E2EE - User Manual

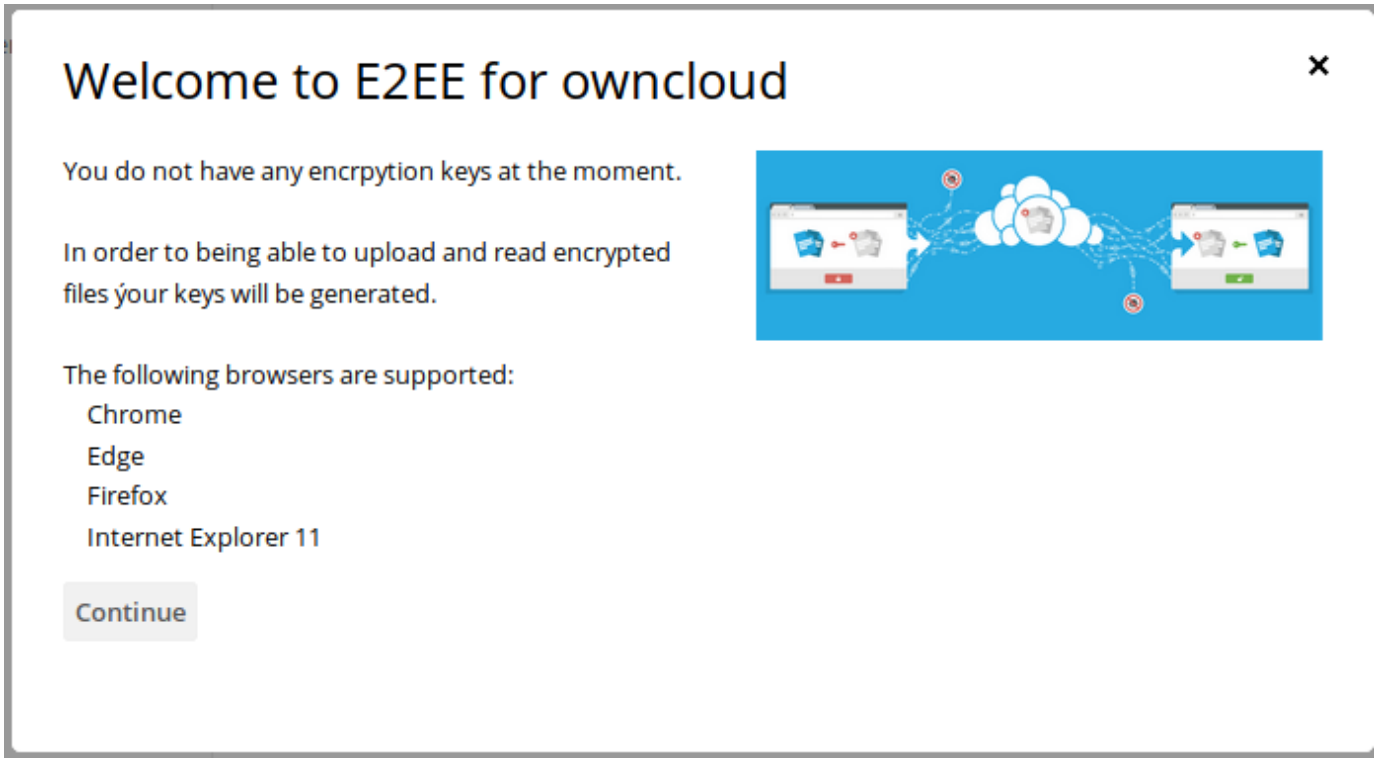
At first login a wizard will open which guides through the creation of a key pair for encrypting and decrypting files. This pair comes with a private (secret) key and a public (not secret) key.

- The **public key** will be used to encrypt files
- The **private key** will be used to decrypt files

While the public key will be saved in the server's database ("anybody may encrypt files for me"), the private key must be kept secret ("only I may decrypt files").

