Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

KEEPASS PLUGIN - BENUTZERHANDBUCH

Graz, am 12. Jänner 2015

Alexander Marsalek – alexander.marsalek@iaik.tugraz.at

Abstract: Dieses Dokument beschreibt die Installation und Verwendung des Smartcard-Plugins für den Passwortmanager Keepass. Dieses Plugin ermöglicht die Verwendung von österreichischen Bürgerkarten zur Absicherung der Passwort-Datenbank. Wie gewohnt kann die Datenbank weiterhin zusätzlich mittels eines Passwortes geschützt werden.

Inhaltsverzeichnis

1. Allgemeines

KeePass (Reichl, 2014) ist ein freies Programm zur Kennwortverwaltung. Der Zugriff kann mittels Passwort, Schlüsseldatei oder Bindung an den jeweiligen Windows Account abgesichert werden.
Die Funktionalität von Keepass kann mittels Plugins erweitert werden. Dieses „Smartcard“ Plugin fügt Unterstützung für Österreichische Bürgerkarten (Ecard G2 & G3 Karten, ACOS Karten) zur Funktionalität von Keepass hinzu. Bei Verwendung dieses Plugins kann der Zugriff auf die Passwort-Datenbank mittels Bürgerkarte geschützt werden. Dafür wird ein zufälliger Schlüssel generiert und mittels der Bürgerkarte verschlüsselt. Bei jedem Zugriff auf die Passwort-Datenbank wird der gespeicherte verschlüsselte Schlüssel geladen und mittels Bürgerkarte entschlüsselt und an Keepass übergeben. Zusätzlich zur Bürgerkarte kann die Datenbank auch weiterhin mittels Passwort oder Bindung an den Windows Account geschützt werden. Die folgenden Kapitel beschreiben die Installation und Verwendung des Plugins.

2. Installation

Die Dateien des ZIP-Archivs müssen in den KeePass Ordner (in dem die KeePass.exe liegt) extrahiert bzw. kopiert werden.
Durch Entfernen dieser Dateien kann das Plugin deinstalliert werden.

3. KeePass Plugin

Nach der Installation des Plugins kann entweder eine neue Passwort-Datenbank angelegt werden oder der Hauptschlüssel einer bestehenden Datenbank geändert werden.

ACHTUNG: Wenn Sie Ihre Bürgerkarte zur Verschlüsselung verwenden, besteht bei Verlust oder defekt kein Zugriff Ihre mit Keepass-Datenbank mehr. Es wird empfohlen, einen Backup-Schlüssel zu erstellen und an einem sicheren Ort zu verwahren. Dies wird in diesem Abschnitt beschrieben.

3.1. Anlegen einer neuen Passwort-Datenbank

Eine neue Passwort-Datenbank kann im Menü unter „**File->New…**“ erstellt werden. Anschließend kann der Speicherort der Datenbank sowie der Name ausgewählt werden. Im darauffolgenden Schritt muss unter „**Key File / provider**“ das Plugin „**SmartCard Plugin**“ ausgewählt werden (siehe Abbildung 1).

Abbildung 1: Verschlüsselungsschlüssel erstellen.

Zusätzlich kann der Schlüssel mit einem Passwort geschützt werden oder an das Windows Benutzer Konto gebunden werden. Im darauffolgenden Schritt kann der Speicherort sowie der Name der verschlüsselten Schlüsseldatei gewählt werden. Es wird empfohlen, den Namen sowie den Speicherort nicht zu verändern, da sonst jedes Mal der Schlüssel ausgewählt werden muss. Anschließend listet das Plugin alle in Frage kommenden Zertifikate auf (siehe Abbildung 2).

