LiveBox

2015

Crypt Theory

FILES FROM SEPTEMBER 2015

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 Server generates a unique symmetric key (AES 256 BIT) for each file.
3. The user's public key is used to sign the symmetric keys.
4. The user's private key is used to decrypt the symmetric key and to share files with other users.
5. The User can decide when and how to encrypt (files are not encrypted by default).
6. The Server cannot decrypt the files on its storage.
7. The Administrators cannot decrypt files on the storage.

PRAGMA

1. The Files are encrypted by the BACKEND (Server side).
2. All the private keys are stored in the BACKEND.
3. The Private keys are stored encrypted (RSA 2048 BIT).
4. All files are encrypted with a symmetric Key (AES 256 BIT).
5. All the keys are stored encrypted on the server.
6. The user's password and pin 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 each User and encrypts the private key with the given PIN.
c. The User can download his personal Private Key for recovery purposes.
d. The User completes the login process.
e. The Server saves the PIN's hash to compare against during subsequent login operations.

2. File Upload

a. The User uploads a file.
b. The Server generates a random symmetric key to encrypt the files.
c. The Server encrypts the symmetric key with the User's Public Key.

3. File Download

a. The User requests a download on the server.
b. The Server requests the User's PIN (through PGP) in session.
c. The Server encrypts the PIN with a random symmetric key.
d. The Server flushes his copy of the PIN.
e. The Server sends to the user the random symmetric key (This key is stored in session and will be flushed at the end of the session).
f. The Server uses the key to decrypt the user's Private Key and decrypts the symmetric key previously used to encrypt the file.
g. 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 users'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 used symmetric key with the Public key of users that the file (or folder) is shared with.

CONCLUSIONS

1. All files are encrypted by user requests.
2. The server has no knowledge of the user's Private Keys.
3. If a user loses his PIN and also loses the backup (Downloaded upon first registration) he can recover access to LiveBox but will lose all encrypted files.
4. All files syncronized on pc are encrypted and not available if the LiveBox client is not running on pc.