

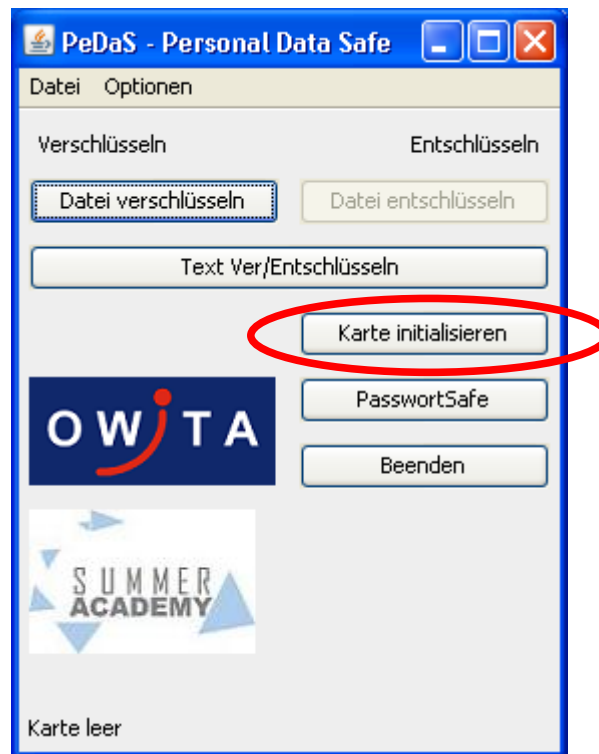
# PeDaS – Personal Data Safe

## - Bedienungsanleitung -

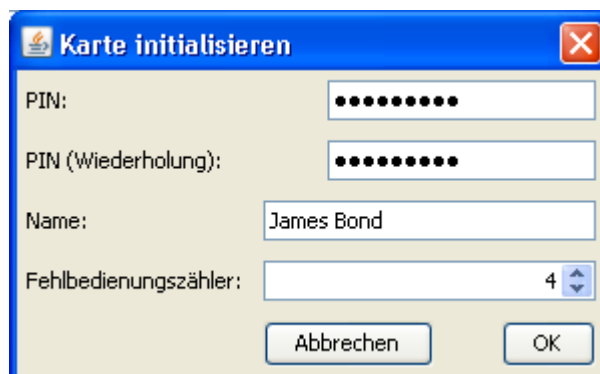


## 1 Initialisierung einer neuen SmartCard

Starten Sie die **PeDaS**-Anwendung, nachdem Sie eine neue noch nicht benutzte SmartCard in einen mit Ihrem PC verbundenen Kartenleser eingelegt haben, bzw. den USB-Kartenleser mit eingelegter SmartCard im SIM-Format an Ihrem Rechner angeschlossen haben. Im **PeDaS**-Hauptfenster klicken Sie auf „Karte initialisieren“:



Im folgenden Dialog legen Sie Ihre persönliche PIN fest. Sie können hier eine beliebige Folge von mindestens 4 und maximal 16 Zahlen und Zeichen wählen. Als nächstes geben Sie einen Namen an, der auch in die von **PeDaS** benutzte Bezeichnung des exportierbaren öffentlichen Schlüssels eingeht. Schließlich können Sie die Anzahl möglicher falscher PIN-Eingaben im Fenster „Fehlbedienungszähler“ im Bereich von 4 bis



8 festlegen. Klicken Sie nun auf „OK“. Die Generierung des RSA-Schlüsselpaares auf der SmartCard benötigt einige Sekunden. Bitte haben Sie etwas Geduld.

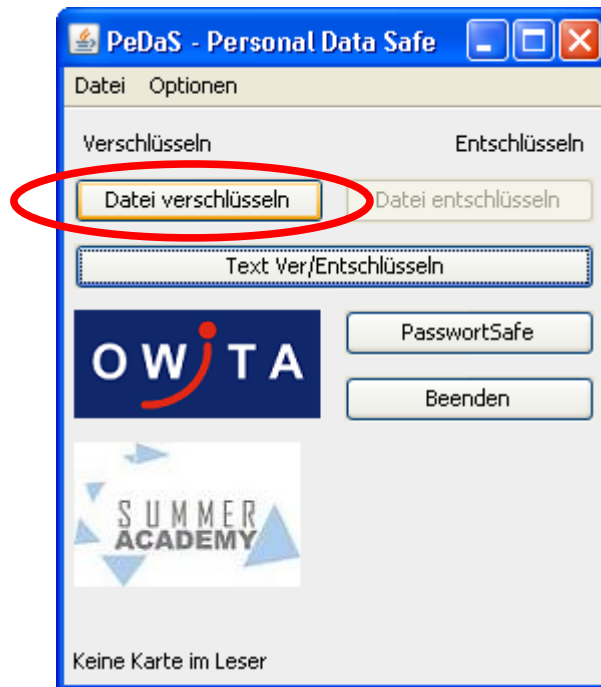
Im Anschluss an den Initialisierungsvorgang steht **PeDaS** der öffentliche Schlüssel des soeben erzeugten RSA-Schlüsselpaares für Verschlüsselungsvorgänge (auch ohne die SmartCard) zur Verfügung. Der private Schlüssel befindet sich auf der SmartCard und kann für Entschlüsselungsvorgänge nur zusammen mit der SmartCard genutzt werden.

