

Verschlüsseln und Signieren mit GnuPG VS-Desktop®

Kurzanleitung für Anwender

Die Anleitung gilt entsprechend auch für GnuPG Desktop®

Dokumentversion 2.3

Einleitung

Dies ist eine Kurzanleitung zum schnellen Einstieg in die asymmetrische bzw. Public-Key Verschlüsselung mit GnuPG VS-Desktop®. Nachfolgend finden Sie eine Schritt-für-Schritt-Beschreibung des VS-NfD konformen Ver- und Entschlüsselns von Dateien über das Windows Explorer-Menü.

Die Software unterstützt ebenfalls die weniger sichere symmetrische bzw. passwortbasierte Verschlüsselung. Diese wird in der Kurzanleitung "Passwortbasierte Verschlüsselung mit GnuPG VS-Desktop®" beschrieben.

Bitte beachten Sie auch die Informationen ihrer Geheimschutzbeauftragten, die Verschlussachenanweisung und das Handbuch zur Zulassung von GnuPG VS-Desktop® vom BSI.

Funktionsbeschreibung

GnuPG VS-Desktop® ermöglicht Ihnen eine programmübergreifende Ende-zu-Ende-Verschlüsselung, mit der Sie Mails und Dateien sowohl ver- und entschlüsseln, als auch digitale Signaturen erzeugen und prüfen können. Es besteht aus unabhängig entwickelten Programmen, u.a. dem Zertifikatsmanager Kleopatra, der Outlook-Erweiterung GpgOL zur Mailverschlüsselung sowie dem Windows Plug-in GpgEX für die Datenverschlüsselung.

Smartcards bzw. Security-Token können optional beim Einsatz von GnuPG VS-Desktop® verwendet werden. Dann ist das geheime Schlüsselmaterial darauf gespeichert und signifikant besser gegen unbefugten Zugriff gesichert.

Es ist empfehlenswert, sich bei technischen Fragen oder Unklarheiten an ihre IT Administration bzw. ihren IT Support zu wenden.

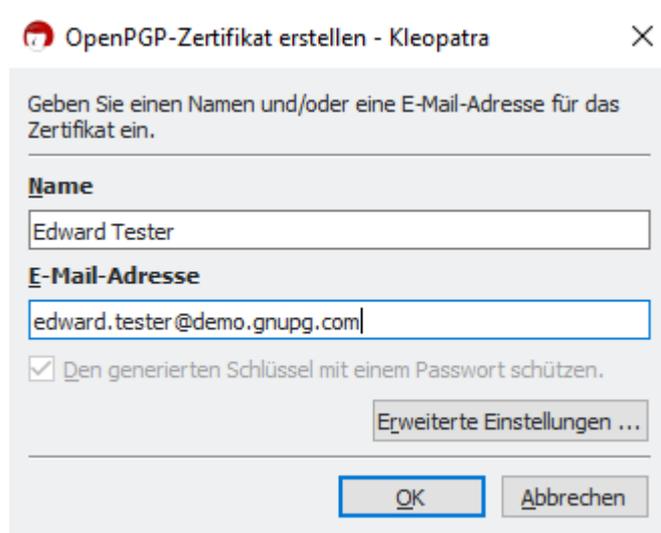
1 Schlüssel erstellen

Falls Sie noch kein eigenes OpenPGP Schlüsselpaar erstellt bzw. importiert haben, sehen Sie beim Start von Kleopatra die „Willkommensansicht“. Sollten Sie bereits einen eigenen Schlüssel haben, können Sie ihn nun importieren. Ansonsten klicken Sie auf den Button **Neues Schlüsselpaar**:



Sollte die Willkommensnachricht nicht erscheinen, weil bereits Schlüssel oder Zertifikate vorhanden sind, können neue Schlüssel über **Datei** > **Neues Schlüsselpaar** erstellt werden.

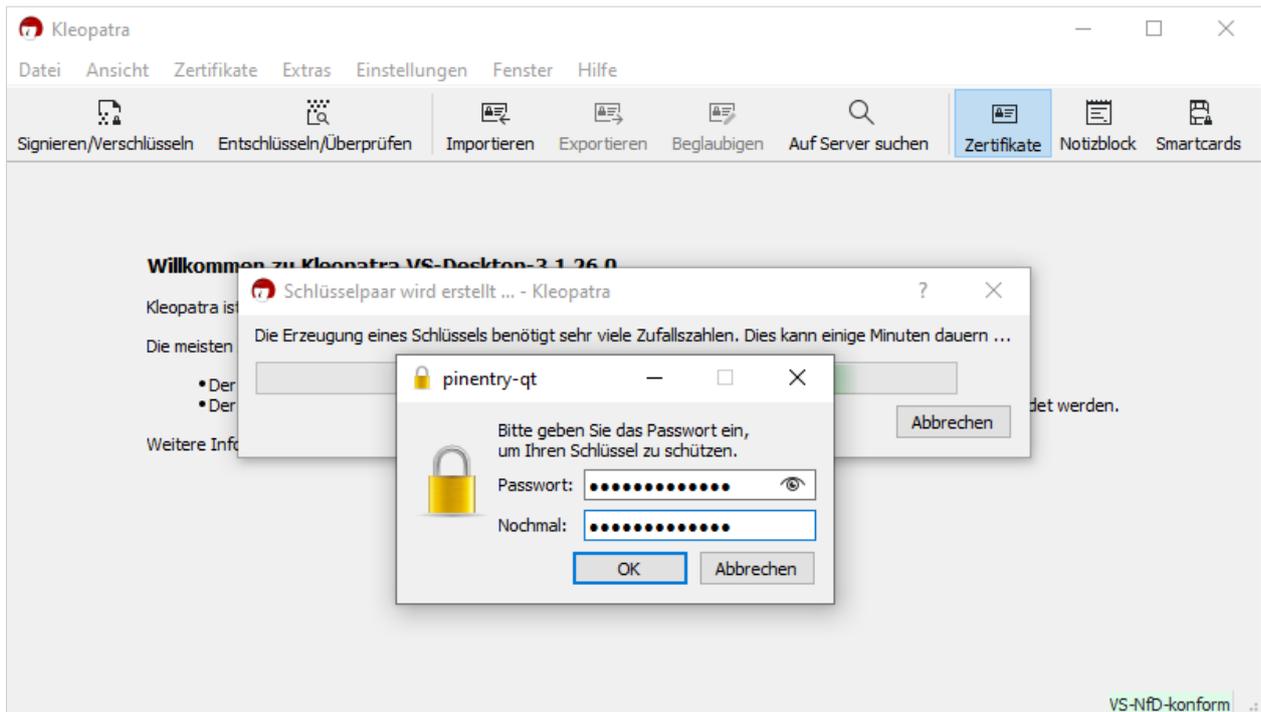
Geben Sie einen Namen und eine Mailadresse ein und klicken Sie auf **OK**:




Hinweis

Schlüssel müssen nicht immer an eine Mail-Adresse gebunden sein. Ebenso können Sie z.B. auch Projekt- oder Gruppennamen verwenden.

Anschließend werden Sie aufgefordert, ein Passwort mit mind. 9 Zeichen einzugeben. Verwenden Sie am besten unsinnige Wortketten oder Sätze, welche Sie sich leicht merken können. Beachten Sie dabei ggf. Ihre internen Passwortrichtlinien:

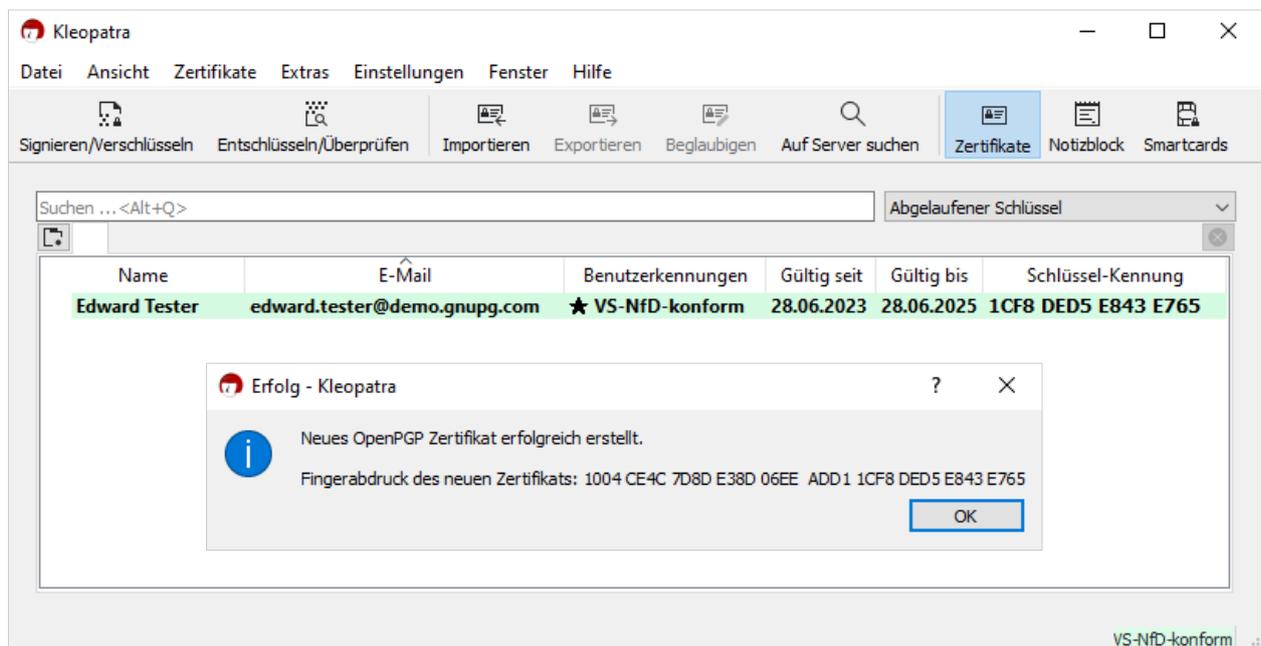

Wichtig

Das Passwort des Schlüssels kann **nicht** zurückgesetzt werden. Wenn Sie das Passwort verlieren, können Sie an diesen Schlüssel verschlüsselte Daten nicht mehr entschlüsseln. Sie sollten das Passwort also sofort notieren und sicher sowie VS-NfD konform aufbewahren.

Sie haben jedoch unendlich viele Versuche, um ein Passwort für einen OpenPGP Schlüssel einzugeben, der auf der Festplatte gespeichert ist. Die angezeigten 3 Versuche können immer wiederholt werden. (Dies **gilt nicht für PINs**, also wenn der Schlüssel sich auf einer Smartcard befindet.)

Sowohl der geheime Teil des OpenPGP Schlüssels als auch das dazugehörige Passwort sind zu behandeln sind wie Informationen mit der Einstufung „Verschlussache – Nur für den Dienstgebrauch“ (VS-NfD). Es gelten die entsprechenden Schutzmaßnahmen.

Kleopatra zeigt Ihnen abschließend an, ob die Generierung erfolgreich war. Bestätigen Sie den Dialog mit **OK**. Ihr neuer Schlüssel erscheint in der Zertifikatsliste:



Ein mit GnuPG VS-Desktop® erstellter Schlüssel hat standardmäßig eine Gültigkeitsdauer von 3 Jahren (ab Version 3.2.0, vorher 2 Jahre), das ist die vom BSI empfohlene Zeitspanne.

Einige Zeit (z.B. einen Monat) vor dem Ablauf Ihres Schlüssels sollten Sie ihn per Rechtsklick → **Ablaufdatum ändern** verlängern.

Sowohl nach der Erstellung als auch der Verlängerung Ihres OpenPGP Schlüssels müssen Sie das dazugehörige Zertifikat (= öffentlicher Schlüssel) an Ihre Kommunikationspartner verteilen, siehe nächstes Kapitel.

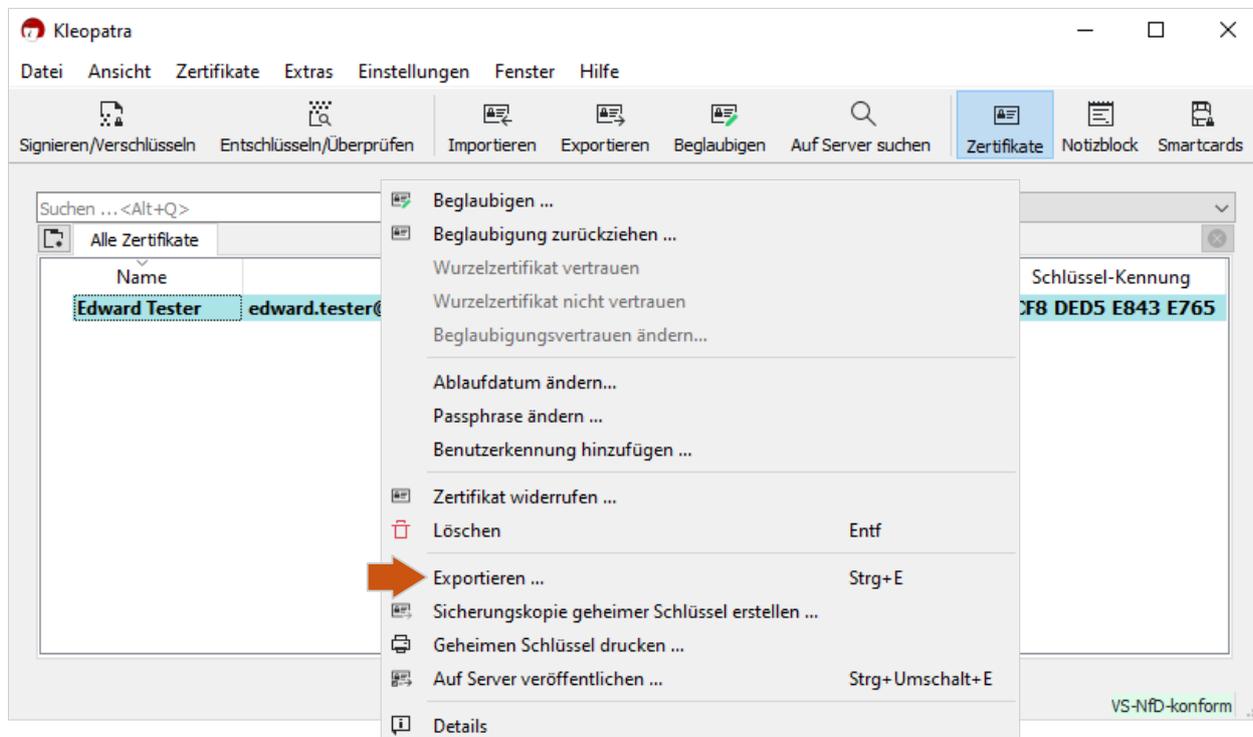
Hinweis

Wenn Sie bei der Verwendung Ihres **auf dem Computer gespeicherten** OpenPGP Schlüssels nach dem dazu gehörenden Passwort gefragt werden, wird bei einem Fehlversuch der Hinweis gezeigt, dass nur noch 2 Versuche verbleiben und so fort. Dies bezieht sich nur auf den aktuellen Vorgang. Sie können den Vorgang beliebig oft wiederholen und haben jeweils erneut 3 Versuche.

Bitte beachten Sie: **Bei der Verwendung von Smartcards gilt dies nicht!** Smartcards werden gesperrt, sobald deren PIN 3x falsch eingegeben wurde.

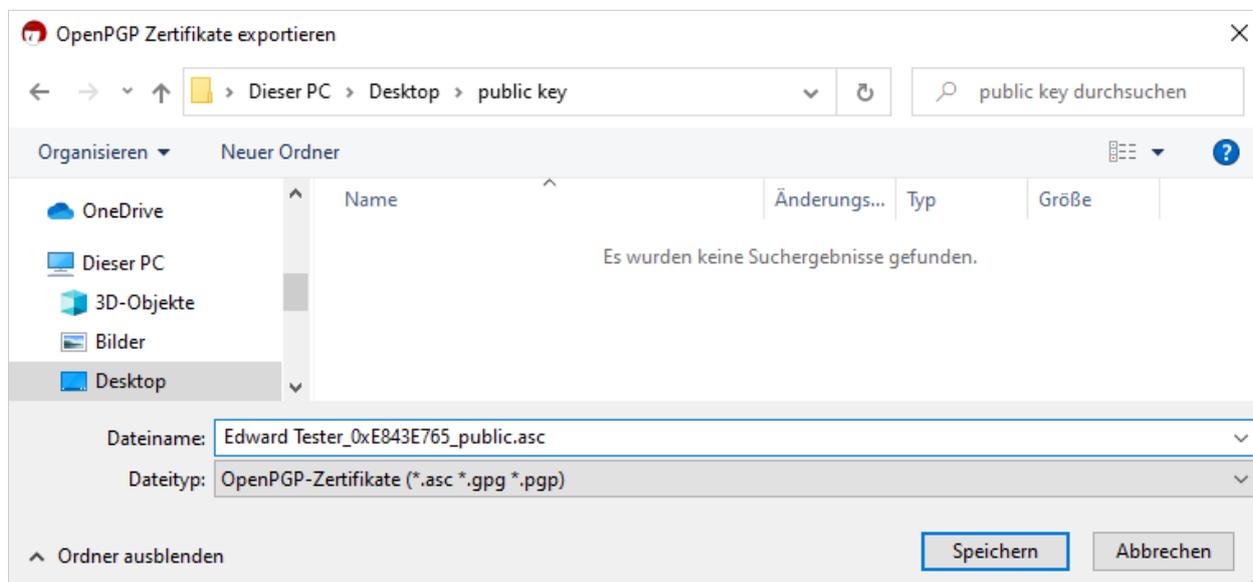
2 Zertifikate verteilen

Öffnen Sie mit der rechten Maustaste das Kontextmenü Ihres Schlüssels und klicken Sie auf **Exportieren**. Diesen Befehl finden Sie auch im oberen Menüband:



Sie können beliebig viele Zertifikate auf einmal exportieren.

