SEEYOU Security WhitePaper

(End-to-End Encryption)

(Public)

SEEYOU Security WhitePaper
(End-to-End Encryption)
(Public)
- Introduction
- Device Types
- Key Types
- User Registration
- Sender Session Setup
  - Steps to Establish a secure session between client and server
- Receiver Session Setup
- Exchanging Messages
- Transmitting Media Attachments
- Group Messages
- Desktop Session (Secondary device)
  - The process:
- Data Storage
- Backup and Restore
  - Backups
  - Restore Backups
  - Additional Notes
- Definitions

Introduction

This white paper provides a technical explanation of SEEYOU's end-to-end encryption system.

SEEYOU messenger allows users to communicate by messages, one to one chats, group chats up to 256 users in a group, images and videos, and where communication between sender and receiver are end-to-end encrypted.

See "Defining End-to-End Encryption" for information about which communications are end-to-end .

This End-to-End encryption protocol is designed to prevent third parties and SEEYOU from having plaintext access to messages. Due to the short life span (ephemeral) nature of the cryptographic keys, they cannot be used to decrypt previously transmitted messages. This is also valid in the situation where the current encryption keys from a user's device are physically compromised,

A user can have multiple devices, each with its own set of encryption keys. If the encryption keys of one device are , an attacker cannot use

them to decrypt the messages sent to other devices, even devices registered to the same user. The reason why is because each device has it's own set of unique keys.

Device Types

We have two types of devices, primary device and secondary device.

- Primary device is a device that used to create a SEEYOU account with an email address. Each SEEYOU account is associated with a single primary device. This primary device can be used to link additional secondary devices to the account. Our supported primary device platforms include Android and iOS.
- Secondary device is a device that linked to an existing SEEYOU account by the account's primary device. The SEEYOU desktop apps for Windows, macOS, Linux are classed as secondary devices all of which are connected to the single primary device.

Key Types

- **Identity Key Pair:** A long term **ECDH NIST curve P-256** key generated at the time of login on mobile devices (Android/iOS). This is considered the primary device.
- **Session Key/Token:** The session key/token will be generated when a client login to the application and verify its identity. This is a long term key, and will only change if clients get logged out or reinstall the application.
- **Message Key**: Shared calculated key between sender and receiver to exchange messages. This key will be calculated at the time of sending/receiving messages.

User Registration

At registration time, a SEEYOU client app transmits its public Identity Key, then the SEEYOU server stores these public keys associated with the user's identifier.

Sender Session Setup

In order for SEEYOU users to communicate with each other securely and privately, the sender client establishes a pairwise encrypted session with each of the recipient's devices. Additionally, the sender client establishes a pairwise encrypted session with all other devices associated with the sender account. Once these pairwise encrypted sessions have been established, clients do not need to rebuild

new sessions with these devices unless the session state is lost, which can be caused by an event such as an app reinstall or device change.

Before sharing information with another SEEYOU user, a SEEYOU client must first establish a secure session with the SEEYOU server. This session is between the client and the SEEYOU server, and it uses the session key and token.

SEEYOU uses “client-fanout” approach for transmitting messages to multiple devices, where the SEEYOU client transmits a single message N number of times to N number of different devices. Each message is individually encrypted using the established pairwise encryption session with each device.