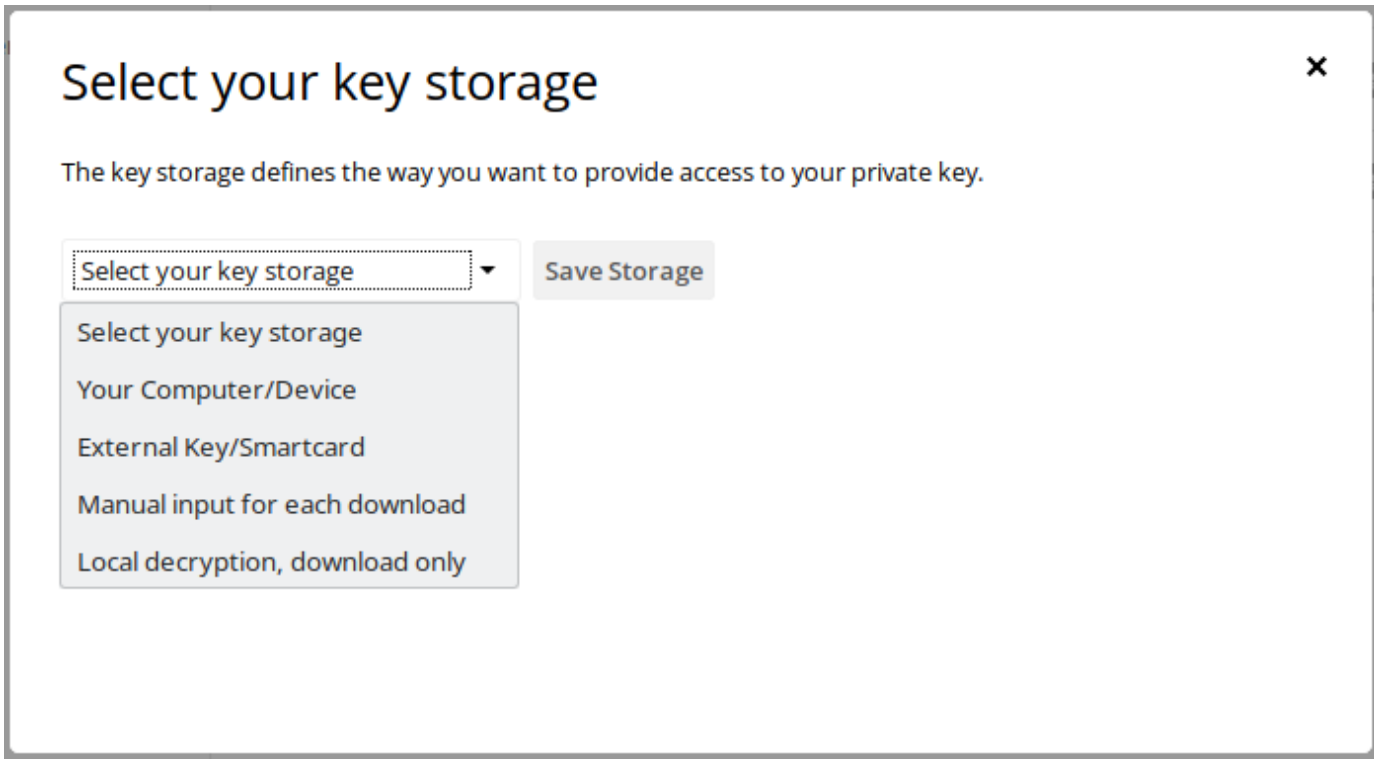
Depending on the server administrator's configuration you will see the default wizard or the Simple Share wizard.

User Setup (default wizard)



After the welcome screen you choose the key storage, where your keys will be saved.

The select box provides all available key storages, as they were set up by the administrator.