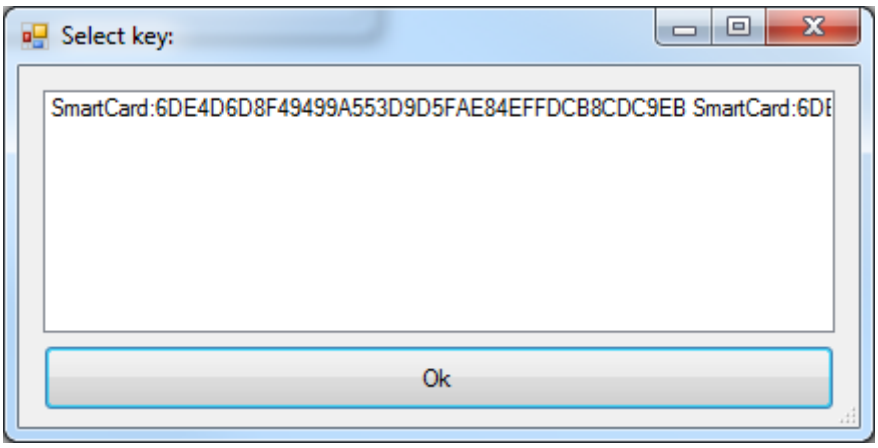

Abbildung 2: Zertifikatsauswahl

Nach der Auswahl eines Zertifikates generiert das Plugin einen zufälligen Schlüssel und verschlüsselt diesen mittels des ausgewählten Zertifikats. Der Schlüssel kann dann nur mehr unter Verwendung dieser Smartcard entschlüsselt werden.

3.1.1. Erstellung des Backup-Schlüssels

Da im Falle eines Defektes oder Verlusts der Smartcard nicht mehr auf die Schlüssel-Datenbank zugegriffen werden könnte, wird empfohlen einen Backup-Schlüssel zu generieren. Das Plugin bietet dazu zwei Möglichkeiten an:

- Verschlüsseln des Schlüssels mit einer zweiten Smartcard.
- Erstellen eines Unverschlüsselten Backup-Schlüssels.

Es können auch beide Backupvarianten benutzt werden. Um den Schlüssel mittels einer zweiten Smartcard zu verschlüsseln, oder beide Backup-Varianten zu nutzen, muss bei der Frage in Abbildung 3 „Ja“ ausgewählt werden. Falls nur ein (unverschlüsselter) Backup-Schlüssel erstellt werden soll muss „Nein“ ausgewählt werden.

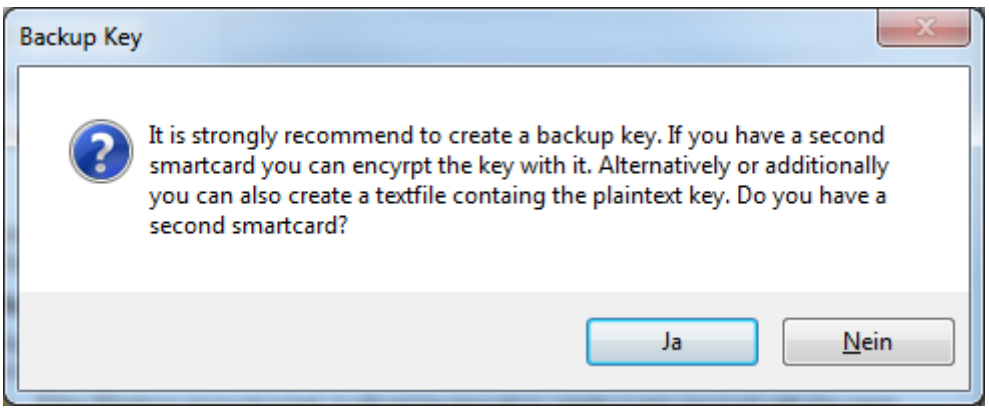

Abbildung 3: Wahl zwischen den beiden Backup Möglichkeiten.

Die beiden folgenden Abschnitte erklären die beiden Methoden zur Erstellung des Backup-Schlüssels.

Zur **Verschlüsselung des Schlüssels mit einer zweiten Smartcard** muss nach Aufforderung des Plugins (siehe Abbildung 4) eine andere Bürgerkarte eingelegt werden. Es kann hierfür auch eine bereits abgelaufene ältere Karte verwendet werden.

