

Bedienungsanleitung KeePass2 Plugin KeePerso v0.7

KeePerso ist ein Plugin für KeePass2 Password Safe. Damit kann man zusätzlich zum KeePass Masterpassword eine Zwei-Faktor-Authentifizierung erreichen. Optional erlaubt KeePass zusätzlich noch WindowsUserAccount anzuwählen. KeePerso erstellt aus den Personalausweisdaten einen Schlüssel der zu einem Hash verarbeitet wird und dann mittels einem KeePass-KeyProvider an KeePass übergeben wird. KeePass verarbeitet dann den Key gemeinsam mit dem Masterpassword weiter.

Voraussetzungen:

KeePass2 - wir beschreiben hier die englische Version, weil die default ist

Plugin KeePerso (dieses Plugin ist nicht für KeePass1)

ein 64bit Computer (weil KeePerso 64bit ist),

Visual C++ Redistributable for Visual Studio 2015/2017/2019

AusweisApp2,

Kartenleser,

Personalausweis (ob dieser auslesbar ist kann in AusweisApp2 unter "Meine Daten einsehen" getestet werden)

Internetanschluss

Installation:

Bitte lesen Sie dazu "Plugin Installation and Uninstallation" im KeePass Help Center:

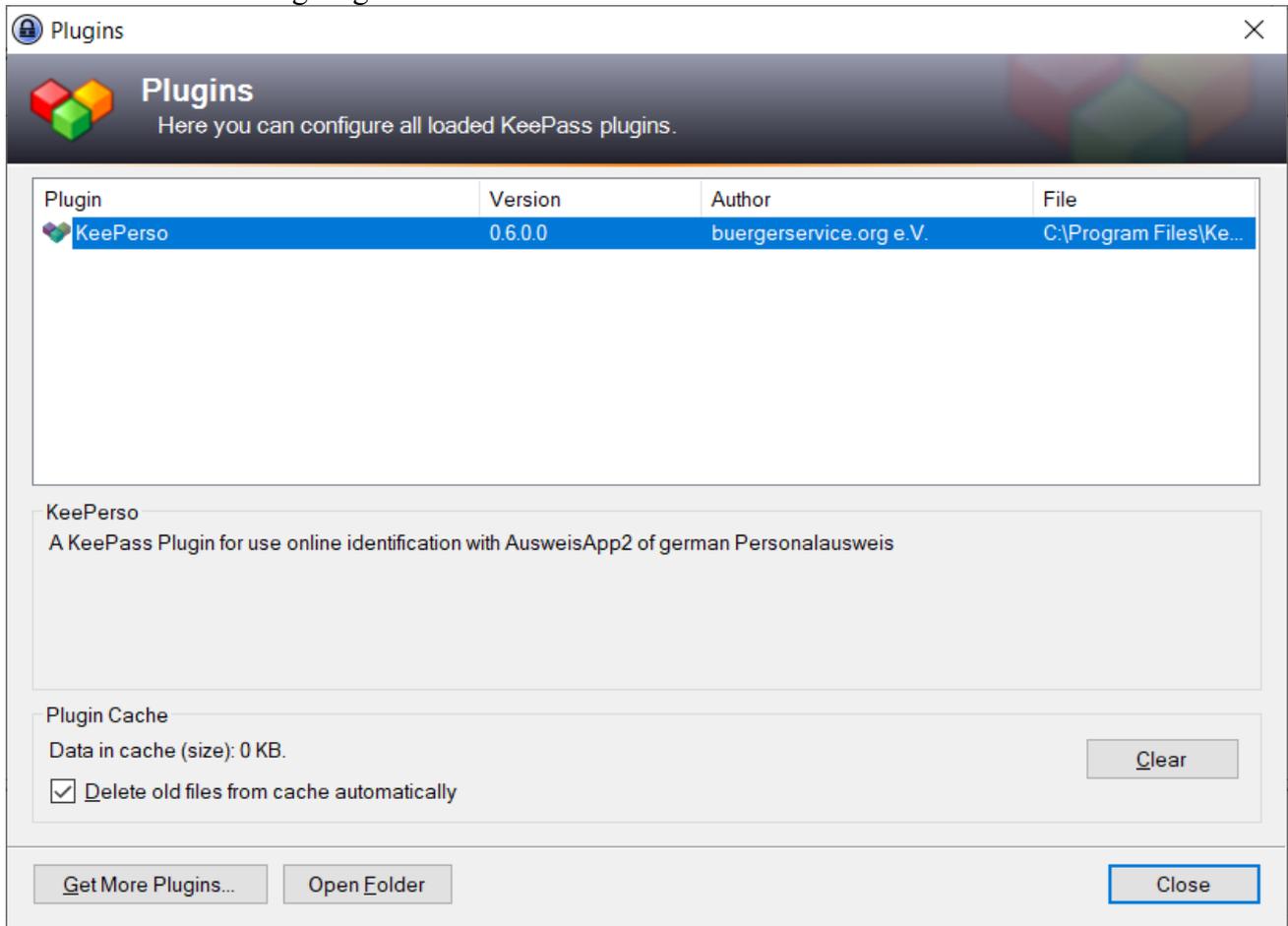
<https://keepass.info/help/v2/plugins.html>

