

# Passwortbasierte Verschlüsselung mit GnuPG VS-Desktop®

## Kurzanleitung für Anwender

Die Anleitung gilt entsprechend auch für GnuPG Desktop®

Dokumentversion 2.1

## Einleitung

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

Die Software unterstützt ebenfalls die asymmetrische Public Key Verschlüsselung. Diese wird in unserem Guide "Verschlüsseln und Signieren mit GnuPG VS-Desktop®" beschrieben.

## Funktionsbeschreibung

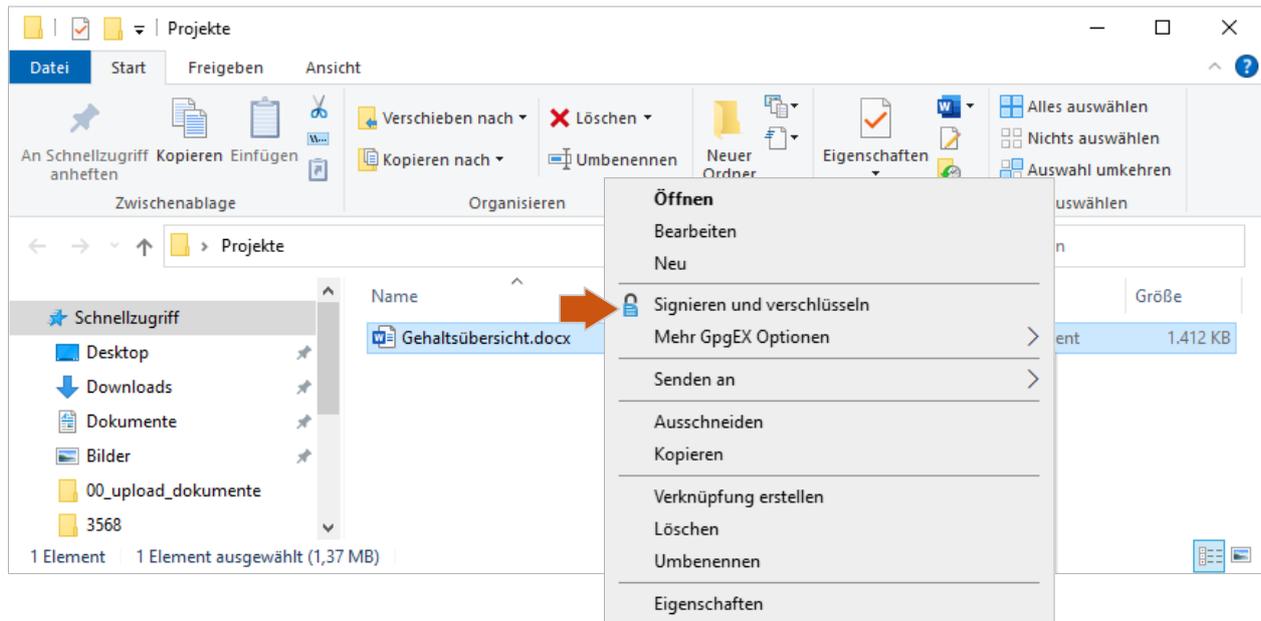
GnuPG VS-Desktop® bietet Ihnen die Möglichkeit, Dateien und Ordner einfach und schnell durch die Eingabe eines geeigneten Passworts zu ver- und entschlüsseln.