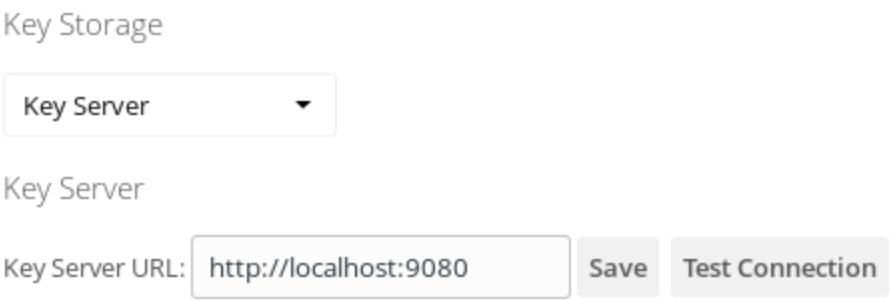
Depending on the system settings you can choose if and where the private key is saved and how you want the decryption to be performed. This depends on your security requirements and possibilities:

	Description	Usability	Security
Your Computer/Device	The private key is stored in the browser local storage (similar to a cookie)	★★★	👍
External Key/Smartcard	The private key is available through an external process running on the client machine. Then the browser can only request decryption. You have to install an extra Key Server on your machine, which is able to both recognize provided key files or Smart Cards (currently Windows only). The key is never saved in the browser. The Key Server supports reading the key from a storage location (.pem file) or from a pkcs#11 compatible hardware device.	★★	👍👍👍
Manual input for each download	When downloading an E2EE file, the private key has to be copy/pasted into a browser form. The key is never saved in the browser.	★	👍👍
Local decryption	The E2EE file is downloaded locally and a secondary tool is required to decrypt (E2EE Reader). The E2EE Reader supports both file and Smart Card decryption (currently Windows only). The key is never saved in the browser.	★/★★	👍👍👍

Key Storages

External Key/Smartcard Configuration

For the *External Key/Smartcard* key storage, a key server URL has to be provided. In most cases this will be the default value `http://localhost:9080`.



By clicking the *Test Connection* button you will receive a message whether the key server was found or not. You will be asked to register your Smartcard when it had been found.

An additional button *Connection Info* will show up which either opens the key server's status information or a browser error page, in case the key server did not respond.

All other storages

Except of the variant External Key/Smartcard, where the key is retrieved from the hardware, in any other keys a new key pair will be generated.

The public key will be uploaded to the server's database, the private key is show in the next step.

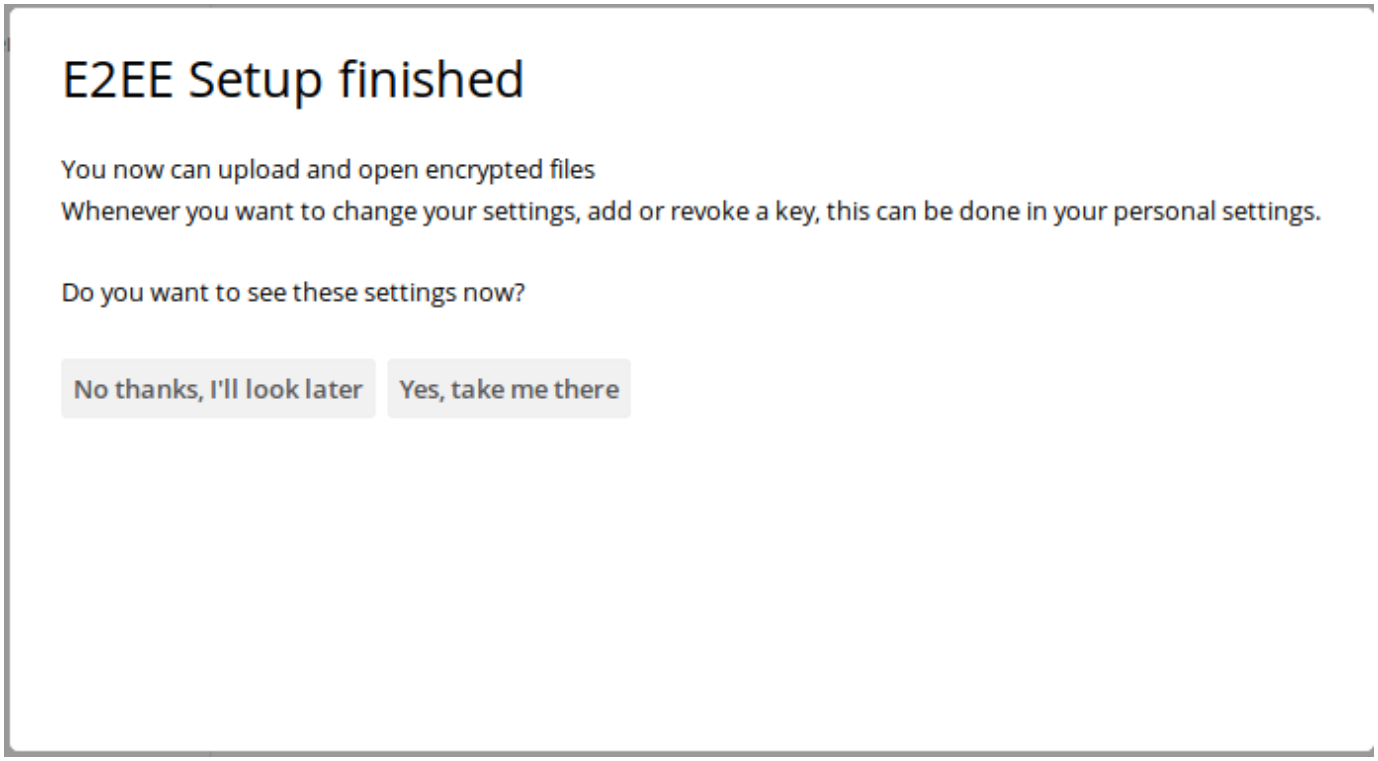
From now on you are able to create or read end-to-end encrypted files.

