GnuPGUI

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Überblick

Dieses Dokument beschreibt das Programm GnuPGUI der PVS Baden-Württemberg eG, daß auch in unserer Tochterfirma PVS HAG GmbH eingesetzt wird.

GnuPG steht dabei für **GNU P**rivacy **G**uard. Es handelt sich somit um ein freies (GNU-Lizenz) Kryptographiesystem. Die Buchstaben UI stehen dabei für User Interface. Somit stellt GnuPGUI eine von der PVS Baden-Württemberg eG für Windows-Systeme entwickelte Benutzeroberfläche zur Verfügung, um die Funktionen von GNU Privacy Guard nutzen zu können. Konkret wird die Software benötigt, wenn berechtigte Personen von der PVS HAG GmbH dem Datenschutz unterliegende Daten per Email erhalten möchten. Diese Daten werden von der PVS HAG ausschließlich in verschlüsselten Dateien versendet. Sowohl zum Erstellen der benötigten Schlüssel als auch zum Entschlüsseln der Dokumente wird eine GnuPG-Software benötigt. Selbstverständlich können auch andere erhältliche GnuPG-Software-Systeme verwendet werden, um von der PVS HAG verschlüsselte Dokumente erhalten zu können.

2 Funktionsweise des Verschlüsselungsverfahrens

GnuPG arbeitet mit Paaren von elektronischen Schlüsseln. Mit dem öffentlichen Schlüssel werden die Dateien verschlüsselt. Nur mit dem dazugehörenden privaten Schlüssel können die Dateien wieder entschlüsselt werden. Die beiden Schlüssel können nur gemeinsam in einer GnuPG- Software erstellt werden. Der öffentliche Schlüssel muss an den Ersteller der verschlüsselten Emails übertragen werden, während der private Schlüssel auf dem Rechner verbleibt und nicht über das Internet verschickt werden sollte, damit er nicht in falsche Hände gelangen kann.

3 Installation der GnuPGUI-Software

Die Software kann kostenlos von der Internetseite der PVS HAG GmbH http://www.hag-service.de/ herunterladen werden (im Bereich Downloads unter Aktuelles + Downloads). Auf Wunsch wird auch eine Installations-CD versendet. Durch Doppelklick

auf die heruntergeladene Datei bzw. durch Einlegen der CD startet das Installationsprogramm und installiert GnuPGUI in dem angegebenen Verzeichnis. Nach der Installation kann das Programm durch Doppelklick auf das folgende Symbol gestartet werden:  .

4 Der erste Start der GnuPGUI - Software

Nur beim ersten Start öffnet sich nach dem Bestätigen der Meldung, dass ein neuer Schlüssel erstellt werden muss, automatisch die Maske zur Neuerstellung eines Schlüsselpaares (nachfolgend nur noch Schlüssel genannt). Falls noch kein Schlüssel von einer vorigen Version vorhanden ist und auch kein, auf einem anderen Rechner erstellter, Schlüssel eingelesen werden soll, muss ein neuer Schlüssel erstellt werden (siehe Kapitel 6 Erstellen eines neuen Schlüssels auf Seite 9). Anschließend muss der öffentliche Teil des neuen Schlüssels an die PVS HAG GmbH übertragen werden (siehe Kapitel 7.1.2. Öffentlichen Schlüssel exportieren auf Seite 14). Auch das zugehörige Fingerabdruck-Dokument muss an die PVS HAG gesendet werden. Erst danach ist es für die PVS HAG möglich, verschlüsselte Emails an die im Schlüssel enthaltene Email-Adresse zu versenden.

5 GnuPGUI-Toolbox

Nach dem Start von GnuPGUI öffnet sich die Toolbox.

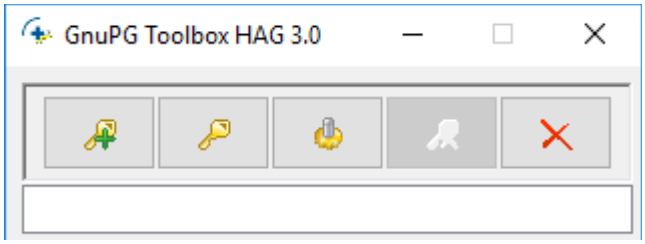


Abbildung 1: GnuPGUI-Toolbox

Sie hat folgende Auswahlfelder:

- Schlüssel erstellen 

- Schlüsselverwaltung 
- Einstellungen 
- Entschlüsseln  (inaktiv)
- Toolbox schließen 

Durch Klick auf eines der Felder öffnet sich die entsprechende Maske bzw. GnuPGUI wird beendet. Die einzelnen Masken sind nachfolgend beschrieben. Durch Auswahl des Fragezeichens  wird in allen Masken die Hilfe geöffnet.

6 Erstellen eines neuen Schlüssels 

Für jede Email-Adresse, an die verschlüsselte Emails verschickt werden sollen, muss **genau ein** Schlüssel angelegt werden. Unerheblich ist dabei, ob eine Email-Adresse für ein oder mehrere Konten bei der PVS HAG verwendet wird. Der Schlüssel ist immer an die angegebene Email-Adresse gebunden. Bei einer Änderung der Email-Adresse muss ein neuer Schlüssel erstellt werden.
Sollen Emails einer Email-Adresse an mehreren Rechnern entschlüsselt werden, dann darf nicht auf jedem Rechner für diese Email-Adresse ein eigener Schlüssel erstellt werden. In diesem Fall darf der Schlüssel nur an einem Rechner erstellt werden und muss auf die anderen Rechner übertragen werden. Siehe dazu die Beschreibung unter 10.2 Empfangen der verschlüsselten Mails mit gleicher Email-Adresse auf verschiedenen Rechnern auf Seite 31.
Soll für eine Email-Adresse ein neuer Schlüssel erstellt werden, obwohl bereits ein Schlüssel vorhanden ist (zum Beispiel, weil das Passwort vergessen wurde), dann muss der vorhandene Schlüssel gelöscht werden, da sonst der neue Schlüssel vom Programm nicht verwendet wird. Siehe dazu die Beschreibung unter 7.2.2 Löschen von Schlüsseln auf Seite 21.

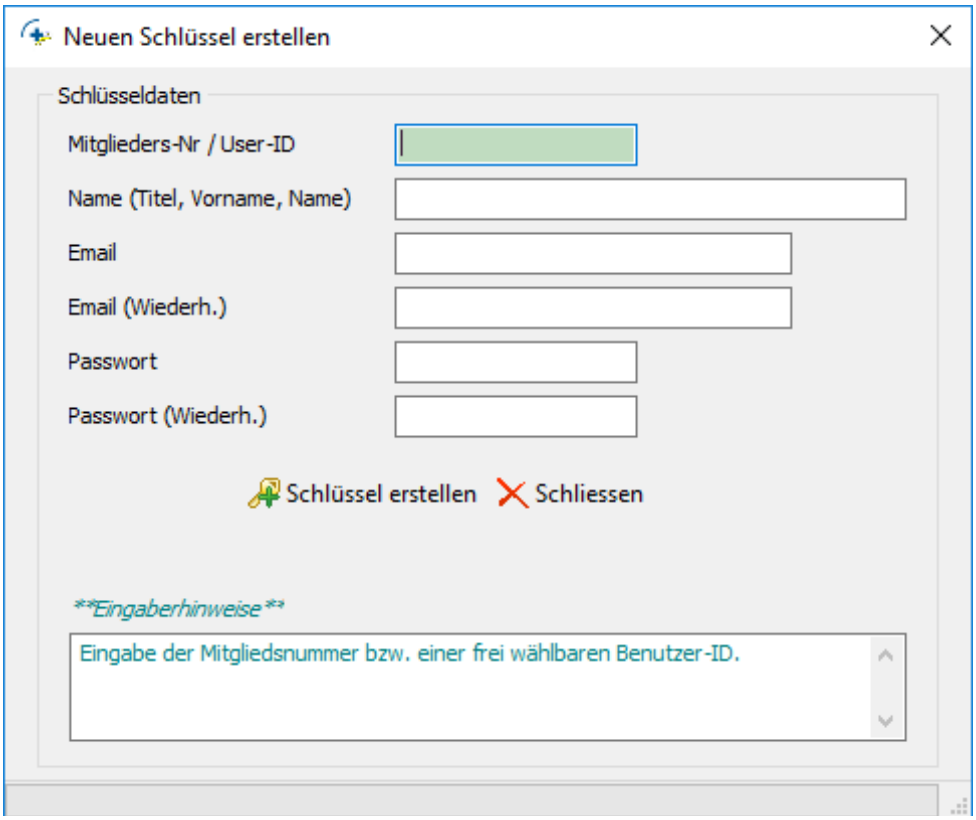


Abbildung 2: Maske zur Schlüsselerstellung

Um einen neuen Schlüssel zu erstellen, muss die oben angezeigte Maske ausgefüllt werden:

- **Mitglieds-Nr. / User-ID**: Hier soll die Mitgliedsnummer eingetragen werden. Falls mehrere Konten bei der PVS HAG dieselbe Email-Adresse verwenden, dann ist es ausreichend, wenn nur eine Mitgliedsnummer eingetragen wird, wenn möglich die Hauptnummer.
- **Name**: Name der Praxis oder des Krankenhauses.
- **Email und Wdh.**: Hier muss die Email-Adresse eingetragen werden, an die die verschlüsselten Dokumente gesendet werden. Da ein Fehler in der Email-Adresse dazu führt, dass die Dokumente nicht zugestellt werden können, muss die Eingabe wiederholt werden.
- **Passwort und Passwort Wiederholung**: Hier wird das Passwort eingegeben mit dem die verschlüsselten Dokumente wieder entschlüsselt werden können. Es dürfen keine Sonderzeichen oder deutsche Umlaute im Passwort verwendet

werden. Sollte das Passwort vergessen werden, dann können die mit diesem Schlüssel erzeugten Dokumente nicht mehr entschlüsselt werden. Das Auslesen des Passworts ist nicht möglich. Siehe dazu auch die Beschreibung in Kapitel 10.4 Passwort vergessen auf Seite 31.

