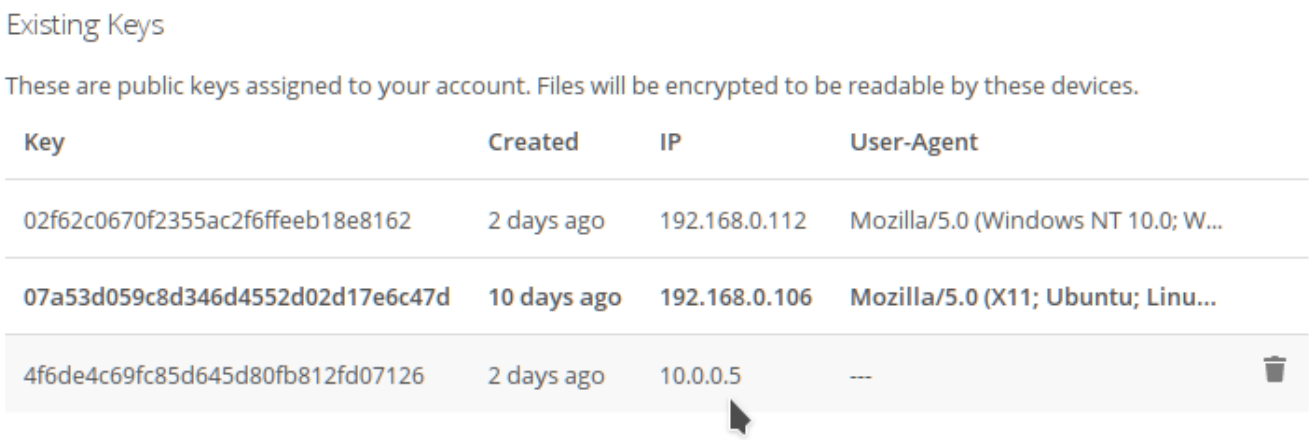
E2EE - Security Tips

General Considerations

As a user it is important that you keep your private key save. It is strongly recommended to make a backup to be able to restore files, e.g. in case you reinstalled the browser.

Note that the key is saved in your browser profile, so make sure your home folder is encrypted and no one has access to it.

Check your keys



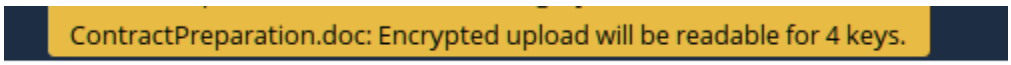
You should regularly check the keys on your system.

> If you notice a new key or don't recognize one, notify the system administrator to check the logs. This might be an incursion attempt.

You should also avoid having too many different keys, in case one is compromised.

Uploading

When uploading, always check for how many users the file is shared, and take note of the message telling you for how many keys the file will be encrypted:



If you only share the file with one person, then it should usually be encrypted for 2 keys (your own and the target user's).

If there are shown more it might be:

- That you or your target have activated more than one device for e2ee with different keys (in that case the number should be equal to your keys + number of the target keys). Make sure to verify with the recipient how many different keys he has.
- You shared the folder with more people

> If the number of keys does NOT match up, make sure to notify the administrator immediately as this might possibly be an incursion attempt.

Private Key Access

The E2EE app allows various way how to handle the private key. The public key is public and stored on the cloud server - if you send files only the public key is required. The private key comes into play only when you want to open an encrypted file. **The private key is never sent to the server.**

It is important to keep the private key safe and prevent external access to it.

When creating a private key, make sure to save it on an external drive (i.e. an USB stick) which is kept at a save place, in case you lose your private key (by deleting it accidentally or through a re-installation).

Depending on the security requirements or the usability make sure to select the correct key access method (*Key Storage*, see E2EE - User Manual).

If you have specific requirements (i.e. HSM support) please contact the epiKshare team.