> **Be sure to save the private key** and store it at a secure location (e.g. in a safe). Make a backup of this key. Without the private key you cannot open any files, e.g. when the web browser was reinstalled.
>
> **The private key is never sent to the server.** The private key cannot be restored.
>
> In case this key is lost, you have to create a new one. However, you only can access files encrypted for your old key when
>
> - You re-upload the files
> - Another user who shared an encrypted folder with you re-encrypts it for your new key.

> For key storage **Your Computer/Device** you can **only use one browser or browser profile for one account**. Since the private key is

stored in the browser (or the profile) a different ownCloud user would receive the message *Your key was not found on the server*, because the stored private key does not match the other user's public key.

After you are done with the wizard, the key management is always available in your **Personal Settings - section Security**

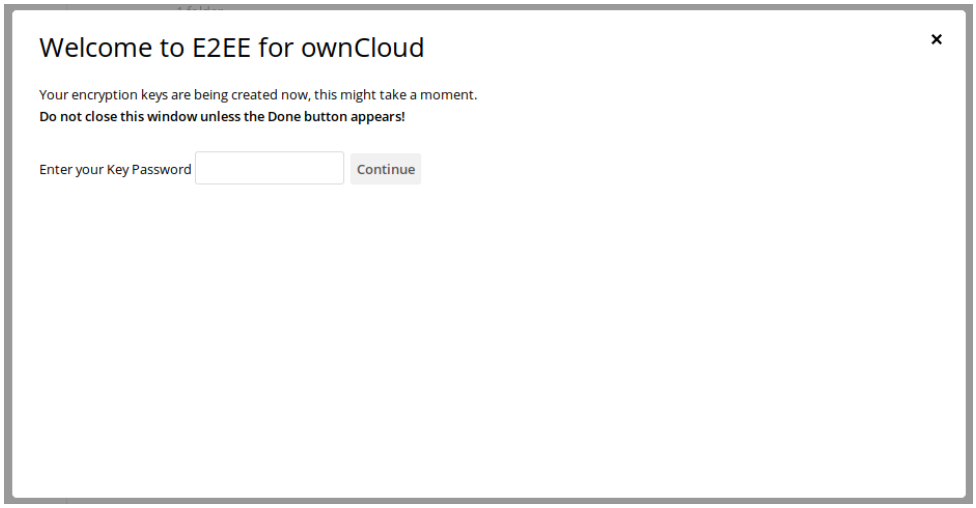


Click **Yes, take me there** to find the section Security in your Personal Settings.

