuk mendekripsi percakapan, termasuk perusahaan yang memiliki jasa

pengiriman pesan itu sendiri. Sayangnya, hal ini dapat disalahgunakan oleh pihak tidak bertanggung jawab, seperti digunakan untuk aktivitas kriminal maupun hal-hal lainnya. Fitur ini membuat pelacakan susah dilakukan serta tidak ada bukti dikarenakan pihak pemberi jasa tidak dapat melihat isi pesan.

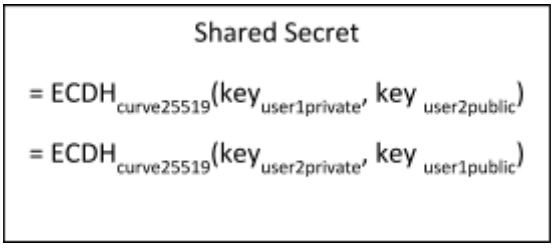
Pada perusahaan LINE, *Letter Sealing* adalah nama umum dari semua protokol terenkripsi end-to-end (E2EE) yang terintegrasi dalam LINE layanan pesan dan VoIP. Oleh karena itu, LINE memiliki dua jenis sistem *Letter Sealing,* yaitu untuk pengiriman pesan dan juga untuk VoIP. Tetapi, pada artikel ini hanya fokus pada *Letter Sealing* untuk pengiriman pesan.

## Bagaimana *Letter Sealing* untuk Pengiriman Pesan?

Pada *Letter Sealing* untuk pengiriman pesan, pesan pada LINE di enkripsi secara lokal oleh tiap perangkat milik klien sebelum dikirim ke server perpesanan LINE dan hanya bisa didekripsi oleh penerima yang dituju. *Letter Sealing* hanya berlaku pada *payloads* dari pesan yang dikirim, informasi lain seperti identitas pengirim, penerima, dan metadata lainnya tidak mengalami proses enkripsi.

Untuk dapat melakukan proses enkripsi, tiap aplikasi LINE klien menghasilkan pasangan kunci ECDH *Letter Sealing* dan menyimpan kunci tersebut di tempat penyimpanan rahasia pada aplikasi. Pasangan kunci tersebut dihasilkan saat pengguna pertama kali menggunakan aplikasi LINE atau saat pengguna menyalakan fitur *Letter Sealing* setelah mematikan fitur tersebut. Kunci yang baru dihasilkan juga saat aplikasi LINE di *install* ulang atau pengguna *log in* akun LINE dari suatu perangkat baru. Setelah pasangan kunci dihasilkan, tiap klien LINE mendaftarkan *public key*-nya ke server LINE. Server mengasosiasikan kunci tersebut kepada pengguna yang terautentifikasi dan mengembalikan kunci ID yang unik ke klien. Tiap kunci ID hanya dimiliki oleh satu pengguna dan merepresentasikan *public key* dari pengguna tersebut.

Untuk dapat saling mengirimkan pesan antar pengguna, kedua pengguna harus memiliki sebuh *cryptographic secret.* Saat seorang klien LINE ingin mengirim pesan, pengguna tersebut harus mengambil *public key* milik penerima. Algoritma pertukaran kunci yang digunakan adalah Algoritma ECDH *over* Curve25519. Setelah itu, klien memasukkan *private key* miliknya beserta *public key* milik penerima ke algoritma ECDH untuk menghasilkan *shared secret.* Sang penerima pun juga melakukan hal yang sama, yaitu memasukkan *private key* milik penerima dan *public key* milik pengirim ke algoritma ECDH. Prosesnya adalah seperti di bawah ini.




Tiap pesan di enkripsi LINE dengan sebuah *encryption key* yang unik dan IV. Kedua hal tersebut didapat dari *shared secret* yang sudah dijelaskan sebelumnya beserta 8-*byte salt* yang dihasilkan secara random, seperti berikut ini.

$$Key_{encrypt} = SHA256(Shared\ secret \,||\, salt \,||\, \text{“Key”})$$
$$IV_{pre} = SHA256(Shared\ secret \,||\, salt \,||\, \text{“IV”})$$
$$IV_{encrypt} = IV_{pre}[0:15] \oplus IV_{pre}[16:31]$$

$Key_{encrypt}$ dan $IV_{encrypt}$ yang dihasilkan digunakan untuk mengenkripsi *payload* pesan M menggunakan 256-bit AES dalam mode blok CBC.

$$C = AESCBC(Key_{encrypt}, IV_{encrypt}, M)$$

Setelah *ciphertext* C dihasilkan, LINE mengkalkulasi kode autentikasi pesan (MAC - *Message Authentication Code*) dari C seperti berikut ini.

$$MAC_{plain} = SHA256(C)$$
$$MAC_{enc} = AESECB(Key_{encrypt}, MAC_{plain}[0:15] \oplus MAC_{plain}[16:31]$$