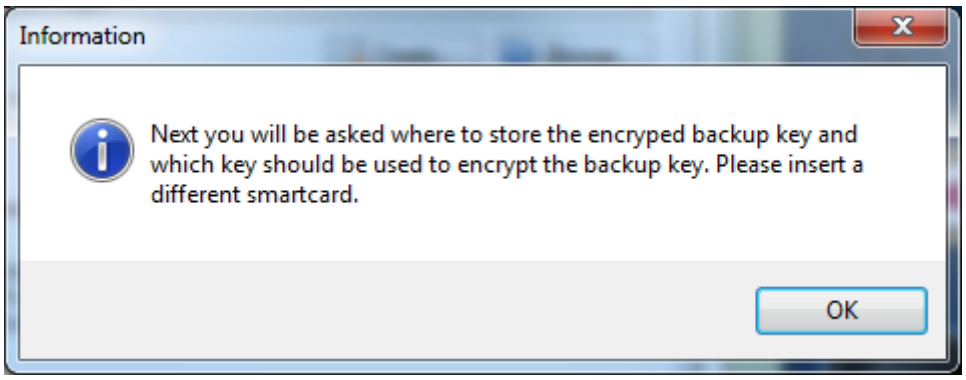

Abbildung 4: Smartcard wechseln

Die Erstellung des Backup-Schlüssels läuft im Wesentlichen gleich ab wie die Erstellung des primären Schlüssels, d.h. zuerst kann der Speicherort ausgewählt werden, anschließend das Zertifikat. Es wird empfohlen die verschlüsselten Schlüssel zu sichern, da bei einem Verlust der Zugriff auf die Schlüssel-Datenbank unmöglich ist. Die verschlüsselten Schlüssel müssen nicht besonders geschützt werden, ohne die zugehörige Bürgerkarte sind Sie nutzlos. Nach der Erstellung des verschlüsselten Backup Schlüssels kann noch ein unverschlüsselter Backup Schlüssel erstellt werden.

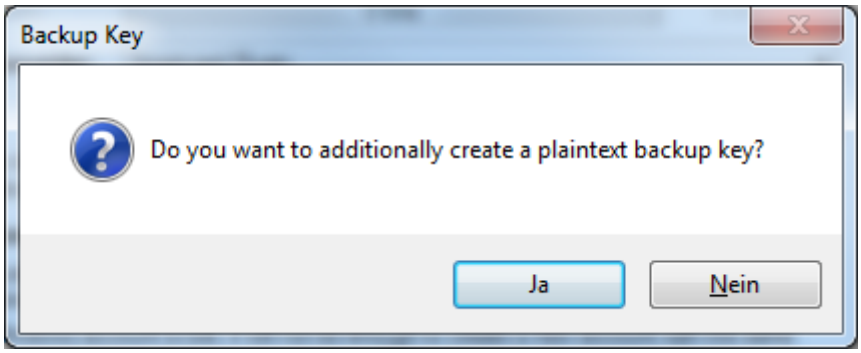

Abbildung 5: Abfrage, ob zusätzlich ein unverschlüsselter Backup Schlüssel erstellt werden soll.

Dazu muss die Frage in Abbildung 5 mit „Ja“ beantwortet werden. Ansonsten übergibt das Plugin die Kontrolle zurück an Keepass und es können die Datenbank Einstellungen nach den eigenen Wünschen angepasst werden (siehe Abbildung 7).

Bei der **Erstellung eines Unverschlüsselten Backup-Schlüssels** erscheint zuerst die in Abbildung 6 gezeigte Mitteilung. Diese informiert darüber, dass ein unverschlüsselter Schlüssel erstellt wird. Es wird empfohlen den Schlüssel auf einem portablen Speichermedium abzulegen. Dieses Medium sollte dann an einem sicheren Ort (z.B.: Tresor, Schließfach) aufbewahrt werden. Zusätzlich sollte die erstellte Datei mit einem Texteditor (z.B.: Notepad) geöffnet und ausgedruckt werden, falls das portable Speichermedium defekt wird. Der Ausdruck sollte ebenso an einem sicheren Ort aufbewahrt werden.

Achtung: Jeder mit Zugriff auf den unverschlüsselten Backup-Schlüssel, bzw. den Ausdruck kann auf die Passwort-Datenbank zugreifen.