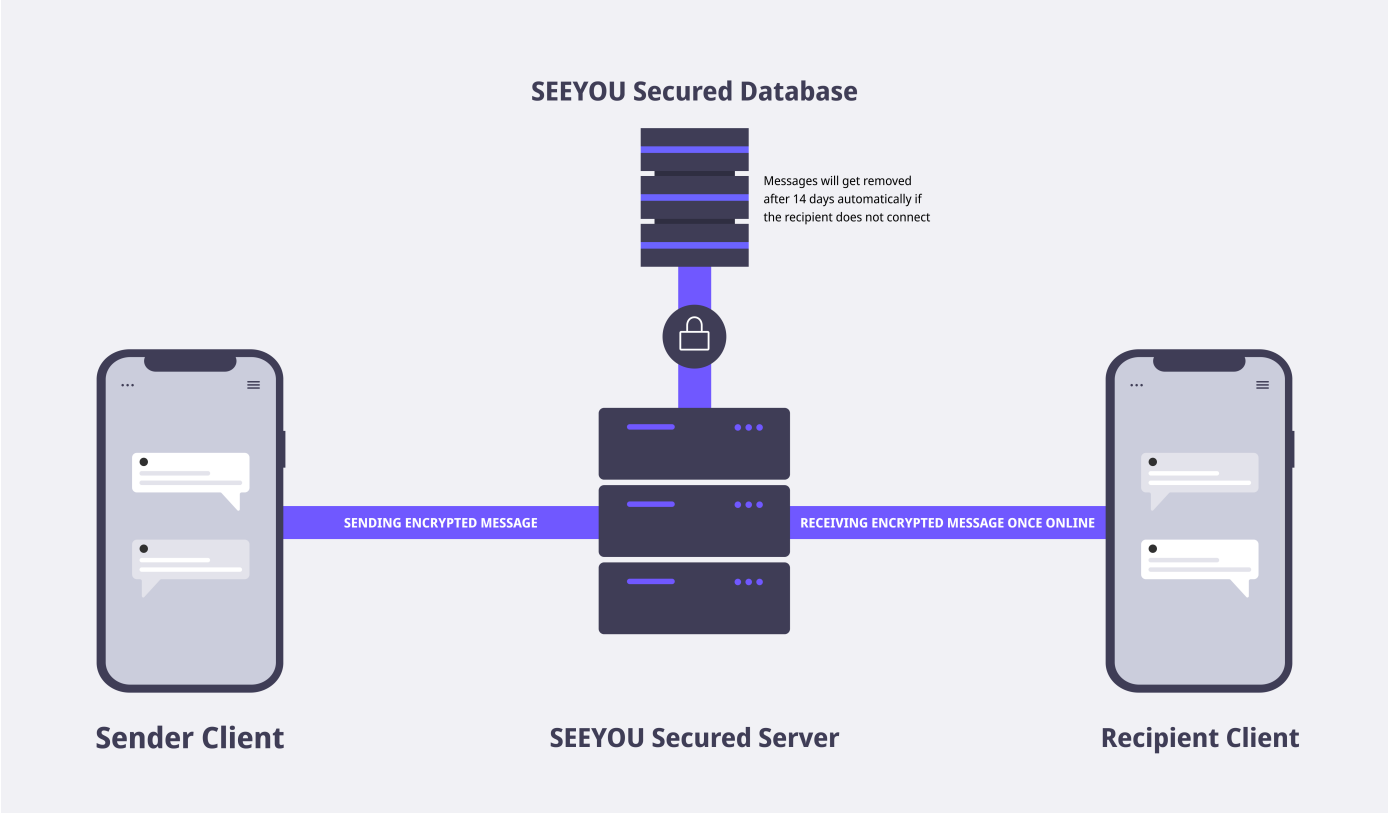
Steps to Establish a secure session between client and server

- The sender client requests the public **Identity Key Pair** of the recipient which is securely stored on the SEEYOU server.
- The SEEYOU server will send the public Identity key to the sender.
- The sender will store this key in the local storage.
- The sender will calculate the shared key on run time which will be used to encrypt the information.

Receiver Session Setup

After establishing a secure session, the sender can begin delivering messages to the receiver immediately, even if the recipient is offline.

- If the recipient is online, the message will be delivered to them instantly. • If the receiver is not available, the message will be stored on the SEEYOU server. Because this communication was encrypted by the client, no one (including SEEYOU) can see or read it.
- When the recipient reconnects to the SEEYOU server, all stored messages are sent to the recipient's device and simultaneously permanently deleted from the SEEYOU server.
- Encrypted messages that are not sent to the receiver within 30 days will get automatically removed from SEEYOU servers at the end of the 30th day.



Exchanging Messages

After establishing a secure connection between the client and the SEEYOU server, clients exchange encrypted messages using a Message Key (Shared Key) using **AES256** encryption in **GCM** mode, and an authentication tag is added for authentication. Only the sender and recipient can produce the Message Key, which is used to encrypt messages.

Calculating Message Key from an Identity Key

- The identification key is automatically calculated during the application's login process.
- The key is divided into two parts: the private key and the public key.
- The private information will be kept private on the client's device, while the public information will be shared with the contacts.

Let us assume there are two users, one named Alice and the other named Bob. When Alice wishes to send a message to Bob, she will get Bob's public key from the SEEYOU server, which is securely held on the SEEYOU server. Then **(Alice's private key + Bob's public key)** will form a shared key known as the **Message Key**. The message will be encrypted using this key.

When Bob receives a message, **his private key and Alice's public key** will produce the shared message key once more. Bob will decode the message and see its content using that key.

Transmitting Media Attachments

Attachments (video, and images) are as all communication in SEEYOU end- to-end encrypted.