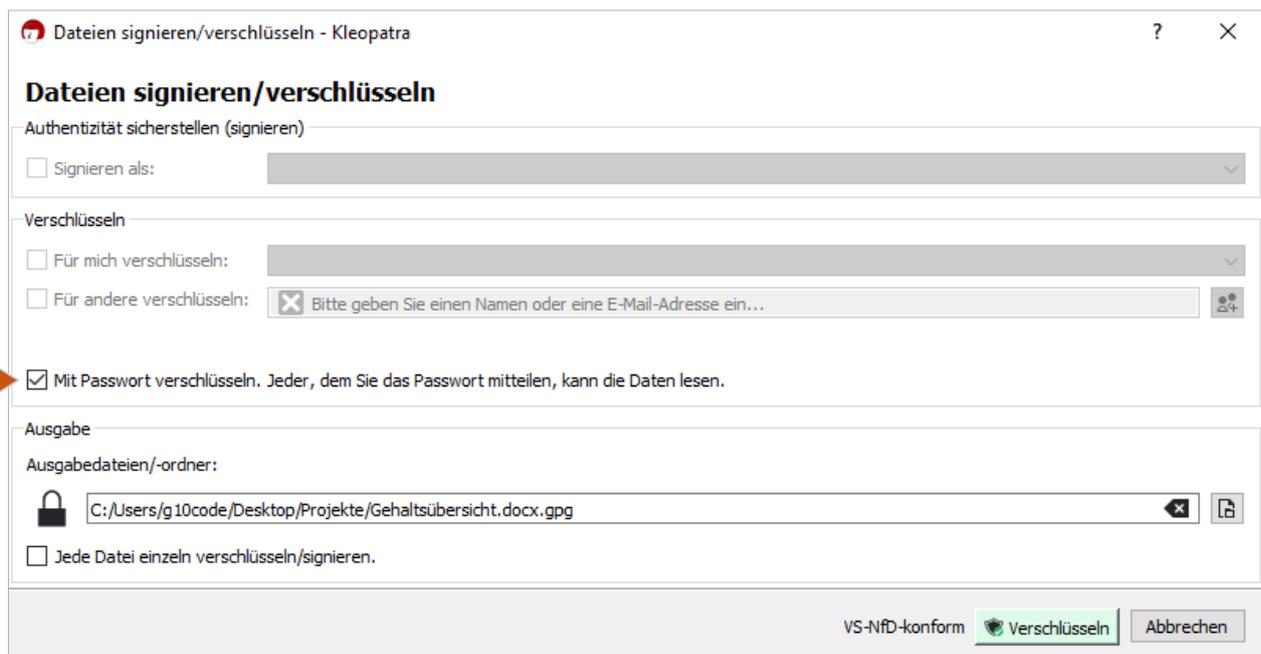
Das Video zur passwortbasierten Dateiverschlüsselung finden Sie hier:  
<https://media.gnupg.org/sc/gnupg-vsd-symmetrische-verschluesselung.mp4>

# 1 Verschlüsseln

Wählen Sie im Windows Datei-Explorer<sup>1</sup> eine oder mehrere Dateien bzw. Ordner aus, die Sie verschlüsseln möchten. Öffnen Sie mit der rechten Maustaste das Untermenü und klicken Sie **Signieren und Verschlüsseln** :



Es öffnet sich der "Dateien signieren/verschlüsseln"-Dialog. Wenn keine Schlüssel oder Zertifikate in Kleopatra erstellt oder importiert wurden, wird standardmäßig die passwortbasierte Verschlüsselung voreingestellt:



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

Sollten bereits Schlüssel vorhanden sein, entfernen Sie die Häkchen bei "Signieren als" sowie bei "Für mich verschlüsseln" und "Für andere verschlüsseln". Setzen Sie statt dessen das Häkchen bei "Mit Passwort verschlüsseln. Jeder, dem Sie das Passwort mitteilen, kann die Daten lesen".