Bedienung:

Das Plugin KeePerso (KeePersoCpp.dll) muss installiert werden (siehe oben Installation).

Wenn Sie dann KeePass2 starten, können Sie als erstes prüfen ob KeePerso unter

Menu → Tools → Plugins gelistet wird:



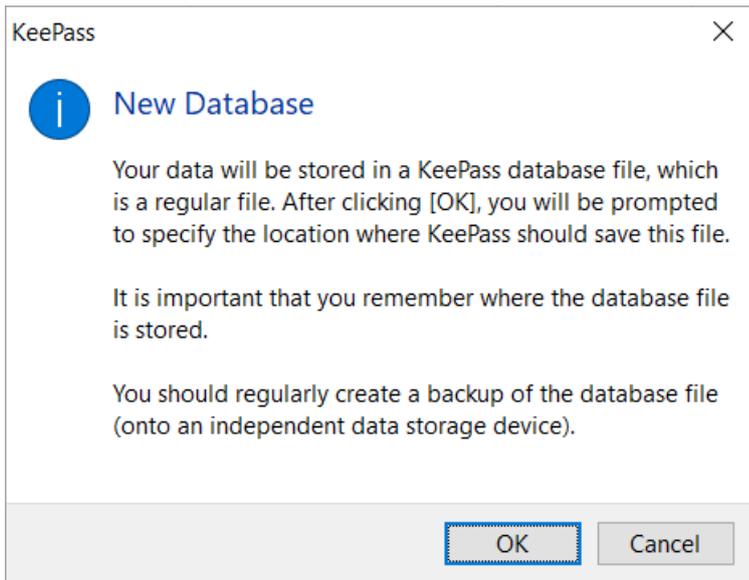
Man sollte vorher die AusweisApp2 auf dem PC starten und gegebenenfalls die Firewall/Viruswall/Webfilter stoppen/umkonfigurieren.

Ausserdem sollte ein Kartenleser aktiv sein und ein Personalausweis aufgelegt sein.

Neue Datenbank erstellen

Wenn man eine neue Datenbank für KeePerso anlegen will klickt man in KeePass2 auf

Menu → File → New, es erscheint das Fenster "New Database", wenn gewünscht OK klicken:



Dann erscheint das Fenster "Create New Database" in dem man das Verzeichnis und den Namen für die

Datenbank wählen kann zb man wählt sein Dokumente-Verzeichnis und den Datei-Namen zB "KeePersoDatabase"

In dem neuen Fenster "Create Master Key" sollte man als erstes ein Masterpassword wählen, hier wurde zum Test das Passwort "Test" eingegeben (natürlich sollte man ein bessere Passwort wählen).

Ausserdem wählt man "Show expert options" an und "Key file / provider" und in dem Pulldownmenu wählt man "KeePerso KeyProvider". Damit hat man eine Zwei-Faktor-Authentisierung. Optional erlaubt es KeePass2 sogar noch zusätzlich WindowsUserAccount anzuwählen. Dann klickt man OK.

Create Master Key

Create Master Key

C:\Users\... \Documents\KeepersoDatabase.kdbx

Specify the master key that will be used to encrypt the database.

A master key consists of one or more of the following components. All components that you specify will be required to open the database. If you lose one component, you will not be able to open the database anymore.

Master password:

Repeat password:

Estimated quality: 13 bits 4 ch.