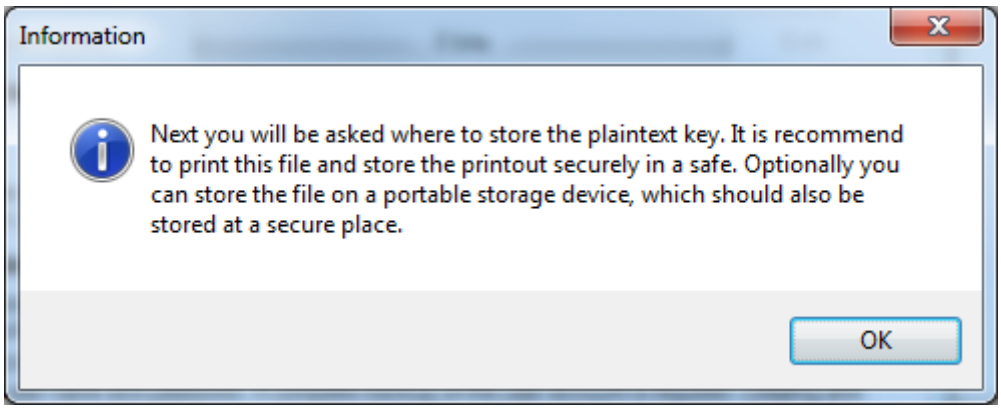

Abbildung 6: Information zur Erstellung eines unverschlüsselten Backup Schlüssels.

Um die Sicherheit der Passwort-Datenbank zu gewährleisten darf der unverschlüsselte Backup-Schlüssel nicht in falsche Hände gelangen. Die wichtigsten Punkte hierfür sind:

- Der verwendete PC muss frei von Schadsoftware sein.
- Der (unverschlüsselte) Backup-Schlüssel muss sicher aufgewahrt werden. Eventuelle Kopien am PC müssen sicher gelöscht werden.
- Beim Ausdrucken ist darauf zu achten, dass das Dokument nicht am Drucker gespeichert wird.

Datenbank Einstellungen:

Nach der Erstellung des Schlüsselmaterials übergibt das Plugin die Kontrolle an KeePass, wo die Datenbank Einstellungen angepasst werden können (Abbildung 7).