Wählen Sie anschließend ein Verzeichnis und einen Dateinamen für Ihren öffentlichen Schlüssel bzw. Ihr Zertifikat und klicken Sie **Speichern**:



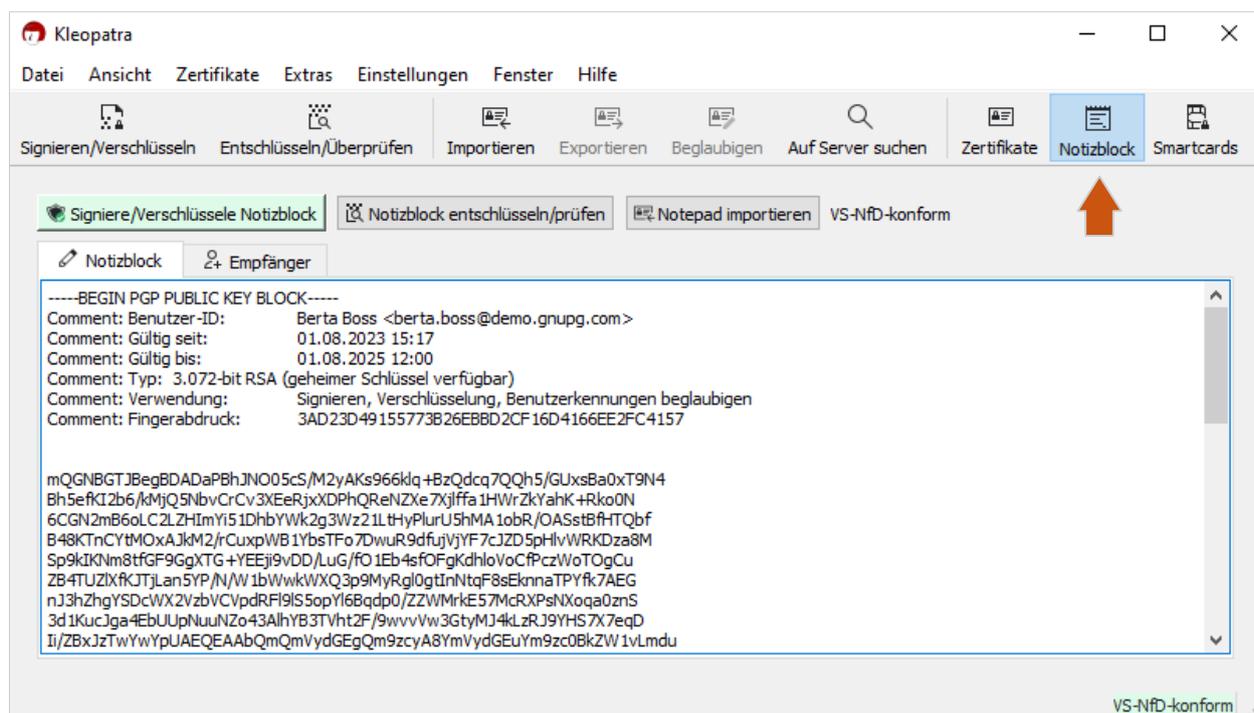


Öffentliche Schlüssel (Zertifikate) sind nicht eingestuft und dürfen unverschlüsselt versendet werden. Der Fingerabdruck gewährleistet dabei Integrität.

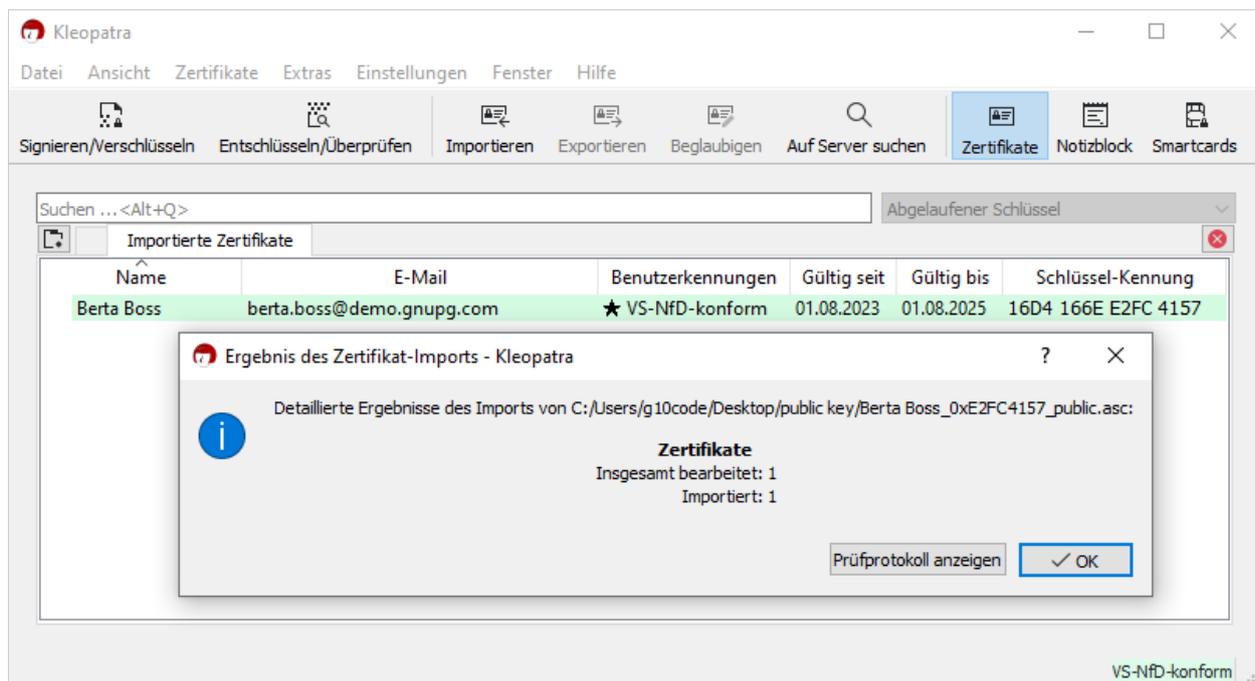
3 Zertifikate importieren

Für eine sichere Kommunikation benötigen Sie die öffentlichen Schlüssel bzw. Zertifikate Ihrer Kommunikationspartner. Wenn Sie diese als Datei erhalten, üblicherweise mit der Dateiendung ***.asc** oder ***.key**, können Sie sie per Doppelklick importieren.

Alternativ ist es auch gebräuchlich, öffentliche Schlüssel, z.B. von Webseiten, als Textblock per Kopieren/Einfügen in Kleopatra zu importieren. Dazu verwenden Sie die **Notizblock**-Funktion:

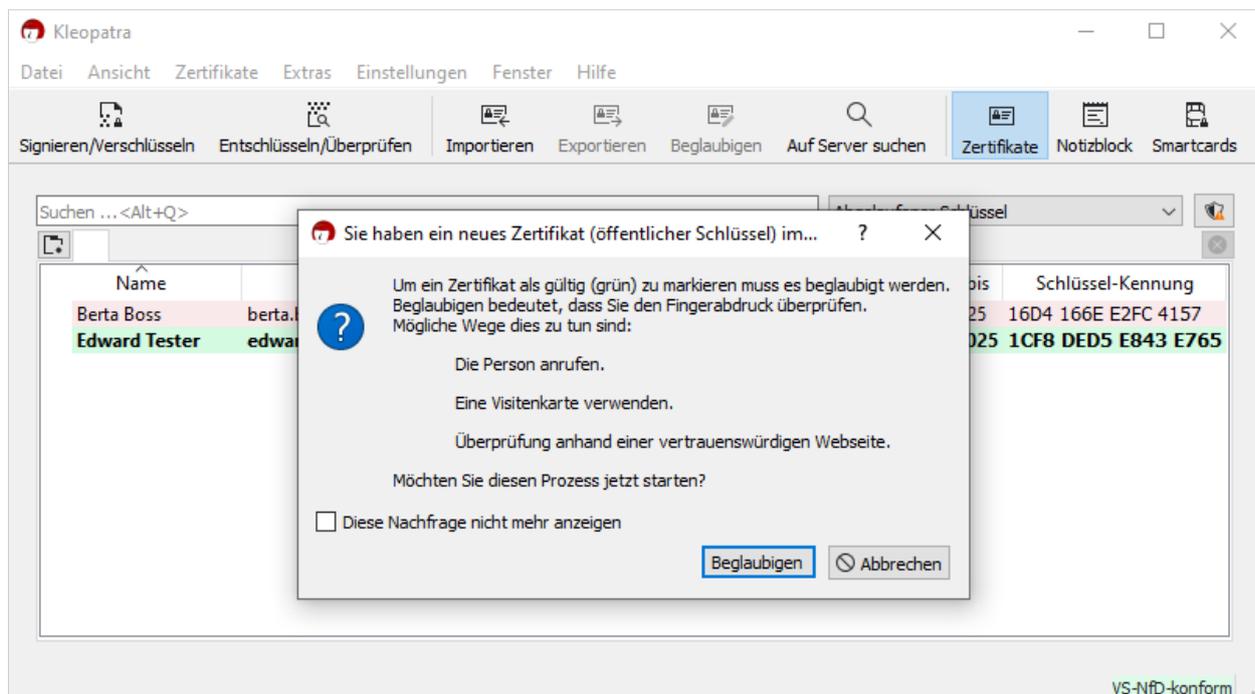


Falls das importierte Zertifikat bereits durch Ihre Organisation beglaubigt wurde, werden Sie lediglich über den Import informiert. Es ist dann grün hinterlegt und als VS-NfD konform markiert:



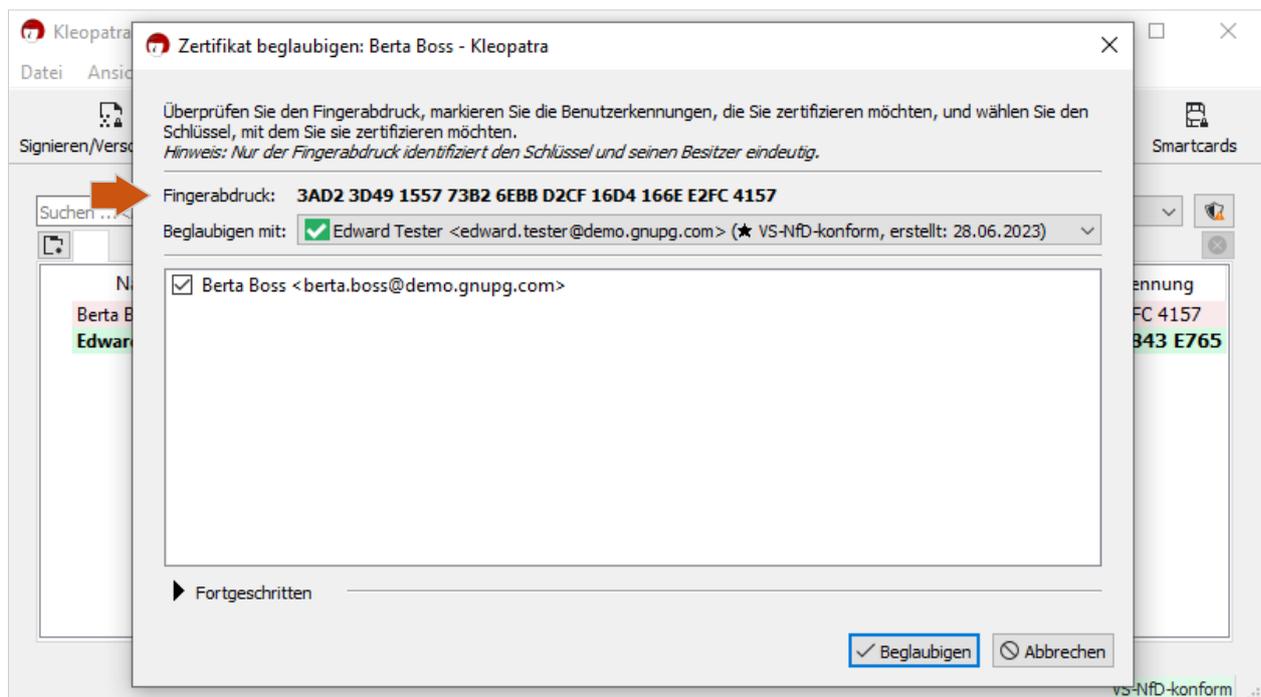
In diesem Fall fahren Sie mit Kapitel 5 fort.

Anderenfalls werden Sie gefragt, ob Sie das Zertifikat jetzt beglaubigen wollen:



Wir empfehlen, mit **Beglaubigen** zu bestätigen.

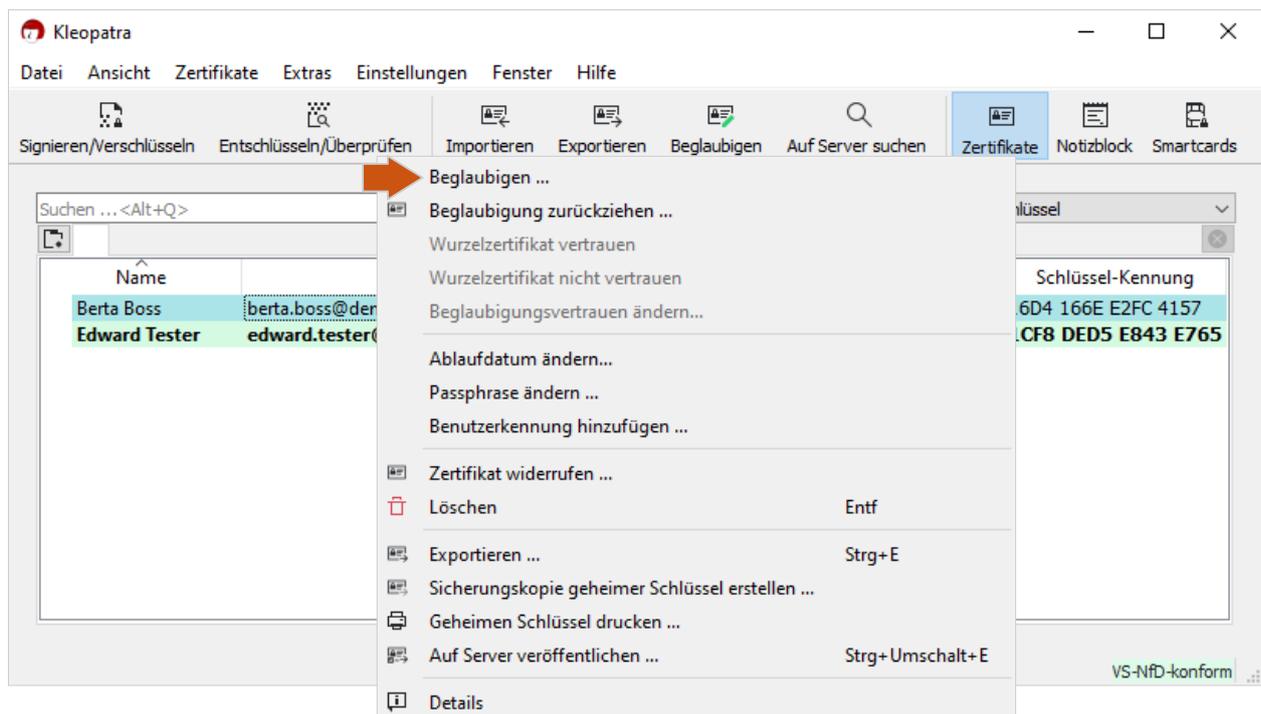
Verifizieren Sie den Fingerabdruck über einen zweiten Kanal, z.B. telefonisch, und klicken Sie abschließend auf **Beglaubigen** :