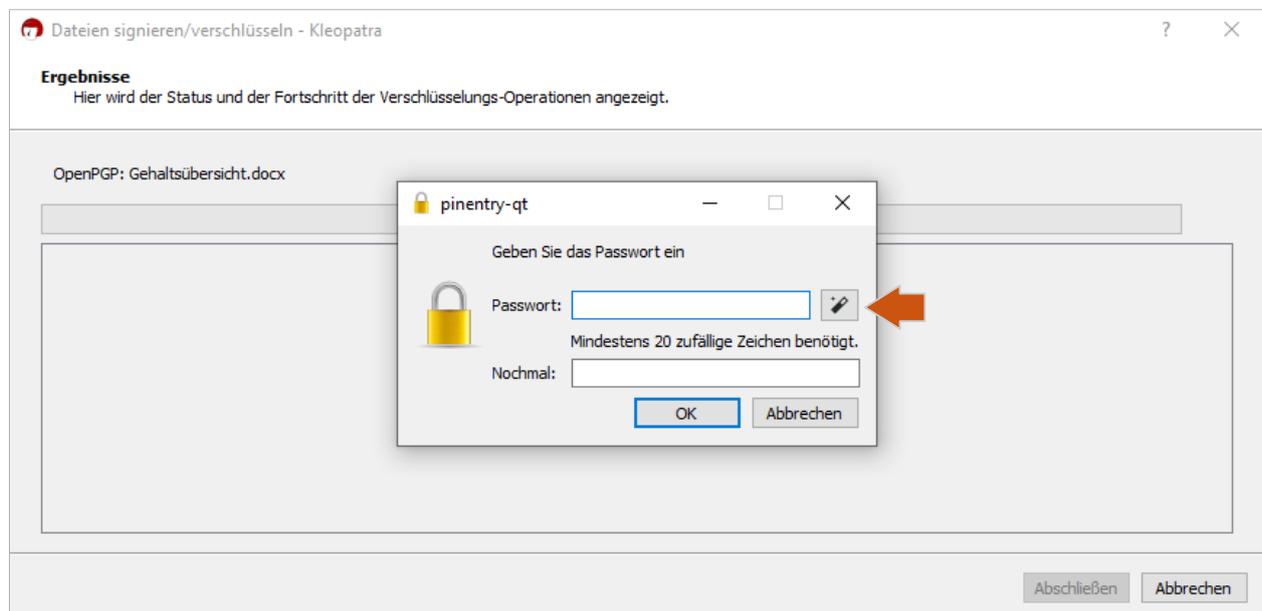
Wählen Sie noch das Ausgabeverzeichnis für Ihre verschlüsselte Datei - dies ist i.d.R. der aktuelle Ordner - und klicken Sie auf **Verschlüsseln**.

## 1.1 Sicheres Passwort erstellen

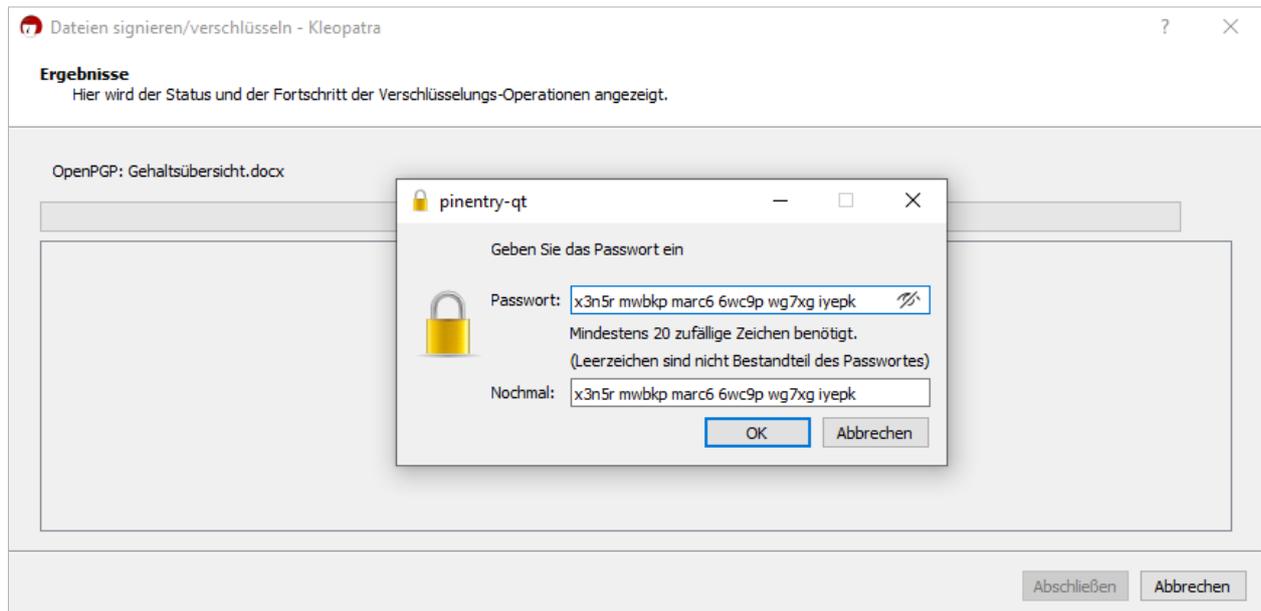
### Hinweis

Der alleinige Besitz des Passwortes reicht aus, um die Datei zu entschlüsseln. Benutzen Sie daher unseren Passwortgenerator, um stets sichere Passwörter zu generieren.