Show expert options:

Key file / provider: KeePerso KeyProvider

A key file can be used as part of the master key; it does not store any database data. If an attacker has access to the key file, it does not provide any protection.

 If the key file is lost or its contents are changed, the database cannot be opened anymore. You should create a backup of the key file.
[More information about key files.](#)

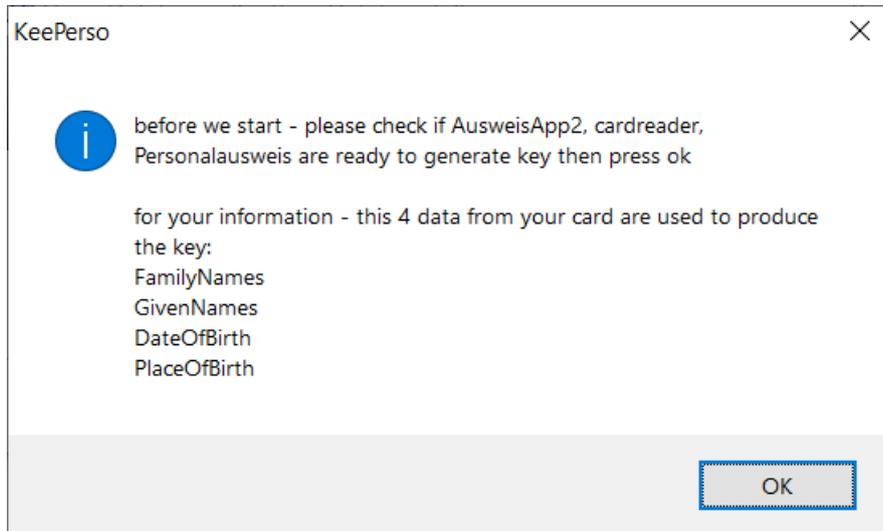
Windows user account

This source uses data of the current Windows user account. This data does not change when the account password changes.

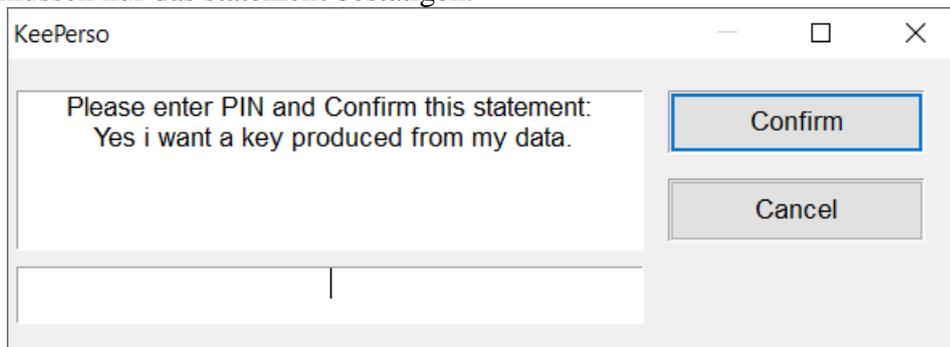
 If the Windows user account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the account is required. Creating and restoring such a backup is a very complicated task. If you don't know how to do this, don't enable this option.
[More information about Windows user accounts.](#)

Falls ihr Masterpassword schlecht ist fragt KeePass2 noch ob sie dieses wirklich verwenden möchten, wenn ja geht es weiter.

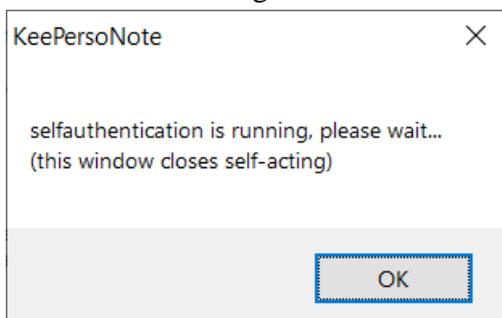
Das nächste Fenster ist vom Plugin KeePerso, hier wird gefragt ob alles bereit ist, bitte prüfen Sie und klicken dann OK:



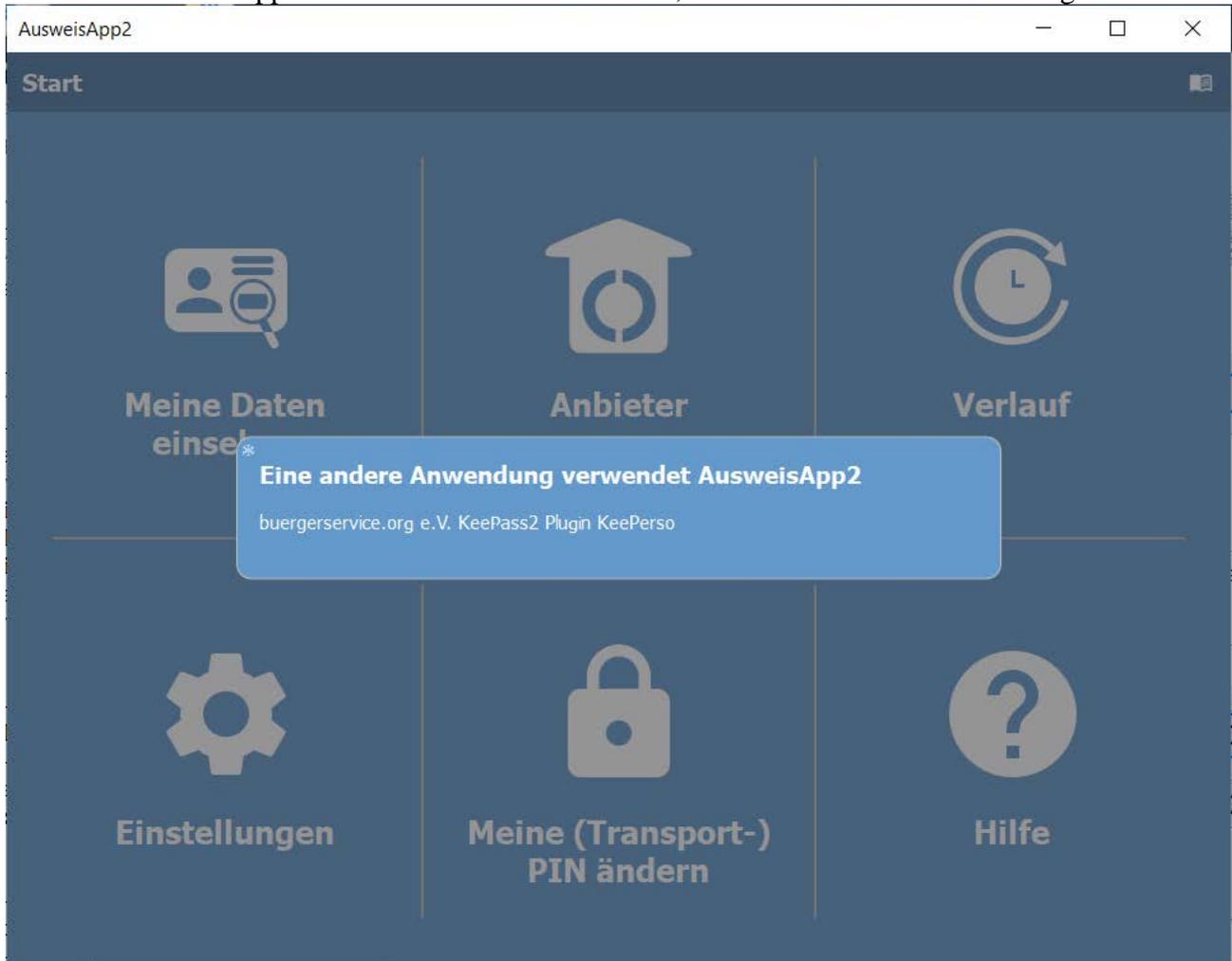
Falls Sie einen Kartenleser ohne Keypad besitzen, kommt ein Fenster in dem Sie Ihre Personalausweis-PIN eingeben sollen und mit Confirm bestätigen Sie ausserdem das angezeigte statement. Wenn Ihr Kartenleser ein Keypad besitzt wird die PIN nicht abgefragt sondern Sie müssen nur das statement bestätigen.