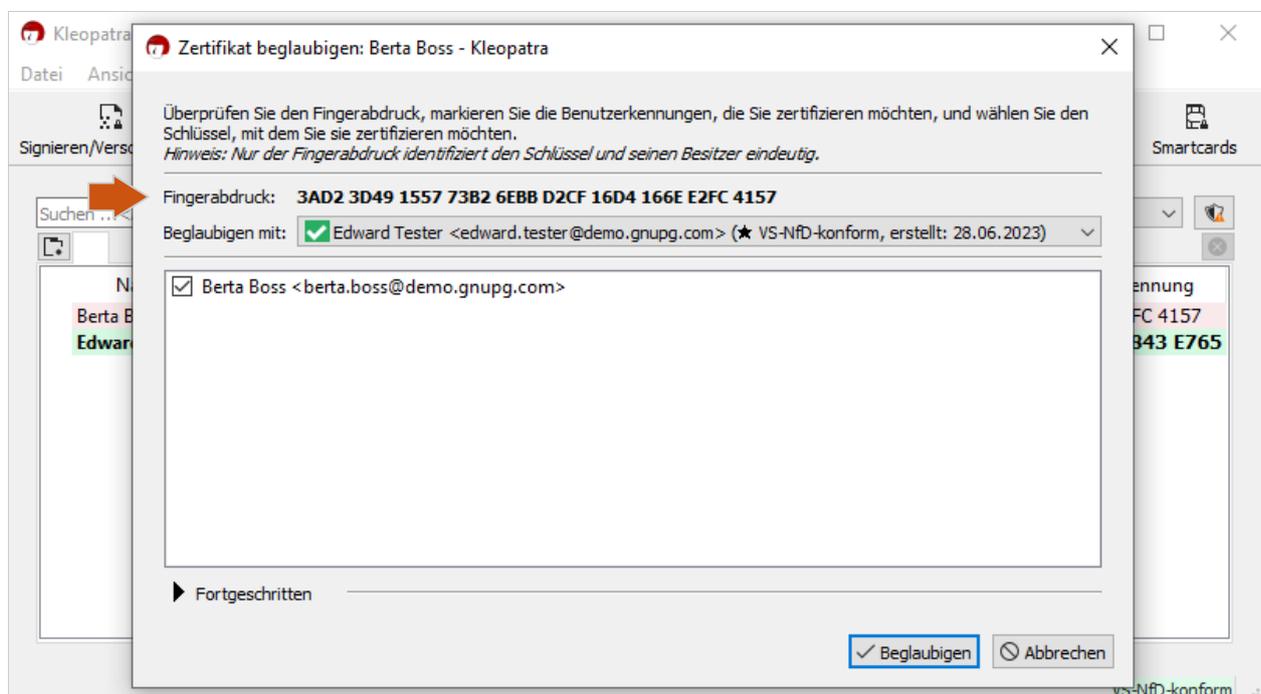
4 Vertrauen und Beglaubigungen

Damit ein Schlüssel bzw. Zertifikat zur VS-NfD konformen Kommunikation verwendet werden darf, muss er/es beglaubigt sein. Idealerweise hat das Ihre Organisation bereits für Sie übernommen.

Wurde ein Zertifikat von keiner vertrauenswürdigen Instanz beglaubigt, ist es rot hinterlegt und mit "nicht beglaubigt" gekennzeichnet. In diesem Fall sind Sie in der Verantwortung, es zu beglaubigen. Gehen Sie dazu mittels Rechtsklick in das Kontextmenü des importierten Zertifikats und wählen Sie **Beglaubigen**. Diesen Befehl finden Sie auch im oberen Menüband von Kleopatra:

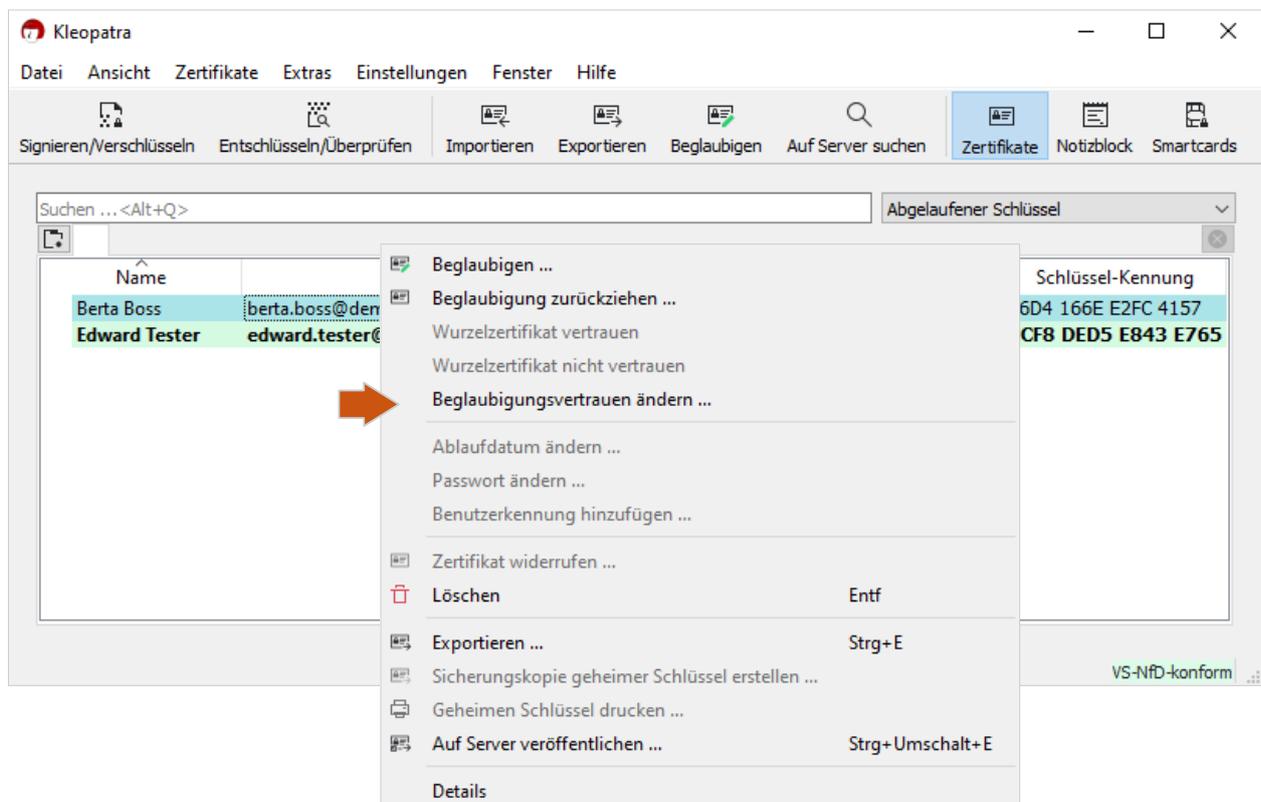


Überprüfen bzw. vergleichen Sie den Fingerabdruck über einen zweiten Kanal, z.B. telefonisch, und klicken Sie abschließend auf **Beglaubigen** :

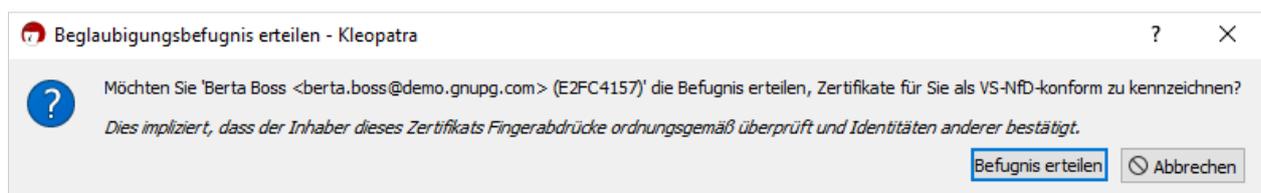


Die Fingerabdruck-Prüfung muss innerhalb einer Organisation nur einmal erfolgen. Hat z.B. ein Kollege den Fingerabdruck bereits telefonisch geprüft, können Sie für das Zertifikat des Kollegen das Beglaubigungsvertrauen auf "volles Vertrauen" setzen; seine Beglaubigungen werden dann auch von Ihnen akzeptiert.

Gehen Sie dazu mittels Rechtsklick in das Kontextmenü des betreffenden Zertifikats und wählen Sie **Beglaubigungsvertrauen ändern** :



Wählen Sie im anschließenden Dialog **Befugnis erteilen** aus:



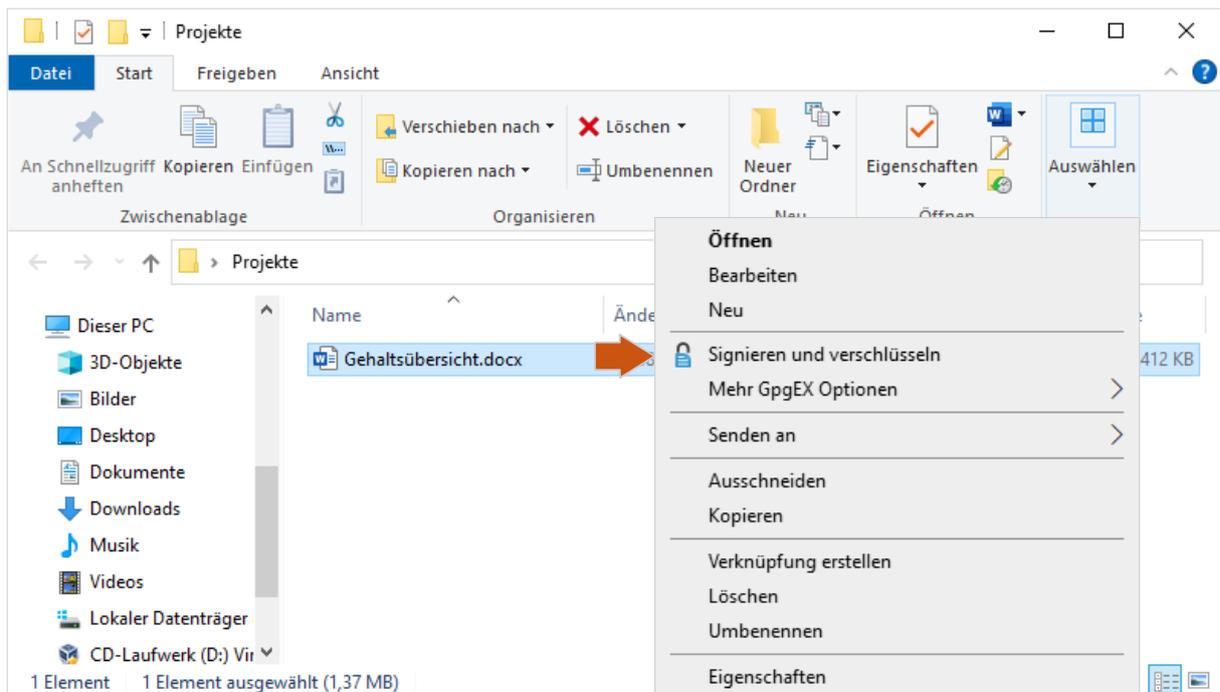
Falls das ausgewählte Zertifikat bereits über ein Beglaubigungsbefugnis verfügt, ermöglicht Ihnen das Dialogfenster, die Befugnis zu widerrufen.

Hinweis

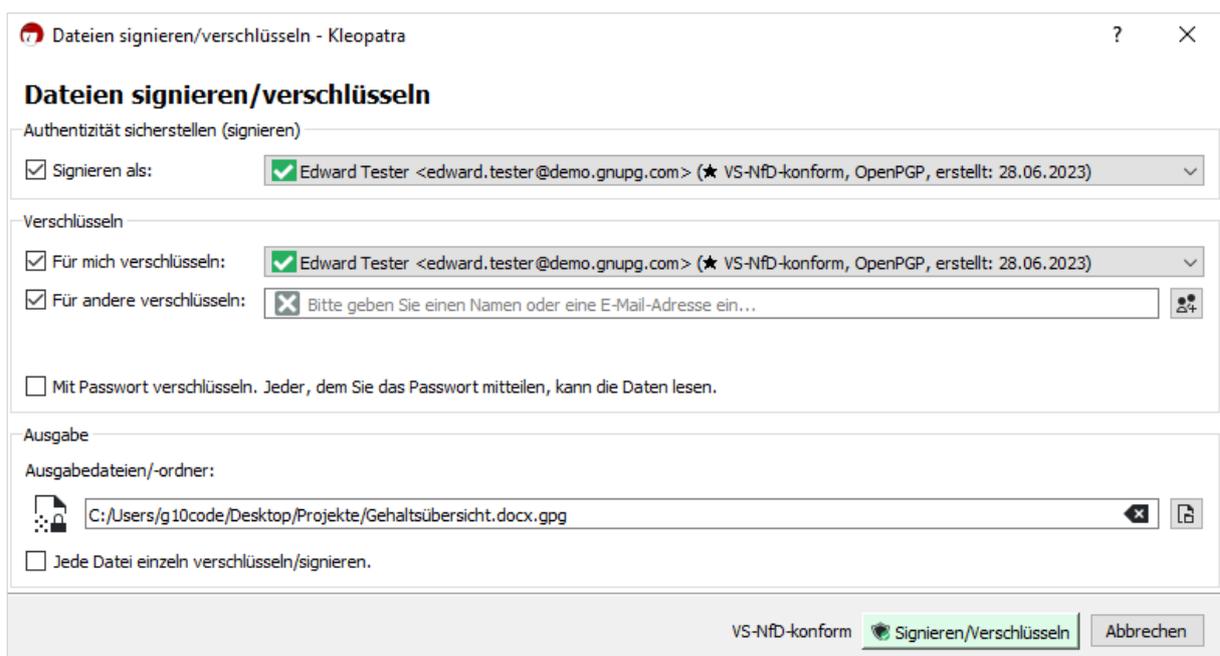
Sie können in der Zertifikatsansicht von Kleopatra per Rechtsklick Spalten einblenden. Eine optionale Spalte ist das Beglaubigungsvertrauen. Bei "vollständig" oder "ultimativ" besteht Beglaubigungsbefugnis.

5 Daten verschlüsseln

Markieren Sie im Windows Explorer¹ ein oder mehrere Dateien bzw. Ordner, die Sie verschlüsseln möchten. Öffnen Sie mit der rechten Maustaste das Kontextmenü und wählen Sie **Signieren und verschlüsseln** :



Wählen Sie hier aus, wer Ihre Datei entschlüsseln können soll:



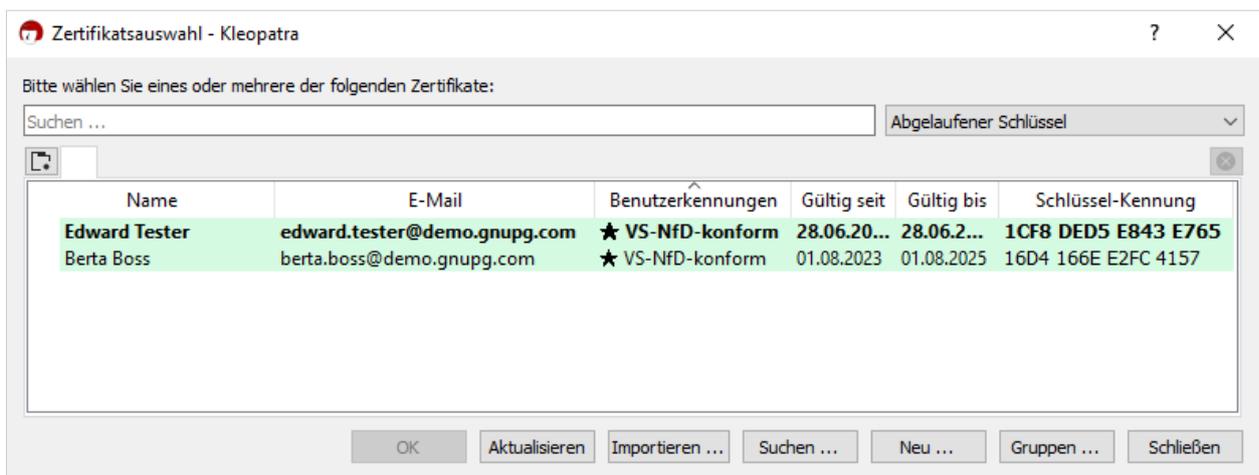
¹ Falls Sie den Weg über „(Ordner) Signieren/Verschlüsseln“ in Kleopatra gehen, beachten Sie, dass hier jeweils nur Ordner oder nur Dateien ausgewählt werden können.


Wichtig

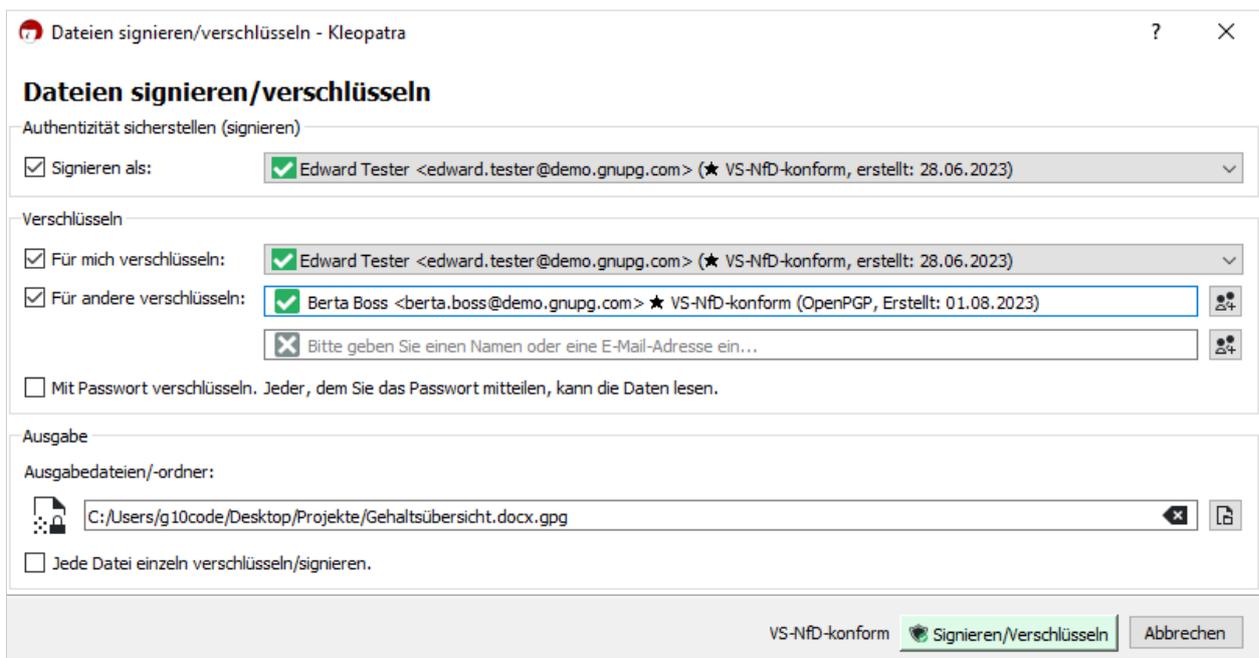
Wenn Sie keine weiteren Empfänger eintragen, kann niemand außer Ihnen die Datei entschlüsseln!

