Instrucio

1. généralités

MyLastKey a été conçu pour fournir un logiciel fiable, sûr et clair pour le stockage de :

- les mots de passe et les données d'accès
- Lieux de cachettes
- Secrets
- Recettes
- Combinaisons de coffres-forts
- Semences et clés pour les crypto-monnaies
- Adresses de personnes et d'entreprises importantes
- Numéros de client (par ex. assurance retraite)
- d'autres données sensibles

de l'entreprise.

Pour des raisons de sécurité, il est conseillé d'installer le logiciel MyLastKey sur une clé USB et de conserver les données d'accès et la clé USB dans un coffre-fort.

2. l'innovation

L'avantage le plus innovant de MyLastKey est que vous ne devez **pas** obligatoirement transmettre vos données d'accès au logiciel MyLastKey à une personne de confiance de votre vivant ou les déposer sous forme manuscrite, donc non cryptée.

MyLastKey protège au mieux vos données sensibles et vos secrets contre **tout accès non autorisé, par** exemple par des cambrioleurs, des voleurs d'héritage ou des organisations gouvernementales, grâce au **port de passeport MyLastKey**.
Plus d'informations sur le port de passe MyLastKey au point 4.5.

Vous pouvez également utiliser MyLastKey comme **logiciel de gestion des mots de passe**. Dès que vous avez sélectionné un champ, son contenu est automatiquement copié dans le cache, de sorte que vous n'avez plus qu'à coller le nom d'utilisateur ou le mot de passe sur une page Internet en appuyant sur (CTRL+V).

3. masque de connexion

3.1 Première utilisation

- Lorsque vous utilisez MyLastKey pour la première fois, il vous suffit d'appuyer sur le bouton "Démarrer". Les données d'accès par défaut sont les suivantes : "MyLastKey !

3.2 Réglages d'usine

- Ici, vous pouvez réinitialiser l'ensemble du logiciel aux paramètres d'usine.
- Veuillez noter que toutes les données qui ont été saisies jusqu'à présent seront perdues.

3.3 Importer et exporter un portefeuille

- Sous ces points, vous pouvez importer ou exporter un portefeuille.
- Si vous souhaitez importer un portefeuille, le portefeuille actuel est sauvegardé par sécurité dans le dossier "/Logs".
- Si vous souhaitez exporter un portefeuille (Backup), les répertoires "Config" et "Filesafe" sont exportés dans deux fichiers ZIP. Si vous souhaitez réimporter cette sauvegarde, vous devez d'abord décompresser les fichiers ZIP de sauvegarde et ensuite importer le portefeuille.
- Pour des raisons de sécurité, les fichiers "Filesafe" ne sont pas importés automatiquement. Si nécessaire, vous pouvez les copier dans le dossier "Filesafe".
- Sous "Backup Cloud", vous pouvez sélectionner un dossier Dropbox ou OneDrive intégré. À chaque changement, un "fichier de sauvegarde" chiffré est stocké ici.

3.4 Réactiver l'assistant

- Lorsque vous configurez MyLastKey pour la première fois, l'assistant de saisie est automatiquement activé et vous guide à travers les premiers réglages.
- Sous ce point, vous pouvez le réactiver ultérieurement.

3.5 Décodage

- Sous ce point, vous pouvez demander un décryptage du portefeuille.
- La suite de la procédure y est décrite.

4. masque principal

4.1 Champ de saisie (mots de passe / banques / autres)

- Vous pouvez enregistrer vos données de manière illimitée dans les champs de saisie.
- Dans les champs de saisie, vous pouvez utiliser la combinaison de touches "Shift + Enter" pour insérer un saut de ligne.
- Vous pouvez supprimer une ligne en la sélectionnant et en appuyant sur la touche "Delete".

4.2 Coffre-fort de fichiers

- Le coffre-fort de fichiers se trouve dans le dossier "/Filesafe".
- Vous pouvez y sauvegarder des documents cryptés, comme par exemple votre testament.
- Les fichiers cryptés reçoivent l'extension de fichier *.encrypt.
- Seule une copie du fichier original est cryptée. Le fichier original reste inchangé.
- Si nécessaire, vous pouvez décrypter à nouveau les fichiers.

4.3 Modifier le nom d'utilisateur et le mot de passe

- Vous pouvez changer votre mot de passe aussi souvent que vous le souhaitez.
- Le mot de passe doit comporter au moins 10 caractères.

4.4 Exportation

- Pour des raisons de sécurité, aucune exportation des données n'est proposée.
- Les attaques de pirates et les tentatives d'hameçonnage sont ainsi rendues plus difficiles.
- Vous pouvez, à vos risques et périls, sélectionner les tableaux (CTRL+A) et les copier (CTRL+C), puis les coller dans une feuille de calcul Excel.

4.5 KeyPass

- Ici, vous pouvez émettre un **KeyPass** pour des personnes de confiance.
- Inscrivez tout d'abord votre prénom et votre nom, votre adresse, votre code postal et votre lieu de résidence.
- Ensuite, vous inscrivez également ces données pour la personne de confiance.

- Le bouton **"Crypter le PW"** permet de crypter votre mot de passe pour le logiciel MyLastKey.
- La personne de confiance ne peut demander un décryptage que sur présentation du **KeyPass, d'une carte d'identité et, le cas échéant, d'un certificat d'hérédité**, à l'adresse suivante : service@mylastkey.com.
- Ce n'est que si la personne de confiance présente tous les documents que nous décrypterons et délivrerons vos **données d'accès** au logiciel MyLastKey.
- **Important : notre entreprise ne fait que décrypter votre nom d'utilisateur et votre mot de passe. Nous n'avons à aucun moment accès à vos données et à vos secrets.**

5. coordonnées

Decrypta Technologies GmbH
Gillstr. 30
58239 Schwerte
Allemagne

office@mylastkey.com