**Achtung:** Nach der Initialisierung der SmartCard führt eine Eingabe falscher PINs nach einer Überschreitung der hier festgelegten Zahl dazu, dass die SmartCard auf Dauer gesperrt wird. Alle Daten, die ausschließlich mit dem zu dieser SmartCard gehörigen Schlüssel verschlüsselt wurden, können dann unter keinen Umständen mehr entschlüsselt werden. In Abhängigkeit vom Einsatz empfiehlt es sich daher, entweder die PIN zusätzlich an einem weiteren sicheren Ort zu verwahren, um so auf diese ggf. nochmals zurückgreifen zu können, bevor der Fehlbedienungsähler auf 0 steht und die SmartCard keine weitere Nutzung des privaten Schlüssels zulässt, oder aber die Verschlüsselung jeweils parallel mit einem weiteren öffentlichen Schlüssel durchzuführen, der zu einer weiteren (Master-)SmartCard gehört.

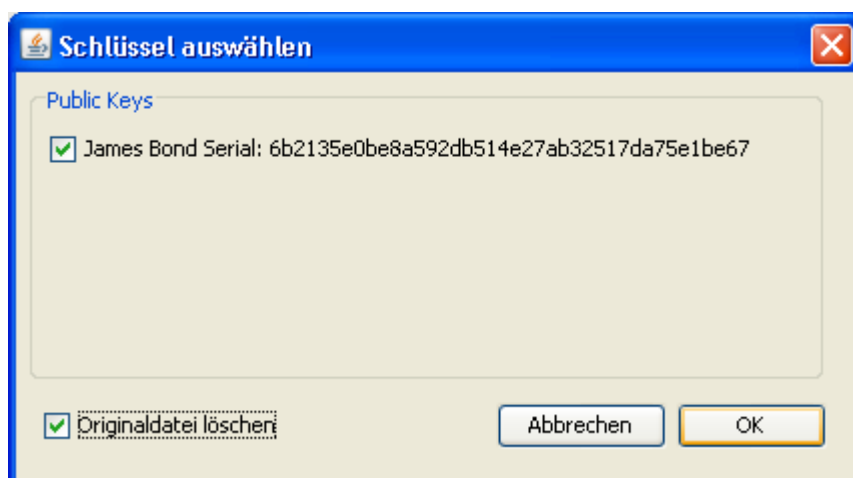
## 2 Ver- und Entschlüsselung von Dateien

Nachdem Sie die **PeDaS**-Anwendung gestartet haben, können beliebige Dateien mit den öffentlichen Schlüsseln verschlüsselt werden, die **PeDaS** aufgrund einer Initialisierung von SmartCards oder über einen Import („Datei“ > „Öffentlichen Schlüssel Importieren“) zur Verfügung stehen.

Zur **Verschlüsselung** einer Datei klicken Sie bitte auf „Datei verschlüsseln“:



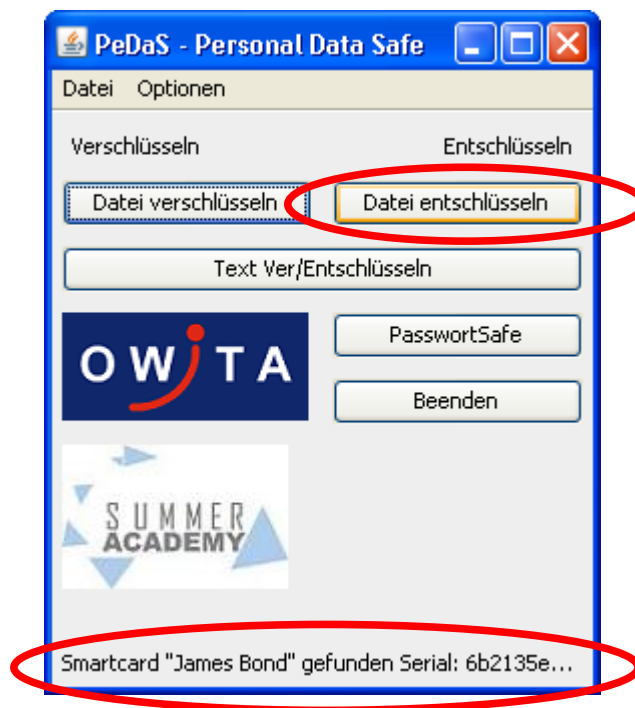
Wählen Sie im nun erscheinenden Menü die zu verschlüsselnde Datei aus und bestätigen Sie Ihre Wahl durch einen Klick auf „Öffnen“. Im nachfolgenden Menü können Sie die öffentlichen Schlüssel auswählen, mit denen die Datei verschlüsselt werden soll, und festlegen, ob die Originaldatei nach der Verschlüsselung gelöscht werden soll.