Tippen Sie im Feld "Für andere Verschlüsseln" den Namen des gewünschten Empfängers, um ein Zertifikat auszuwählen.

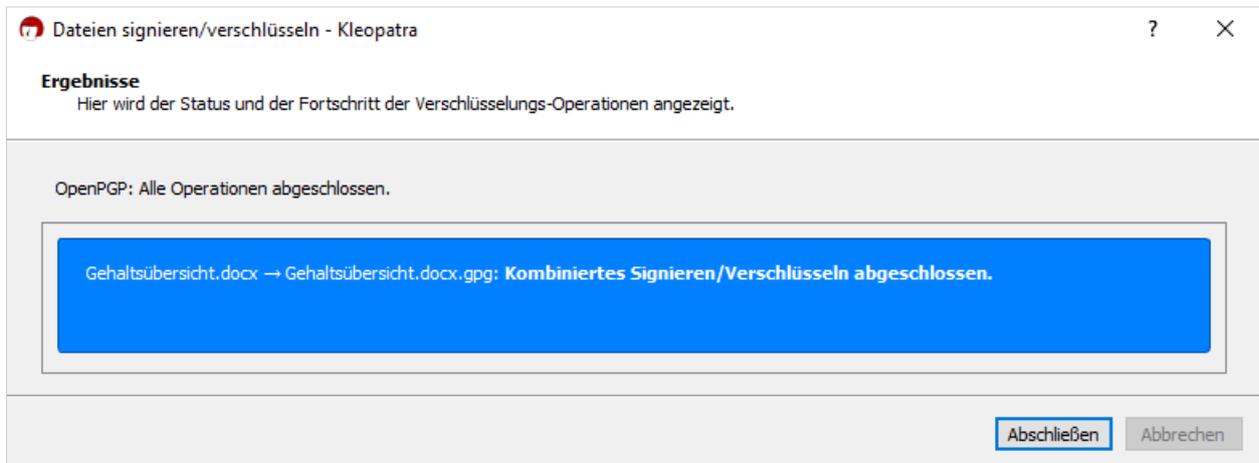
Alternativ öffnen Sie mit dem Button am rechten Rand der Empfängerzeile den Auswahldialog, sozusagen Ihr persönliches Krypto-Adressbuch:



Nach Eingabe der Empfänger wählen Sie den Ort, wo Ihre Datei abgelegt werden soll und klicken auf **Signieren / Verschlüsseln** :

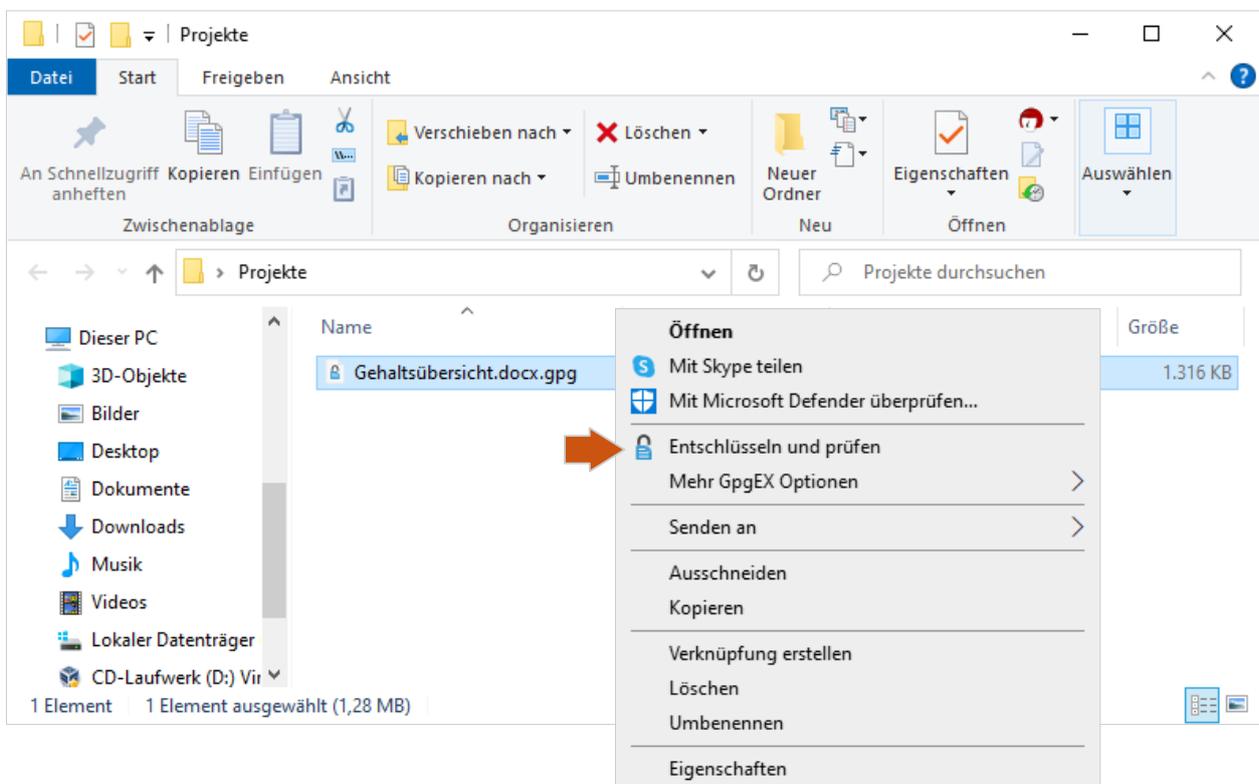


Kleopatra zeigt Ihnen an, ob die Dateiverschlüsselung erfolgreich war. Zum Beenden klicken Sie auf **Abschließen** :