Nach Auswahl von Schlüssel erstellen oder mit der Tastenkombination Strg + E wird der Schlüssel erstellt und das Fenster kann durch Auswahl von Schliessen oder mit der Tastenkombination Strg + X wieder geschlossen werden. Auf die Frage „Sollen die Schlüsselbunde gesichert werden?“ kann mit Ja geantwortet werden, wenn eine Sicherung erwünscht ist, sonst mit Nein. Eine Sicherung der Schlüssel ist auch im Einstellungsfenster möglich. Benötigt wird die Sicherung der Schlüssel zur Wiederherstellung auf einem anderen Rechner, zum Beispiel weil der Originalrechner defekt ist oder weil die Emails auch auf einem anderen Rechner entschlüsselt werden sollen.

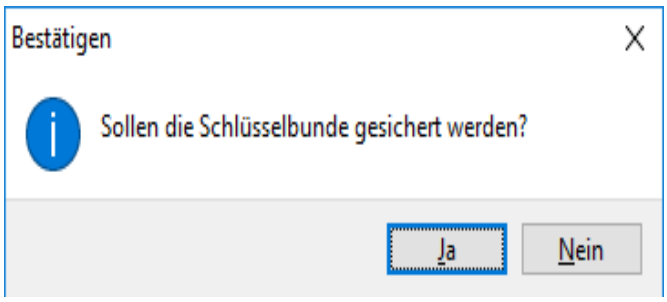


Abbildung 3: Mögliche Sicherung der Schlüssel nach der Erstellung

Danach muss der neue Schlüssel und das zugehörige Fingerabdruck-Dokument an die PVS HAG übertragen werden. Siehe dazu Kapitel 7.1.2 Öffentlichen Schlüssel exportieren auf Seite 14.

7 Schlüsselverwaltung

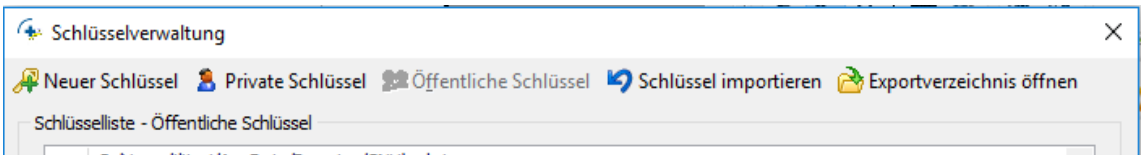


Abbildung 4: Auswahlmenü der Schlüsselverwaltung

In der Schlüsselverwaltung werden die öffentlichen und privaten Schlüssel angezeigt. Es ist möglich, Schlüssel an die PVS HAG zu übertragen oder Schlüssel zu löschen. Auch können zuvor gesicherte Schlüssel importiert werden. Das Passwort einzelner Schlüssel kann geändert werden. Das von der PVS HAG benötigte Fingerabdruck-Dokument kann hier ebenfalls gedruckt werden. Über das Menü der Schlüsselverwaltung können folgende Punkte aufgerufen werden:

- Neuer Schlüssel (wurde bereits zuvor beschrieben)
- Öffentliche Schlüssel (siehe Kapitel 7.1)
- Private Schlüssel (siehe Kapitel 7.2)
- Schlüssel importieren (siehe Kapitel 7.3)
- Exportverzeichnis öffnen (siehe Kapitel 7.4)
- Hilfe zur Schlüsselverwaltung

7.1 Schlüsselliste öffentliche Schlüssel

Beim Öffnen der Schlüsselverwaltung öffnet sich zunächst die Schlüsselliste der öffentlichen Schlüssel.

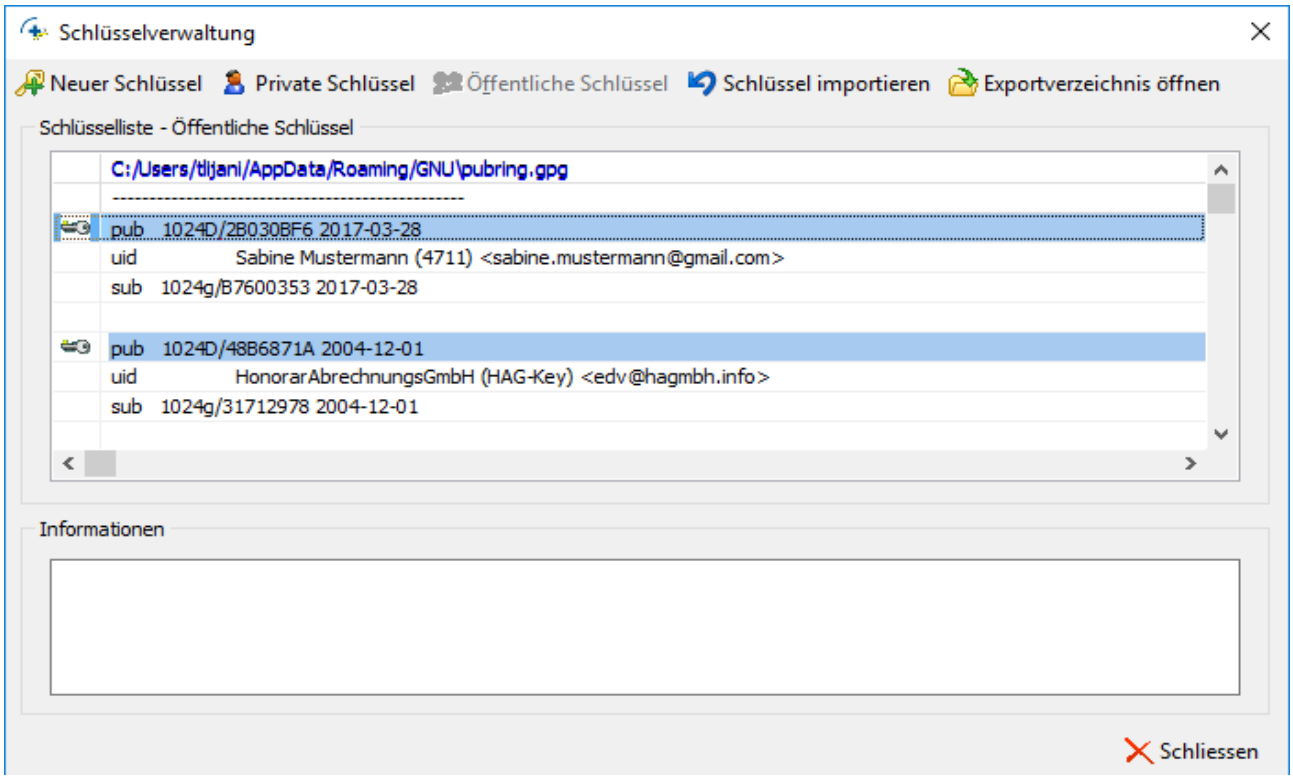


Abbildung 5: Schlüsselliste öffentliche Schlüssel

In Abbildung 5 ist ein Beispiel für eine Schlüsselliste der öffentlichen Schlüssel zu sehen. Der Schlüssel der PVS HAG GmbH ist bereits im Lieferumfang der Software enthalten. Weitere Schlüssel werden automatisch bei der Erstellung eines Schlüssels eingetragen. In der ersten Zeile der Schlüsselliste ist der Name und Speicherort der Datei mit allen öffentlichen Schlüsseln eingetragen. Danach folgen nach einer Leerzeile die Einträge für jeden vorhandenen öffentlichen Schlüssel. Jeder Beginn eines Schlüsseleintrags ist durch das Schlüsselsymbol in der linken Spalte und durch die blaue Markierung gekennzeichnet. Diese Zeile enthält die ID des Schlüssels nach dem Zeichen „/“ und das Erstellungsdatum. In der folgenden Zeile ist der Name, Mitgliedsnummer und die Email-Adresse, wie bei der Schlüsselerstellung festgelegt, angegeben. Durch Rechtsklick mit der Maus auf der hellblauen Zeile öffnet sich ein Kontextmenü zum Schlüssel.

