

Smartcards einrichten mit GnuPG VS-Desktop®

Anleitung für Schlüsselmanager:innen

Dokumentversion: 1.1

Stand Bilder: GnuPG VS-Desktop® 3.1.24

Einleitung

Nachfolgend finden Sie eine Schritt-für-Schritt Beschreibung der OpenPGP Schlüsselstellung mit GnuPG VS-Desktop® und der anschließenden Übertragung auf eine Smartcard bzw. ein Hardware-Token.

Hierbei wird das graphische Frontend von GnuPG VS-Desktop®, der Schlüssel- und Zertifikatsmanager Kleopatra verwendet. Die Erstellung und Übertragung des Schlüssels ist auch auf der Kommandozeile möglich.

Die Anleitung ist auch für spätere Versionen von GnuPG VS-Desktop® geeignet, mindestens bis Version 3.1.26, sowie für GnuPG Desktop®.

Hintergrund

Wenn eine Smartcard verwendet wird, die nicht in der BSI-Zulassung genannt ist (zum Beispiel ein YubiKey), ist es erforderlich, dass das OpenPGP Zertifikat mit GnuPG VS-Desktop® erstellt wird. Die Generierung des Zertifikats auf der Smartcard selber ist dann nicht durch das BSI zugelassen.

Die Nutzung selbst von nicht vom BSI zugelassenen Smartcards, wie z.B. einem YubiKey, erhöht die Sicherheit des geheimen Schlüsselmaterials. Durch seine Übertragung auf das Token wird verhindert, dass Nutzer den geheimen Schlüssel auf ein nicht VS-NfD-konformes System kopieren können. Auch ein versehentliches Versenden an Kommunikationspartner ist damit unmöglich.

Dieses Dokument wurde unter der Lizenz „Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0)“ veröffentlicht. Den rechtsverbindlichen Lizenzvertrag finden Sie unter: <https://creativecommons.org/licenses/by-sa/4.0/deed.de>

GnuPG VS-Desktop® ist ein eingetragenes Warenzeichen der g10 Code GmbH.

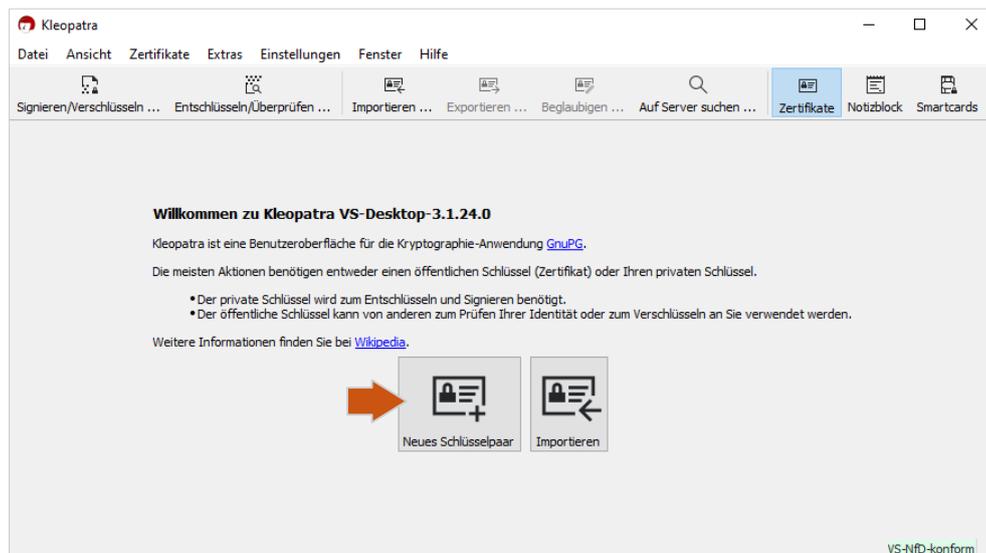
g10 Code GmbH • Bergstr. 3a • 40699 Erkrath, Germany • +49 2104 4938 790 • info@gnupg.com • www.gnupg.com

Inhalt

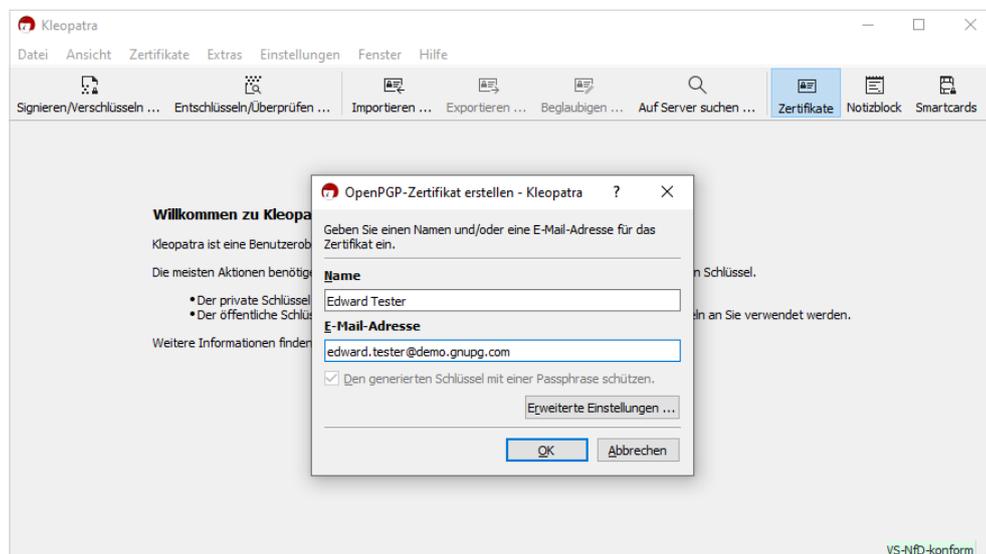
1 Schlüssel erstellen.....	3
2 Sicherungskopie erstellen.....	6
2.1 Sicherung des geheimen Schlüssels als Datei.....	6
2.2 Sicherung des geheimen Schlüssels als Ausdruck (Paperkey).....	8
3 Öffentlichen Schlüssel exportieren.....	10
4 Smartcard einrichten.....	11
4.1 Admin-PIN ändern.....	11
4.2 Nutzer-PIN ändern.....	12
4.3 Reset-Code setzen (optional).....	14
4.4 Kartennamen ändern.....	14
4.5 Schlüssel auf Smartcard / Token übertragen.....	16
5 Schlüssel löschen.....	20
6 Öffentlichen Schlüssel importieren.....	23
7 Smartcard zurücksetzen (Factory Reset).....	26

1 Schlüssel erstellen

Öffnen Sie die Anwendung Kleopatra. Bei der ersten Anwendung, bzw. wenn noch keine Schlüssel vorhanden sind, erscheint der Einführungsbildschirm. Klicken Sie hier auf [Neues Schlüsselpaar]. Alternativ wählen Sie [Datei] > [Neues OpenPGP-Schlüsselpaar].



Geben Sie eine Mailadresse und/oder einen Namen für Ihr neues Schlüsselpaar ein:

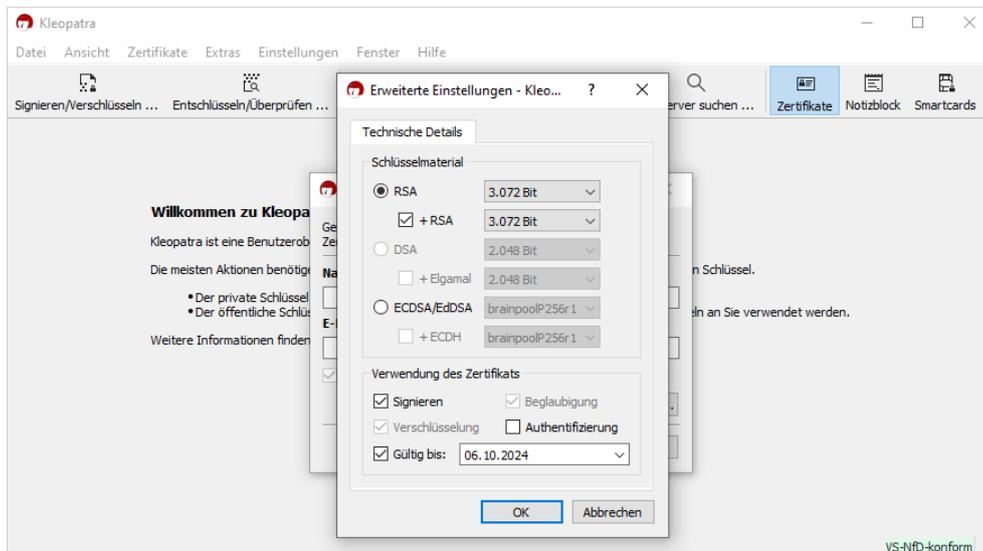


Hinweis

Schlüssel müssen nicht immer an eine Mailadresse gebunden sein. Sie können auch nur einen Namen, z.B. einen Projekt- oder Gruppennamen, verwenden. Für eine unkomplizierte Anwendung beim Verschlüsseln und Signieren von Mails ist die Angabe der Mailadresse jedoch erforderlich.

Unter dem Menü [Erweiterte Einstellungen] können Sie optional die Eigenschaften Ihres Schlüssels im Rahmen der vom BSI zugelassenen Optionen konfigurieren.

Für bessere Performance-/ Sicherheitseigenschaften wählen Sie „*ECDSA/EdDSA*“. Dies kann jedoch zu Kompatibilitätsproblemen mit veralteter, nicht VS-NfD-konformer Software führen:



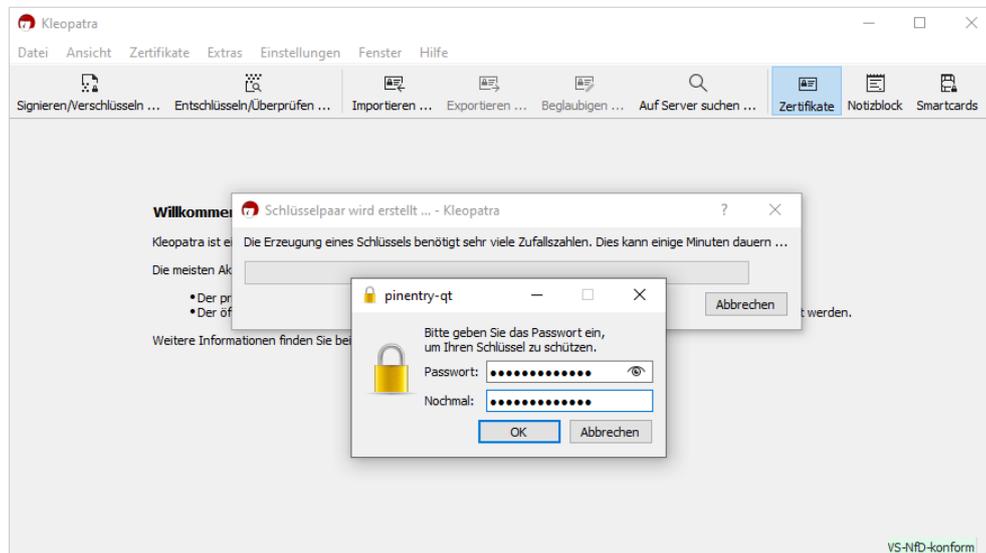
Schließen Sie die Einstellungen und klicken Sie auf [OK], um Ihren Schlüssel zu generieren.

Sie werden nun aufgefordert ein Passwort einzugeben. Dadurch wird sichergestellt, dass es für Unberechtigte nicht alleine ausreicht Ihren Schlüssel als Datei zu erlangen, sofern sie nicht auch das Passwort kennen. Es muss **mindesten 9 Zeichen** lang sein. Notieren Sie es und bewahren es VS-NfD-konform auf.

