Secure Communications using Linphone & Flexisip

Solution description

Versions

1.0 2015	Initial version 2015
2.0 2019	Add Trusted messaging

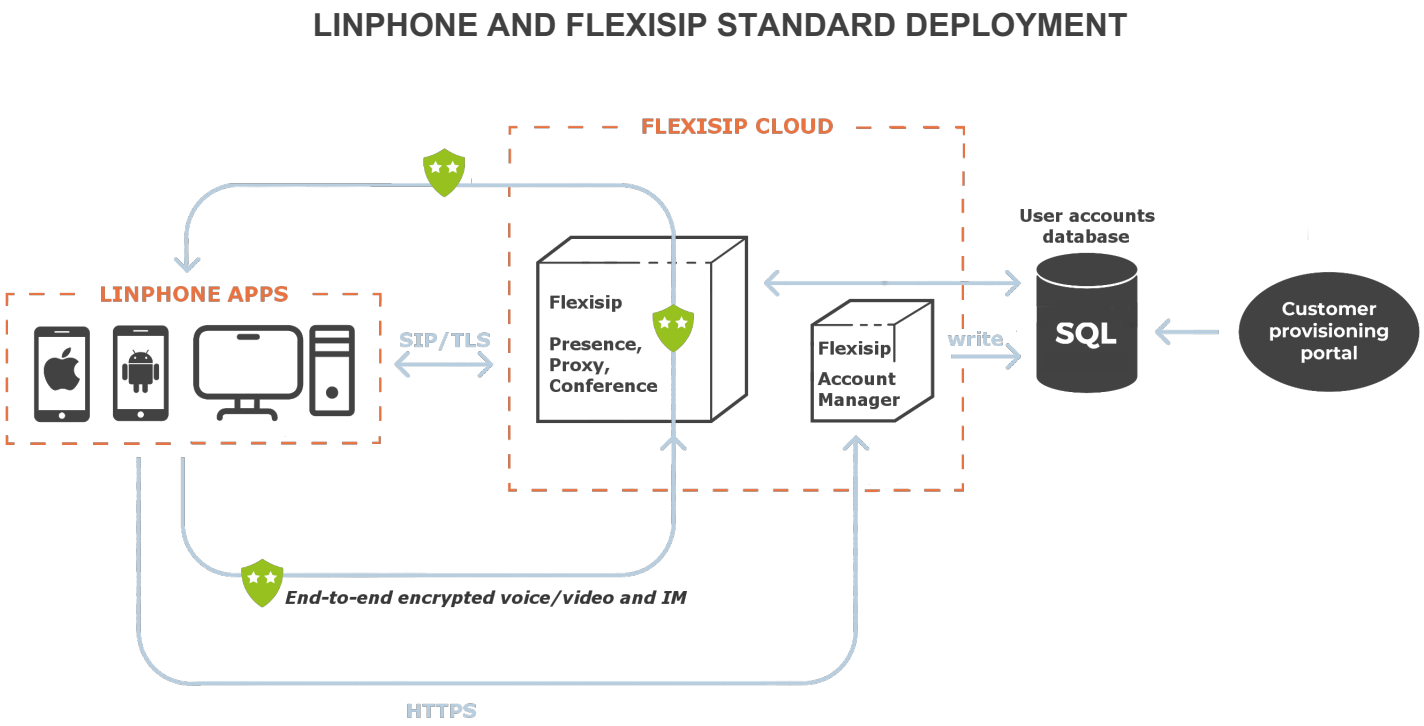
Index

Office: Le Trident Bat A - 34, avenue de l'Europe 38100 Grenoble - France Tel. : +33 (0)9 52 63 65 05	**Headquarters:** 12, allée des Genêts 38100 Grenoble - France Tel. : +33 (0)9 52 63 65 05	**Company legal information:** SARL au capital de 604000 € SIRET : 520 318 437 00016 EU VAT Number : FR89 520 318 437

info@belledonne-communications.com - https://www.linphone.org/

Introduction

Digital communications including voice, video and messaging are sensitive user data that need to be protected against unauthorised access. Both Linphone and Flexisip provide built-in security capabilities allowing to create a secure communications service across the public internet. This document describes key technologies taking place into a Linphone/Flexisip SIP network.



Office: Le Trident Bat A - 34, avenue de l'Europe 38100 Grenoble - France Tel. : +33 (0)9 52 63 65 05	**Headquarters:** 12, allée des Genêts 38100 Grenoble - France Tel. : +33 (0)9 52 63 65 05	**Company legal information:** SARL au capital de 604000 € SIRET : 520 318 437 00016 EU VAT Number : FR89 520 318 437

info@belledonne-communications.com - https://www.linphone.org/

Trusted registration and call setup

The first level of security is to make sure both end-user registration and call setup are performed in a secure way. These operations involve both Linphone and Flexisip SIP proxy. The Linphone client establishes and maintains a SIP-TLS connection to the Flexisip server. The Linphone client verifies the SIP server's authenticity based on x509 server certificates checked against a list of trusted root authorities provided at compilation time. This first step guarantees the integrity and the confidentiality of all the information exchanged between the Linphone client and the Flexisip server.