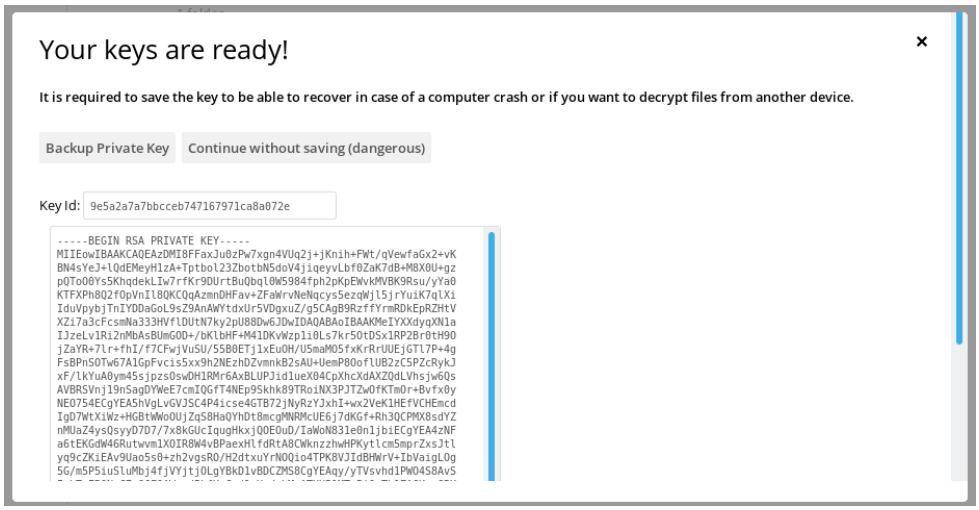
User can have multiple private keys assigned to their accounts i.e. for multiple devices. Files uploaded into one of their encrypted folders will automatically be encrypted for ALL of their private keys.

User Setup (Simple Share)

When the server administrator had set up Simple Share, then a password protected private key was already generated, so you can open your shares shortly after login. You have received your key password by email. When the wizard below appears, please enter or paste the provided password:



A new key pair will be generated where the private key is only stored in your device's browser and never sent to or retreived from the internet. The setup process is finished when you reach the following page:



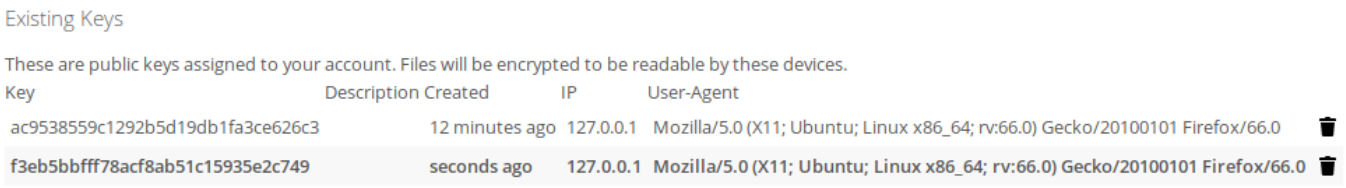
> **Be sure to save the private key** and store it at a secure location (e.g. in a safe). Make a backup of this key. Without the private key you cannot open any files, e.g. when the web browser was reinstalled.
>
> **The private key is never sent to the server.** The private key cannot be restored.
>
> In case this key is lost, you have to create a new one. However, you only can access files encrypted for your old key when
>
> - You re-upload the files
> - Another user who shared an encrypted folder with you re-encrypts it for your new key.

From then on you can manage your keys in your *Personal Settings*, details are found in the section below.

Key Management

The key management is found in your Personal Settings. You may reach this space by clicking on your user name in the upper right corner of your ownCloud. This opens a dropdown menu, choose **Settings**. The settings for end-to-end encryption are found in the section **Security**.

