Instructions

1. General

MyLastKey is designed to provide reliable, secure and clear software for storing:

- Passwords and access data
- Hiding places
- Secrets
- Recipes
- Safe combinations
- Seeds and Keys for Cryptocurrencies
- Addresses of important people and companies
- Customer numbers (e.g. pension insurance)
- other sensitive data

to offer.

For security reasons, it is advisable to install the MyLastKey software on a USB stick and to keep the access data and the USB stick in a safe.

2. Innovation

The most innovative advantage of MyLastKey is that you do **not** have to give your access data to the MyLastKey software to a trusted person during your lifetime or to deposit them handwritten, i.e. unencrypted.

MyLastKey protects your sensitive data and secrets in the best possible way against **unauthorized access**, e.g. by burglars, legacy hunters or government organizations, by means of the **MyLastKey KeyPass**.
More information about the MyLastKey-Passport under point 4.5.

Once you have selected a field, the content is automatically copied to the cache, so you only have to paste the username or password on a web page with (CTRL+V).

3. Login

3.1 First use

- When you use MyLastKey for the first time, you just need to press the "Start" button. The default credentials are: MyLastKey!

3.2 Factory settings

- Here you can reset the entire software to factory settings.
- Please note that all data that was previously recorded will be lost.

3.3 Import and export wallets

- Under these buttons you can import or export a wallet.
- If you want to import a wallet, the current wallet is saved as a backup in the "/Logs" folder for security reasons.
- If you want to export (backup) a wallet, then the directories "Config" and "Filesafe" are exported in two ZIP files. If you want to import this backup again, then you have to unzip the backup ZIP files first and then import the wallet.
- The „Filesafe files" are not automatically imported for security reasons. You can copy them to the Filesafe folder if needed.
- Under the buttom "Backup Cloud" you can select an Dropbox or OneDrive folder. Each time a change is made, an encrypted backup file is stored here.

3.4 Re-enable wizard

- When you set up MyLastKey for the first time, the input wizard is automatically activated to guide you through the initial settings.
- Under this point you can activate it again afterwards.

3.5 Decryption

- Under this item you can request a wallet decryption.
- The further procedure is described there.

4. Main mask

4.1 Input field (passwords / banks / addresses / others)

- In the input fields, you can save your data indefinitely.
- In the input fields you can insert a line break with the key combination "Shift + Enter" to insert a line break.
- You can delete a line by selecting it and pressing the "Delete" button.

4.2 File safe

- The file safe is located in the "/Filesafe" folder.
- Here you can save documents such as your will in encrypted form.
- The encrypted files are given the file extension *.encrypt.
- Only a copy of the original file is encrypted. The original file remains unchanged.
- If necessary, you can decrypt the files again.

4.3 Change user name and password

- You can change the password as often as you want.
- The password must be at least 10 chars.

4.4 Export

- For security reasons, no export of the data is offered.
- This makes hacker attacks and phishing attempts more difficult.
- At your own risk, you can select (CTRL+A) and copy (CTRL+C) the tables and then paste them into an Excel spreadsheet.

4.5 KeyPass

- Here you can issue a **KeyPass** for trusted persons.
- First enter your first and last name, address, zip code and city of residence.
- Then enter this data for the trusted person as well.
- Using the "**Encrypt PW**" button you can encrypt your password for the MyLastKey software.
- The trusted person can only request decryption on presentation of the **KeyPass, an ID card and, if applicable, a certificate of inheritance** at service@mylastkey.com.

- Only if the trusted person presents all the documents, we will decrypt and issue your MyLastKey software access **data.**
- **Important: Our company only decrypts your username and password. We do not get access to your data and secrets at any time.**

5. contact details

Decrypta Technologies GmbH
Gillstr. 30
58239 Schwerte
Germany

office@mylastkey.com