The second step is to perform the authentication of the SIP messages coming from clients. The Flexisip server is responsible for this task, using either digest authentication from a password database, or better by using TLS client-based authentication: in the latter case, the client certificate presented by the Linphone client must be valid and must match the identity (From header) claimed in the SIP messages.
The choice between the two methods (sha256 digest or TLS client certificate authentication) is a matter of configuration in Flexisip and the Linphone clients.

Trusted voice and video streams

Voice and video over RTP are encrypted using AES with either a 128- or 256-bit key length. The way RTP packets are encrypted is described in RFC 3711. For ciphering key exchange, Linphone implements three different IETF standards.

SDES (Session Description Protocol Security Descriptions)

This is the original way to exchange ciphering keys. Basically, idea is to exchange encryption keys during call setup. RFC 4568 describes a new SDP attribute used to encode an AES key in base64. As SDP messages are secured by SIP over TLS, key exchanges can be considered as secured as long as SIP network integrity is guaranteed.

The main concern about SDES is that security entirely relies on the SIP network. A SIP network is generally composed of one or several SIP servers. As SIP/TLS is a point-to-point encryption solution, each SIP server has access to media ciphering keys in clear text. Trusting SDES requires that all the SIP servers involved in the routing of the call or message are trusted.

ZRTP (Media Path Key Agreement for Unicast Secure RTP)

To reduce security pressure on SIP proxies, ZRTP (RFC 6189) proposes an end-to-end encrypted key exchange based on Diffie-Hellman. ZRTP protocol messages use the same media path as regular RTP packets. The main concern with Diffie-Hellman key exchange is that it can be subject to man-in-the-middle (MITM) attacks. To prevent this, ZRTP proposes a mechanism based on a Short Authentication String (SAS). This SAS has to be checked by each participant using voice during the first call, and this guarantees that there is no man-in-the-middle attack.

Unlike SDES, having a compromised SIP proxy would have no effect on the integrity or the confidentiality of the audio & video streams exchanged between two clients.
Linphone brings its own implementation of ZRTP in the bZRTP library. bZRTP supports four types of key agreements.

- Regular 2048 and 3072 bit key length Diffie-Hellman for applications requiring time-proven algorithms.
- Curve25519 and Curve448 (RFC 7748) for state-of-the-art key agreement based on elliptic curve cryptography.

Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)

Like ZRTP, SRTP-DTLS (RFC 5764) provides end-to-end encryption, but it is based on public/private key to encrypt key exchanges. X509 certificates are used for authentication. The main advantage of this protocol is interoperability with WebRTC.
The Linphone implementation of SRTP-DTLS is based on the mbedTLS library, enhanced with a specific patch created and maintained by Belledonne Communications.

Trusted messaging and file sharing (mobile only)

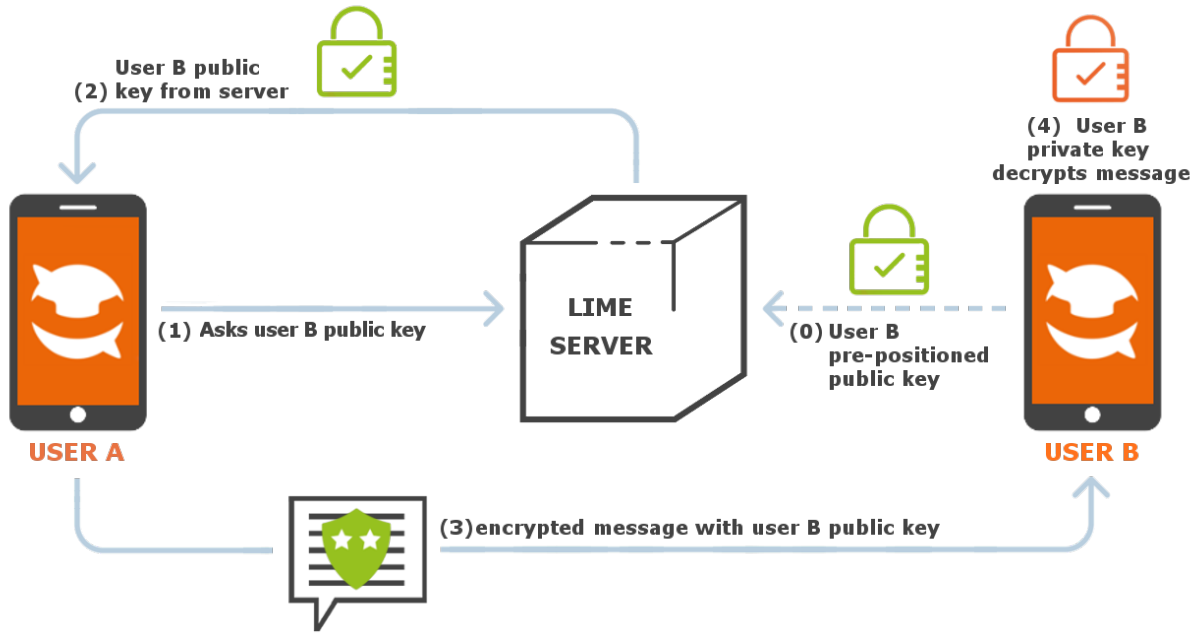
IM features are powered by a clever integration of the SIP signaling techniques used in Linphone/Flexisip together with our own end-to-end encryption protocol, called LIME (Linphone Instant Message Encryption). Inspired by the Signal Protocol, LIME allows users to privately and asynchronously exchange messages. LIME's unique features are to support multiple devices per user and the use of the advanced cryptographic curve x448.