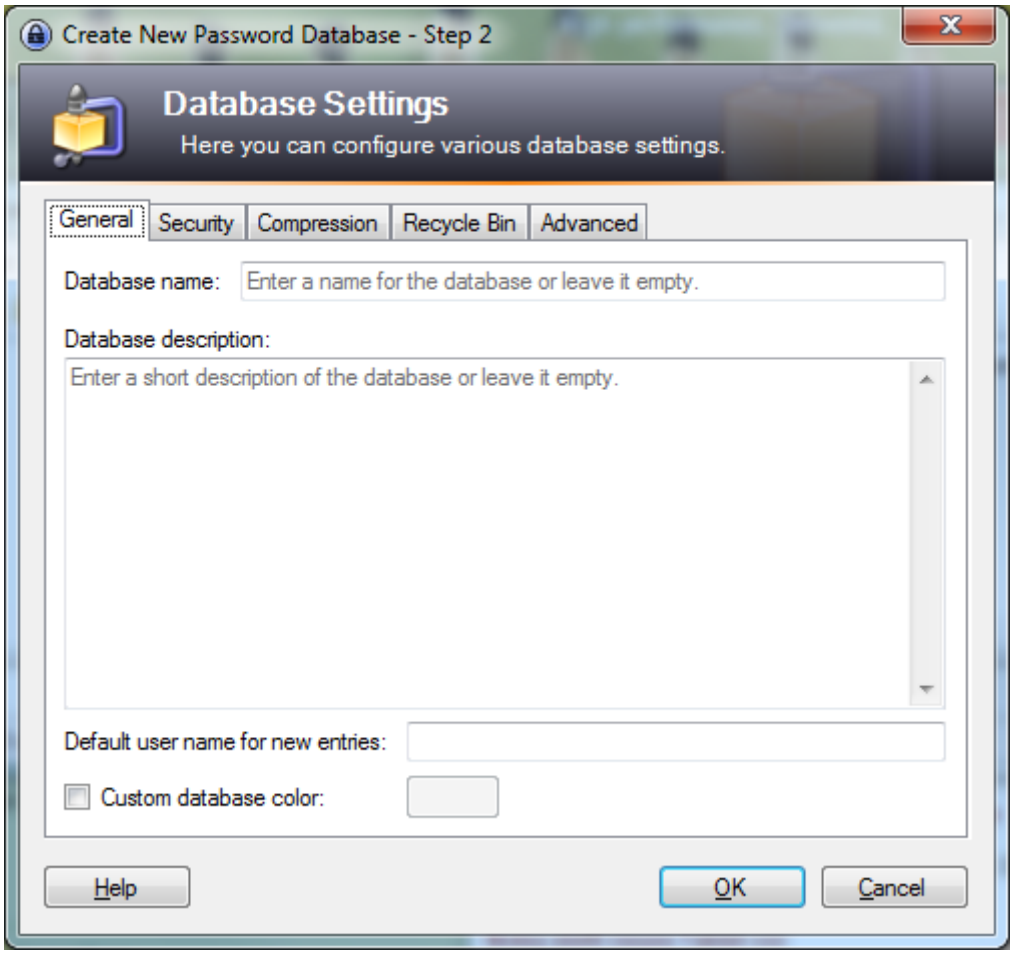

Abbildung 7: Datenbank Einstellungen

3.2. *Anpassen einer bestehenden Passwort-Datenbank*

Es wird empfohlen eine Sicherungskopie der bestehenden Datenbank zu erstellen, für den unwahrscheinlichen Fall, dass während der Umstellung ein Problem auftritt.
Um eine bestehende Passwort-Datenbank mittels Bürgerkarte zu schützen muss die Datenbank geöffnet werden und anschließend im Menü der Punkt „**File->Change Master Key…**“ ausgewählt werden. Es öffnet sich dann das in Abbildung 1 dargestellte Fenster. Die folgenden Schritte sind analog den in Punkt 3.1 erläuterten Schritten. Nach der erfolgreichen Umstellung (siehe Abbildung 8) muss die Datenbank gespeichert werden um die Änderungen zu übernehmen.

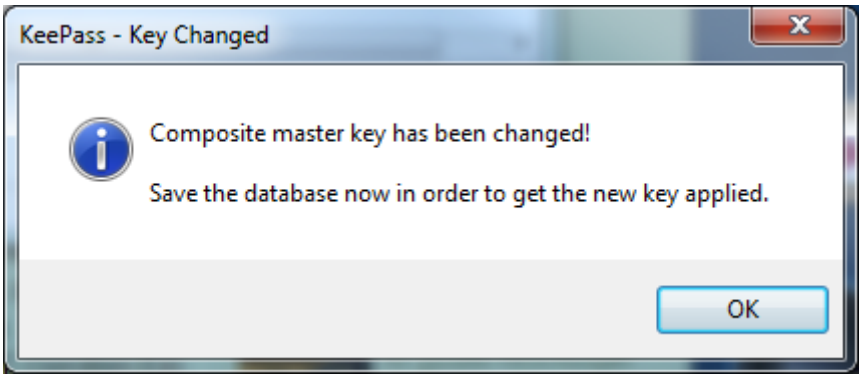

Abbildung 8: Der Hauptschlüssel wurde erfolgreich geändert.

3.3. *Benutzung der erstellten Passwort-Datenbank*

Nach dem Start der Keepass Anwendung sollte automatisch die zuletzt benutzte Datenbank geladen und das in Abbildung 9 dargestellte Fenster geöffnet werden. Sollte dies nicht der Fall sein kann die Datenbank über „**File->Open**“ ausgewählt werden.