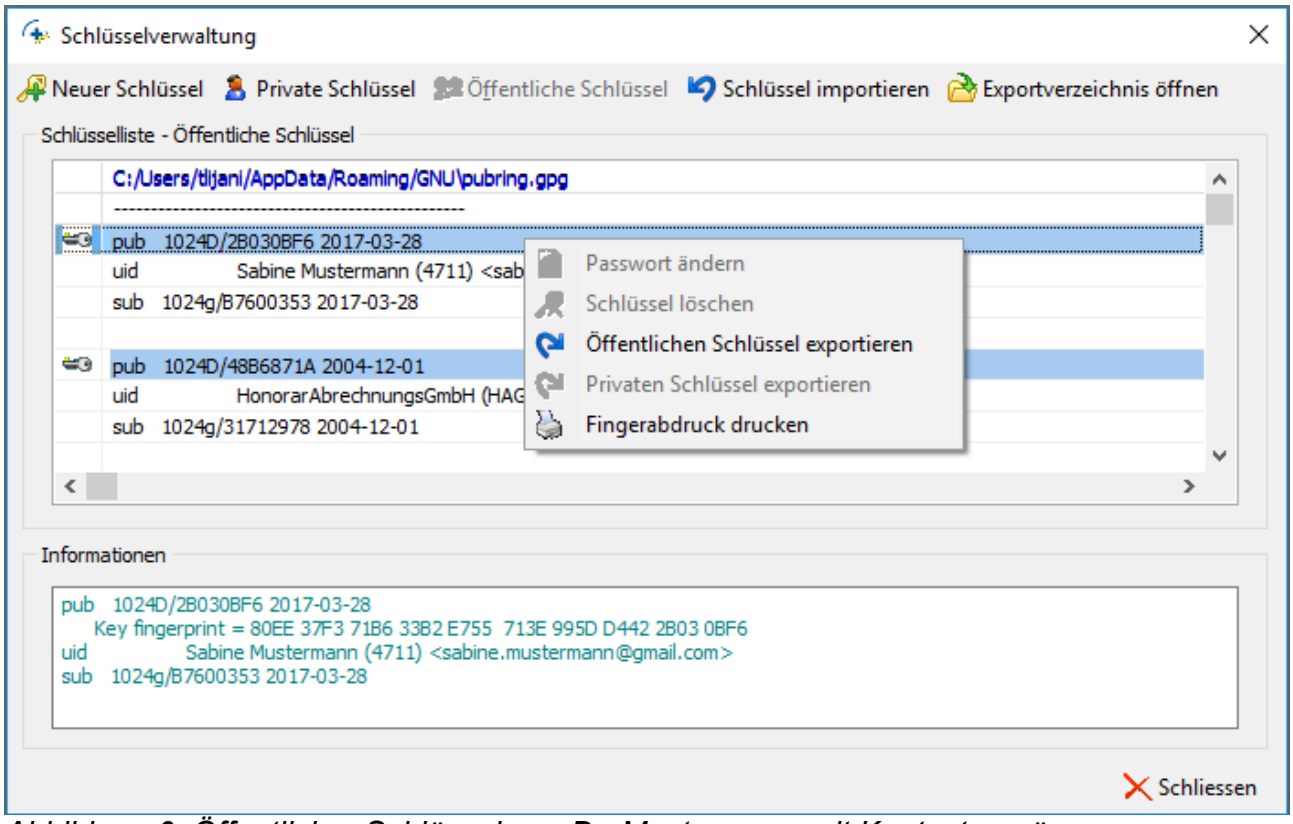


Abbildung 6: Öffentlicher Schlüssel von Dr. Mustermann mit Kontextmenü

In der Schlüsselliste der öffentlichen Schlüssel sind nur drei der fünf Einträge des Kontextmenüs aktiv. Es ist möglich, den öffentlichen Schlüssel zu löschen, den öffentlichen Schlüssel zu exportieren oder einen Fingerabdruck zu drucken.

7.1.1 Öffentlichen Schlüssel löschen

Es wird nicht empfohlen über diesen Menüpunkt nur den öffentlichen Schlüssel zu löschen. Zur Löschung eines Schlüsselpaares sollte dieser Menüpunkt in der Liste der privaten Schlüssel aufgerufen werden. Der öffentliche Schlüssel der PVS HAG kann nicht gelöscht werden.

7.1.2 Öffentlichen Schlüssel exportieren

Damit der öffentliche Schlüssel von der PVS HAG GmbH zur Verschlüsselung von Dokumenten verwendet werden kann, muss er an die PVS HAG übermittelt werden. Dazu kann der Schlüssel aus dem Programm exportiert und direkt über das Internet an die PVS

HAG übertragen oder als Datei abgespeichert und in einer Email als Anhang an die PVS HAG gesendet werden. Durch Auswahl von „öffentlichen Schlüssel exportieren“ im Kontextmenü öffnet sich ein Fenster zur Auswahl.

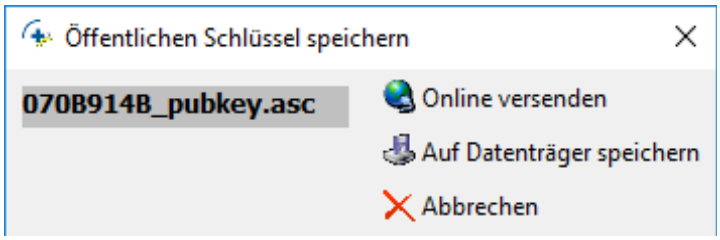


Abbildung 7: Fenster zum Export und Speichern des öffentlichen Schlüssels

Durch Auswahl von Online versenden wird der Schlüssel direkt an die PVS HAG GmbH versendet. Sollte das nicht möglich sein, weil zum Beispiel aktuell kein Internet zur Verfügung steht oder weil in einer komplexen Software-Umgebung der direkte Versand von Dateien aus Programmen heraus nicht zugelassen ist, dann sollte der Punkt Auf Datenträger speichern ausgewählt werden. In der folgenden Maske kann ein Speicherort ausgewählt werden.

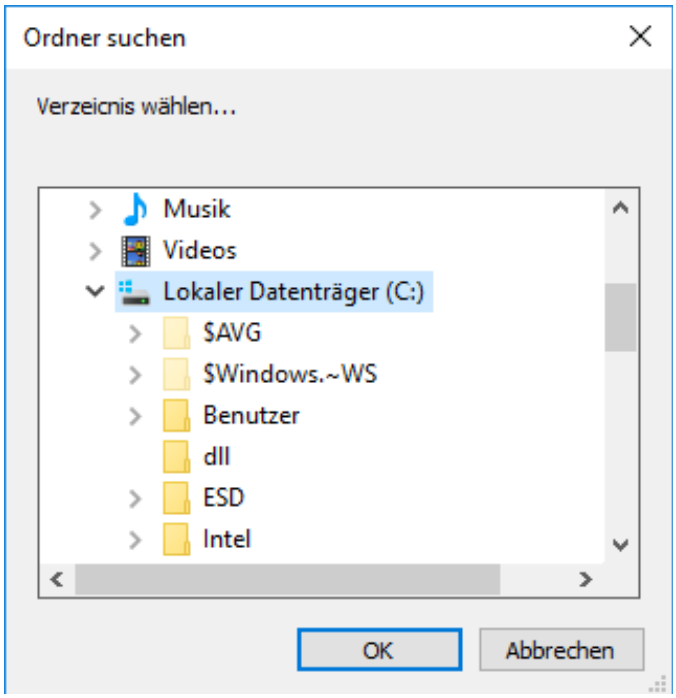


Abbildung 8: Auswahl des Speicherortes beim Speichern des öffentlichen Schlüssels

Nach Auswahl von OK wird die Datei mit dem öffentlichen Schlüssel abgespeichert.

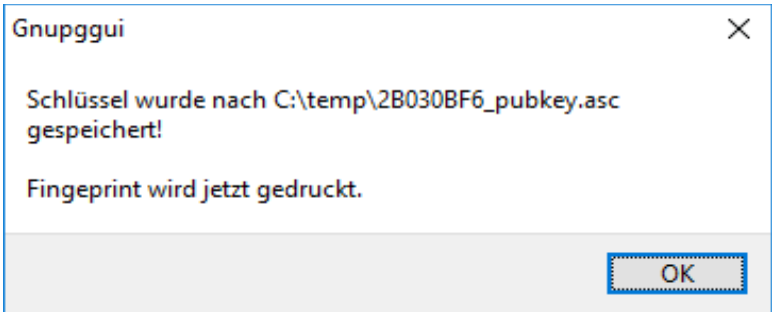


Abbildung 9: Bestätigung der Speicherung des öffentlichen Schlüssels

Die angegebene Datei kann anschließend als Anhang einer Email an edv@hag-service.de gesendet werden.

Sowohl nach dem direkten Versenden des öffentlichen Schlüssels als auch nach dem Abspeichern in einer Datei wird direkt das sogenannte Fingerabdruck-Dokument zum Ausdruck angezeigt.

Abbildung 10: Fingerabdruck-Dokument

Durch Auswahl des Drucksymbols wird das Dokument auf dem Standarddrucker

gedruckt. Andere Druckeinstellungen können über das Symbol  eingestellt werden. Das Dokument muss von demjenigen, der berechtigt ist verschlüsselte Dokumente (zum Beispiel Kontoauszüge) zu erhalten, unterschrieben und mit einem Praxisstempel versehen werden. Anschließend kann das Dokument an die PVS HAG per Fax oder Post gesendet werden. Die Faxnummer ist oben auf dem Dokument aufgedruckt.