Für die symmetrische Verschlüsselung wird ein Passwort mit mindestens 20 zufällig gewählten Zeichen benötigt. Wir empfehlen den **GnuPG Passwortgenerator** zu nutzen, um sich automatisch ein sicheres Passwort erzeugen zu lassen. Dazu klicken Sie auf den  (Vorschlagen) Button rechts neben dem Passwortfeld:



Ein 30-stelliges Passwort bestehend aus einer Zahlen-/Buchstabenkombination wird in beide Eingabefelder eingefügt:



Sichern Sie das Passwort, z.B. indem Sie es per Kopieren/Einfügen in eine einfache Textdatei übertragen und diese an einem geeigneten Ort speichern, der gegen unbefugten Zugriff geschützt ist.

### Hinweis

Sollten Sie sich das Passwort aufschreiben, beachten Sie, dass die Leerzeichen nicht Bestandteil des Passwortes sind und lediglich der besseren Lesbarkeit dienen.

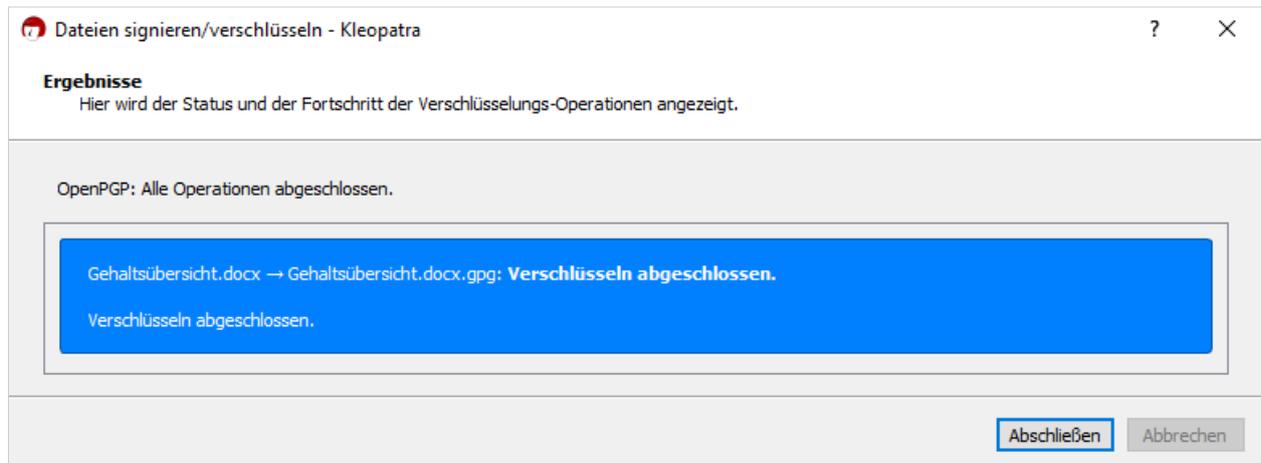
Dieses Passwort müssen Sie über einen sicheren Kanal übergeben - wie ehemals auch bei "Chiasmus" - an die Empfänger, die Ihre verschlüsselten Dateien öffnen sollen.

### Wichtig

Das Passwort selbst ist eine Information mit der Einstufung **Ver-  
schlusssache – Nur für den Dienstgebrauch**. Hierfür gelten die entsprechenden Schutzmaßnahmen, insbesondere, dass es nicht im Klartext übertragen werden darf.

Versenden Sie ein Passwort daher niemals per unverschlüsselter Mail. Auch Telefon, SMS oder Fax sind unzulässig.