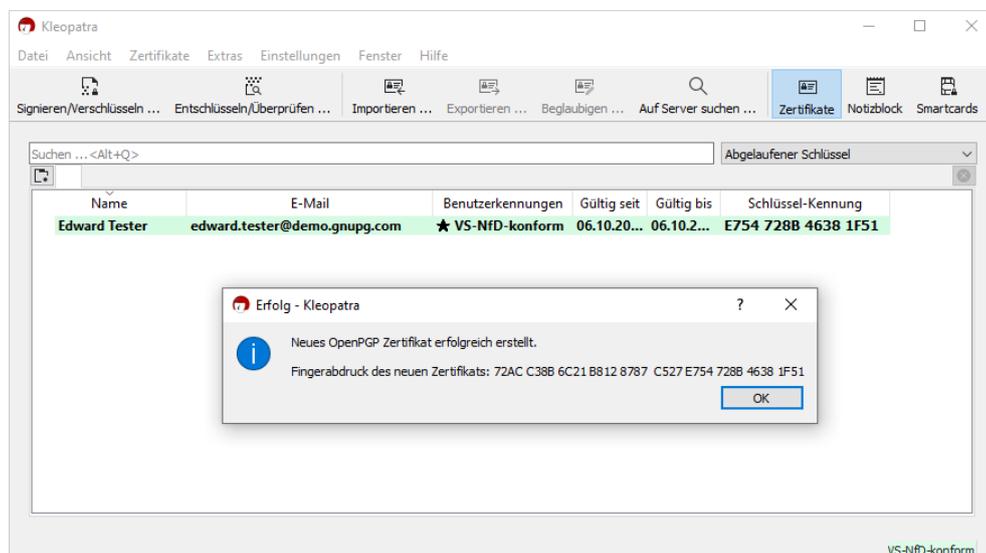
Hinweis

Das Passwort kann weder wiederhergestellt noch zurückgesetzt werden – sollte es verloren gehen, ist Ihr Schlüssel als Software-Token unbrauchbar!

Allerdings brauchen Sie bei der Verwendung eines Hardware-Tokens anstelle des Passwortes nur die PIN der Smartcard. Lediglich wenn Sie den Schlüssel aus einem Backup wiederherstellen, ist dann noch die Eingabe des Passwortes erforderlich:



Sie haben erfolgreich ein neues Schlüsselpaar erstellt. Klicken Sie auf [OK], um das Fenster zu schließen:



2 Sicherungskopie erstellen

Zunächst muss die Frage beantwortet werden, ob eine Sicherungskopie des Schlüssels gespeichert werden oder ob sich der geheime Schlüssel ausschließlich auf einer Smartcard befinden soll. Wenn sich der Schlüssel nur auf der Smartcard befinden soll, kann er im Nachhinein nicht mehr kopiert oder übertragen werden. **Sobald Ihre Smartcard defekt ist oder abhanden kommt, haben Sie folglich auch keinen Zugriff mehr auf das geheime Schlüsselmaterial.**

Sie haben drei Möglichkeiten, Ihren Schlüssel zu sichern:

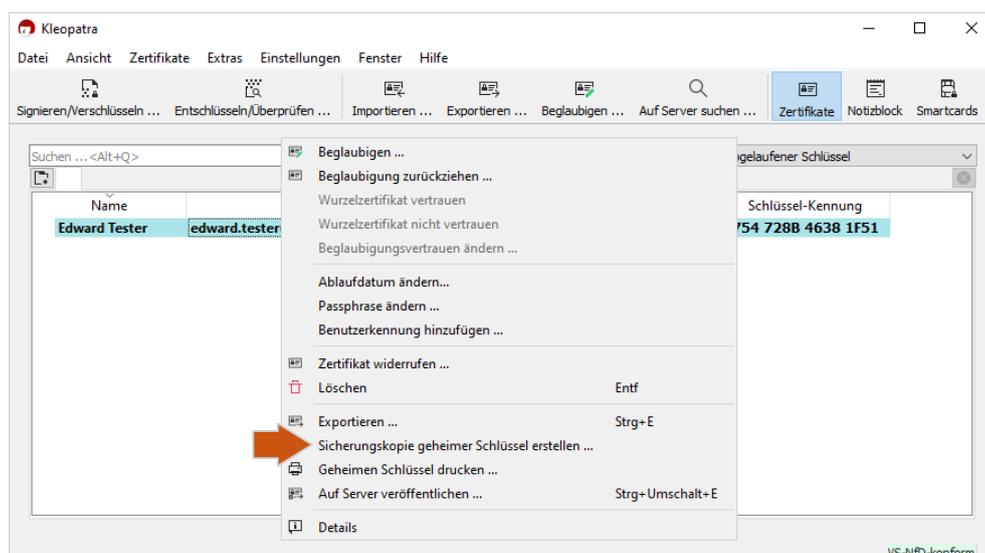
- parallel auf eine zweite Ersatz-Smartcard kopieren
- als Datei exportieren
- auf Papier ausdrucken („Paperkey“).

Für die meisten Fälle bietet es sich an, den Schlüssel auf einem VS-NfD-konformen Rechner zu erstellen, dann auszudrucken, ihn anschließend auf eine Smartcard zu übertragen und abschließend direkt vom Rechner zu löschen.

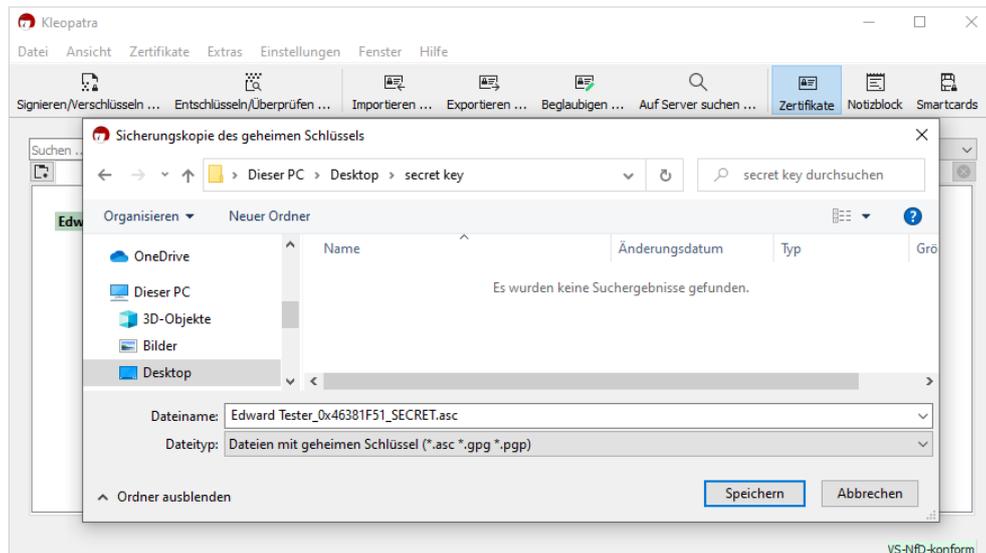
Hinweis | Die Sicherungskopie ist stets VS-NfD-konform aufzubewahren.

2.1 Sicherung des geheimen Schlüssels als Datei

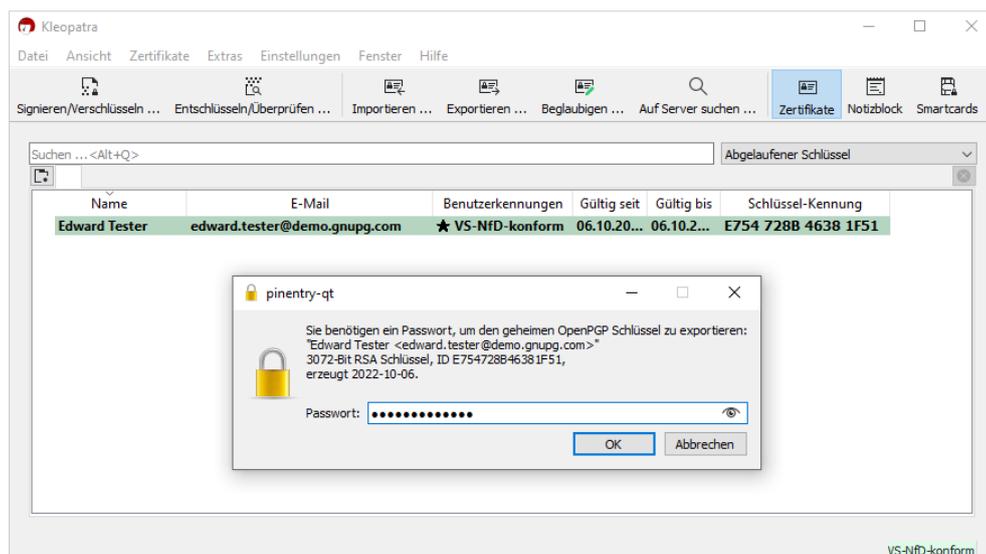
Wählen Sie Ihren zu sichernden Schlüssel und klicken Sie im Untermenü auf [Sicherungskopie geheimer Schlüssel erstellen]:



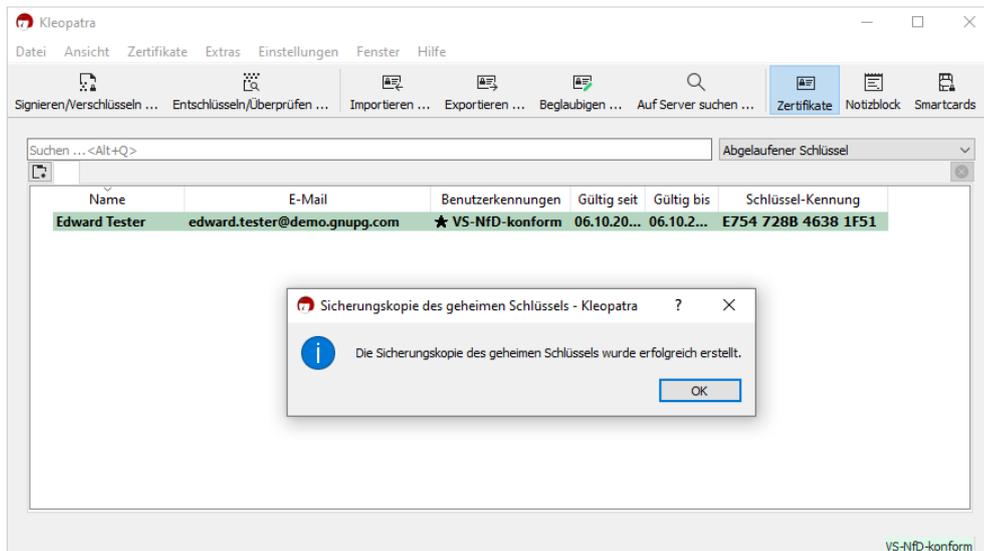
Wählen Sie einen Dateinamen und einen Speicherort zum Ablegen Ihrer Sicherungskopie und klicken Sie auf [Speichern]:



Sie werden nach dem Passwort gefragt. Geben Sie es ein und klicken Sie auf [OK]:

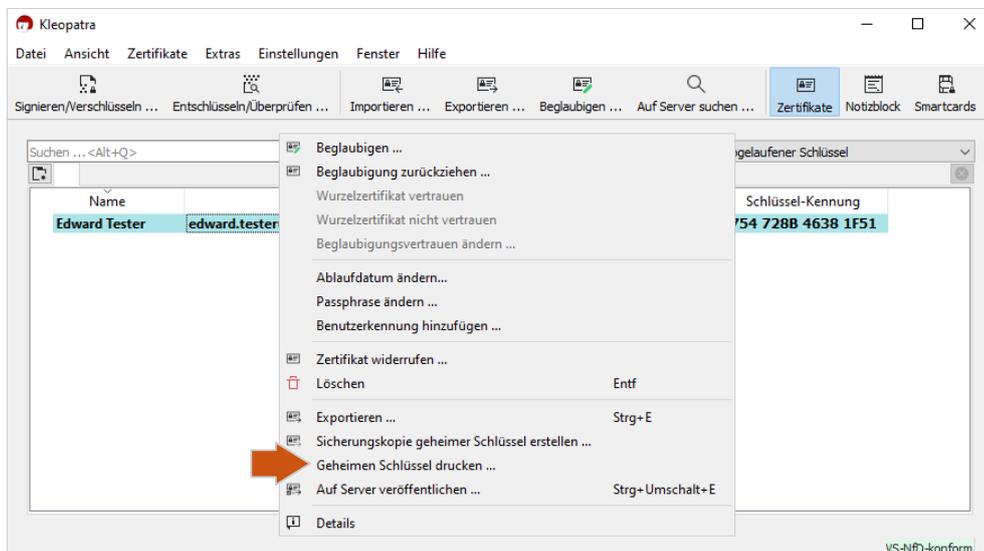


Sie haben den geheimen Schlüssel erfolgreich als Datei exportiert. Beenden Sie den Vorgang mit [OK]:

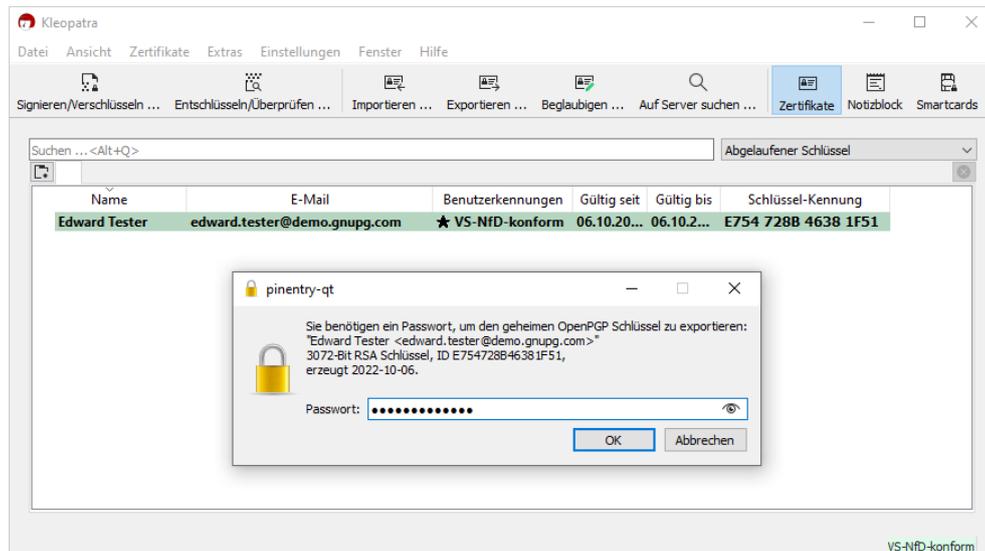


2.2 Sicherung des geheimen Schlüssels als Ausdruck (Paperkey)

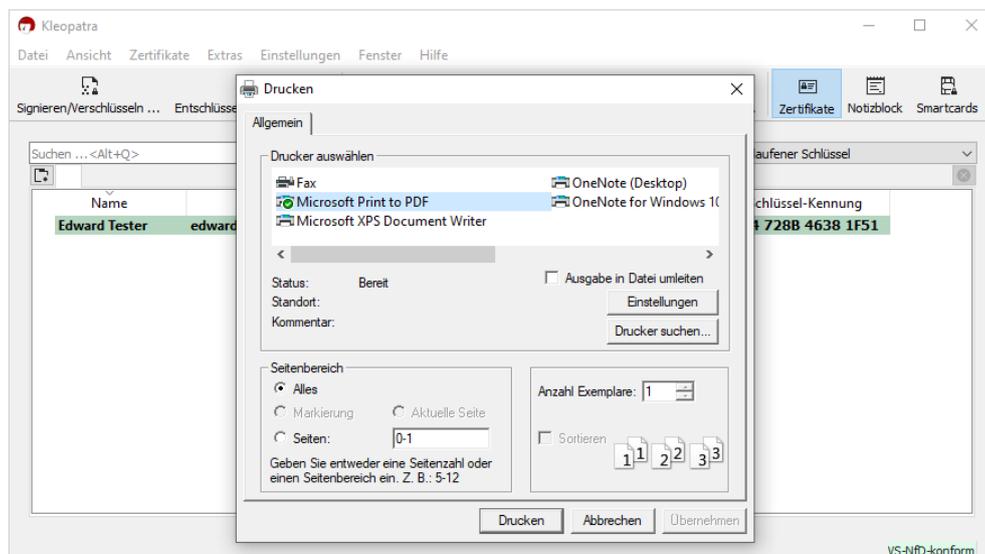
Klicken Sie im Schlüssel-Untermenü auf [Geheimen Schlüssel drucken]:



Geben Sie das Schlüssel-Passwort ein und bestätigen Sie dieses mit [OK]:



Wählen Sie Ihr Ausgabegerät und klicken Sie [Drucken]:



Sie haben den geheimen Schlüssel erfolgreich ausgedruckt.

Bewahren Sie Ihren (i.d.R. zweiseitigen) Ausdruck sicher auf, um im Notfall damit und dem dazu gehörenden öffentlichen Schlüssel Ihr geheimes Schlüsselmaterial rekonstruieren zu können.

Hinweis

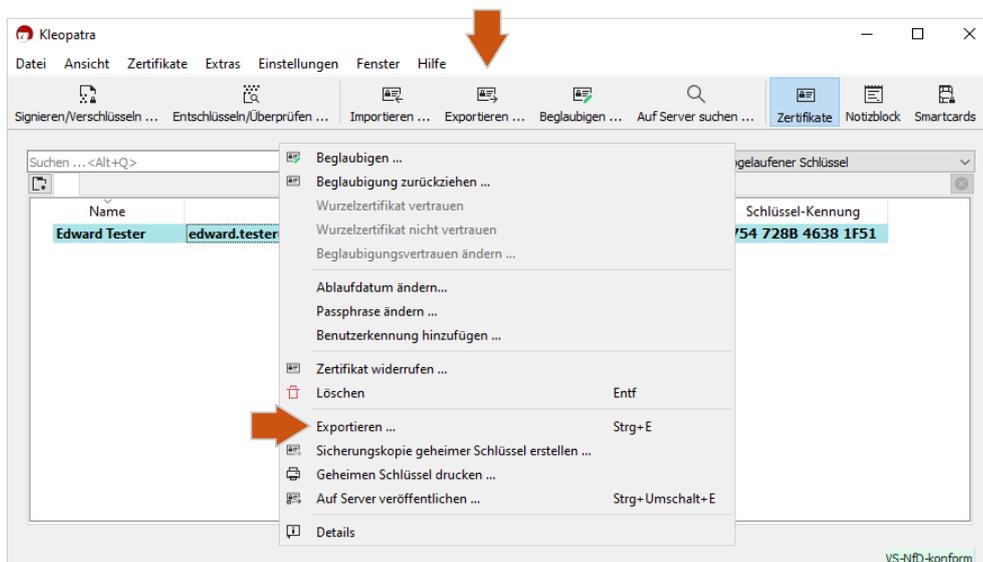
Das Blatt zur Aufbewahrung nicht im Datenblock falten – dadurch könnten Zeilen unleserlich und die Rekonstruktion im schlimmsten Fall unmöglich werden.

3 Öffentlichen Schlüssel exportieren

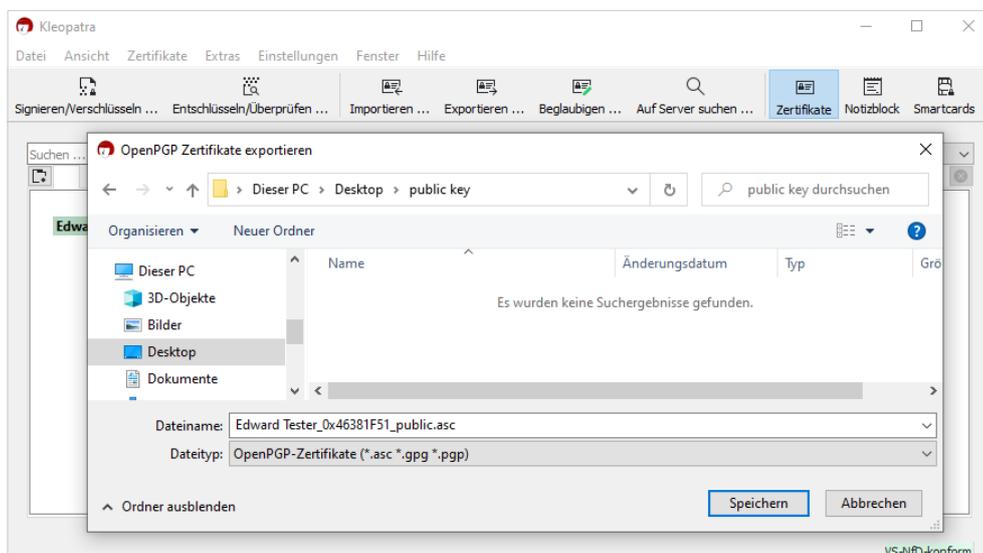
Hinweis

Der öffentliche Schlüssel muss an dieser Stelle exportiert werden, da er nach dem Kopieren des geheimen Schlüssels auf die Smartcard zusammen mit diesem von der Festplatte gelöscht wird. Anschließend muss er reimportiert werden.

Wählen Sie Ihren Schlüssel aus und klicken Sie im Untermenü auf [Exportieren]. Diese Funktion steht Ihnen auch im oberen Menüband zur Verfügung:



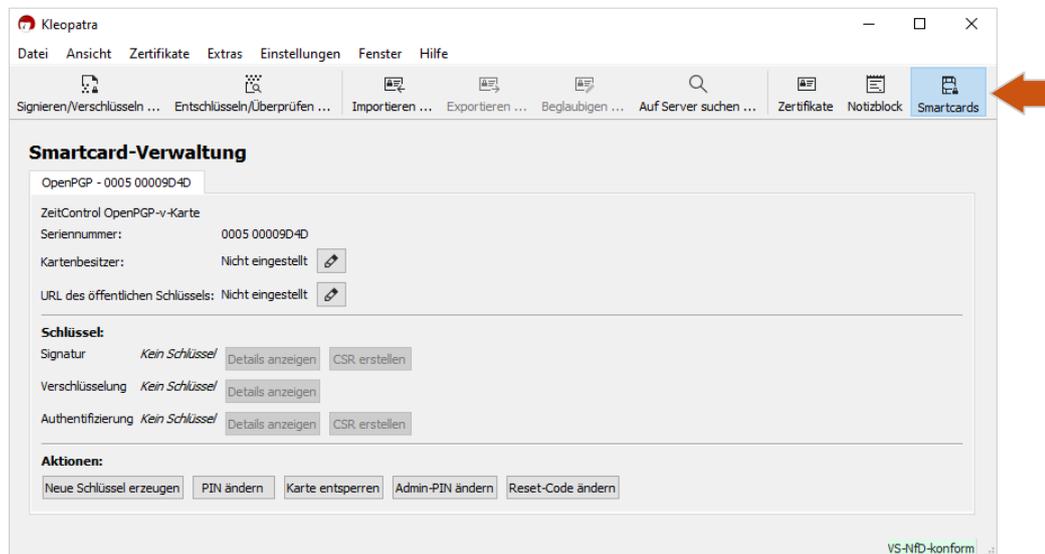
Wählen einen Dateinamen und einen Ort zum Ablegen Ihres öffentlichen Schlüssels als Datei und klicken Sie auf [Speichern]:



Sie haben den öffentlichen Schlüssel erfolgreich exportiert.

4 Smartcard einrichten

Die „*Smartcard-Verwaltung*“ finden Sie im Menüband unter [Smartcards]:



Hinweis

Sollte Ihre Smartcard nicht dargestellt werden, obwohl sie eingesteckt ist und Sie [F5] gedrückt haben, entfernen Sie diese und stecken sie erneut ein.

Je nach Smartcard weichen die Angaben und Optionen u. U. leicht von einander ab.

Die Nutzung der Aktion [Neue Schlüssel erzeugen] wird von uns aktuell nicht empfohlen. Bitte generieren Sie die Schlüssel so, wie in Kapitel 1. beschrieben.