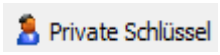
Das Fingerabdruck-Dokument ist für die PVS HAG die Bestätigung, dass der Schlüssel von einer für das jeweilige Mitgliedskonto berechtigten Person ausgestellt wurde.

Sobald die Schlüsseldatei und das Fingerabdruck-Dokument bei der PVS HAG eingegangen ist, wird der Schlüssel eingelesen und ein verschlüsseltes Testdokument versendet.

7.1.3 Fingerabdruck-Dokument drucken

Das Fingerabdruck-Dokument kann direkt nach dem Exportieren (siehe Kapitel 7.1.2 auf Seite 14), und über das Kontextmenü der Liste der öffentlichen Schlüssel aufgerufen werden. Zur Beschreibung siehe Kapitel 7.1.2..

7.2 Schlüsselliste private Schlüssel

Durch Auswahl von 

in der Schlüsselverwaltung wird die Liste der privaten Schlüssel geöffnet.

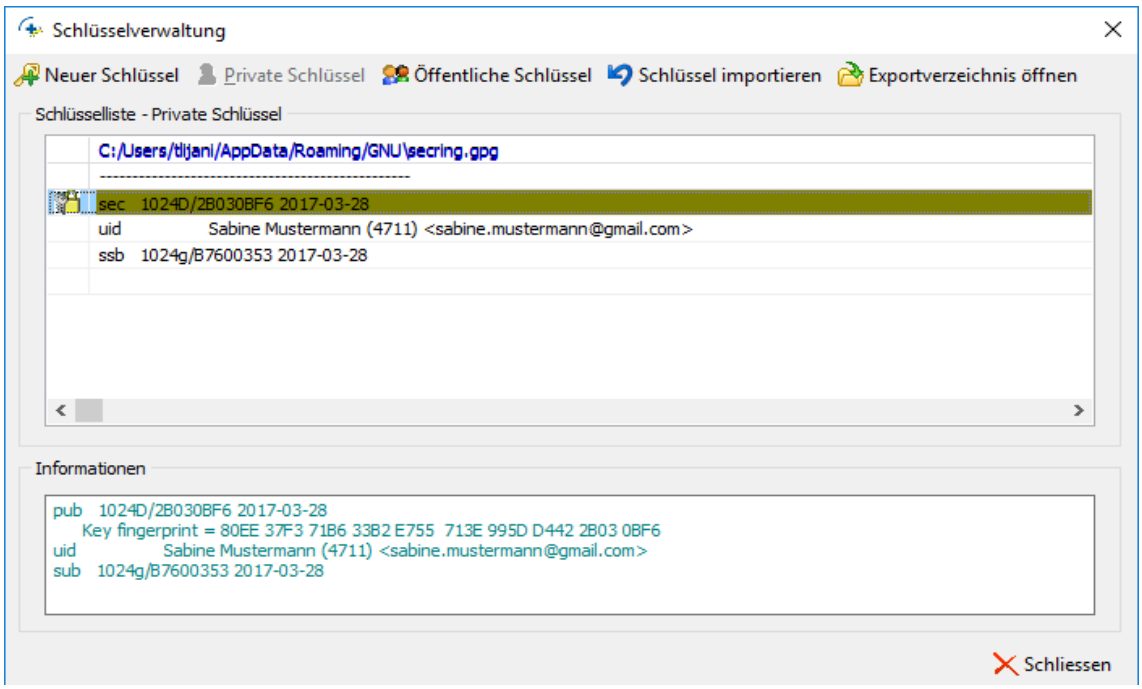


Abbildung 11: Schlüsselliste der privaten Schlüssel

Für jeden selbst erstellten Schlüssel existiert ein privater Schlüssel, der vom Programm zum Entschlüsseln von Dokumenten benötigt wird, die zuvor mit dem passenden öffentlichen Schlüssel verschlüsselt wurden. In der ersten Zeile der Liste ist der Name und Speicherort der Datei angegeben, die die privaten Schlüssel enthält. Danach folgt die Liste der privaten Schlüssel. Die erste Zeile eines privaten Schlüssels ist durch ein Schloss-Symbol und eine farbige Markierung gekennzeichnet.

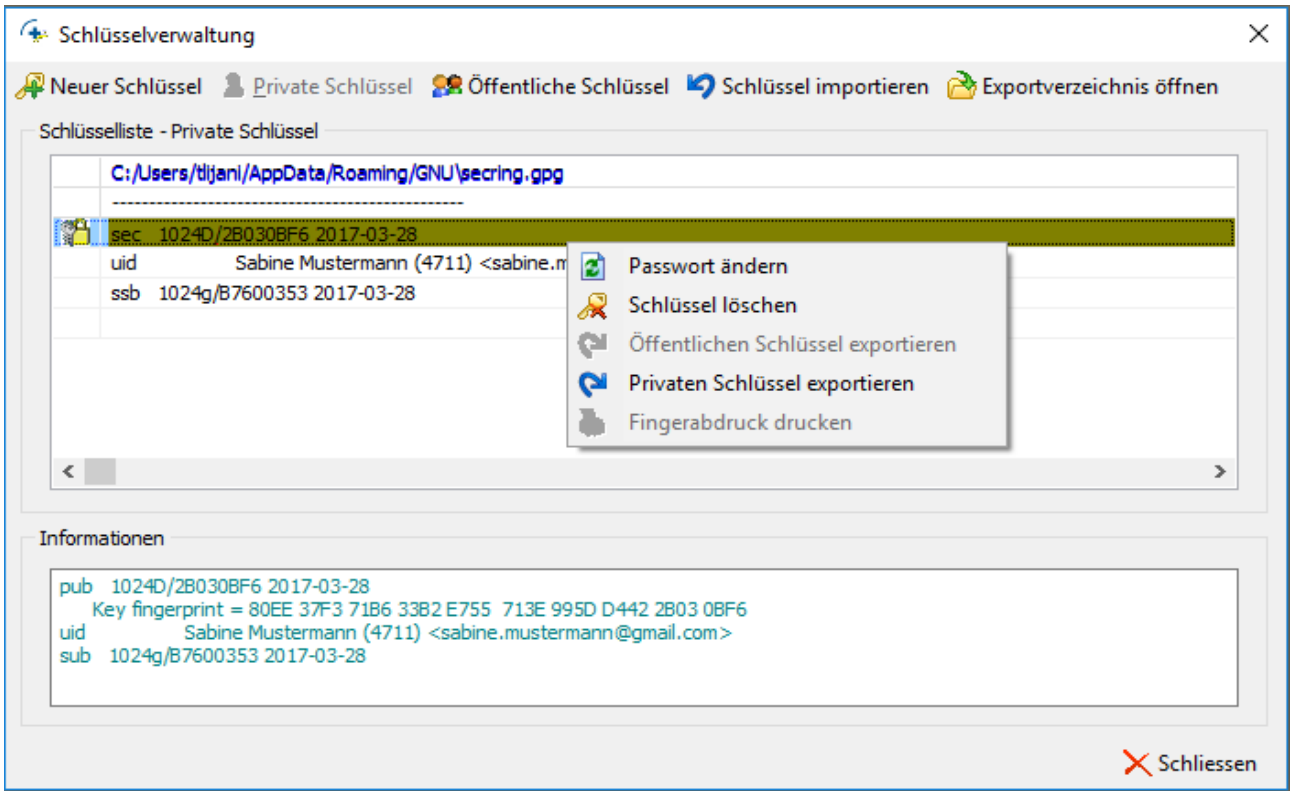


Abbildung 12: Privater Schlüssel von Dr. Mustermann mit Kontextmenü

Durch Rechtsklick auf die farbige Zeile eines Schlüssels öffnet sich ein Kontextmenü.

In der Schlüsselliste der privaten Schlüssel sind drei der fünf Einträge des Kontextmenüs aktiv. Es ist möglich, das Passwort zu ändern, den Schlüssel zu löschen und den privaten Schlüssel zu exportieren.

7.2.1 Passwort ändern

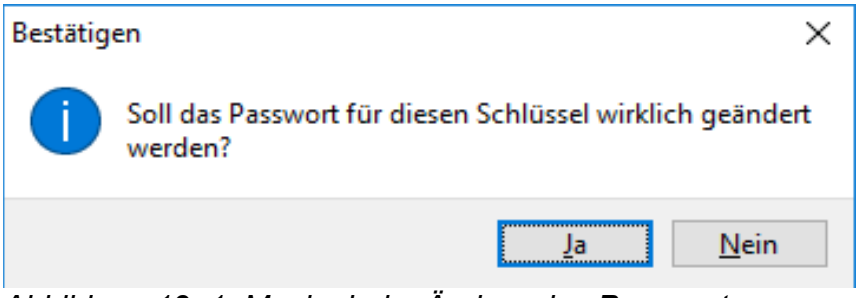


Abbildung 13: 1. Maske beim Ändern des Passworts

Nach der Auswahl von „Passwort ändern“ und Auswahl von „Ja“ bei der Nachfrage, ob das Passwort wirklich geändert werden soll, und der Bestätigung des nachfolgenden

Hinweises mit einer Beschreibung des Passwort-Änderungs-Vorgangs öffnet sich die Maske zur Änderung des Entschlüsselung-Passworts.