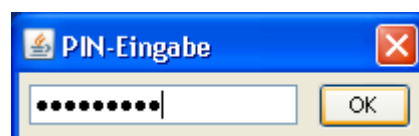
Eine Entschlüsselung ist später jeweils mit jeder der zu den ausgewählten Schlüsseln korrespondierenden SmartCards einzeln möglich.

Nach einem Klick auf „OK“ wird die verschlüsselte Datei mit der zusätzlichen Endung „.pds“ in dem gleichen Verzeichnis abgespeichert, in dem sich die Originaldatei befindet.

Zur **Entschlüsselung** einer Datei schließen Sie zunächst Ihre SmartCard an Ihren Rechner an und starten sie anschließend **PeDaS**. **PeDaS** zeigt in der Statuszeile am unteren Rand die gefundene SmartCard an und bietet nun die Option zur Entschlüsselung einer Datei an. Klicken Sie auf „Datei entschlüsseln“:

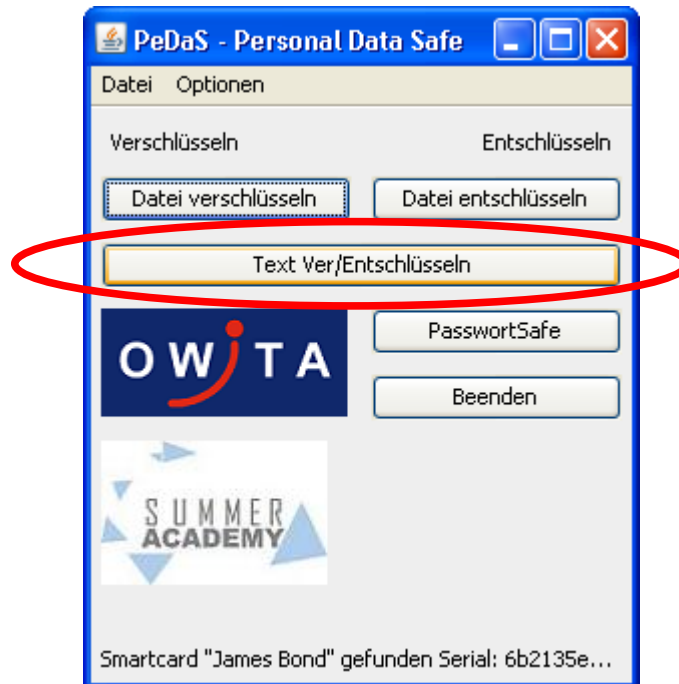


In den folgenden Menüs wählen Sie zunächst die zu entschlüsselnde Datei aus, bestimmen den Ort und Namen unter dem die entschlüsselte Datei abgelegt werden soll und werden schließlich zur Eingabe des PINs aufgefordert, mit dem der private Schlüssel auf der SmartCard geschützt ist.



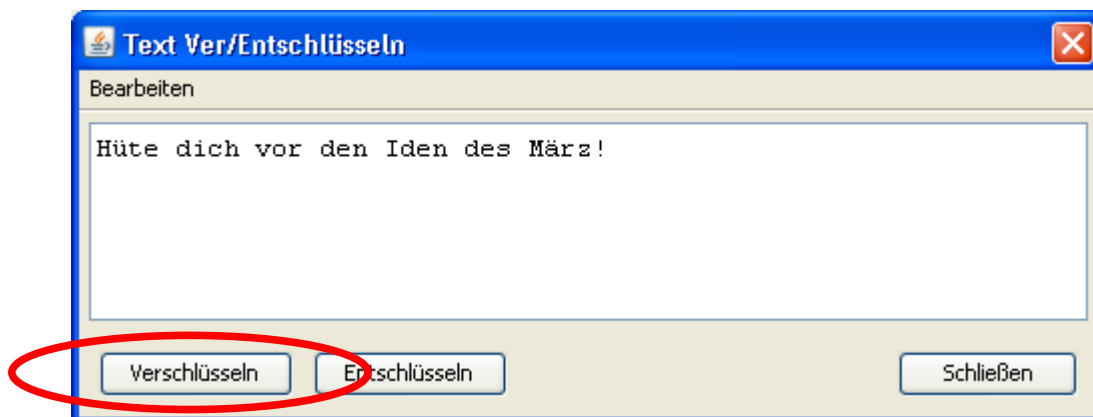
### 3 Ver- und Entschlüsselung von Texten