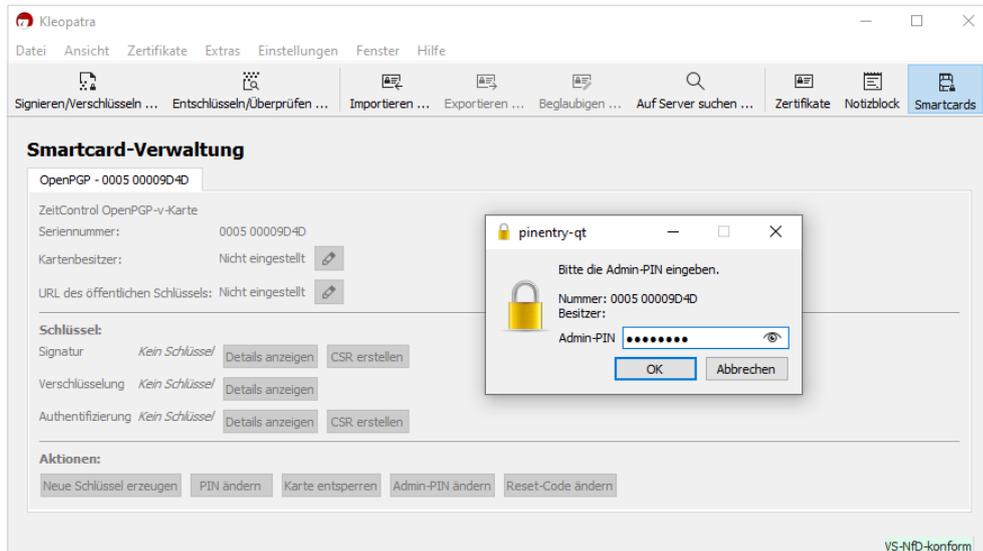
4.1 Admin-PIN ändern

Hinweis

Wenn Sie Ihre Admin-PIN verlieren oder 3 Mal nacheinander falsch eingeben, können Sie keine Änderungen mehr vornehmen. Ihnen bleibt dann nur der Factory Reset (siehe Kapitel 7.), bei dem die Daten auf Ihrer Smartcard vollständig gelöscht werden.

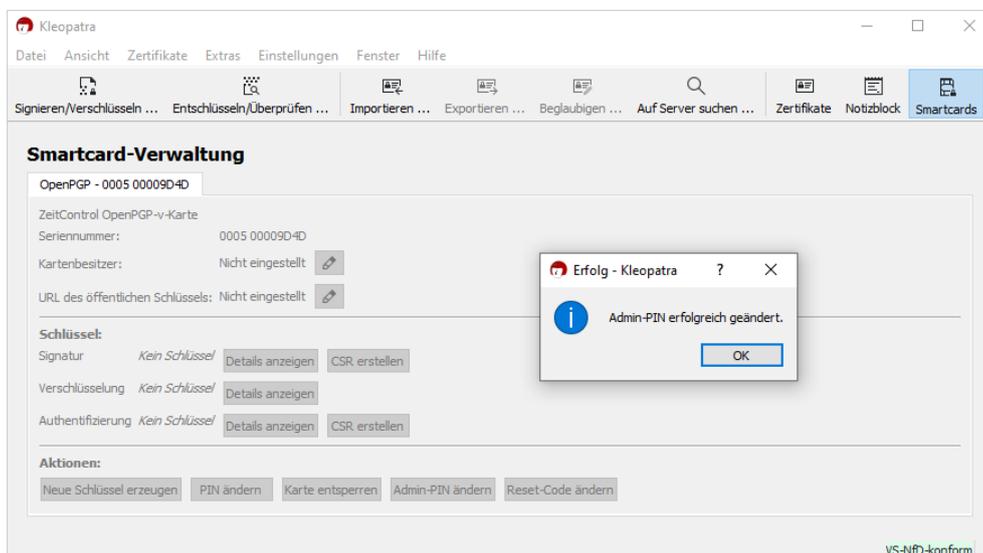
Notieren Sie sich die neue Admin-PIN am Besten schon vor dem folgenden Schritt und bewahren Sie diese stets VS-NfD-konform auf.

Sobald Sie auf [Admin-PIN ändern] klicken, erscheint die Abfrage für die werksseitige 8-stellige Admin-PIN Ihrer Smartcard (i.d.R. 12345678). Geben Sie diese ein und klicken auf [OK]:



Geben Sie anschließend Ihre neue (mindestens 8-stellige) Admin-PIN ein und wiederholen Sie diese im nächsten Eingabefenster.

Sie haben die Admin-PIN erfolgreich geändert. Klicken Sie zum Beenden auf [OK]:



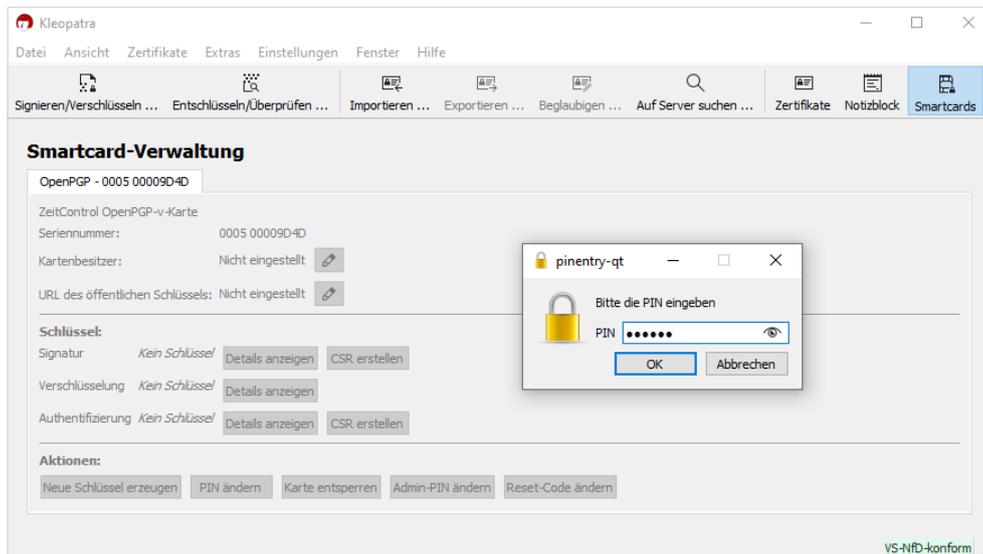
4.2 Nutzer-PIN ändern

Hinweis

Wenn Sie Ihre PIN verlieren oder wenn sie 3 Mal nacheinander falsch eingegeben wird, können Sie diese mit Hilfe der Admin-PIN oder des Reset-Codes neu setzen.

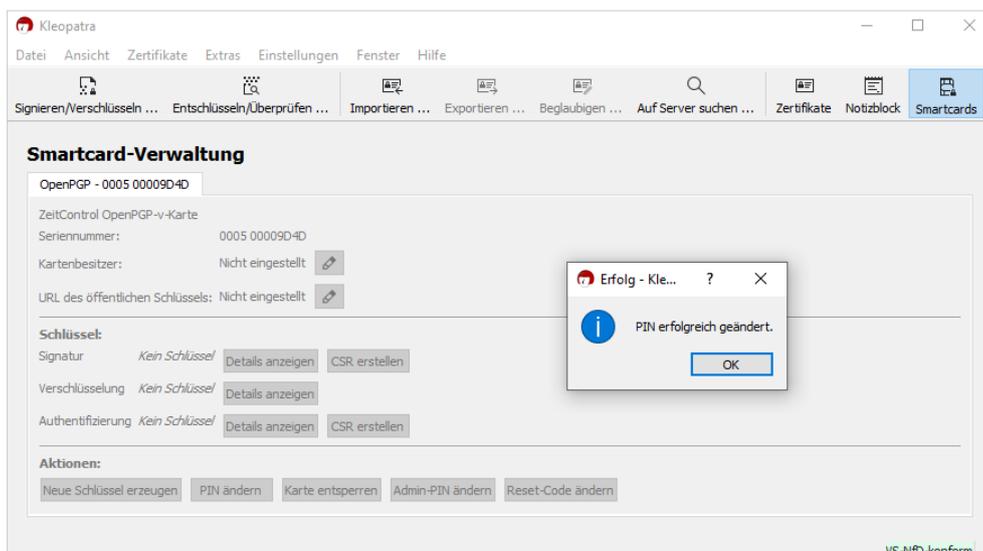
Notieren Sie sich die neue PIN am Besten schon vor dem folgenden Schritt und bewahren Sie diese stets VS-NfD-konform auf.

Sobald Sie auf [PIN ändern] klicken, erscheint die Abfrage für die werksseitigen 6-stelligen Nutzer-PIN der Smartcard (i.d.R. 123456). Geben Sie die PIN ein und klicken auf [OK]:



Geben Sie anschließend Ihre (mindestens 6-stellige) neue PIN ein und wiederholen Sie diese im nächsten Fenster.

Sie haben die PIN Ihrer Smartcard erfolgreich geändert. Klicken Sie [OK] um das Fenster zu schließen:



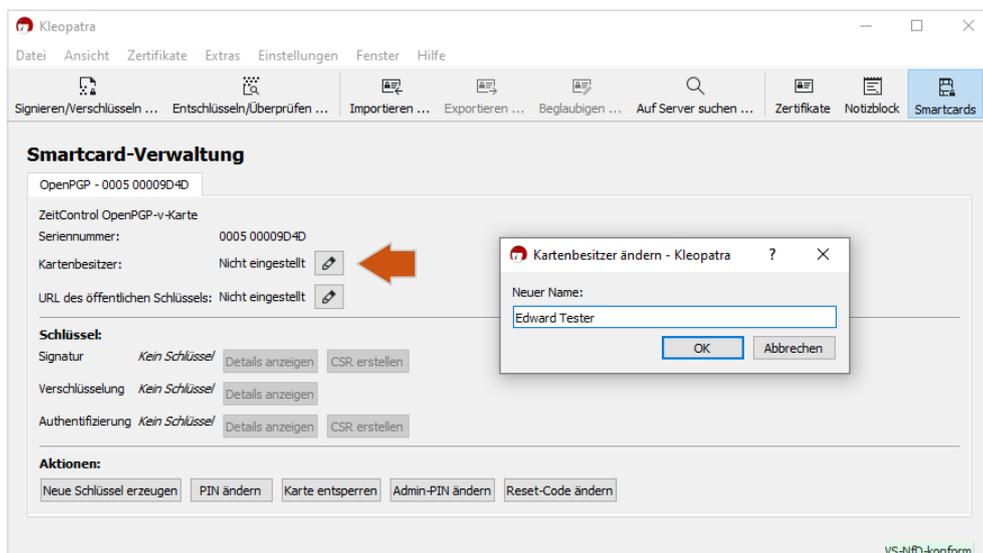
4.3 Reset-Code setzen (optional)

Die Option [Reset-Code ändern] (entspricht etwa einem PUK bei SIM-Karten) kann sinnvoll sein, wenn die Smartcards für eine Organisation zentral erstellt werden und die späteren Nutzer die Admin-PIN nicht erhalten sollen.

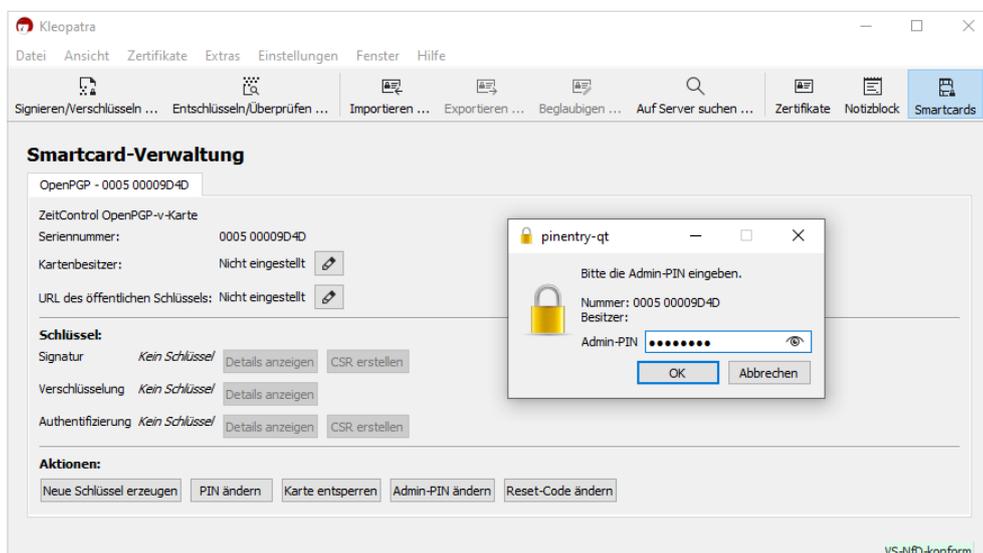
Mit dem Reset-Code kann man die Nutzer-PIN neu setzen, wenn diese versehentlich 3 Mal falsch eingegeben wurde. Für das Setzen des Reset-Codes ist die Admin-PIN erforderlich.