- To encrypt the attachment, the sender generates automatically a safe random key.
- The sender encrypts the attachment in AES256 with a random IV and appends it to the file.
- The sender will safely upload it to the SEEYOU server.
- The sender sends a regular message to the receiver, including the encryption key and the URL of the attachment. This key and URL will be encrypted end-to-end, just like a normal text transmission.
- The message will be decoded and the encryption key will be discovered by the receiver.
- Following that, it will download the attachment from the SEEYOU server and decode it in order to view the attachment's content.
- The attachment will be stored on the SEEYOU server for **30 days** from the day it was uploaded.
- If the recipient does not download the attachment, it will be permanently deleted from the SEEYOU server.

Group Messages

We use the "client-side fan-out" in SEEYOU enabling the data to be updated across several devices. The sender encrypts the message for each group member and sends it to each member individually. The message will be encrypted end-to-end using the participants' key.

The same is true for group attachments. The sender will encrypt the attachment and send the encryption key to each participant separately using end-to-end encryption.

We use the "client-side fan-out" in SEEYOU. The sender encrypts the message for each group member and sends it to each member individually. The message will be encrypted end-to-end using the participants' key.

- The sender client requests the public **Identity Key** of the group recipient which is securely stored on the SEEYOU server.
- The SEEYOU server will send the public Identity key to the sender.
- The sender will store this key in the local storage.
- The sender will calculate the shared key on run time which will be used to encrypt the information.
- The message will then be encrypted and transmitted to the participant.

Desktop Session (Secondary device)

We offer the opportunity to use chat messaging on two devices at the same time. The first is a mobile device this can be on SEEYOU iOS app or SEEYOU Android app, and the second is a desktop application on any of the native desktop apps Windows, macOS, Linux.

- One mobile device at any given time (iOS mobile app or Android mobile app).
- One desktop device at any given time (Windows, Linux, macOS).

The process:

- When you request a session from the Desktop app, Desktop generates their own Identity key pair and your mobile device will get a notification in which you have to approve/reject the request.
- The desktop will send the Public Identity key to the mobile device.
- When you authorise the request, the mobile application will encrypt your local messages with a shared key calculated using the Desktop's public key and the Mobile's private key and send them to the Desktop. The desktop will then decode the data and begin processing the messages.

Data Storage

All messages (pictures, videos, and text) exchanged via the SEEYOU app will be securely stored on the SEEYOU server in the encryption format used by the customer mobile. If this information is not transferred to the receiver's device, SEEYOU will keep it for up to 30 days. The SEEYOU will totally destroy this information once it has been transferred to the receiver's device.

Once a message is delivered or received, the SEEYOU application saves it in your mobile phone as a permanent backup. Only you will be able to see your messages. If you uninstall the SEEYOU app from your device, these will be gone. You would be required to restore your backup.

We have enabled the possibility to backup your data to the cloud so that you do not lose your message. That information can be found in the section below.

Backup and Restore

The section below outlines how backups and restore works within our SEEYOU encryption.

Backups

- Fully encrypted chat messages database as a single file.
- Fully encrypted media folders, one folder images and one folder videos.
- The upload process sequence [chat messages database file, images folder, video folder], where allowing a sequence of the upload process.
- All uploaded files to the cloud are fully encrypted.

Restore Backups

- Restore from Google or iCloud if available.
- Download encrypted chat messages database file.
- Decrypt the encrypted chat messages.
- Download the two media folders (images & videos), this is done in the background.
- Decrypt the encrypted media folders in the background, while still allowing the

  chat to function.

Additional Notes

- We are encrypting the file with AES256 with a password generated by the user's Identity.
- We are allowing for multiple SEEYOU accounts to backup on a single cloud account. A unique naming convention has been used to also allow for that.
- Restore will only perform at the time of login. The application will prompt an alert to restore if a backup exists.

Definitions

AES256 encryption in GCM mode	**A**dvanced **E**ncryption **S**tandard **(AES)** algorithm in **Galois Counter Mode (GCM)** with 256 bit sized keys
Client-fanout	The approach for transmitting messages to multiple devices.
Client-side fan-out	For enabling the data to be updated across several devices.
Cryptographic Keys	A key in cryptography is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data.
ECDH NIST curve P-256	A long term **ECDH NIST curve P-256** key generated at the time of login on mobile devices
Encryption	The **process of encoding information**. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
Ephemeral	Something that lasts for a very short time.
Plaintext	In computing, **plain** text is a loose term for data (e.g. file contents) that represent only characters of readable material but not its graphical representation nor other objects (floating-point numbers, images, etc.).