Manage Existing Keys



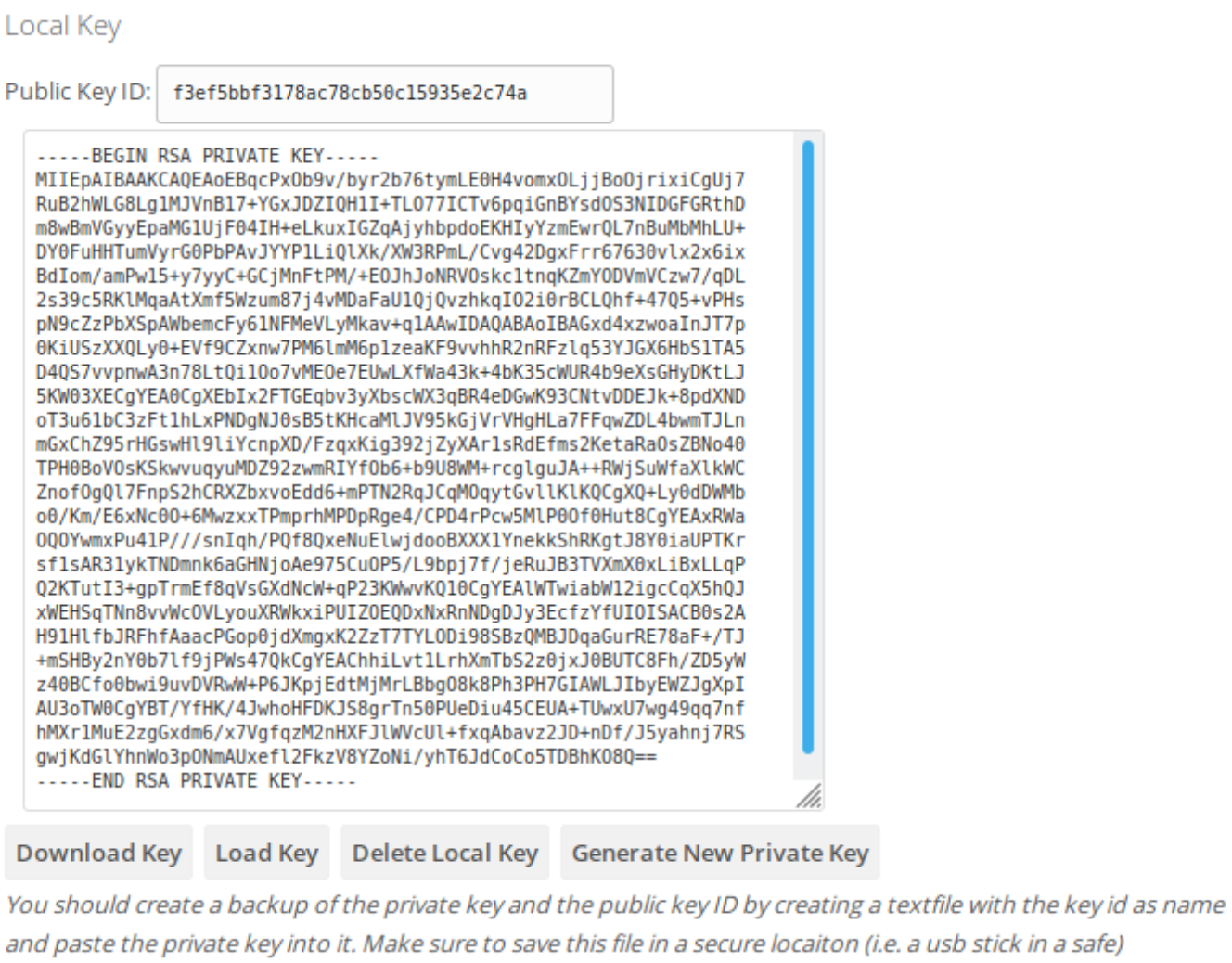
All public keys, which are stored on the server are shown here, including the date and IP address of creation as well as the user agent (usually browser) from which the public key was uploaded.

In case you use the Your Computer/Device storage, the public key, which matches your stored private key is marked bold.

You can delete public keys by clicking the trash bin icon. From then on all files cannot be decrypted with the corresponding private key any longer.

Key Management depending on your Key Storage

Your Computer/Device - Local Key



Download Key

Save the private key which is currently stored on the server/device to a file

Load Key

Paste a previously downloaded key and click load to be ready to use it in your current device. With this feature you can transfer the key from one browser/device to another when you download it in the first browser/device and load it into the second.