4.4 Kartennamen ändern

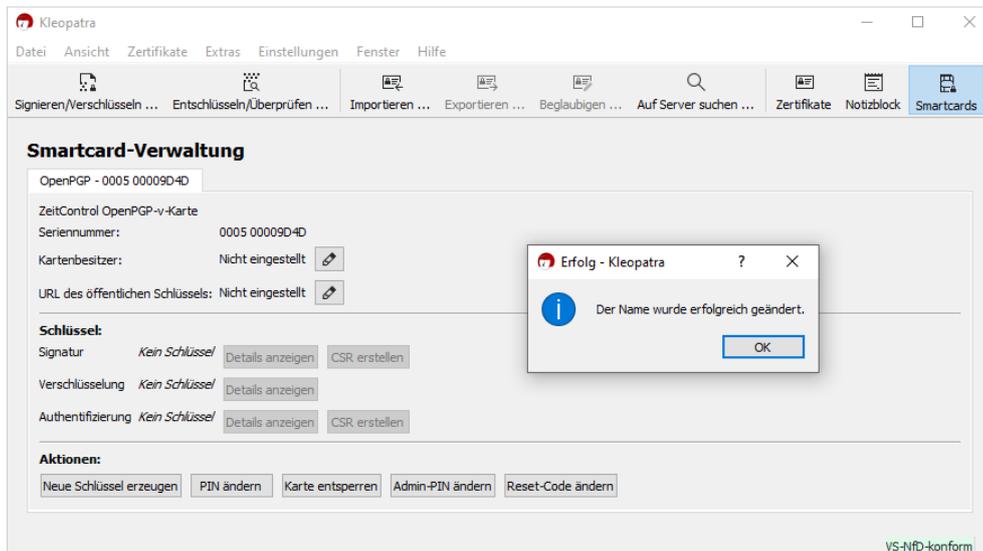
Um Ihre Smartcard namentlich einem Besitzer zuzuordnen, klicken Sie auf die [Kartenbesitzer]-Einstellungen und geben Sie einen neuen Namen ein:



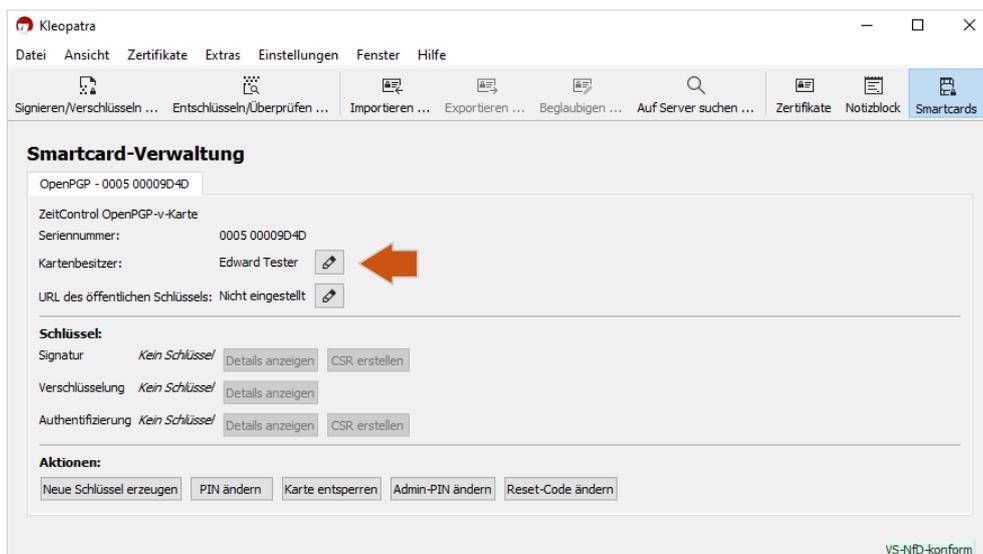
Bestätigen Sie die Namensänderung mit der Eingabe Ihrer Admin-PIN:



Sie haben den Namen des Kartenbesitzers erfolgreich geändert. Klicken Sie [OK] um das Fenster zu schließen:

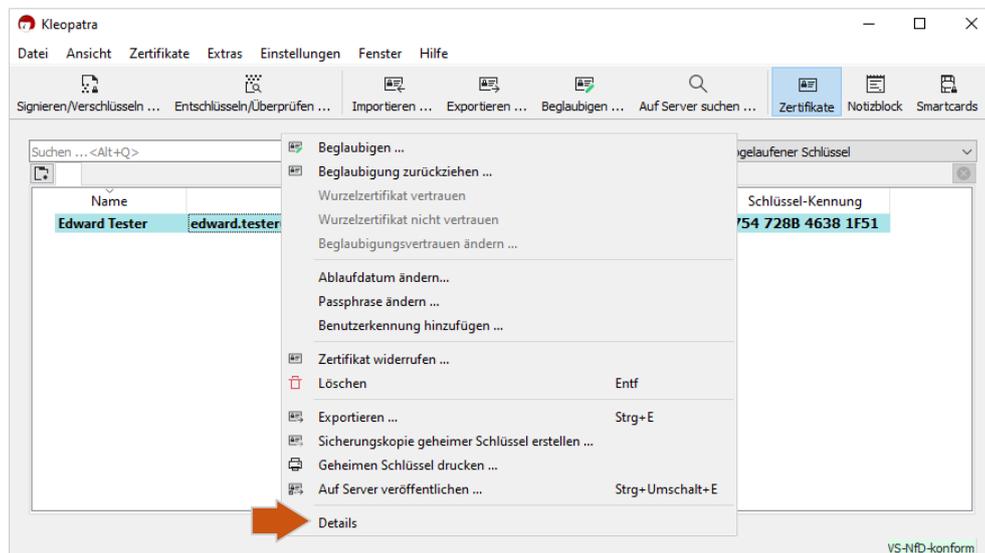


In der „*Smartcard-Verwaltung*“ wird nun der neue Kartenbesitzer dargestellt:

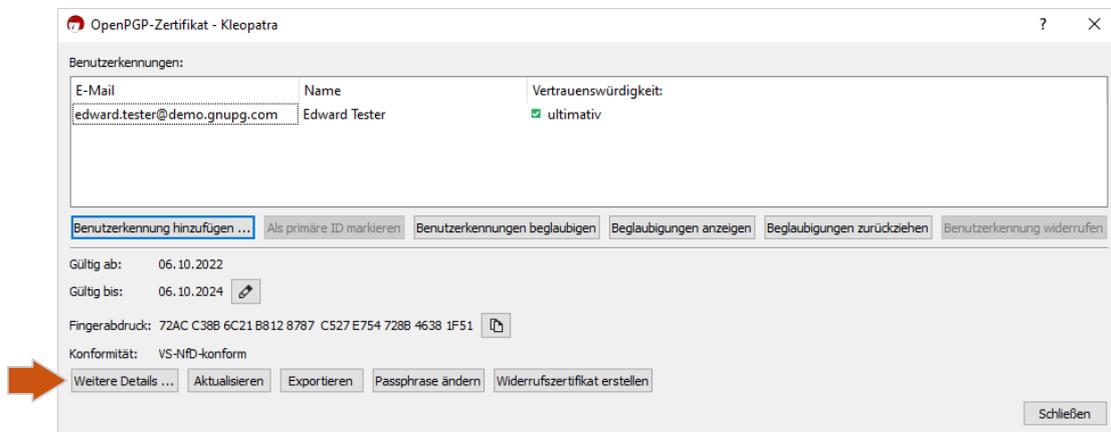


4.5 Schlüssel auf Smartcard / Token übertragen

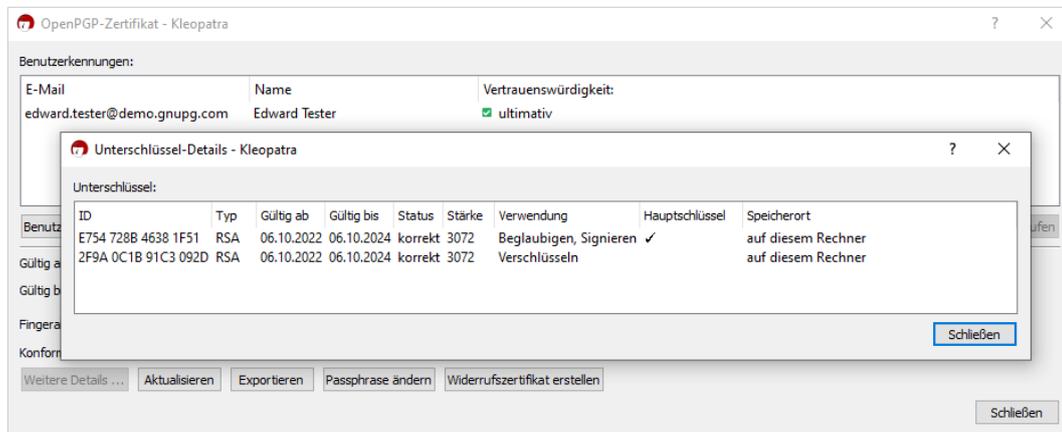
Wählen Sie den Schlüssel aus, den Sie auf Ihre Smartcard übertragen möchten, öffnen Sie mit der rechten Maustaste das Untermenü und klicken Sie auf [Details]:



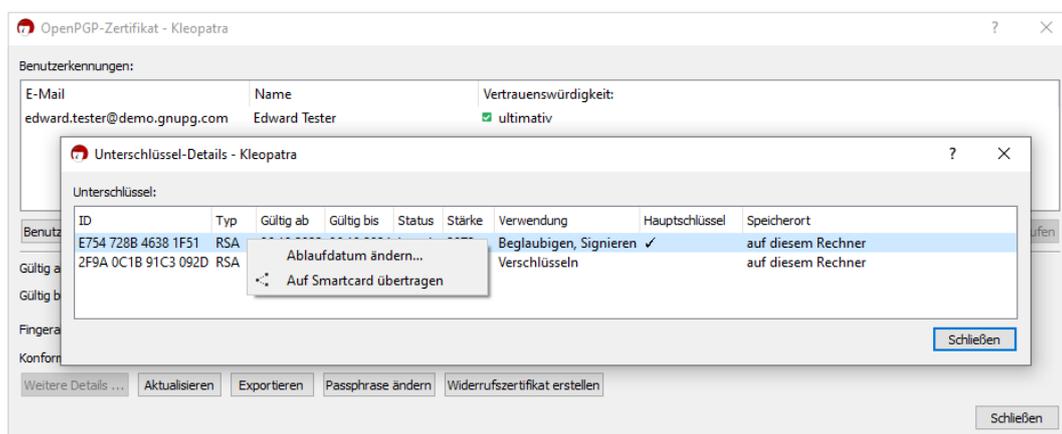
Im folgenden Dialog wählen Sie die Option [Weitere Details]:



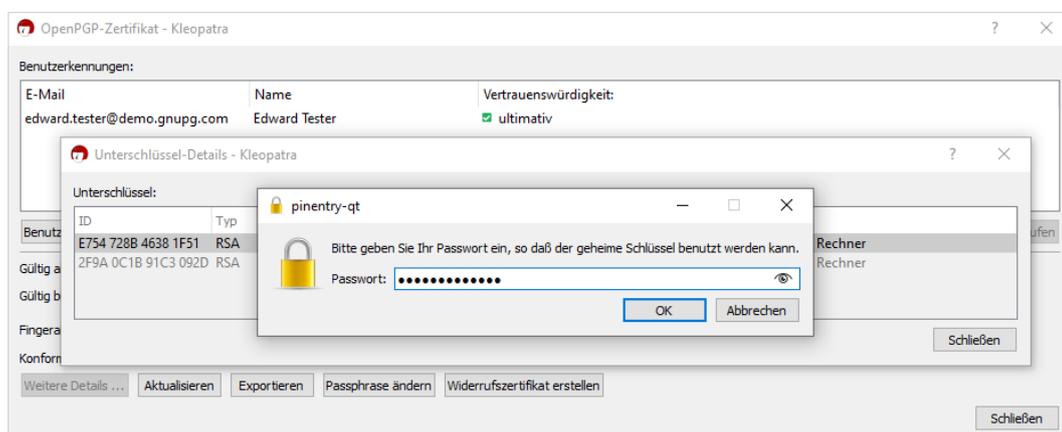
Es öffnen sich das „*Unterschlüssel-Details*“-Fenster. Der obere Schlüssel dient zum Beglaubigen und Signieren, der untere zum Verschlüsseln. Beide Schlüssel müssen von Ihnen auf die Smartcard übertragen werden:



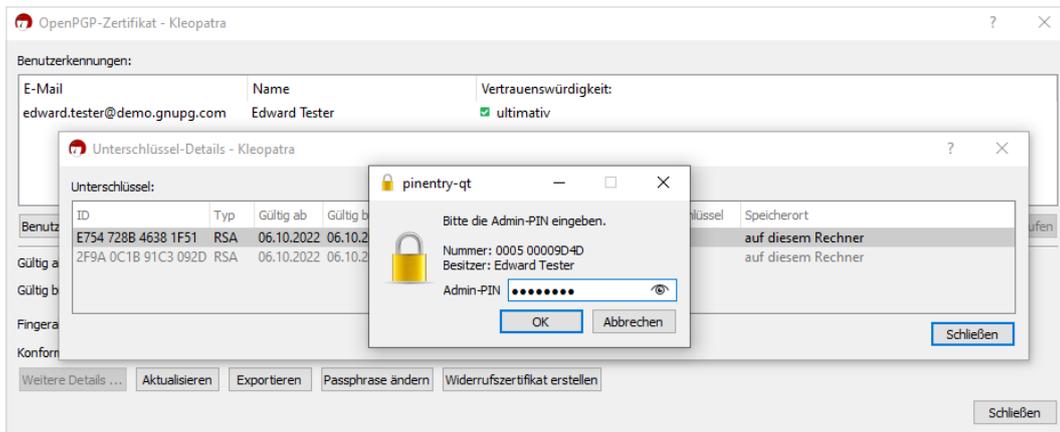
Zum Übertragen der Informationen wählen Sie den ersten Schlüssel aus, klicken auf die rechte Maustaste und wählen die Option [Auf Smartcard übertragen]:



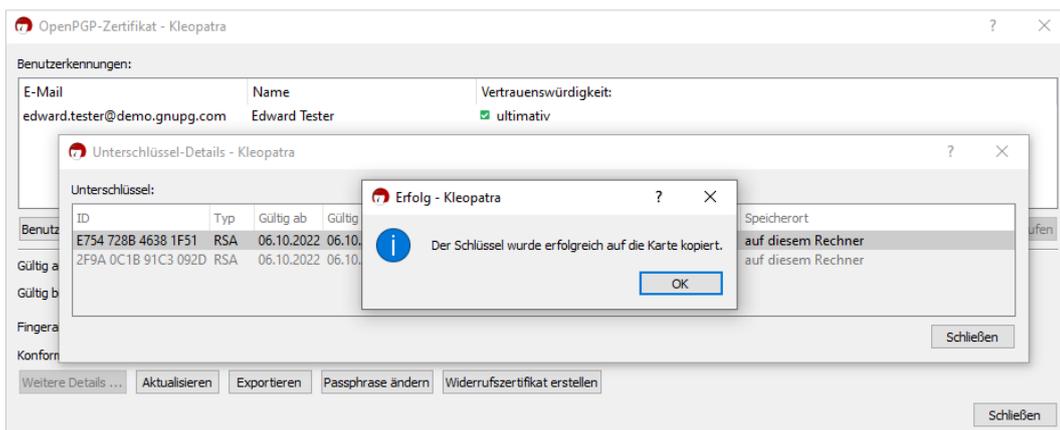
Da eine Sicherungskopie angefordert wurde, werden Sie nach dem **Passwort Ihres geheimen Schlüssels** gefragt (aus Kapitel 1.):



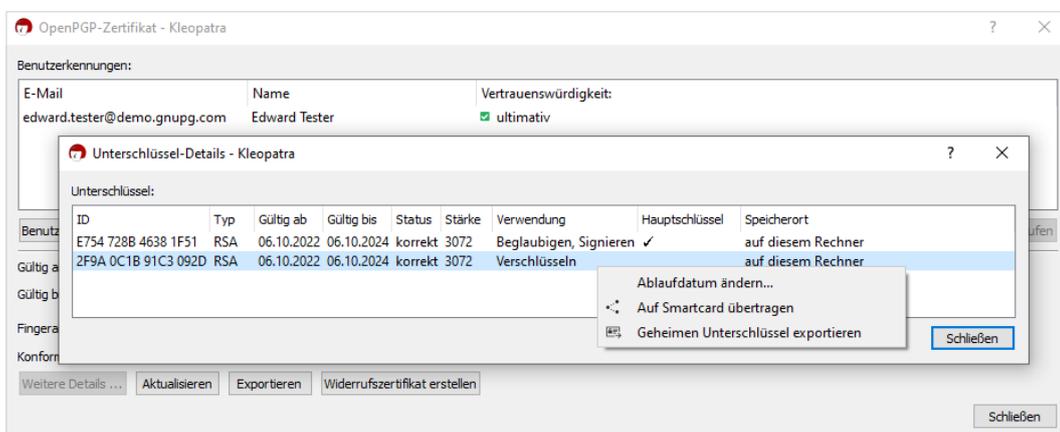
Anschließend werden Sie aufgefordert, die **Admin-PIN der Smartcard** einzugeben (je nach Token 1 - 2 Mal):



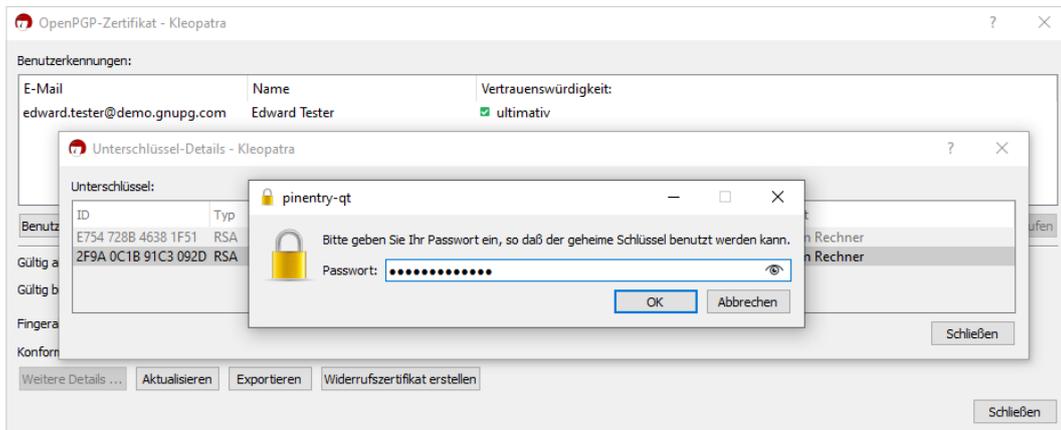
Sie haben den ersten Unterschlüssel (Beglaubigen und Signieren) erfolgreich auf Ihre Smartcard übertragen. Bestätigen Sie mit [OK]:



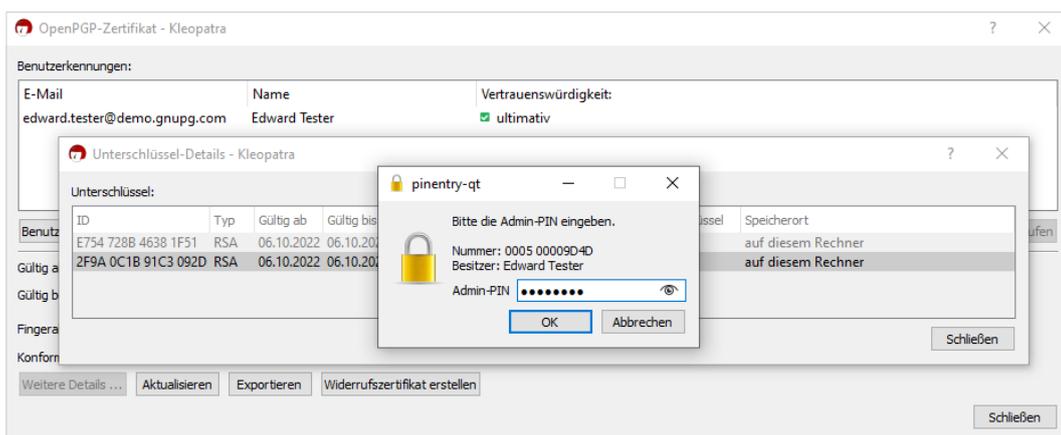
Wiederholen Sie den Prozess anschließend auch für den zweiten Unterschlüssel (Verschlüsseln):



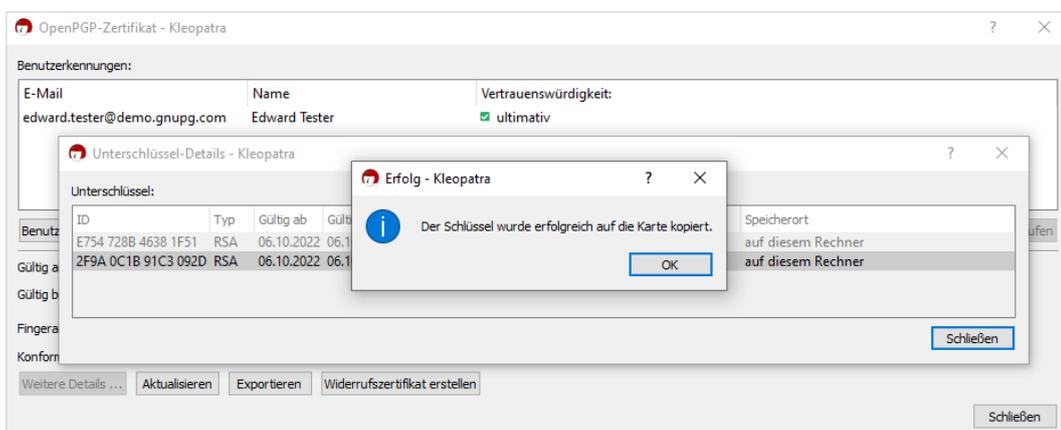
Auch hier müssen Sie das **Passwort Ihres geheimen Schlüssels** eingeben:



Anschließend werden Sie wieder aufgefordert, Ihre **Admin-PIN der Smartcard** einzugeben (je nach Token 1 - 2 Mal):

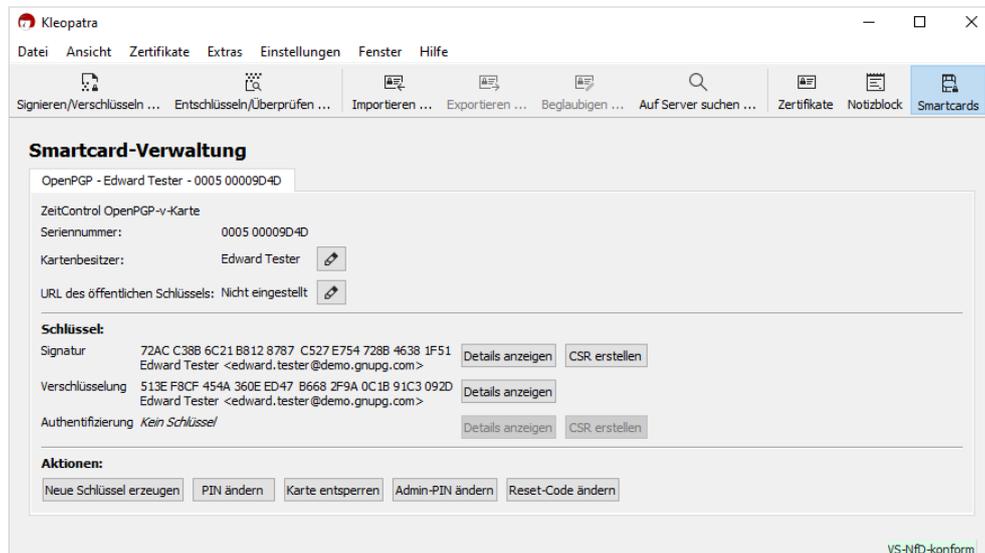


Sie haben auch den zweiten Unterschlüssel (Verschlüsseln) erfolgreich auf Ihre Smartcard übertragen:



Schließen Sie anschließend die Zertifikatsdetails.