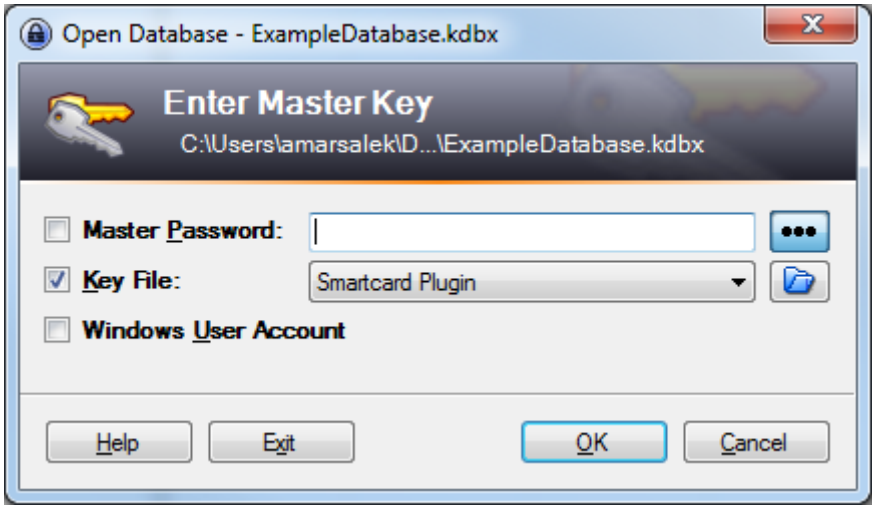

Abbildung 9: Passwort-Datenbank öffnen

Nach einem Klick auf „**OK**“ öffnet sich eine PIN-Eingabe. Je nach benutzter Karte muss der „Karten-PIN“ oder der „Geheimhaltuns-PIN“ eingeben werden und mit „**OK**“ bestätigt werden. Anschließend kann die Passwort-Datenbank wie gewohnt benutzt werden.

3.4. *Kartendefekt / Kartenverlust*

Sollte die **primäre Karte** defekt werden oder verloren gehen, muss der Backupschlüssel zum Öffnen der Datenbank verwendet werden. Dazu muss die Schlüsseldatei (in diesem Bsp. „ExampleDatabase.SkyTrustKey“) verschoben oder umbenannt werden. Die folgenden Schritte sind unter Punkt 3.5 erläutert.

Sollte die **Backup Karte** defekt werden oder verloren gehen, empfiehlt es sich einen neuen Backup-Schlüssel zu erstellen. Dies kann wie im Punkt 3.2 beschrieben erledigt werden.

3.5. Schlüsselverlust

Sollte die verschlüsselte Schlüsseldatei verloren gehen, erscheint eine Warnmeldung (siehe Abbildung 10).

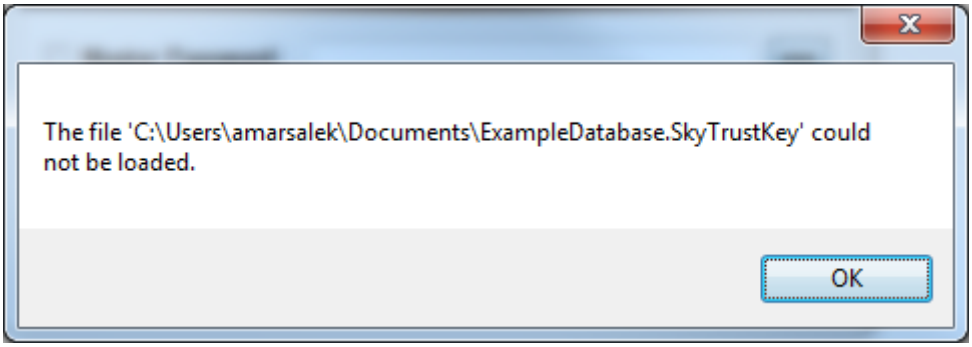

Abbildung 10: Schlüsseldatei wurde nicht gefunden.

Nach Bestätigung der Warnung kann der Backup-Schlüssel ausgewählt werden. Bei einem verschlüsselten Backup-Schlüssel öffnet sich dann wie gewohnt das PIN-Eingabe Fenster. Bei einem unverschlüsselten Backup-Schlüssel wird die Datenbank direkt geöffnet.
Es empfiehlt sich dann einen neuen Backup-Schlüssel zu erstellen (siehe Punkt 3.2).

4. Literaturverzeichnis

Reichl, D. (2014). *KeePass Password Safe*. Von http://keepass.info/ abgerufen