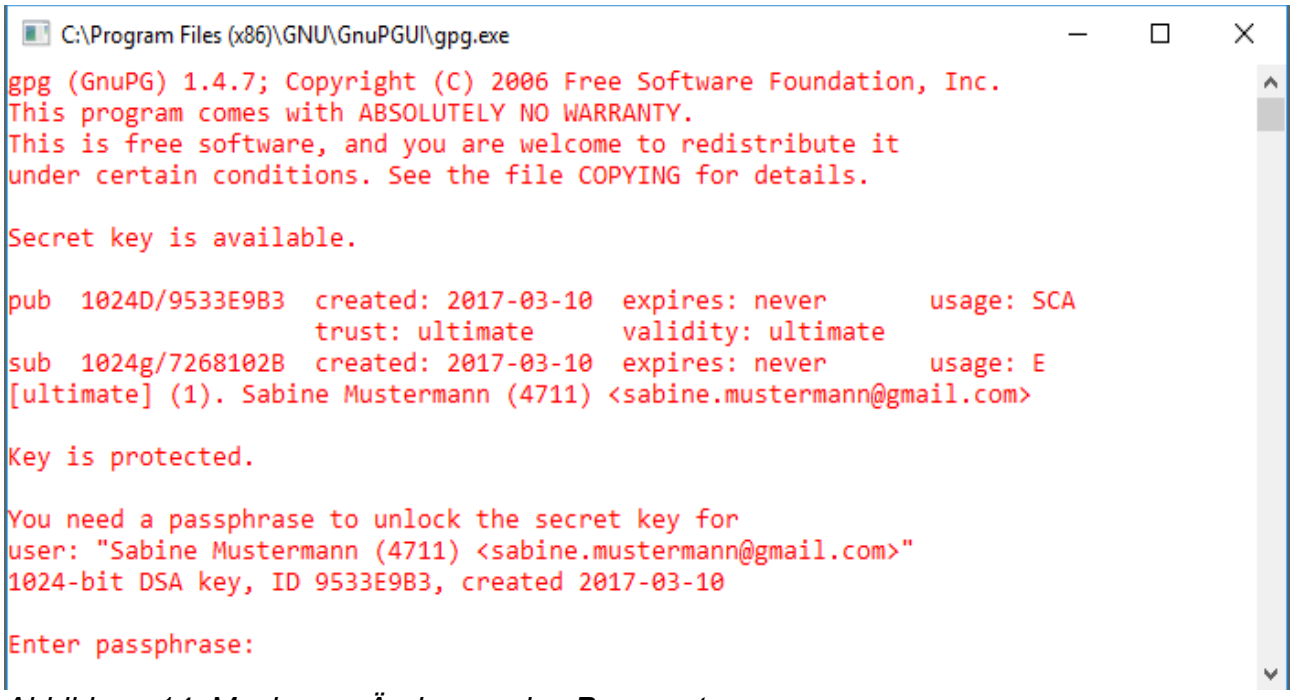


Abbildung 14: Maske zur Änderung des Passworts

Zunächst muss einmal das aktuelle Passwort und anschließend zweimal das neue Passwort eingegeben werden. Das Passwort muss mindestens acht Zeichen enthalten und darf keine Leerzeichen oder deutsche Umlaute enthalten. Jede Eingabe muss mit der Enter-Taste ↵ abgeschlossen werden. Bei der Eingabe des alten bzw. des neuen Passworts ist keine Tastenbewegung sichtbar. Die Zeichen werden aber dennoch vom Programm angenommen. Nachdem das neue Passwort zweimal eingegeben wurde, muss die Sequenz durch Eingabe des Befehls save und anschließend der Enter-Taste ↵ abgeschlossen werden. Daraufhin wird das Fenster automatisch geschlossen und das Passwort wurde geändert. Dokumente, die mit diesem Schlüssel verschlüsselt wurden, können nur noch mit dem neuen Passwort entschlüsselt werden.

Wird das Fenster geschlossen ohne den abschließenden Befehl save, dann wird das Passwort nicht geändert.

7.2.2 Löschen von Schlüsseln

Schlüssel, die nicht mehr benötigt werden, sollten gelöscht werden. Auch Schlüssel, bei denen das Passwort nicht mehr bekannt ist, sollten gelöscht werden, da sie nicht mehr verwendet werden können.

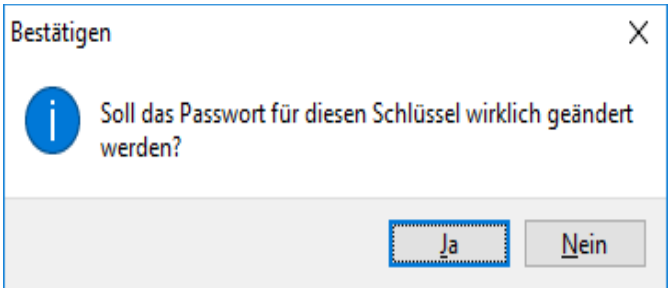


Abbildung 15: Sicherheitsabfrage beim Löschen von Schlüsseln

Nach der Auswahl von „Schlüssel löschen“ und der Bestätigung der Sicherheitsabfrage mit „Ja“ öffnet sich die Maske zum Löschen von Schlüsseln.

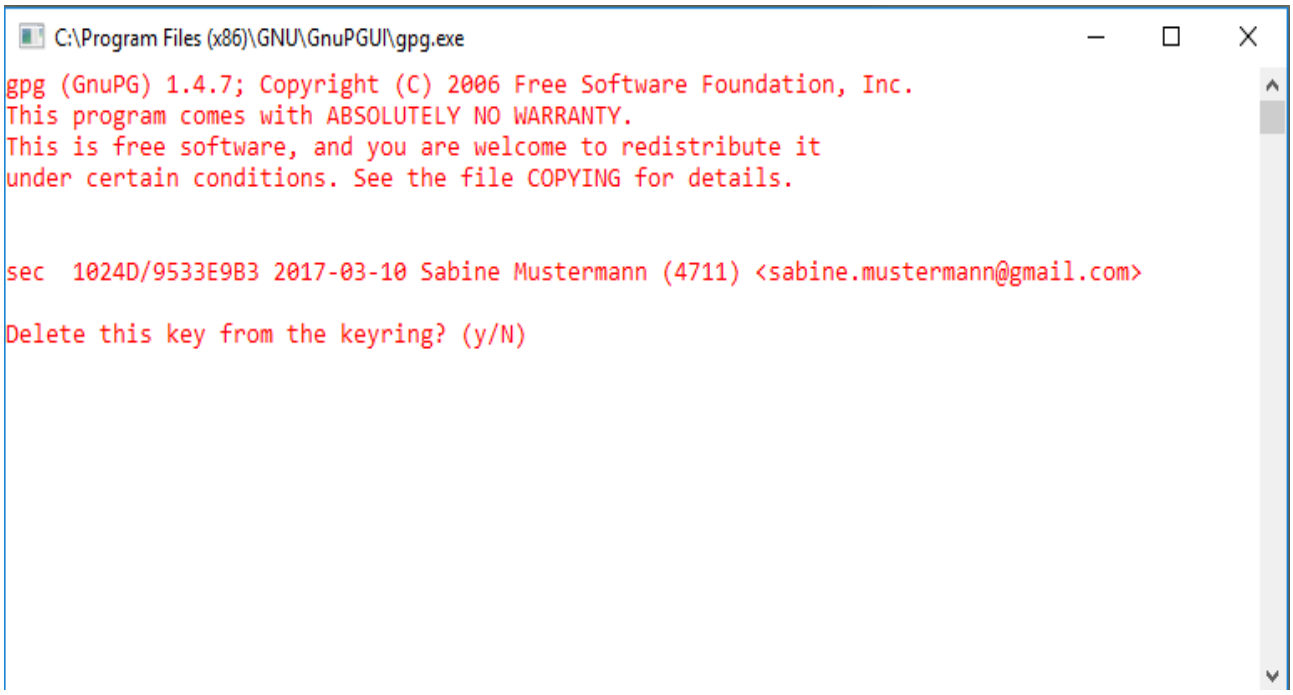


Abbildung 16: Maske zum Löschen von Schlüsseln

Durch zweimalige Eingabe von „y“ und jeweils anschließend der Enter-Taste ↵ wird der

ausgewählte Schlüssel gelöscht. Es wird dabei sowohl der öffentliche als auch der private Schlüssel gelöscht. Dateien, die mit dem gelöschten Schlüssel verschlüsselt wurden, können anschließend nicht mehr entschlüsselt werden. Dateien, die von der PVS HAG in einer verschlüsselten Mail verschickt wurden, können aber jederzeit mit einem neuen Schlüssel wieder verschlüsselt und erneut versendet werden.