Delete Local Key

Delete a key from local storage only. The corresponding public key on the server is not touched.

> If you **do not have a copy** of your private key **it cannot be restored**

Generate New Private Key

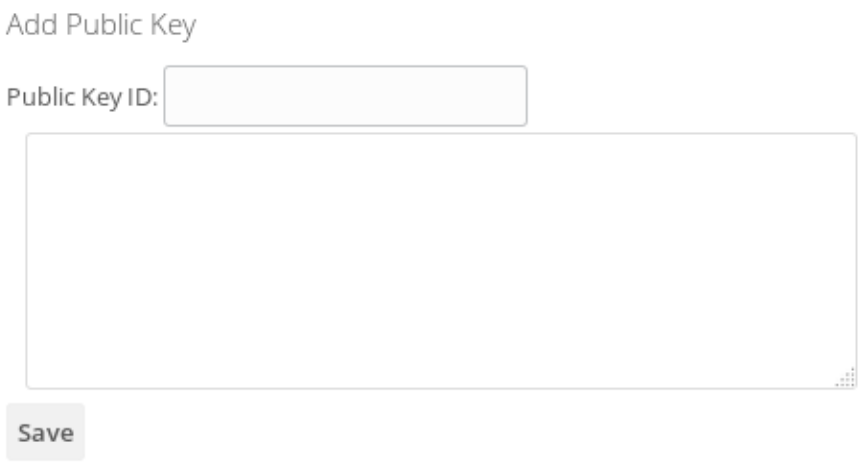
When you lost your private key or you want to create a new one for another device, click **Generate New Private Key**. The private key in the browser is replaced and the new public key is uploaded to the server. The previous public key on the server is not touched.

> In case you lost your private key be sure to delete the corresponding public key before (see Manage Existing Keys above)

Key Storages *Manual input for each download* and *Local decryption*

Both storage options require, that your public key is available on the server. It will be used for encrypting files.

In the Security section of your Personal settings you find a text area:



You might already have keys when

- you at least once have generated a public key in the Personal Settings
- you at least registered once with the Key Server (file key or Smart Card)
- the administrator added your key on the server (occ command)

Decrypting Files

Your Computer/Device

Files will be decrypted on the fly. No interaction is required.

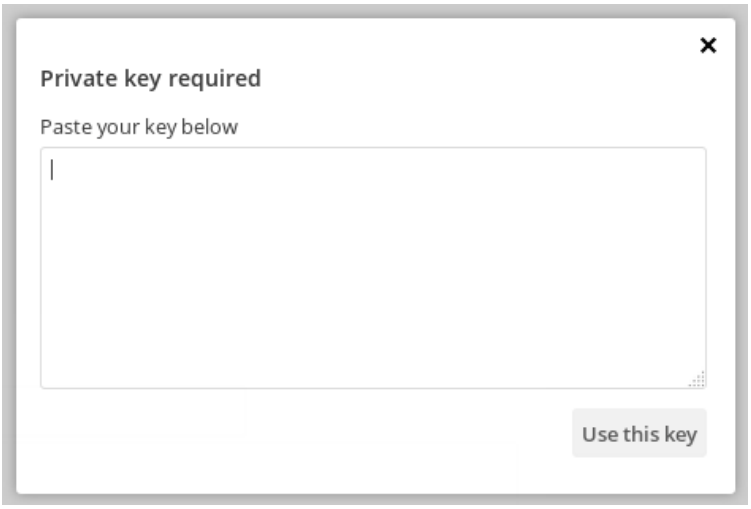
External Key/Smartcard

The key server pops up a notification that you are about to decrypt a file. You must confirm the decryption.

When re-encrypting a folder you will be asked for a confirmation as well.

Manual input for each download

Every time you want to open an encrypted file the browser opens a modal window where you have to provide your private key.



The file is decrypted in the browser only, the private key is never sent to the server.

Local decryption

The raw E2EE file will be downloaded. You need the E2EE Reader to be able to decrypt those files.