POST QUANTUM ENCRYPTION

Current developments in quantum computing pose a threat to the cryptographic algorithms used in VoIP and IM applications. The NIST launched an international competition in 2017 to standardise so-called ‘post-quantum’ cryptographic algorithms. The algorithm selected for general-purpose encryption is CRYSTALS-Kyber.

The Linphone application is probably the first open-source audio/video communication software in the world to have used this algorithm; a modified version of the ZRTP encryption protocol was developed.

We have taken on the following challenges:
- ensuring that the algorithm reaches the same level of effectiveness even if the cryptographic keys are much larger;
- ensuring that the algorithm remains resilient to classic attacks;
- ensuring that the algorithm is interoperable with the encryption features offered by previous versions.

END-TO-END ENCRYPTION OF CALLS AND CHAT

- Support for SRTP, SRTP-DTLS, and ZRTP standard encryption protocols
- Modern encryption based on elliptic-curve Diffie–Hellman (ECDH)
- Asynchronous messaging encryption based on prepositioned keys and the double ratchet algorithm
- Man-in-the-middle attack detection based on additional ZRTP privacy (SAS code)
- Compatible with WebRTC

SECURE USER AUTHENTICATION AND CALL SETUP

- Verification of SIP server authenticity based on x509 certificates
- Verification of the user’s identity, using hash algorithm authentication (SHA 256) or a TLS certificate
- Secure connection between the client (user) and the server using SIP/TLS

ENCRYPTED CALLS, CHATS AND MEETINGS, AS SECURE TODAY AS THEY WILL BE TOMORROW!
To implement your secure communication service, you can rely on our long-standing expertise in end-to-end encryption for IM and VOIP.

**BUILD YOUR VOIP AND IM APPLICATION**

By leveraging the source code of the Linphone apps, you can:
- **DEPLOY YOUR SIP NETWORK**
  - **Flexisip** is a complete, modular and scalable SIP server suite written in C++11; it comprises secure proxy, push notifications, account manager, group chat functions, and meeting solution.
  - **Flexisip services** can be run on different machines or combined on one machine as a single instance or in cluster mode.

By integrating our library, Liblinphone; this is the easiest way to add advanced VoIP and instant messaging (IM) features into software applications or hardware products.
- APIs in Swift/Kotlin/C#/C++
- Easy integration into mobile apps with Maven and Cocoapod
- Tutorials and code examples on Gitlab

**CUSTOMISE LINPHONE FOR YOUR OWN BRAND**

- Internally, using your own development team
- By outsourcing the graphics customisation to us

**SERVER SIDE**

Flexisip is interoperable with most SIP-based PBXs and SBCs and offers all the features needed to deploy your own secure communication service; it has been adapted for mobile applications and is ready to use. We can help you deploy this solution in your infrastructure.

**SUPPORT AND SERVICES**

- Annual Support
- Customisation and features on demand
- Development Assistance

**CONTACT US**

sales@belledonne-communications.com
https://www.linphone.org
+33 (0)9 52 63 65 05

**THEY CHOSE US, DID YOU?**

[Images of logos from Orange, Bouygues, and Thales]

+ 300 others