LiveBox

2015

Crypt Theory

CHAT

LiveBox

LiveBox is a private cloud software that allows you to store, share and edit data stored in a corporate datacenter offering an high security level. It is a multiplatform system accessibile from every mobile and remote device that guarantees business continuity and protects corporate files at all times.

For further details regarding LiveBox platform functionality and the use of its applications we ask you to refer to our web site: http://www.liveboxcloud.com and to the technical documentation contained in it.

LiveBox Support Team

LiveBox

Index

LiveBox

CORNER STONE

1. All users have a pair of keys: one public and one private.
2. The public key is used to sign sent messages.
3. The private key is used to decrypt received messages.
4. The Chat Server cannot decrypt messages.
5. The Administrators cannot decrypt messages.
6. The Users exchange personal private key using Diffie-Hellman protocol.

PRAGMA

1. The Files are encrypted by the ENDPOINT (client side).
2. All the private keys are stored in the ENDPOINT (client side).
3. The Private keys are 2048bit long.
4. Each encrypted chat session has a new pair of keys.
5. Users can decide when and how to encrypt the chat session.

HOW IT WORKS

1. Starting an Encrypted Chat Session

a. The application generates a personal keypair.
b. The initiating User clicks on “encrypt chat”.
c. The Application begins the key exchange process.

2. Send Message

a. The User composes a message.
b. The message is signed with the receiver’s public key.
c. The message is sent encrypted.

3. Receive Message

a. The User receives an encrypted message
b. The application decrypts the message with the user's private key
c. The User reads the message

4. Ending an Encrypted Chat Session

a. The terminating user clicks on "End Encrypted Chat"
b. The application sends a warning encrypted message to receiver
c. The receiver clicks on "End Encrypted Chat" to continue chatting.