Daten können mit **PeDaS** auch direkt über ein einfaches Editorfenster eingegeben oder aus der Zwischenlage geladen werden, um verschlüsselt, bzw. im Falle von verschlüsselten Daten entschlüsselt zu werden. Das Editorfenster ist über einen Klick auf „Text Ver/Entschlüsseln“ erreichbar:

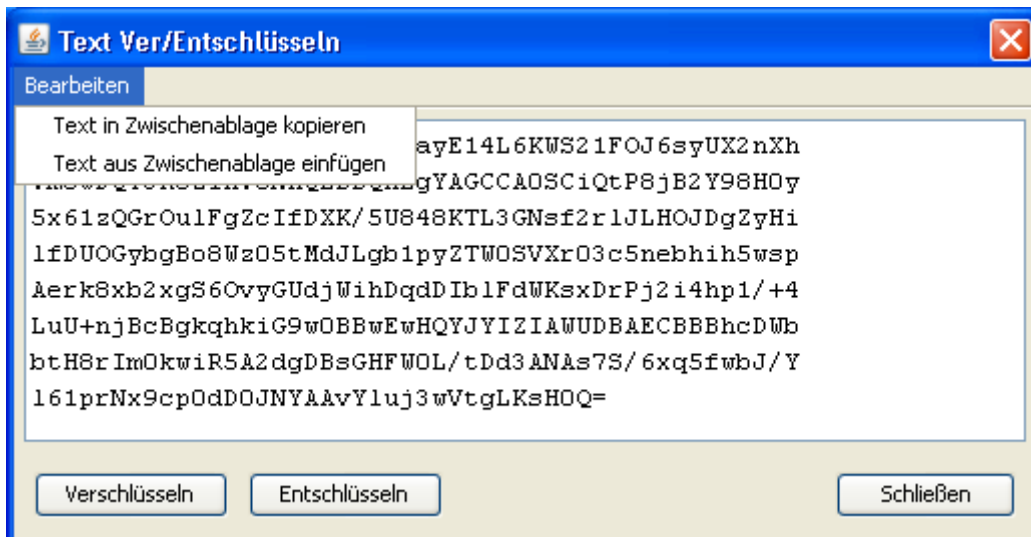


Der Ver- bzw. Entschlüsselungsvorgang verläuft wie bei einer Dateiverschlüsselung (siehe Abschnitt 2), wobei allerdings das Ergebnis nicht in einer Datei abgespeichert wird, sondern direkt im Editorfenster angezeigt wird. Von hier aus kann es z.B. in die Zwischenablage kopiert und in andere Dokumente (z.B. eine eMail) eingefügt werden.

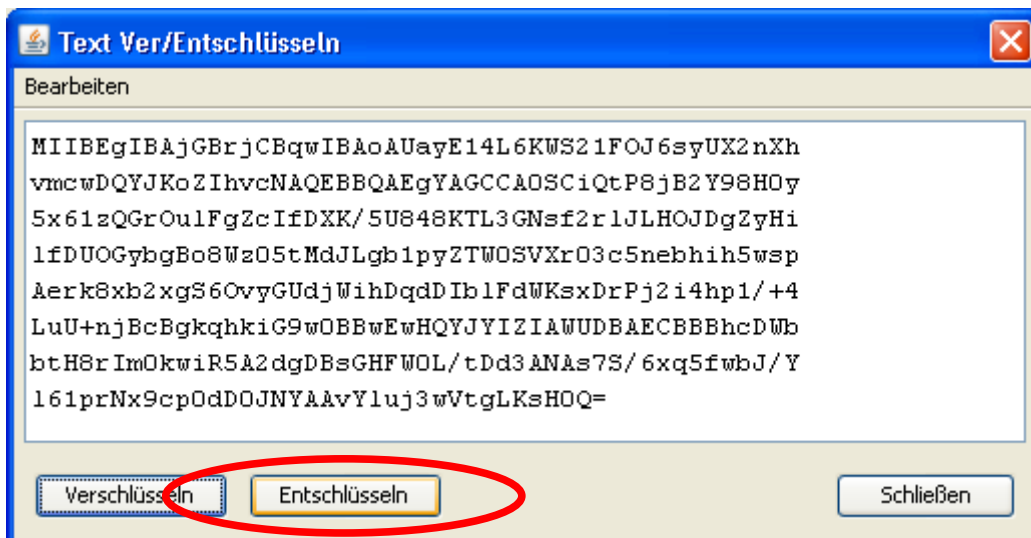
Eingabe eines Textes und **Verschlüsselung** durch Klick auf „Verschlüsseln“:



Der Geheimtext wird angezeigt und kann in die Zwischenablage kopiert werden:



Zur **Entschlüsselung** eines Textes muss vor dem Start von **PeDaS** eine SmartCard an den Rechner angeschlossen werden, mit dessen zugehörigen öffentlichen Schlüssel die Verschlüsselung erzeugt wurde.