Setelah seluruh proses diatas telah dilakukan, maka beberapa data yang disisipkan ke dalam pesan yang dikirim ke penerima adalah seperti dibawah ini.

| version | content type | salt | C | MAC | sender key ID | recipient key ID |
|---|---|---|---|---|---|---|

Dimana penjelasannya adalah sebagai berikut.

a. **Version** berguna untuk mengidentifikasi versi dari *Letter Sealing* yang digunakan untuk membentuk sebuah pesan
b. **Content type** juga berguna untuk mengidentifikasi versi dari *Letter Sealing* yang digunakan untuk membuat sebuah pesan
c. **Sender key ID** berguna untuk mengambil *public key* yang kemudian digunakan untuk mengenkripsi pesan
d. **Recipient key ID** berguna untuk melakukan verifikasi apakah pesan tersebut bisa dideskripsikan dengan menggunakan *local private key*

Setelah *recipient* mendeklarasi bahwa pesan tersebut dapat didekripsikan, langkah selanjutnya adalah memperoleh semua *shared secret, encryption key,* serta IV yang sudah dibahas di atas. Kemudian, LINE akan melakukan kalkulasi untuk menghitung nilai MAC dari *ciphertext* yang diterima, yang kemudian akan dibandingkan dengan nilai MAC yang telah disisipkan ke dalam pesan yang dikirim ke penerima. Jika keduanya cocok, isi pesan akan didekripsikan dan ditampilkan.

## *Letter Sealing* pada *Group Chat*

Lalu bagaimana penggunaan *Letter Sealing* untuk sebuah *group chat*? Untuk sebuah grup, LINE akan menghasilkan sebuah *shared group key* yang akan

diberikan ke semua anggota grup secara aman. *Group key* tersebut biasanya dihasilkan oleh anggota pertama yang ingin mengirimkan pesan ke dalam grup tersebut. Untuk menghubungkan sebuah *group key* dengan suatu grup tertentu, pertama-tama LINE akan menghasilkan sepasang *key* ECDH. Kemudian, LINE akan mengambil kembali semua *public key* dari semua anggota grup tersebut dan mengkalkulasi *encryption key*nya.

Penurunan *key* tersebut selanjutnya akan sama seperti *chat* individu yang telah dijelaskan di atas. Selanjutnya, *shared group key* akan mengenkripsi isi pesan secara individu dengan *encryption key* yang kemudian data yang sudah dienkripsi akan dikirim ke *server* yang akan menghubungkan antara *encrypted group keys* dengan grupnya dan mengembalikan sebuah ID *shared key*.

Ketika seorang anggota grup ingin mengirimkan pesan ke grup tersebut, pertama-tama anggota grup akan menerima *encrypted shared key group*, kemudian mendeskripsikannya, dan akan mengumpulkannya secara lokal. Untuk mengirim pesan, setiap anggota grup akan menurunkan *encryption key* dan IV dengan menggunakan *group shared key* yang sudah disebutkan di atas dan *public key* dari masing-masing anggota sebagai *input* nya. Prosesnya hampir menyerupai chat individu, namun perbedaannya dengan *chat* individu adalah *chat* individu akan menggunakan *recipient key ID*, namun *chat* secara grup akan menggunakan *key ID* dari *group's shared key* untuk melakukan verifikasi terhadap sebuah pesan.

## Keamanan LINE Sebelum *Letter Sealing*

Sebelum adanya fitur Letter Sealing, LINE memiliki beberapa fitur keamanan lainnya. Yang pertama adalah fitur berupa *hidden chat.* Fitur ini merupakan fitur pengiriman pesan dimana pesan yang dikirim hanya berlaku pada jangka waktu tertentu (*time limited feature)*. Sekarang, fitur itu sudah tidak berlaku lagi. Selain itu, LINE juga memiliki fitur penguncian menggunakan *passcode* yang berupa empat digit pin keamanan. Terakhir, LINE memiliki fitur *Bug Bounty*, yaitu fitur yang dapat menemukan celah pada keamanan sistem.

| Dibuat oleh | Tugas |
| --- | --- |
| Azka Nabilah Mumtaz - 13516013 | Apa itu *Letter Sealing*, *Letter Sealing* pada Pengiriman Pesan, *Letter Sealing* pada *Group Chat* |
| Nadija Herdwina Putri Soerojo - 13516130 | Enkripsi *end-to-end, Letter Sealing* pada Pengiriman Pesan, Keamanan LINE Sebelum *Letter Sealing* |

Sumber:


https://www.techno.id/apps/chatting-di-line-lebih-aman-dengan-fitur-letter-sealing-1510139.html

https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver1.0.pdf

https://tobidigital.com/dangers-disadvantage-end-to-end-encryption/