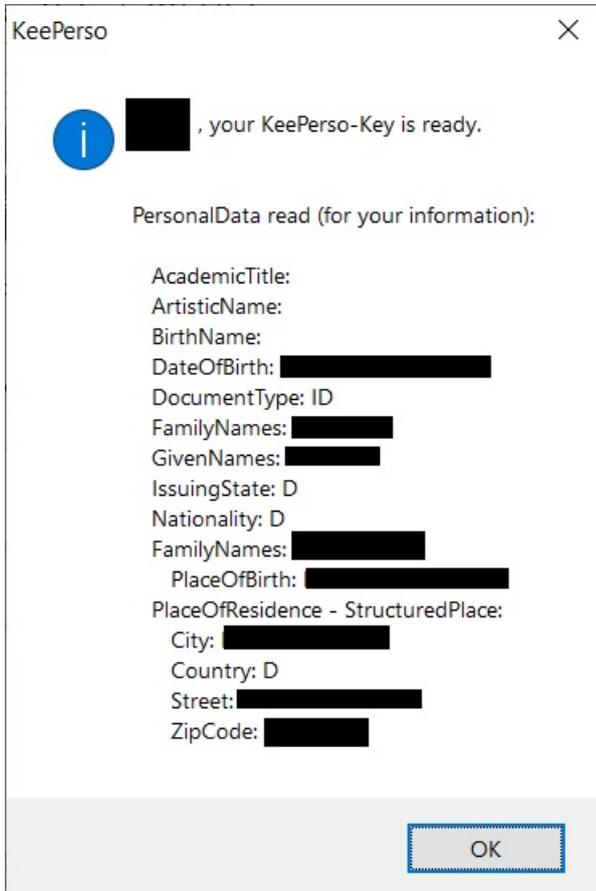
Nach der PIN-Eingabe (egal ob am Kartenleserkeypad oder im Window) erscheint ein Informationsfenster das den User darauf hinweist, dass die Selbstauskunft läuft, wenn die Selbstauskunft fertig ist schliesst das Fenster selbstständig:



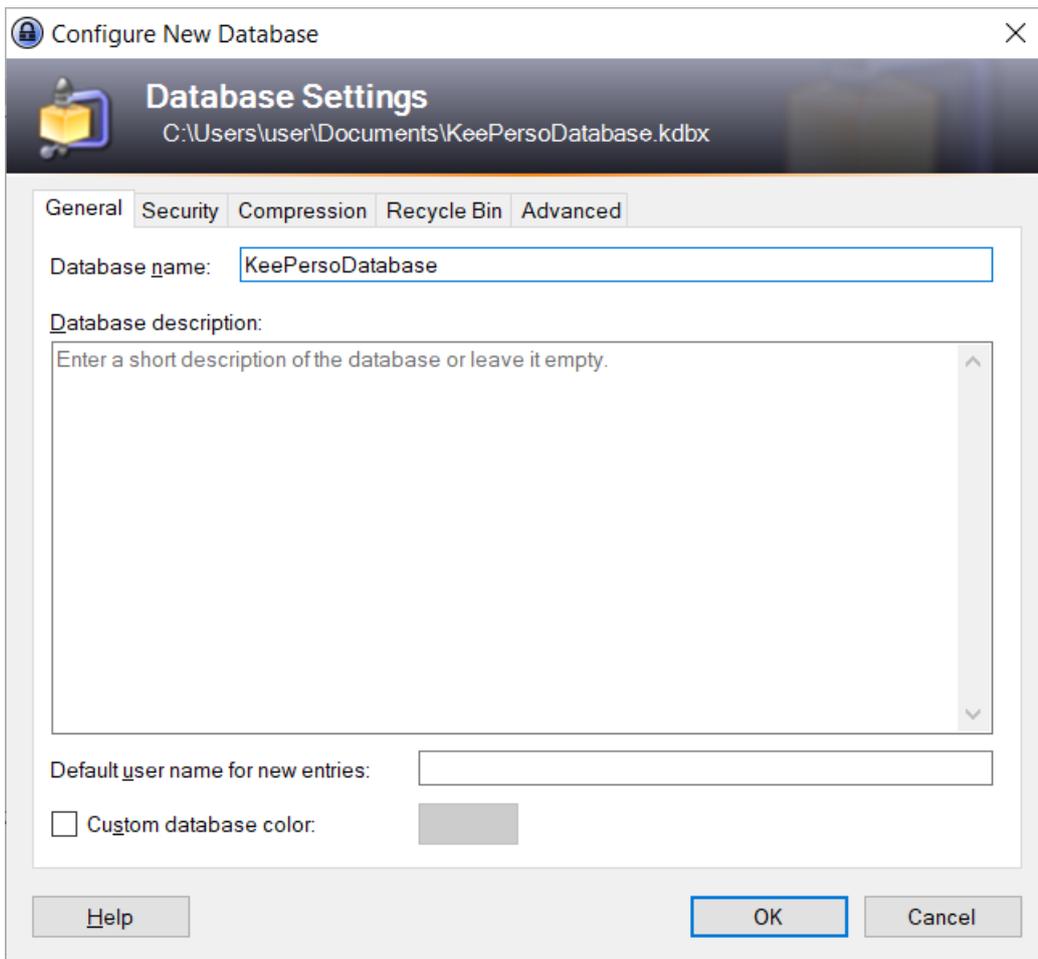
Wenn Sie AusweisApp2 offen haben können Sie sehen, dass KeePerso eine Verbindung aufbaut:



Wenn etwas fehlt kommt eine entsprechende Fehlermeldung, zB falls der Personalausweis nicht aufliegt, ansonsten kommt eine Erfolgsmeldung "KeePerso Key is ready". Da dem Ausweisinhaber die Informationen nach §18 (4) PAuswG angezeigt werden müssen werden die gelesenen Daten angezeigt (persönliche Daten in dem Beispielbild wurden geschwärzt). OK klicken.



Das Plugin übergibt über den KeePerso KeyProvider den nicht lesbaren Schlüssel an KeePass. Das nächste Fenster ist bereits wieder von KeePass2, hier können Sie ua einen Namen für die Database eintragen und OK klicken:



In dem Fenster Emergency Sheet wählen Sie noch ob Sie drucken möchten oder überspringen mit Skip:



Emergency Sheet

A KeePass emergency sheet contains all important information that is required to open your database. It should be printed, filled out and stored in a secure location, where only you and possibly a few other people that you trust have access to.

It is recommended that you create an emergency sheet for your database.

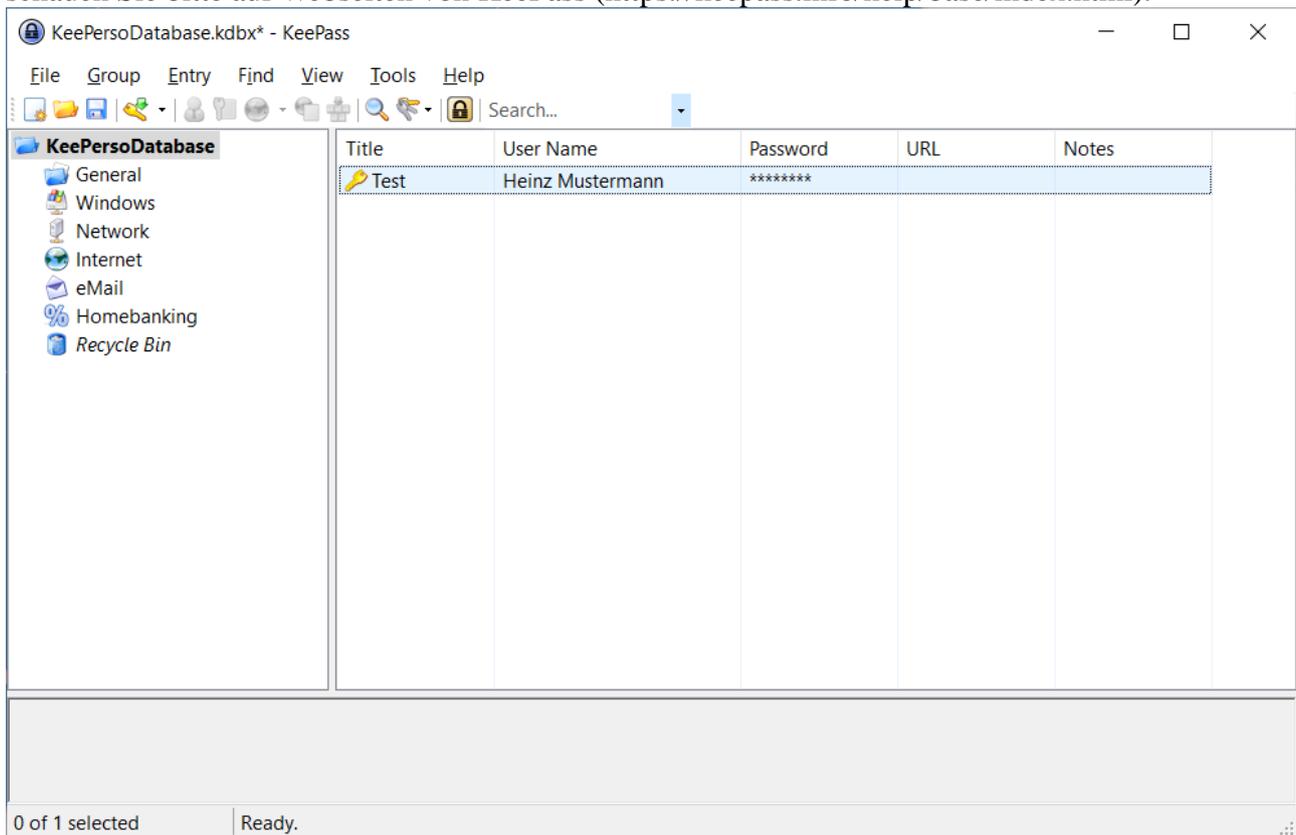
Do you want to print an emergency sheet now?

