LiveBox

2015

# Crypt Theory

FILES NOW

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

## CORNER STONE

1. Each users has a pair of keys: a public key and a private key.
2. A unique symmetric key (AES256bit) is generate for each of the user's files.
3. The user's public key is used to sign symmetric key.
4. The user's private key is used to decrypt the symmetric key and to share files with other users.
5. All files are encrypted by default.
6. The Server cannot decrypt files on its storage.
7. Administrators cannot decrypt the user files.

## PRAGMA

1. Files are encrypted by the ENDPOINT (Client side) except for browsers.
2. Private keys are stored encrypted (RSA 2048 BIT).
3. All files are encrypted with a symmetric Key (256 BIT).
4. All the keys are stored encrypted on the server and in the client devices.
5. All user passwords and pin numbers are exchanged with PGP.

## HOW IT WORKS

### 1. User First Login

a. The User generates a personal PIN.
b. The server generates a key pair for every User and encrypts the private key with user supplied PIN.
c. The User downloads his private and public keys and encrypt the private one with the PIN.
d. The User can download his personal Private Key (not encrypted) for recovery purpose.
e. The User completes the login process.
f. The Server saves the PIN's hash to use for comparison in subsequent authentication operations.

### 2. File Upload

a. The User creates a file.
b. The Client generates a random symmetric key to encrypt the files.
c. The Client signs the symmetric key with User Public Key.

### 3. File Download

a. The User requests a download on the server
b. The Client decrypts the private key with the PIN.
c. The Client uses the key to decrypt the Private User Key and decrypt the symmetric key previously used to encrypt the file.
d. These operations are repeated for each download session.

### 4. Share File or Folder

a. The User asks the server to share a file.
b. The Server requests the user's PIN (through PGP).
c. The Server uses the user's PIN to decrypt the User's Private Key.
d. The Server decrypts the file with the obtained symmetric key.
e. The Server signs the file's symmetric key with the Public keys of the users that the file (or folder) is shared with.

## CONCLUSIONS

1. All files are encrypted by default.
2. The server has no knowledge of the users Private Keys.
3. If a user loses his PIN and also loses the backup (Downloaded upon first registration) he will. lose all his files, but can still recover access to LiveBox.