The main features are:

- End-to-end encryption based on modern elliptic curve cryptography
- Perfect forward secrecy with double ratchet algorithm
- Designed for group communications
- Asynchronous messaging system based on pre-positioned keys
- Man-in-the-middle detection based on ZRTP auxiliary secret
- Signaling protocol agnostic

LIME is composed of a portable client library coupled with a public key server developed by Belledonne Communications to allow end-to-end encryption for messaging, without having to exchange cryptographic keys simultaneously.

END-TO-END IM ENCRYPTION WITH LIME



LIME library is a portable, signaling-independent component designed for sharing end-to-end ciphered text and documents. LIME is not linked to any signaling protocol and can be used with SIP alternatives like XMPP or any proprietary protocol with unique device identifier support.

It exposes a C, C++, Python and Java API for easy integration in mobile and desktop environments. Message overhead is limited thanks to the efficiency of X25519 or X448 elliptic curve Diffie-Hellman. LIME allows key agreements to be done asynchronously using pre-positioned public keys published to the LIME server over a secured https link. The detailed LIME specification can be found at http://www.linphone.org/technical-corner/lime.

Extendable with custom encryption engine

Although Linphone does provide safe built-in security features, in some circumstances it might be required to use a custom encryption library for cyphering audio, video, text messages and shared content.
In order to easily integrate such encryption extension without having to modify library source code, Liblinphone exposes APIs to enable customized code to process at all important stages.

Voice and video streams

Encoded voice and video are exchanged through the network using the Real-time Transport Protocol (RFC 3550), which is implemented by the oRTP library integrated into Linphone. This library provides a C API to hook custom processing on both incoming and outgoing packets, called RtpModifier. Implementing this rtp modifier makes it possible to handle both key exchanges and content ciphering at a very low level.

More information is available at https://www.linphone.org/technical-corner/ortp.

Messaging and file sharing

Messaging and file sharing are usually encrypted using dedicated algorithms. To allow the customisation of message ciphering, including asynchronous operation to query a server for public keys, Liblinphone provides an abstract encryption engine API with the following features:

- Process incoming message: called when a message is received by Linphone;
- Process outgoing message: called when a message is about to be sent by Linphone;
- Process file uploading: called (one time or more) when Linphone is uploading a file to the file sharing server;
- Process file downloading: called (one time or more) when Linphone is downloading a file from the file sharing server.

More information is available on our wiki article.

Cryptographic API

All cryptographic functions used by Linphone or any of its components are centralized into a single low-level API featuring AES encoding/decoding, x509 certificate management, SHA signature and random generators. Its default implementation is made on top of mbedTLS long term release. Thanks to this API layer, the implementation of a custom cryptographic function based on a secure element or an alternative software solution is greatly facilitated.

Conclusion

Making a secure VoIP and messaging architecture requires several technologies to be implemented at both client and server sides. Because they have been developed jointly, Linphone and Flexisip are the perfect couple to address a high level of security. Flexisip and Linphone have been designed with simplicity of use in mind, so that system administrators and developers can have a clear understanding of the security options they have. Beyond the reference architecture exposed in this document, Belledonne Communications' mission is also to adapt it to the customer's specific needs.

Contact

Worldwide sales
sales@belledonne-communications.com

Office
Belledonne Communications
Le Trident Bat A - 34 avenue de l'Europe
38100 Grenoble - FRANCE
Tel +33 (0)9 52 63 65 05
Fax +33 (0)9 57 63 65 05
info@belledonne-communications.com

https://www.linphone.org/