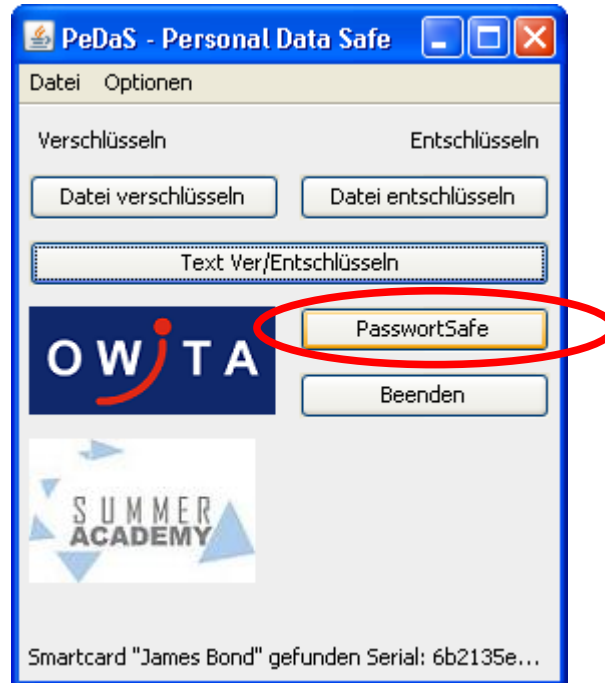
Nach Eingabe des PINs, mit dem der private Schlüssel auf der SmartCard geschützt ist



erscheint der Klartext im Editorfenster.

## 4 Der Passwort-Safe

Mit **PeDaS** können Sie auf Ihrem Rechner einen Passwort-Safe einrichten und zur sicheren Ablage von Pass- und Zugangskennwörtern nutzen. Hierzu klicken Sie auf „PasswortSafe“:



### 4.1 Einrichtung eines Passwort-Safes

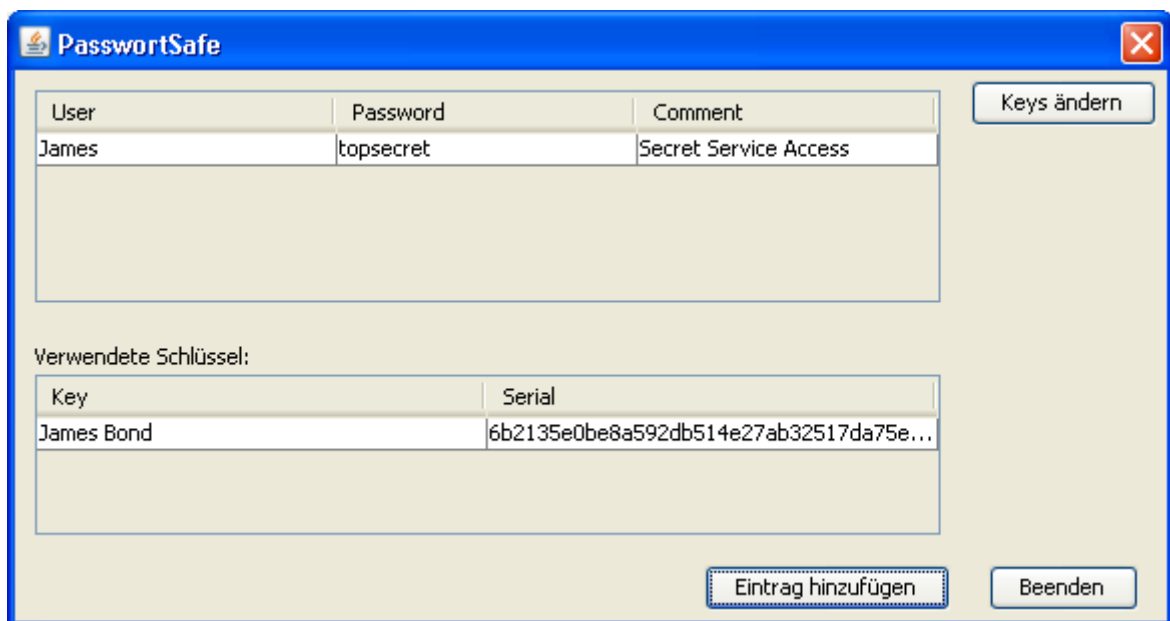
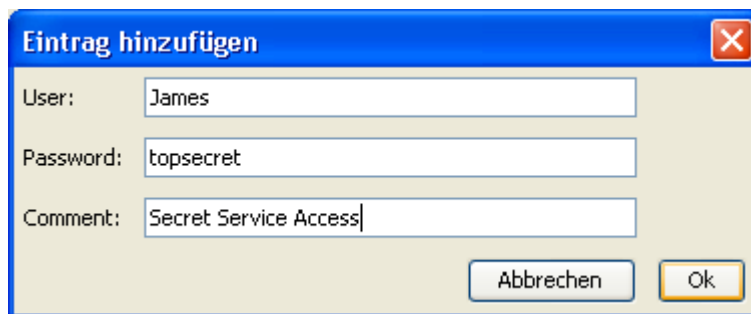
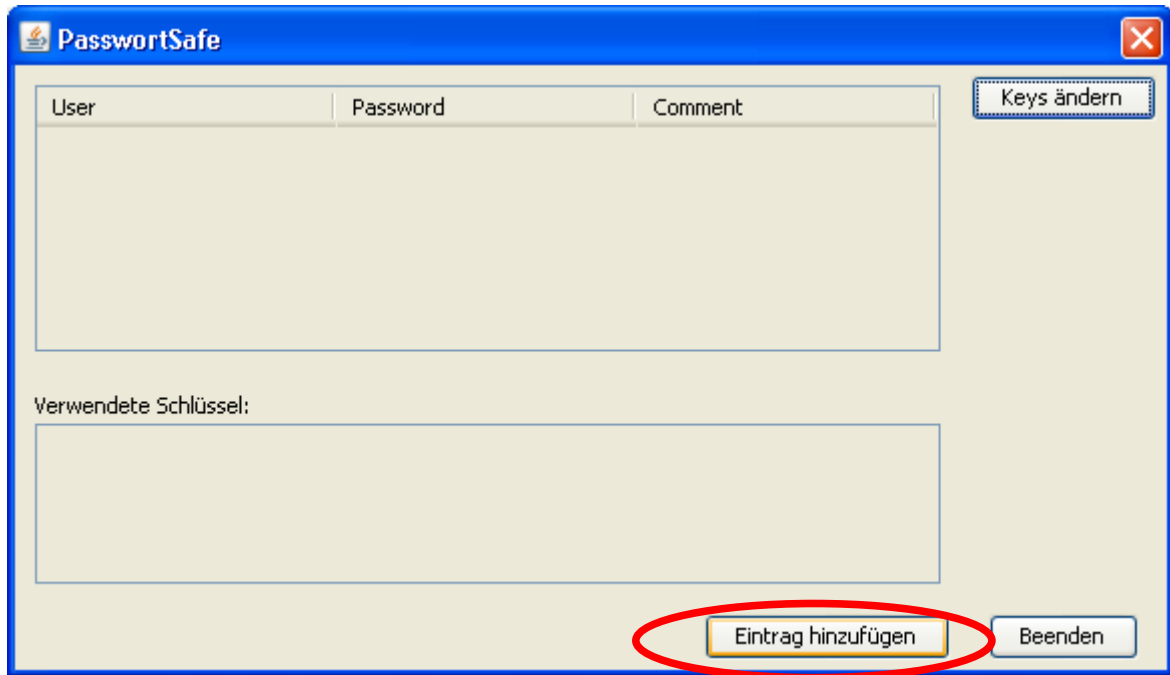
Da der Passwort-Safe mindestens einen Schlüssel (SmartCard) benötigt, wird zur Einrichtung des Passwort-Safes eine initialisierte SmartCard benötigt. Wird eine solche von **PeDaS** vorgefunden, so führt die erste Nutzung und Speicherung eines Passworteintrags zur automatischen Erzeugung des Passwort-Safes.

### 4.2 Passworteinträge zum Passwort-Safe hinzufügen

Nach dem Öffnen des Passwort-Safes können über einen Klick auf „Eintrag hinzufügen“ Passworteinträge dem Passwort-Safe hinzugefügt werden. Nach der Initialisierung des Passwort-Safes ist dies auch ohne SmartCard möglich. Hierbei werden weitere Einträge dem Passwort-Safe hinzugefügt, ohne dass diese allerdings angezeigt werden können, solange die SmartCard nicht zur Verfügung steht.

Nachfolgend abgebildete Screenshots illustrieren den Vorgang der ersten Nutzung des Passwort-Safes, der diesen durch Eintrag eines ersten Passwortes automatisch

initialisiert.