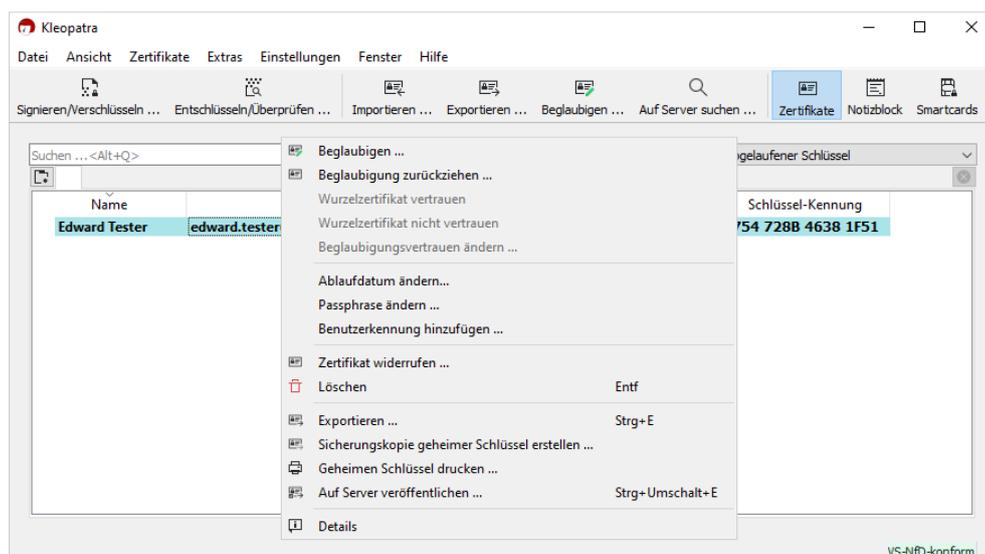
Die übertragenen Schlüssel zum Signieren und Verschlüsseln sind jetzt in der Smartcard-Verwaltung von Kleopatra einsehbar:



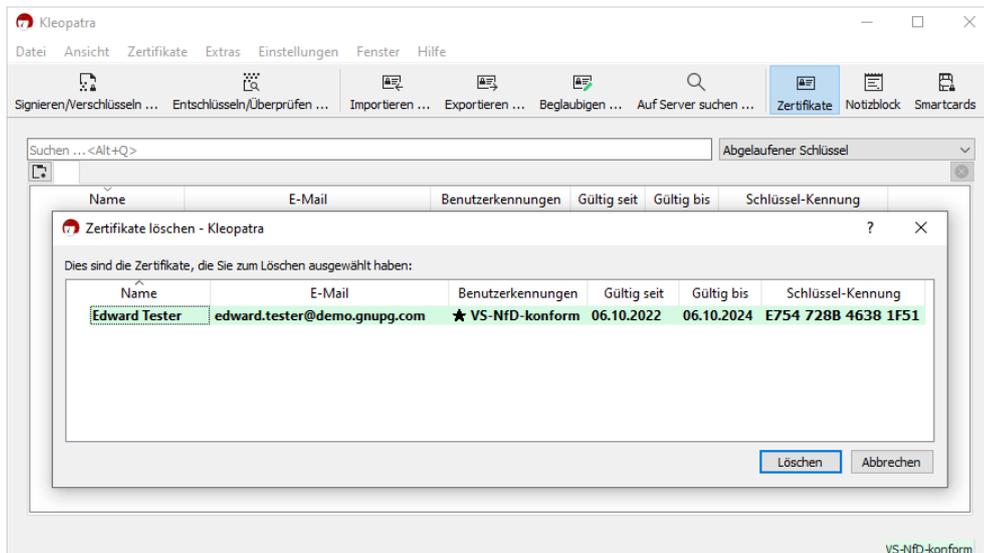
Hinweis | Die Darstellung kann je nach Softwareversion / Smartcard abweichen.

5 Schlüssel löschen

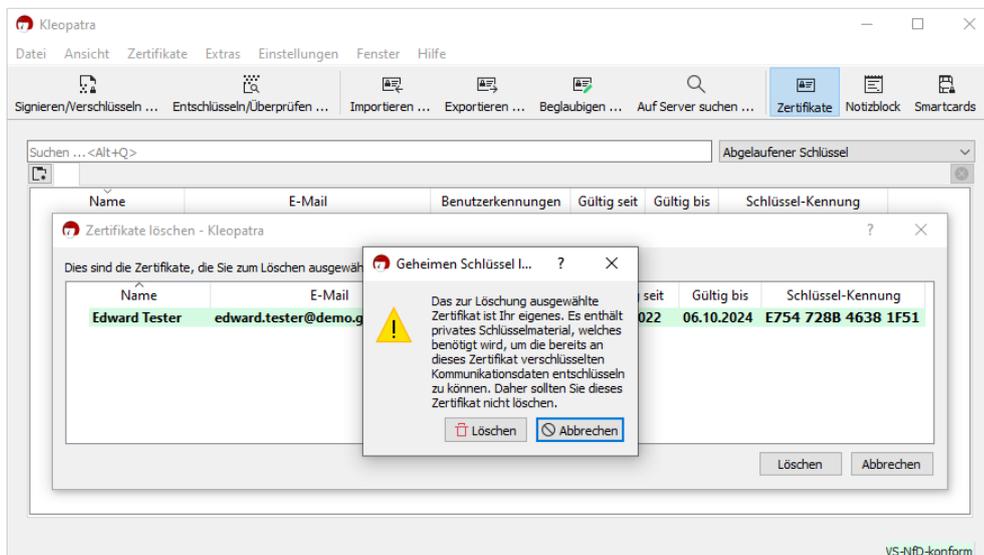
Nachdem Sie Ihren geheimen Schlüssel auf die Smartcard übertragen und **sowohl den geheimen, als auch den öffentlichen Schlüssel gesichert haben**, sollten Sie ihn von Ihrem System löschen. Klicken Sie dazu im Untermenü auf [Löschen]:



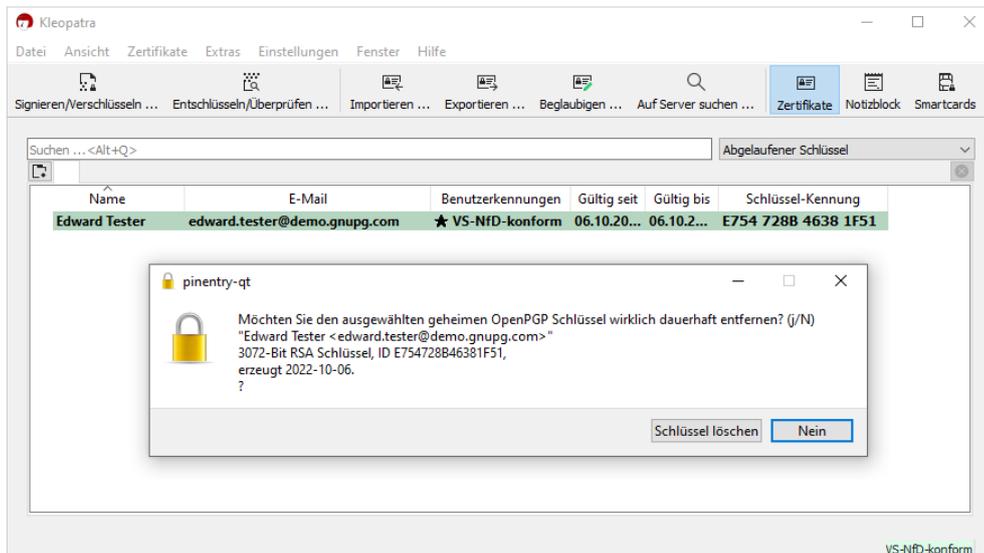
Zur Bestätigung zeigt Ihnen Kleopatra die Zertifikate an, die Sie zum Löschen ausgewählt haben. Bestätigen Sie diesen Dialog und klicken Sie auf [Löschen]:



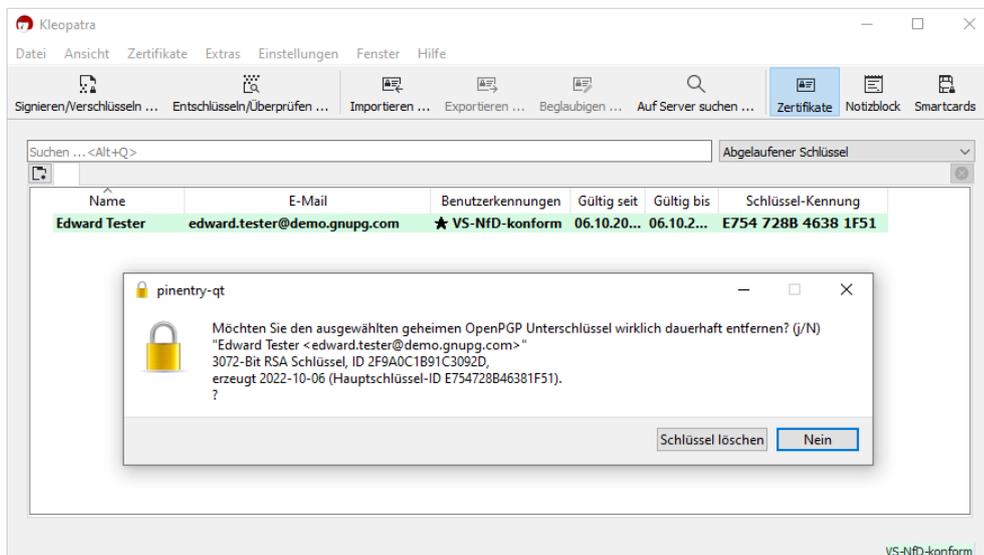
Sie erhalten einen Warnhinweis, da es sich bei der Löschung um privates Schlüsselmaterial handelt. Bestätigen Sie diese Warnung mit [Löschen]:



Es folgt die Information zur Löschung Ihres ersten Unterschlüssels. Bestätigen Sie diese mit [Schlüssel löschen]:



Anschließend folgt der Löschbefehl für Ihren zweiten Unterschlüssel. Bestätigen Sie auch diesen mit [Schlüssel löschen]:

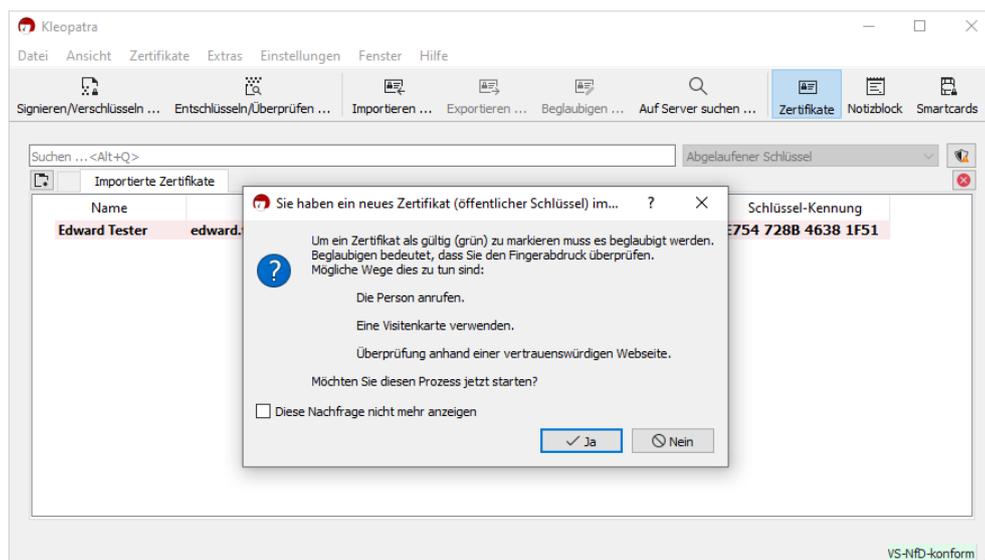


Der ausgewählte Schlüssel wurde gelöscht und wird nicht mehr dargestellt.