Nachdem Sie auf **OK** geklickt haben, zeigt Kleopatra an, ob die Verschlüsselung erfolgreich war. Zum Beenden klicken Sie auf **Abschließen** :

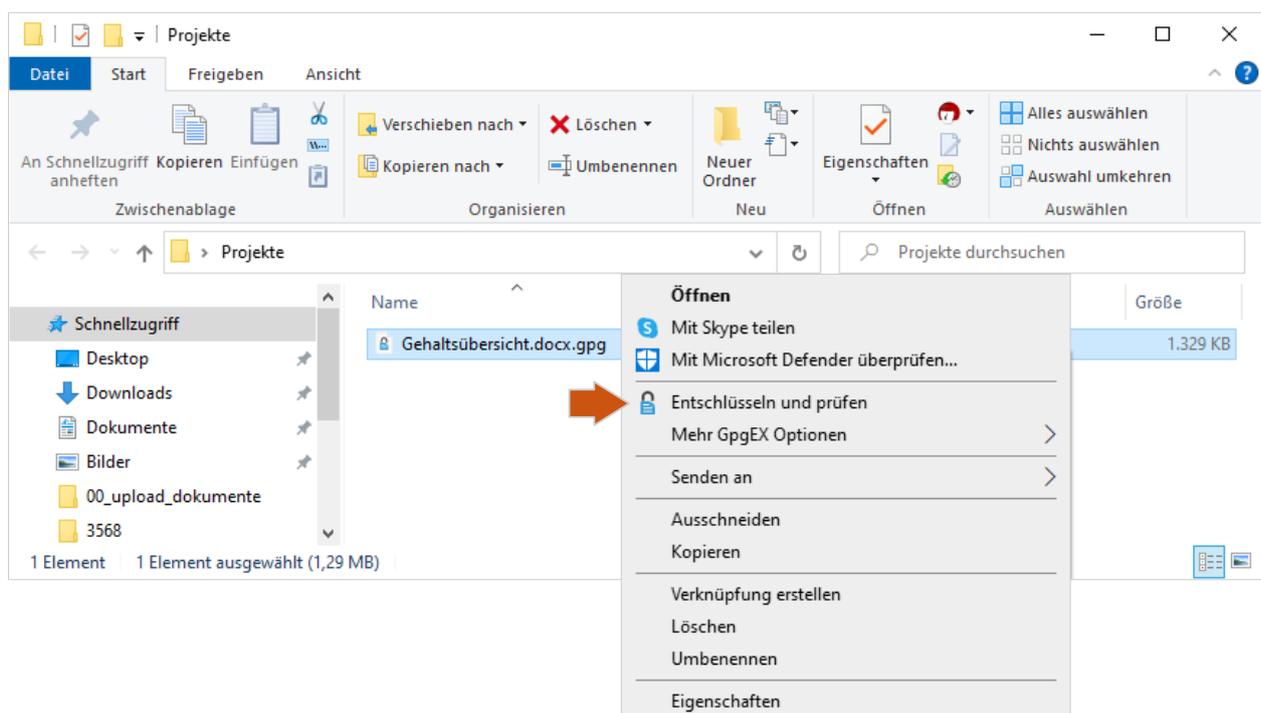


Die Datei wurde verschlüsselt und am Ablageort als **\*.gpg**-Datei gespeichert.

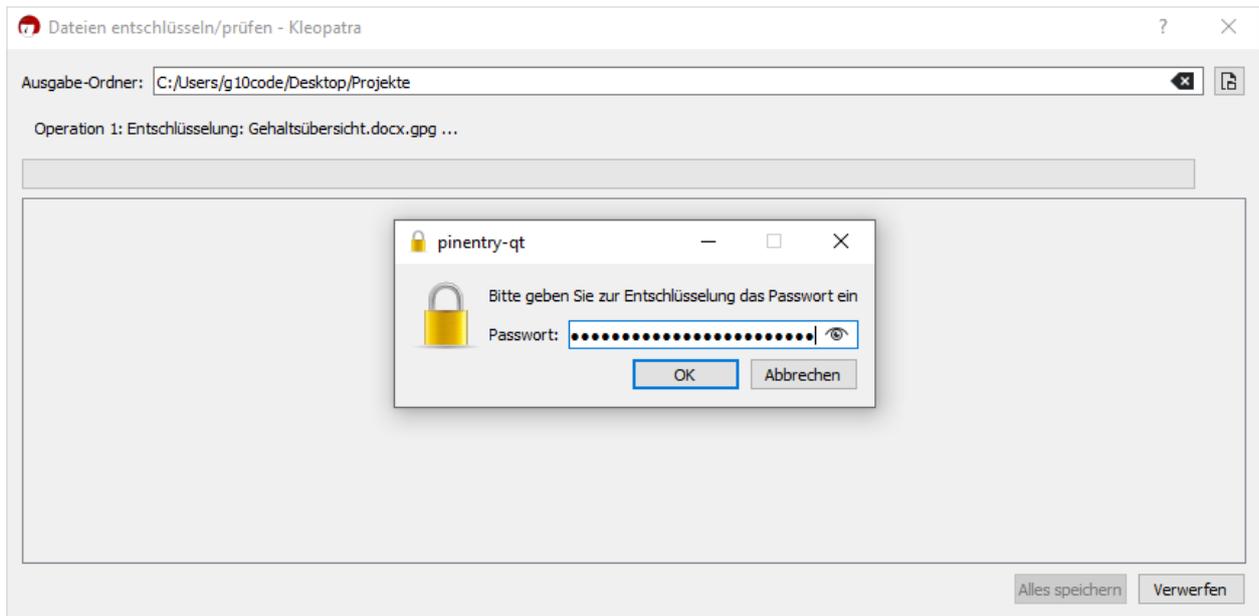
Der Versand bzw. Austausch solcher verschlüsselten Daten kann nun über unsichere Kanäle, wie z.B. unverschlüsselte Mails, erfolgen.