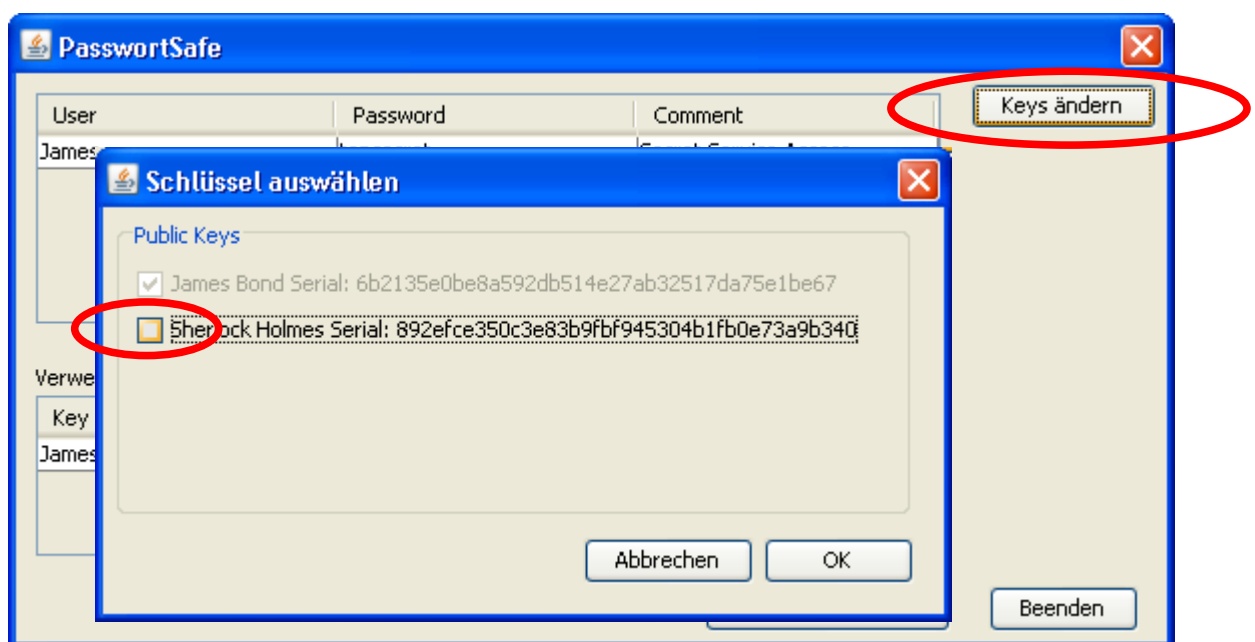
### 4.3 Schlüssel (SmartCards) für Passwort-Safe ändern

Die Schlüssel mit denen die Einträge des Passwort-Safes erstellt und durch Nutzung der entsprechenden SmartCards wieder lesbar gemacht werden können, können nach Initialisierung des Passwort-Safes verändert werden. Insbesondere ist es möglich, alle Einträge mit einem weiteren Schlüssel (Recovery-Schlüssel) zu verschlüsseln, so dass im Falle des Verlustes oder der Beschädigung einer SmartCard, der Passwort-Safe mit dieser zweiten Karte noch geöffnet werden kann.