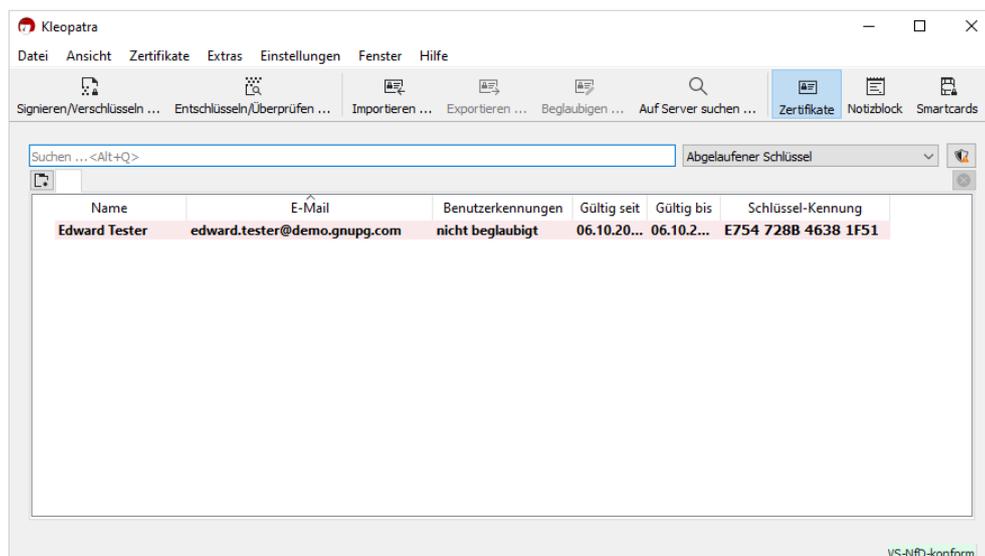
6 Öffentlichen Schlüssel importieren

Da Sie nur den geheimen Schlüssel auf die Smartcard übertragen und das Schlüsselpaar (geheimer und öffentlicher Schlüssel) auf Ihrem Rechner gelöscht haben, müssen Sie nun den öffentlichen Schlüssel wieder importieren. Dieses erfolgt per Doppelklick auf die Datei, die Sie zuvor exportiert haben (siehe Kapitel 3). Alternativ steht Ihnen diese Funktion auch im oberen Menüband zur Verfügung.

Wählen Sie im folgenden Fenster „*Nein*“ auf die Frage hin, ob Sie den Zertifizierungsprozess jetzt starten möchten:

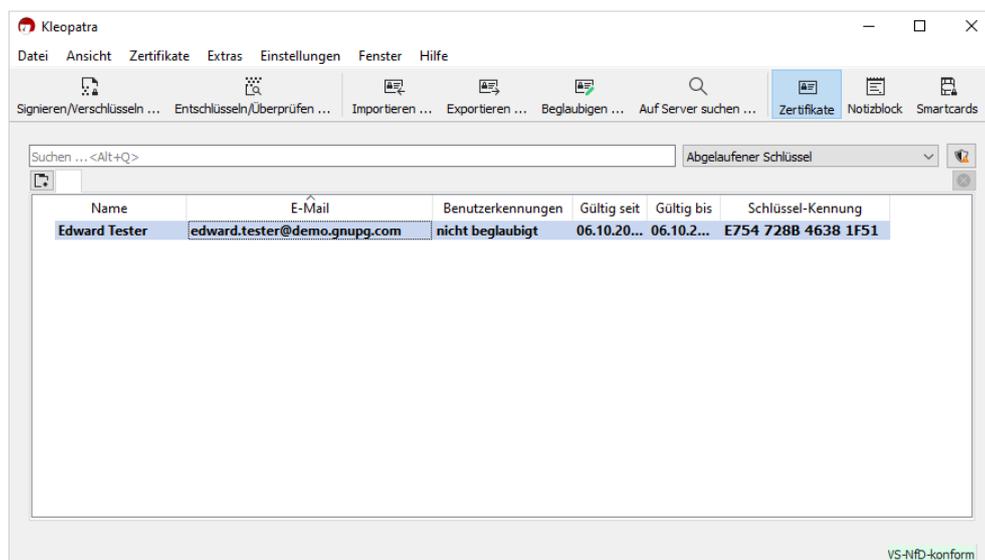


Der importierte Schlüssel wird nun in der Zertifikatsverwaltung dargestellt. Da er noch nicht beglaubigt wurde, wird er als nicht VS-NfD-konform dargestellt:

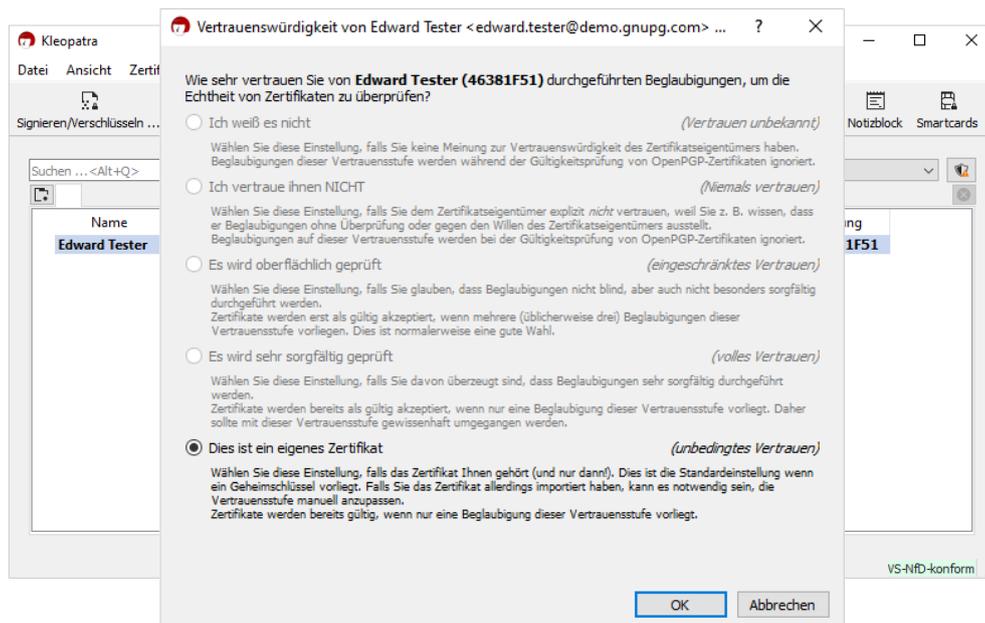


Bevor Sie fortfahren, vergewissern Sie sich, dass der Schlüssel fett gedruckt angezeigt wird. Ist er dies nicht, deutet das darauf hin, dass Kleopatra keinen Zugriff auf den geheimen Schlüssel hat. Wechseln Sie in diesem Fall in die Smartcardverwaltung und drücken Sie [F5]. Nun sollte der Schlüssel in der Zertifikatsverwaltung fett angezeigt sein. Sonst bitte Smartcard entfernen und wieder einstecken und ggf. noch einmal [F5] drücken. Die folgenden Schritte funktionieren nicht, solange der private Schlüssel nicht gefunden wird.

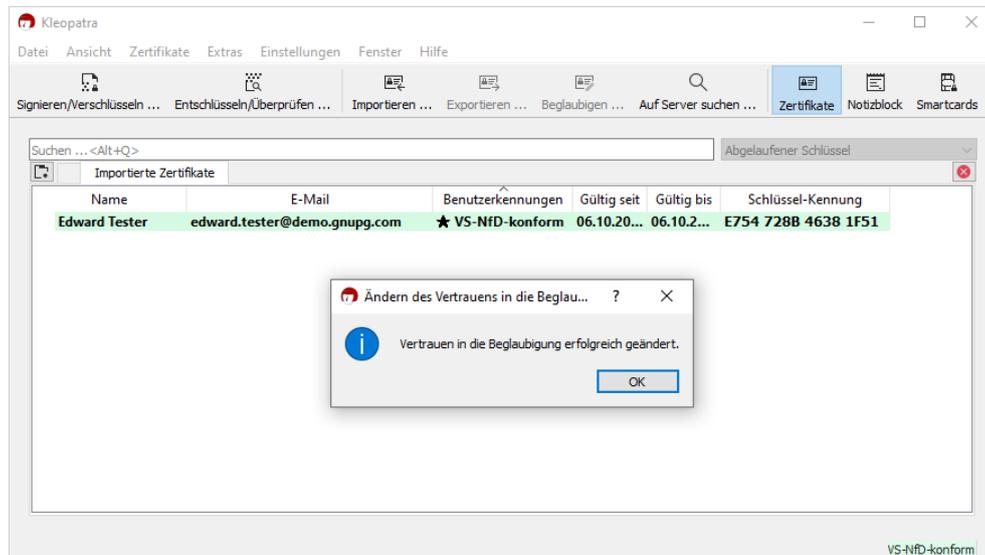
Rechtsklicken Sie nun auf Ihren (fett gedruckten) reimportierten Schlüssel und wählen Sie [Beglaubigungsvertrauen ändern]:



Wählen Sie „Dies ist ein eigenes Zertifikat“ aus und bestätigen Sie mit [OK]:



Nun wird Ihr Schlüssel als VS-NfD-konform dargestellt:



Auf jedem Rechner, an dem Sie die Smartcard einsetzen, müssen Sie den öffentlichen Schlüssel importieren und das Beglaubigungsvertrauen setzen.

7 Smartcard zurücksetzen (Factory Reset)

Falls es nötig ist, mit einer Smartcard noch einmal von vorne zu starten, z.B. weil die zum Testen verwendeten Schlüssel nicht mehr benötigt werden, muss sie zunächst auf ihren Ursprungszustand zurückgesetzt werden. Dies ist nicht in Kleopatra möglich. Hierzu gehen Sie folgendermaßen vor::

- Schließen Sie Kleopatra
- Unter **Linux** muss das GnuPG VS-Desktop® AppImage in einer Shell mit der Option `-c` aufgerufen werden
- Unter **Windows** öffnen Sie die Eingabeaufforderung und geben dort ein:

```
gpg --card-edit
```

Danach sehen Sie einen Prompt

```
gpg/card>
```

Dort geben Sie ein:

```
admin
```

```
factory-reset
```

Hinweis

Mögliche Befehlseingaben können Sie sich durch die Eingabe von „*help*“ anzeigen lassen. Die Eingabe von „*list*“ zeigt Ihnen alle Daten der Karte an.

Folgen Sie anschließend den Anweisungen. Nachdem nun alle Daten von der Smartcard gelöscht sind, können Sie – nachdem Sie die Karte zwischenzeitlich einmal entfernt und neu eingesteckt haben – wieder bei Kapitel 1. anfangen.