7.2.3 Privaten Schlüssel exportieren

Der Export von privaten Schlüsseln dient ausschließlich zu Sicherungszwecken. Private Schlüssel dürfen nicht weitergegeben werden, da sonst anderen Personen die Möglichkeit gegeben wird, Dokumente, die mit diesem Schlüssel verschlüsselt wurden, zu entschlüsseln. Aus diesem Grund kann die Schlüsseldatei ausschließlich auf einem Datenträger abgespeichert werden.

Durch Auswahl von „Privaten Schlüssel exportieren“ im Kontextmenü der privaten Schlüsselliste öffnet sich ein Dialog zur Auswahl des Speicherortes. Nach Auswahl eines Verzeichnisses und Bestätigung mit OK wird die Datei im gewählten Verzeichnis gespeichert. Beim Exportieren des privaten Schlüssels wird immer auch der zugehörige öffentliche Schlüssel gesichert, während beim Exportieren des öffentlichen Schlüssels nur der öffentliche Schlüssel ausgegeben wird.

7.3 Schlüssel importieren

Durch Auswahl von 

in der Schlüsselverwaltung können zuvor gesicherte Schlüsseldateien wieder eingelesen werden. Über diese Funktion werden einzelne Schlüssel eingelesen, die über die Schlüsselliste der öffentlichen oder privaten Schlüssel exportiert wurden. Die Möglichkeit einzelne Schlüssel zu sichern und wiederherzustellen, wird benötigt, wenn auf einem Rechner einzelne Schlüssel eines anderen Rechners benötigt werden. Vorhandene Schlüssel werden dabei nicht verändert. Zur Sicherung und Wiederherstellung aller Schlüssel siehe auch Kapitel 8.1 Schlüsseldateien auf Seite 23.

7.4 Exportverzeichnis öffnen

Im Exportverzeichnis werden alle exportierten Schlüsseldateien abgespeichert. Sie

werden dort immer zusätzlich zum gewählten Ausgabeort abgelegt. Durch Auswahl dieses Punktes in der Schlüsselverwaltung wird das Verzeichnis geöffnet und angezeigt.

8 Einstellungen

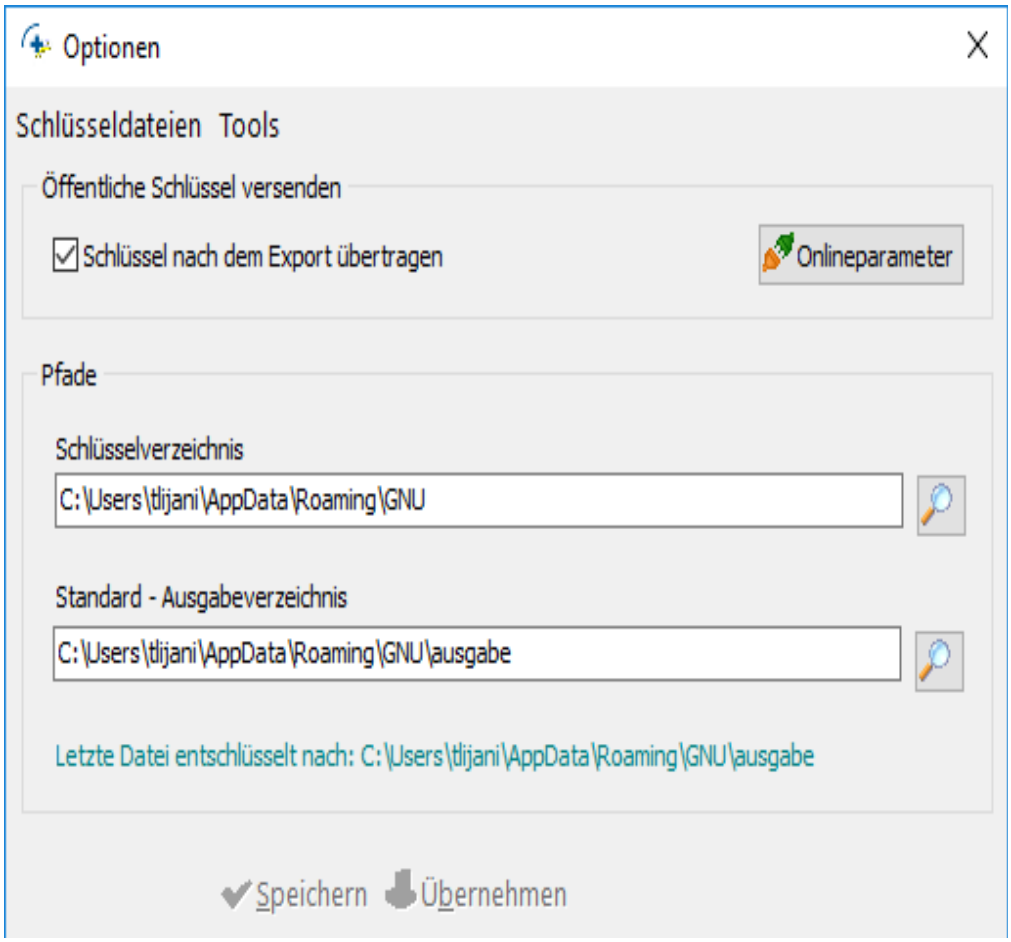


Abbildung 17: Maske Einstellungen

Die Einstellungen können über das Symbol direkt aus der GnuPGUI-Toolbox heraus aufgerufen werden. Sie ermöglichen zum Beispiel das Sichern und Wiederherstellen von Schlüsseldateien und das Setzen einiger Einstellungen, die nachfolgend beschrieben sind.

8.1 Schlüsseldateien

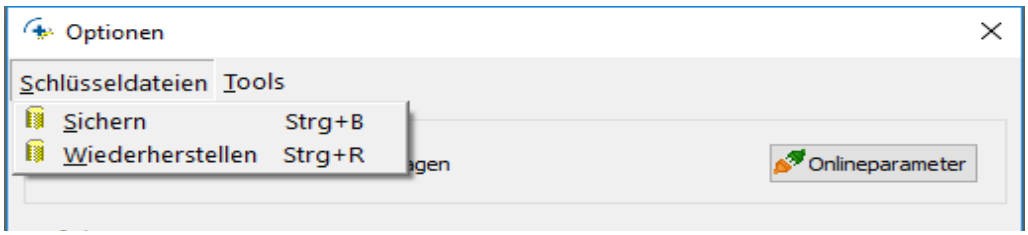


Abbildung 18: Menüpunkt Schlüsseldateien in der Maske Einstellungen

Durch Auswahl von Schlüsseldateien in der Maske Einstellungen öffnet sich ein Untermenü mit den beiden Punkten Sichern und Wiederherstellen.

8.1.1 Schlüsseldateien sichern

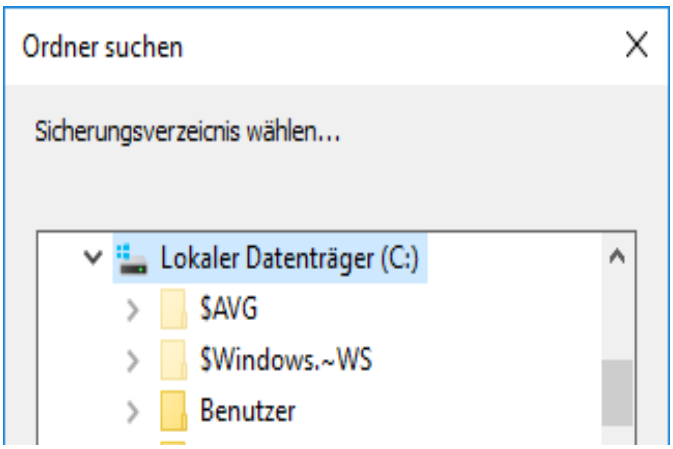


Abbildung 19: Auswahl des Sicherungsortes

Über diesen Menüpunkt können alle Schlüssel durch einen Befehl gesichert werden. Eine Sicherung einzelner Schlüssel ist nur über die Schlüsselverwaltung möglich. Am gewählten Speicherort werden die drei Dateien „pubring.gpg“, „secring.gpg“ und „trustdb.gpg“ erstellt. Diese Dateien werden benötigt um alle gesicherten Schlüssel auf einem anderen Rechner oder auf demselben Rechner nach einem Verlust der Schlüssel wiederherzustellen.

8.1.2 Schlüsseldateien wiederherstellen

Nach der Auswahl des Speicherortes, der die gesicherten Schlüsseldateien enthält, werden die in den Dateien enthaltenen Schlüssel wieder hergestellt. Sind bereits

Schlüssel im Programm vorhanden, werden diese durch die Wiederherstellung aus den Sicherungsdateien gelöscht. Daher wird bei bereits vorhandenen Schlüsseln bei jeder Datei nachgefragt, ob die vorhandenen Schlüssel überschrieben werden sollen. Nur bei Antwort von „Ja“ werden die gesicherten Schlüssel erstellt und die vorhandenen Schlüssel gelöscht.