## 2 Entschlüsseln

Verschlüsselte **\*.gpg**-Dateien öffnen Sie im Windows Datei-Explorer mit einem Doppelklick. Alternativ wählen Sie die verschlüsselte Datei aus, öffnen mit der rechten Maustaste das Untermenü und wählen **Entschlüsseln und prüfen** :

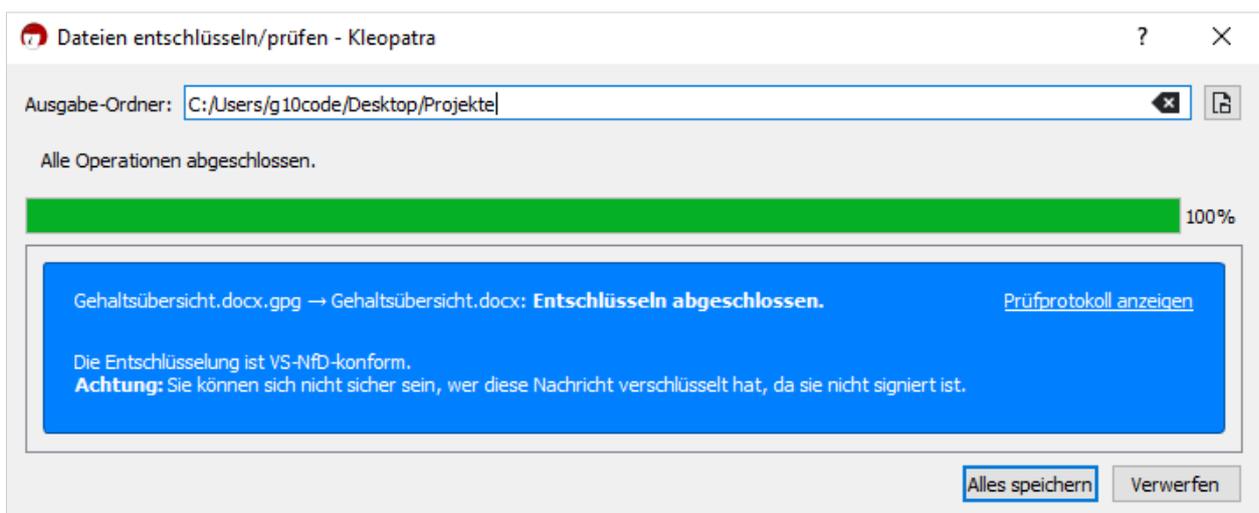


Sie werden aufgefordert, das Passwort einzugeben, das bei der Verschlüsselung verwendet wurde:



Nach der Passwortbestätigung wird Ihnen angezeigt, ob die Entschlüsselung erfolgreich war. Sie können den Hinweis "Sie können sich nicht sicher sein, wer diese Nachricht verschlüsselt hat, da sie nicht signiert ist" ignorieren.

Beenden Sie den Vorgang mit **Alles speichern** und Ihre Datei wird am gewünschten Ort entschlüsselt abgelegt.



## 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.