

Anwenderhandbuch

**Anleitung zur Verifizierung der ene't Dateien
mit Gpg4win**



ene't GmbH
Weserstraße 9
41836 Hückelhoven

Tel. 0 24 33 - 52 60 10
Fax 0 24 33 - 52 60 11

E-Mail: info@enet.eu
Internet: www.enet.eu

geändert am: 18.10.2010
Dokumentversion: 1

Bearbeiter: TS
Tel.0 24 33 - 5 26 01-74

Inhalt

Weshalb werden ene't-Dateien digital signiert?	3
Schritt 1	4
Gpg4win installieren	4
Schritt 2	9
Import bzw. Erstellung eines eigenen Zertifikats	9
Schritt 3	12
Importieren des ene't Zertifikats	12
Schritt 4	18
Dateien manuell verifizieren	18
Die Seite für Systemadministratoren	21
Dateien automatisiert verifizieren	21

Weshalb werden ene't-Dateien digital signiert?

Auch Ihr Computersystem wird über einen leistungsstarken Schutz vor schädlichen Einflüssen von außen verfügen. Dennoch, einen absoluten Schutz kann auch das beste Antivirenprogramm oder eine Firewall nicht bieten. Als zusätzlichen Beitrag zur Sicherheit Ihres Systems werden deshalb alle von ene't zum Download bereit gestellten Dateien digital signiert. Durch die Signierung der Dateien, die einem digitalen Fingerabdruck/Stempel gleicht, können Sie die Authentizität feststellen und so sicherstellen, dass die bei uns heruntergeladenen Dateien tatsächlich auch von ene't stammen und nicht von Dritten manipuliert wurden.

Zur Überprüfung der Signaturen benötigen Sie allerdings eine entsprechende Software – für windows-basierte Betriebssysteme zum Beispiel das kostenlos im Internet erhältliche „Gpg4win“.

Nach der Installation dieser frei verfügbaren Software können Sie die ene't Signaturen schnell und zuverlässig überprüfen.

Die Installation dieses kleinen Programms ist zwar weitestgehend selbsterklärend, an manchen Stellen ist eine kleine Entscheidungshilfe aber ganz praktisch.

Der gesamte Vorgang gliedert sich in vier Schritte. Dabei sind Schritt 1 bis 3 nur einmal –für die Installation des Programms – auszuführen. Ist das Programm einmal installiert, wird für die Verifizierung der jeweiligen Datei nur noch Schritt 4 ausgeführt.

Schritt 1: Download und Speicherung der Freeware „Gpg4win“

Schritt 2: Import bzw. Erstellung eines eigenen Zertifikats

Schritt 3: Importieren des ene't Zertifikats

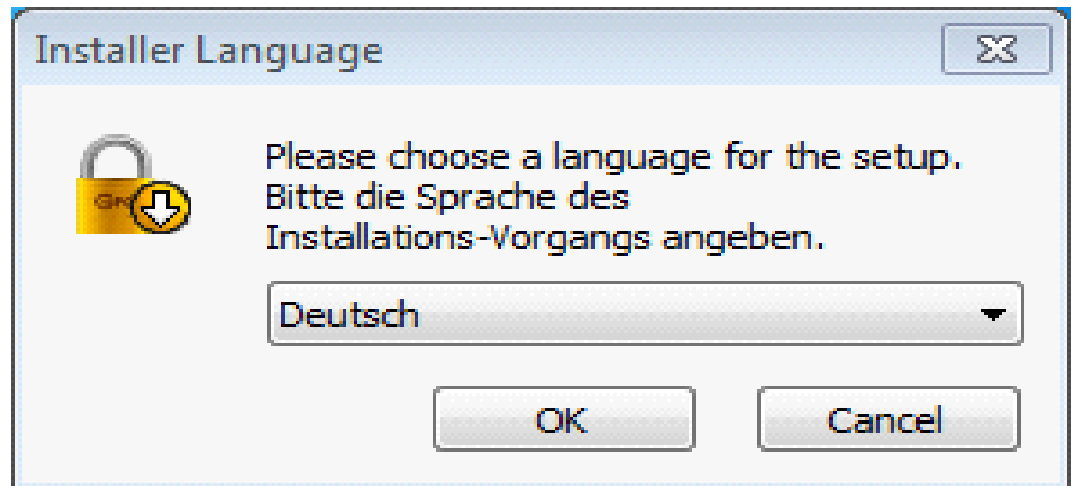
Schritt 4: Dateien manuell verifizieren oder Verifizierung automatisieren