8.2 Tools

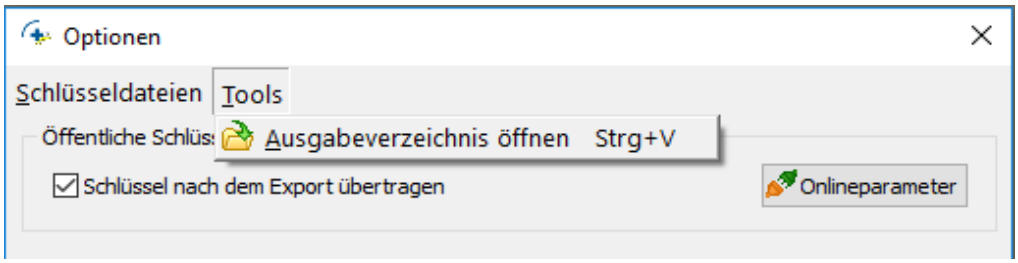


Abbildung 20: Menüpunkt Tools in der Maske Einstellungen

Durch Auswahl von Tools in der Maske Einstellungen öffnet sich ein Untermenü mit dem Punkt „Ausgabeverzeichnis öffnen“.

8.2.1 Ausgabeverzeichnis öffnen

Durch Auswahl von „Ausgabeverzeichnis öffnen“ öffnet sich das im Programm voreingestellte Standard-Ausgabeverzeichnis (siehe Kapitel 8.4 Ändern von Pfaden). In diesem Verzeichnis werden alle entschlüsselten Dateien abgespeichert, wenn bei der Entschlüsselung kein anderes Verzeichnis angegeben wird. Sie können daher aus diesem Verzeichnis ohne erneute Entschlüsselung wieder geöffnet werden.

8.3 Einstellungen beim Versenden von Schlüsseln

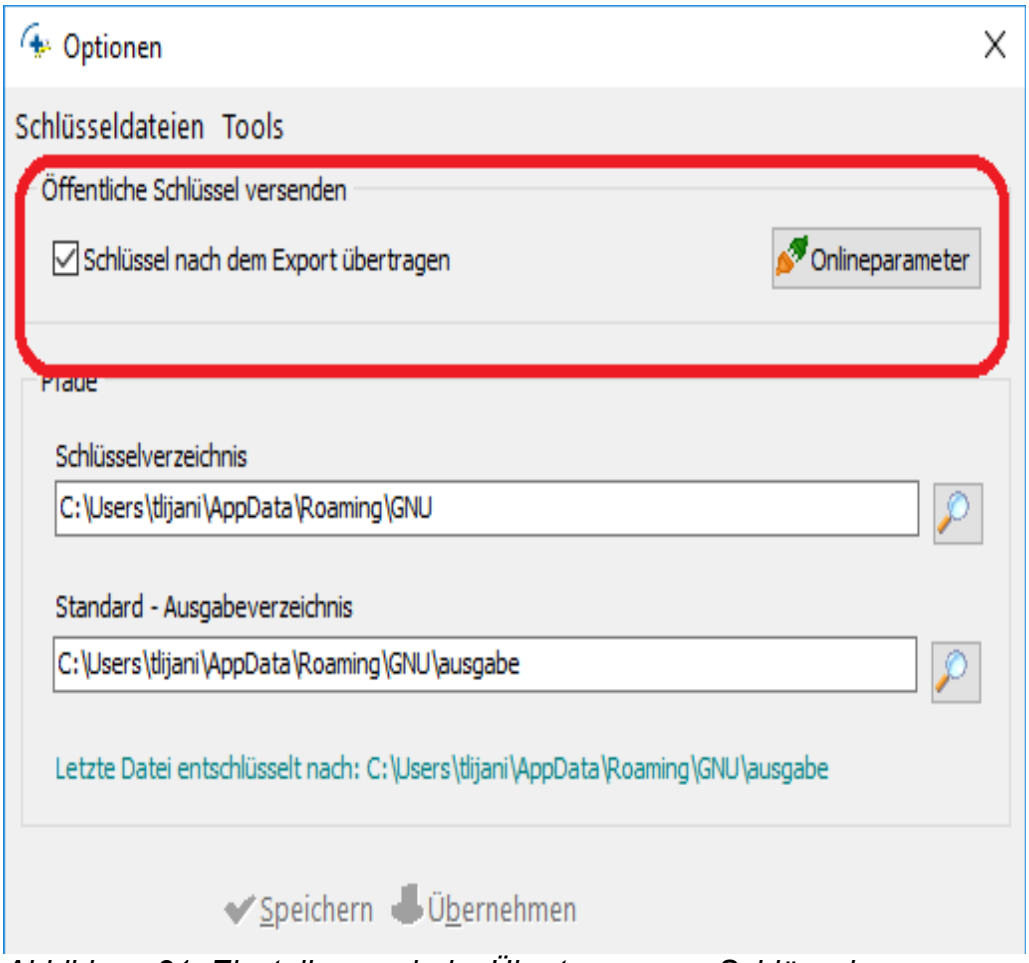


Abbildung 21: Einstellungen beim Übertragen von Schlüsseln

Öffentliche Schlüssel müssen an die PVS HAG GmbH übertragen werden, wenn die PVS HAG für eine Email-Adresse verschlüsselte Dateien erstellen soll. Hier können dafür einige Einstellungen gemacht werden. Änderungen sind normalerweise nicht nötig und sollten nur durch EDV-Fachkräfte gemacht werden.

8.4 Ändern von Pfaden

In der Maske Einstellungen wird das Schlüsselverzeichnis und das Standard-Ausgabeverzeichnis angezeigt. Das Schlüsselverzeichnis wird bei der Installation angelegt und sollte hier nicht geändert werden.

Das Standard-Ausgabeverzeichnis ist das Verzeichnis, in dem die unverschlüsselten Dateien nach dem Entschlüsseln automatisch abgespeichert werden. Dieses Verzeichnis kann nach den eigenen Bedürfnissen beliebig geändert werden. Der Anwender der GnuPG-Software benötigt Schreibrechte in diesem Verzeichnis.

9 Entschlüsseln einer Datei

Die Software ermöglicht das Entschlüsseln einzelner Dateien. Es gibt verschiedene Möglichkeiten, das Entschlüsseln-Fenster, über das Dateien entschlüsselt werden können, aufzurufen.

9.1 Entschlüsseln aus einer Mail heraus

Verschlüsselte Dokumente werden von der PVS HAG GmbH immer als Anhang einer unverschlüsselten Email verschickt. In den meisten Email-Programmen öffnet man Anhänge von Emails durch Doppelklick und Auswahl von „Öffnen“.

Nur wenn folgende Voraussetzungen erfüllt sind öffnet sich nun das GnuPGUI-Entschlüsseln-Fenster:

- Die GnuPGUI-Software muss auf dem Rechner installiert sein.
- Der passende private Schlüssel muss auf dem Rechner vorhanden sein.
- Der angemeldete Benutzer muss Rechte haben, um die GnuPGUI-Software zu starten und auch Zugriffsrechte auf die Schlüsseldateien haben.

9.2 Entschlüsseln im GnuPGUI-Programm 

Ist die GnuPGUI-Toolbox geöffnet, kann eine verschlüsselte Datei direkt mit der Maus in die Toolbox gelegt werden. Dazu führt man die Maus über die verschlüsselte Datei und drückt dann die linke Maustaste. Mit gedrückter Maustaste führt man nun die Maus über die Toolbox bis der Cursor ein kleines Plus zeigt. Erst jetzt darf die Maustaste losgelassen werden. In der Toolbox werden nun die linken Auswahlfelder inaktiv und das Entschlüsseln-Feld aktiv.

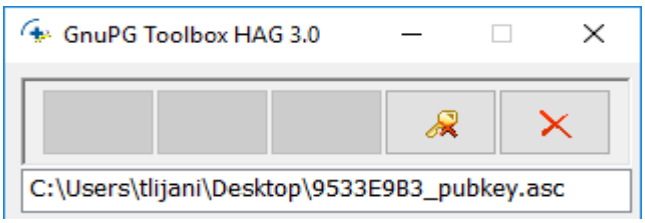
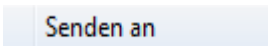


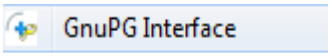
Abbildung 22: GnuPGUI-Toolbox mit aktiver Entschlüsseln-Taste

Durch Auswahl der Entschlüsseln-Taste öffnet sich das Entschlüsseln-Fenster.

9.3 Entschlüsseln aus dem Windows Explorer

Verschlüsselte Dateien, die im Windows Dateisystem abgespeichert sind, können direkt aus dem Windows Explorer (Start zum Beispiel mit der Windows-Taste + E) entschlüsselt werden. Dazu wählt man die gewünschte Datei aus und drückt die rechte Maustaste. Es öffnet sich ein Kontextmenü für die gewählte Datei.

Nach Anwahl von 

und im Untermenü 

öffnet sich das GnuPGUI-Entschlüsseln-Fenster.