→ **Print**

KeePass will print an emergency sheet, which you can then fill out.

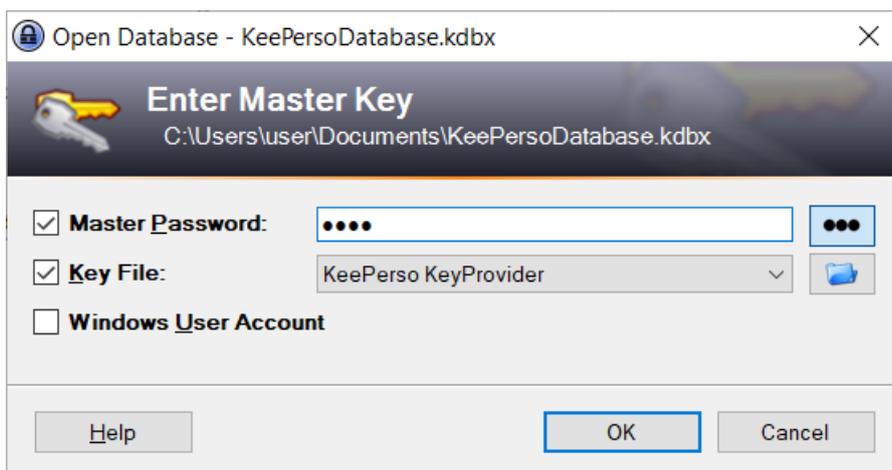
→ **Skip**

Dann öffnet sich die KeePass Datenbank und Sie können Einträge tätigen und abspeichern. Wenn Sie alles eingetragen haben können Sie KeePass2 schliessen. Zur Bedienung von KeePass2 schauen Sie bitte auf Webseiten von KeePass (<https://keepass.info/help/base/index.html>).



KeePass2 mit bestehender Datenbank

Wenn Sie jetzt KeePass2 wieder öffnen können Sie ihr Master Password eingeben und der KeePerso Key Provider sollte bereits angewählt sein. Wenn Sie dann OK klicken wird wieder genau wie beim Erstellen der neuen Datenbank (siehe Ablauf oben) ein neuer key erstellt.



Nach dem Erfolgsfenster vom Plugin KeePerso "..., Key is ready" gelangen Sie wieder in ihre Datenbank. Nun können Sie normal weiterarbeiten.

Die Informationen zu dem Zertifikat mit dem die Daten bei dem Provider abgerufen werden, können Sie im Menu unter Tools → KeePerso → Show Certificate anzeigen lassen:

KeePerso ✕

 information about the certificate you are using to identify at provider:

description:
issuerName: D-Trust GmbH
issuerUrl: <https://www.d-trust.net>
purpose:
subjectName: Governikus GmbH & Co. KG
subjectUrl: <https://www.autentapp.de>

termsOfUsage:
Name, Anschrift und E-Mail-Adresse des Diensteanbieters:
Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen
kontakt@governikus.com

Hinweis auf die fuer den Diensteanbieter zustaendigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren:
Die Landesbeauftragte fuer Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen
Arndtstrasse 1
27570 Bremerhaven
0421/596-2010
office@datenschutz.bremen.de
<http://www.datenschutz.bremen.de>

validity:
effectiveDate: 2021-04-15
expirationDate: 2021-04-16