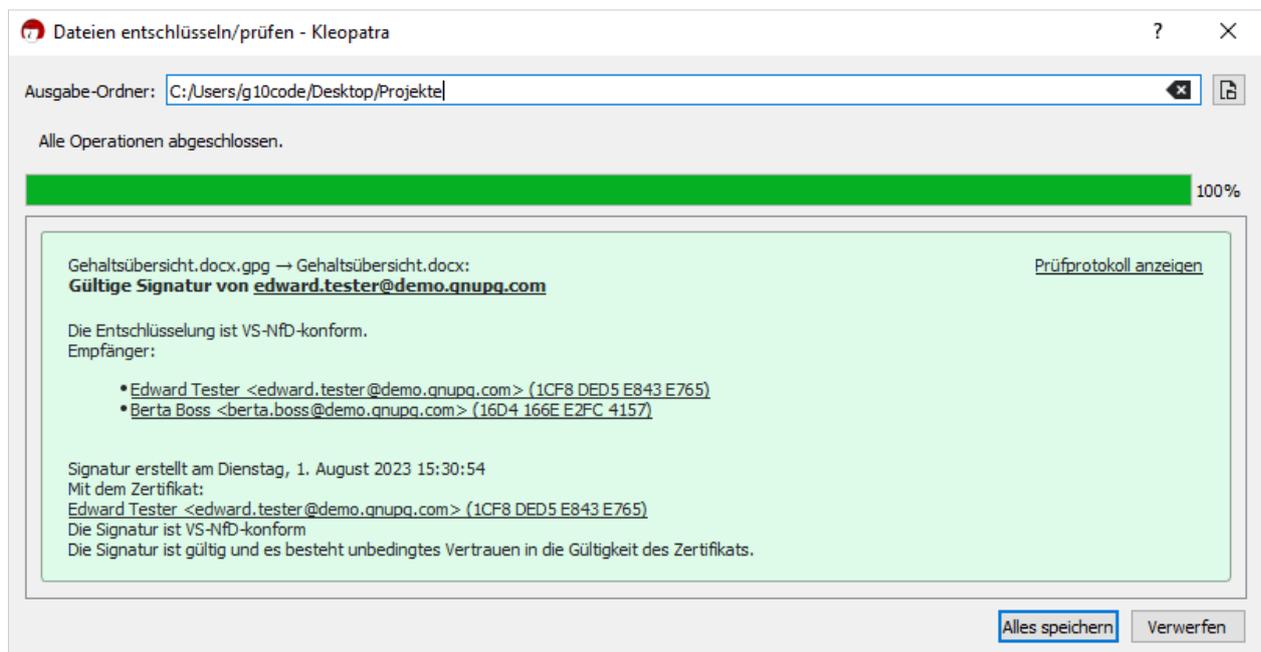


6 Daten entschlüsseln

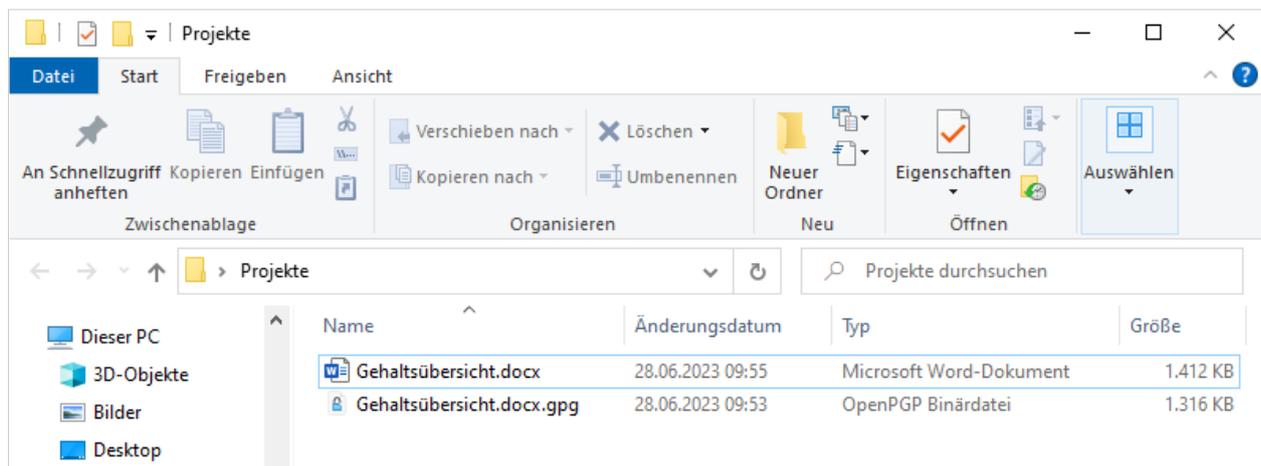
Wählen Sie ein oder mehrere verschlüsselte Dateien aus. Öffnen Sie anschließend mit der rechten Maustaste das Kontextmenü und wählen Sie **Entschlüsseln und prüfen** . Alternativ doppelklicken Sie auf die verschlüsselte Datei:



Kleopatra zeigt Ihnen nun an, ob die Entschlüsselung erfolgreich war und was die Signaturprüfung ergeben hat:

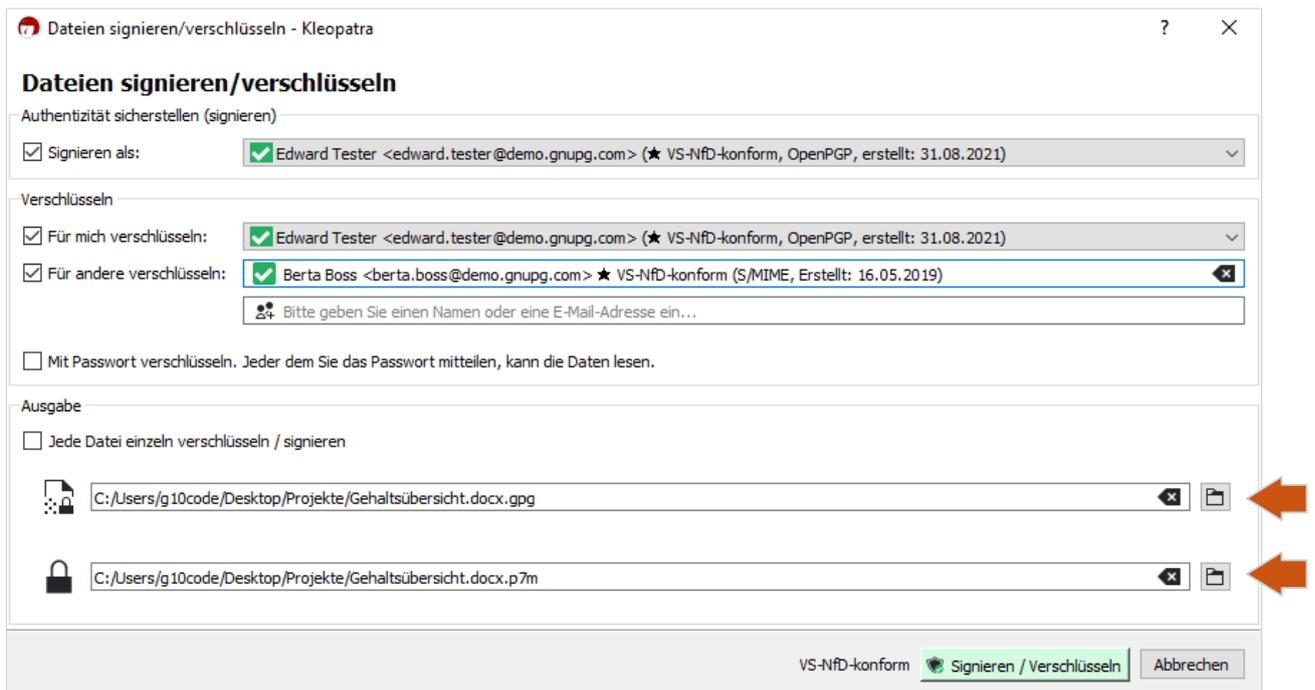


In diesem Fenster können Sie auch den Ort ändern, an dem die entschlüsselte Datei abgelegt werden soll. Voreingestellt ist der Ordner, in dem sich die verschlüsselte Datei befindet. Klicken Sie auf [Alles speichern](#) um die entschlüsselte Datei am gewünschten Ort abzulegen:



7 Kombinierte Verschlüsselung mit OpenPGP und S/MIME

Es kann vorkommen, dass Ihre Kommunikationspartner Ihnen ausschließlich S/MIME Zertifikate zur Verfügung stellen. Das ist kein Problem, denn Sie brauchen kein eigenes S/MIME-Zertifikat, um an S/MIME-Empfänger zu verschlüsseln. In diesem Fall erhalten Sie zwei Dateiformate als Ausgabe:



Die ***.p7m**-Datei geben Sie Ihren S/MIME - Kommunikationspartnern, die ***.gpg** Datei Ihren OpenPGP - Kommunikationspartnern.

8 Schlüssel verlängern

Da ein OpenPGP Schlüssel laut Empfehlung des BSI maximal 3 Jahre gültig sein sollte, läuft ein mit GnuPG VS-Desktop® nach dieser Frist ab und kann nicht mehr zum Verschlüsseln und Signieren verwendet werden, wenn man ihn nicht verlängert. Falls es keinen Anhaltspunkt dafür gibt, dass der Schlüssel kompromittiert wurde (Sicherheitsvorfall), wird man ihn i.d.R. verlängern.

Für die Verlängerung des eigenen Schlüssels müssen Sie lediglich im Kontextmenü (Rechtsklick) "Ablaufdatum ändern" auswählen. Dann können Sie das gewünschte Ablaufdatum wählen.

Optimalerweise verlängert man bereits etwas vor Ablauf der Gültigkeit, aber auch nach Ablauf ist eine Verlängerung möglich.

Nach der Verlängerung muss das Zertifikat erneut verteilt werden. Es kann entweder erneut auf den konfigurierten LDAP-Server hochgeladen werden (via Kontextmenü "Auf Server veröffentlichen ...") und/oder exportiert und auf beliebigem Wege wieder an die Kommunikationspartner verteilt werden mit der Anweisung, es zu importieren. Ansonsten bekommen sie weiterhin das "alte" Ablaufdatum für das Zertifikat angezeigt und können es nach diesem Datum nicht mehr verwenden, um Daten für Sie zu verschlüsseln.

9 Weitere Informationen

Sollten Sie weitere Fragen haben, schauen Sie bitte auch auf unserer Webseite nach: <https://gnupg.com/kb/faq-usage.de.html>

Anhang

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.