9.4 Entschlüsseln

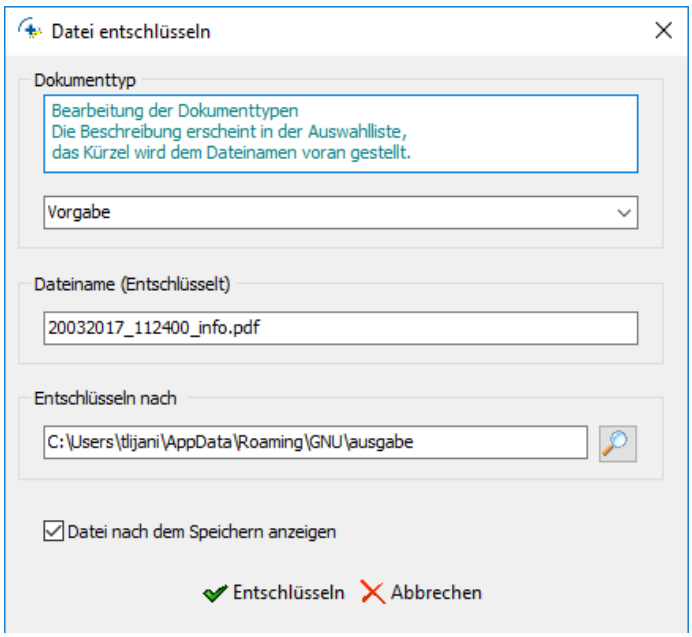


Abbildung 23: GnuPGUI-Entschlüsseln-Fenster

Vor dem Entschlüsseln können noch einige Einstellungen gemacht werden.

Die Auswahl eines Dokumenttyps bewirkt, dass dem Dateinamen das Kürzel des Dokumenttyps vorangestellt wird (siehe auch Kapitel Fehler: Referenz nicht gefunden Fehler: Referenz nicht gefunden).

Der Dateiname der entschlüsselten Datei wird so erzeugt, dass dem von der PVS HAG vorgegebenem Namen das Tagesdatum vorangestellt wird. Die Endung .gpg wird entfernt. Bei einer Änderung des vorgegebenen Namens muss die vorgegebene Endung erhalten bleiben, um die entschlüsselte Datei mit dem richtigen Programm öffnen zu können.

Das vorgegebene Verzeichnis in dem die entschlüsselte Datei abgespeichert wird, entspricht dem Standard-Ausgabeverzeichnis, das in den GnuPGUI-Einstellungen geändert werden kann.

Ist der Haken bei „Datei nach dem Speichern anzeigen“ gesetzt, dann wird die Datei nach dem Entschlüsseln sofort mit dem für den entsprechenden Dateityp auf dem Rechner vorgegebenen Programm geöffnet. Ist im Windowssystem kein Programm zugeordnet (zum Beispiel im obigen Beispiel für den Dateityp .pdf), dann wird die Datei nur entschlüsselt, kann aber nicht geöffnet werden.

Nach Auswahl von Entschlüsseln öffnet sich das Passwort-Eingabefenster.

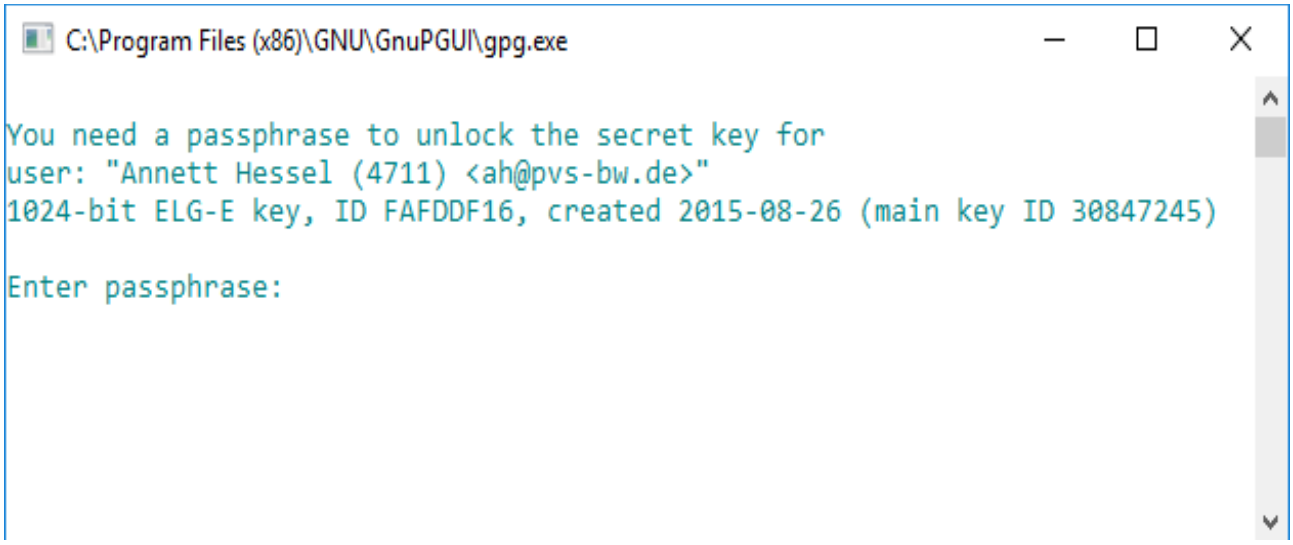


Abbildung 24: Passwort-Eingabefenster beim Entschlüsseln

Das Passwort, das beim Anlegen des Schlüssels vergeben wurde, muss nun eingegeben werden. Bei der Eingabe des Passworts werden keine Zeichen angezeigt und es ist auch keine Bewegung am Bildschirm sichtbar. Nach dem Eingeben des vollständigen Passworts, wobei auf die genaue Schreibweise mit richtiger Groß- und Kleinschreibung geachtet werden muss und dem Drücken der Enter-Taste ↵ wird die Datei entschlüsselt. Sollte das Passwort vergessen worden sein, dann ist eine Entschlüsselung der Datei nicht mehr möglich.

10 Anwendungsfälle

10.1 Ändern der Email-Adresse

Verschlüsselte Dateien können immer nur an die Email-Adresse geschickt werden, die im Schlüssel hinterlegt ist. Bei einer Änderung der Email-Adresse muss daher ein neuer Schlüssel für diese Email-Adresse angelegt werden. Der öffentliche Teil des neuen Schlüssels muss an die PVS HAG GmbH übertragen werden. Ein neues Fingerabdruck-Dokument muss ebenfalls an die PVS HAG GmbH gesendet werden. Erst wenn beides bei der PVS HAG vorliegt, können verschlüsselte Dateien an die neue Email-Adresse

versendet werden.

Wenn der Schlüssel für die alte Email-Adresse nicht mehr benötigt wird, dann sollte er gelöscht werden.

10.2 Empfangen der verschlüsselten Mails mit gleicher Email-Adresse auf verschiedenen Rechnern

Auf jedem Rechner, auf dem Dateien entschlüsselt werden sollen, muss die GnuPGUI-Software installiert werden. Sollen Anhänge von Emails für dieselbe Email-Adresse auf mehreren Rechnern entschlüsselt werden, dann darf der Schlüssel für diese Email-Adresse nur auf einem Rechner erstellt werden. Auf allen anderen Rechnern muss derselbe Schlüssel importiert werden. Siehe dazu auch die Beschreibung in Kapitel 8.1 auf Seite 23 zum Sichern und Wiederherstellen der Schlüsseldateien. Sollen nur einzelne Schlüssel auf einen anderen Rechner übertragen werden, dann siehe die Beschreibung in Kapitel 7.2.3 Privaten Schlüssel exportieren auf Seite 22 und anschließend das darauffolgende Kapitel 7.3 Schlüssel importieren.

10.3 Neuinstallation eines Rechners

Wird ein Rechner durch einen neuen Rechner ersetzt oder muss ein vorhandener Rechner neu installiert werden, dann sollten zunächst die vorhandenen Schlüssel auf einem externen Medium gesichert werden (Kapitel 8.1.1 auf Seite 24). Nach der Installation des neuen Rechners muss zunächst die GnuPGUI-Software installiert werden. Anschließend können die gesicherten Schlüssel wie in Kapitel 8.1.2 auf Seite 24 beschrieben wieder hergestellt werden.

10.4 Passwort vergessen

Wurde das Passwort vergessen, dann können Dokumente, die mit diesem Schlüssel verschlüsselt wurden, nicht mehr entschlüsselt werden. In diesem Fall sollte der vorhandene Schlüssel wie in Kapitel 7.2.2 Löschen von Schlüsseln auf Seite 21 beschrieben wurde, gelöscht werden. Anschließend kann für die Email-Adresse ein neuer Schlüssel angelegt werden. Nach dem Versenden des öffentlichen Teils des Schlüssels

und des Fingerabdruck-Dokuments an die PVS HAG GmbH, können noch nicht entschlüsselte Dokumente erneut angefordert werden.

10.5 Verlust von GnuPG-Schlüsseln

Wenn die Schlüssel eines Rechners verloren gehen, dann können Dateien, die mit diesen Schlüsseln verschlüsselt wurden, nicht mehr entschlüsselt werden. In diesem Fall müssen neue Schlüssel angelegt werden. Nachdem der öffentliche Teil des Schlüssels und das Fingerabdruck-Dokument an die PVS HAG GmbH gesendet wurden, können alle Dokumente erneut mit dem neuen Schlüssel verschlüsselt und versendet werden.