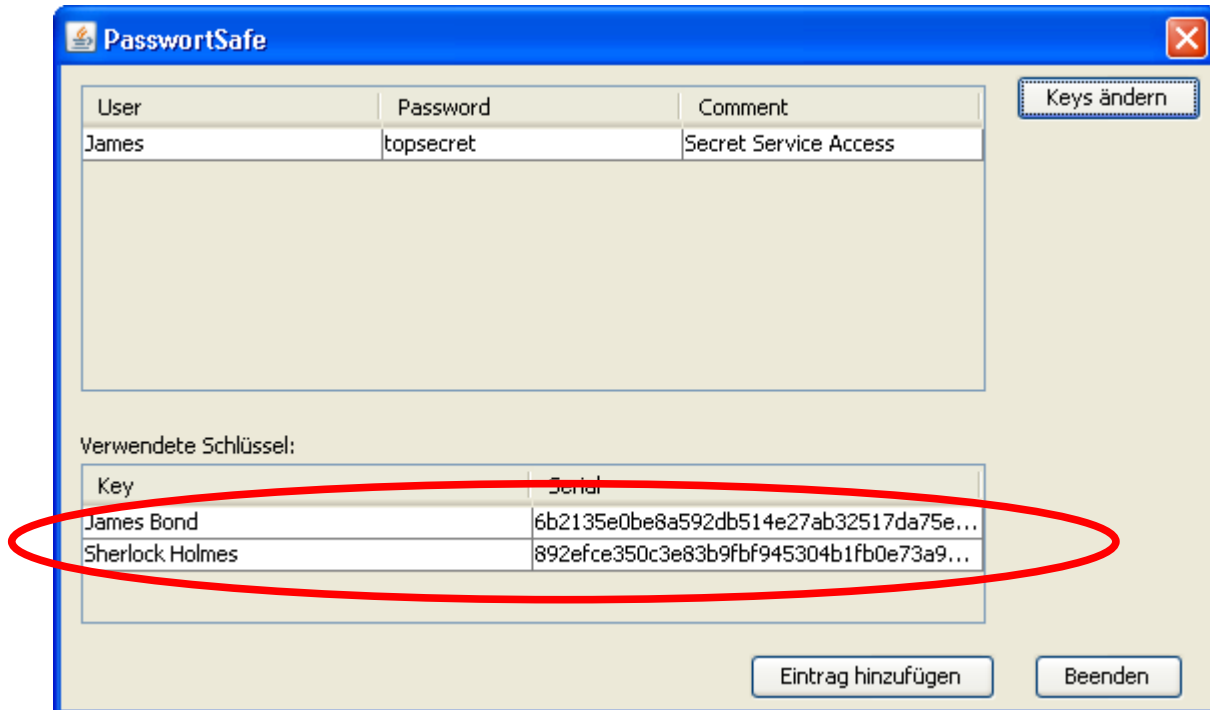
**Hinzufügen** eines weiteren Schlüsselpaars zur Nutzung des Passwort-Safes:

Zunächst benötigt **PeDaS** den öffentlichen Schlüssel des neuen Schlüsselpaars. Durch Initialisierung einer weiteren bisher nicht genutzten „leeren“ SmartCard, wird der öffentliche Schlüssel dieser SmartCard **PeDaS** automatisch hinzugefügt. Eine andere Möglichkeit ist durch den Import des öffentlichen Schlüssels einer bereits im Gebrauch befindlichen initialisierten Karte gegeben („Datei“ > „Öffentlichen Schlüssel Importieren“). Nun kann der Passwort-Safe mit Hilfe der gültigen SmartCard geöffnet werden und nach einem Klick auf „Keys ändern“ kann in dem nun erscheinenden Menü die Auswahl der zur Verschlüsselung selektierten Schlüssel geändert werden.

**Hinweis:** Der zur aktuell genutzten SmartCard gehörige Schlüssel kann nicht deselektiert werden. Damit wird sichergestellt, dass die zur Öffnung des Passwort-Safes zuletzt genutzte SmartCard auch bei der nächsten **PeDaS**-Nutzung noch den Passwort-Safe öffnet.



Nach der Auswahl eines oder mehrerer weiterer öffentlicher Schlüssel werden die Passworteinträge auch mit diesen verschlüsselt, und der Password-Safe kann auch mit den zugehörigen SmartCards verschlüsselt werden. Die benutzten Schlüssel werden im unteren Bereich des Passwort-Safes angezeigt:



## **5 Weitere Funktionen**

### **5.1 „Datei“ > „Öffentlichen Schlüssel Importieren“**

Mit dieser Funktion können Sie öffentliche Schlüssel, die als Datei vorliegen, nach **PeDaS** importieren. Anwendungsbeispiel: Sie erhalten den öffentlichen Schlüssel eines Partners und können nun z.B. Dateien, die Sie an diesen Partner senden wollen, mit **PeDaS** verschlüsseln.

### **5.2 „Datei“ > „Öffentlichen Schlüssel Exportieren“**

Mit dieser Funktion können Sie öffentliche Schlüssel, die bereits von Ihrer **PeDaS**-Anwendung verwaltet werden, als Datei exportieren.

### **5.3 „Optionen“ > „Standardschlüssel auswählen“**

Mit dieser Funktion können festlegen, welche öffentlichen Schlüssel bei dem Aufruf von Verschlüsselungsvorgängen („Datei verschlüsseln“ und „Text Ver/Entschlüsseln“ > „Verschlüsseln“) vorausgewählt werden.

### **5.4 „Optionen“ > „Pin ändern“**

Mit dieser Funktion können Sie die PIN der angeschlossenen SmartCard nach Eingabe der aktuell gültigen PIN ändern. Dies ist natürlich nur solange möglich, wie die Maximalzahl der zulässigen Fehlbedienungen nicht überschritten wurde.

### **5.5 „Optionen“ > „PasswortSafe löschen“**

Mit dieser Funktion wird der gesamte Passwort-Safe unwiederbringlich gelöscht. Anschließend kann ein Passwort-Safe, wie in Abschnitt 4 beschrieben, erneut angelegt werden.