Schritt 1

Gpg4win installieren

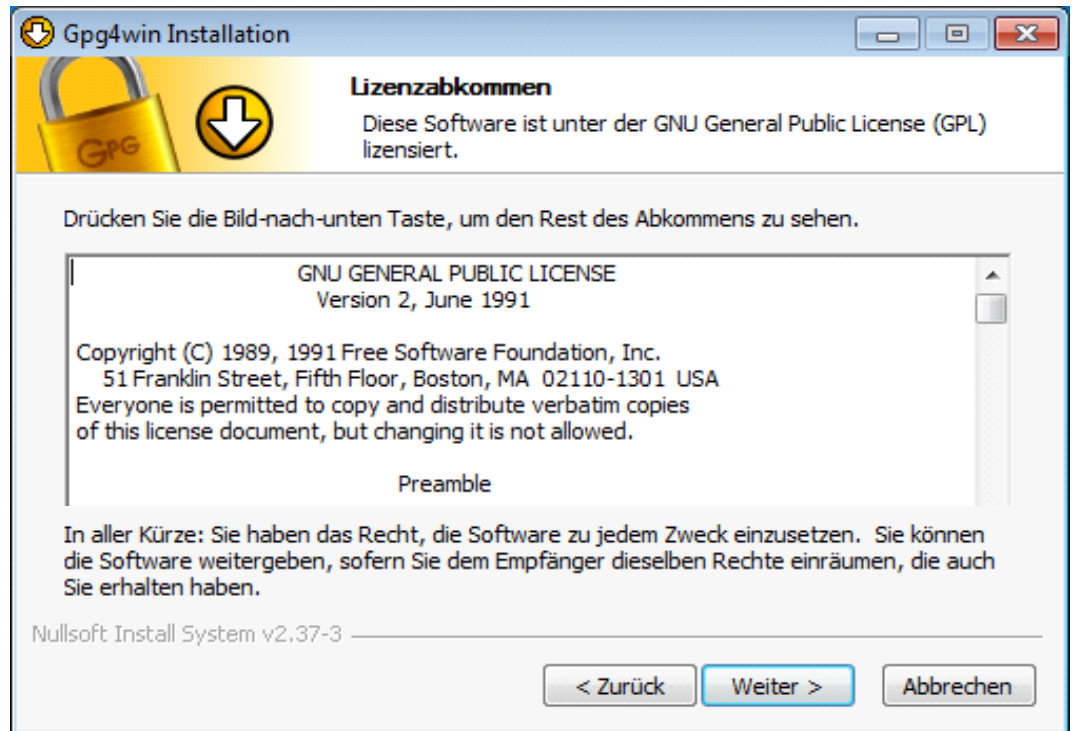
Starten Sie den Download der Software von der Internetseite:

<http://www.gpg4win.de/download-de.html>



Für die Installation der heruntergeladenen Software benötigen Sie Administratorrechte. Wählen Sie zu Beginn des Installationsvorgangs die gewünschte Sprache aus.

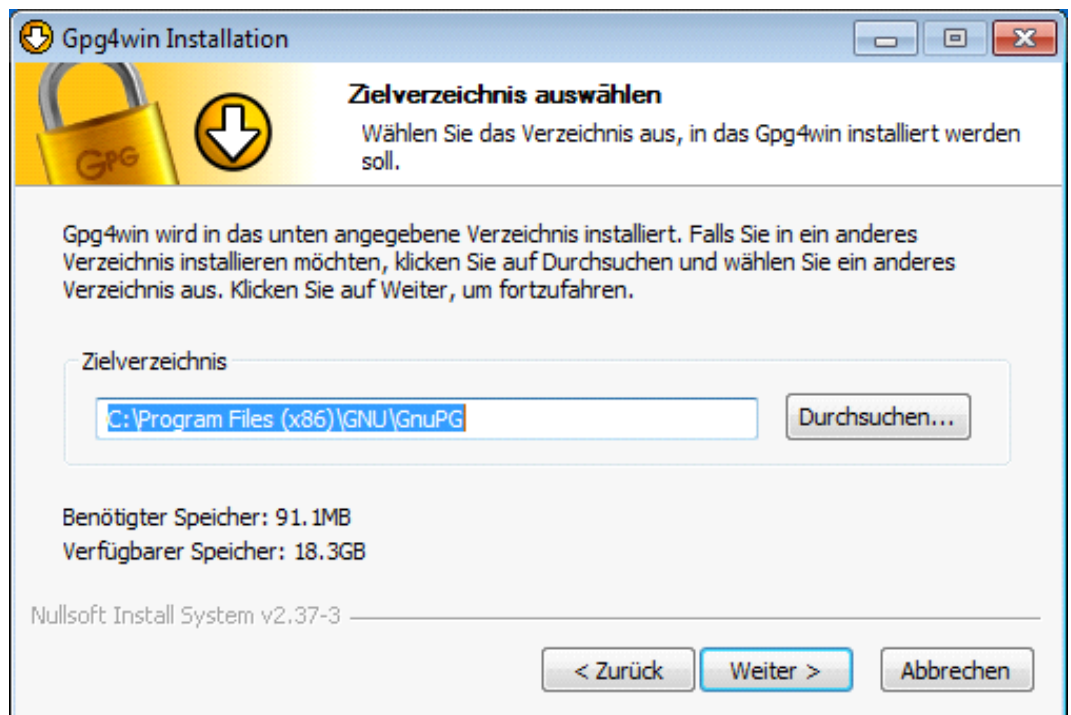




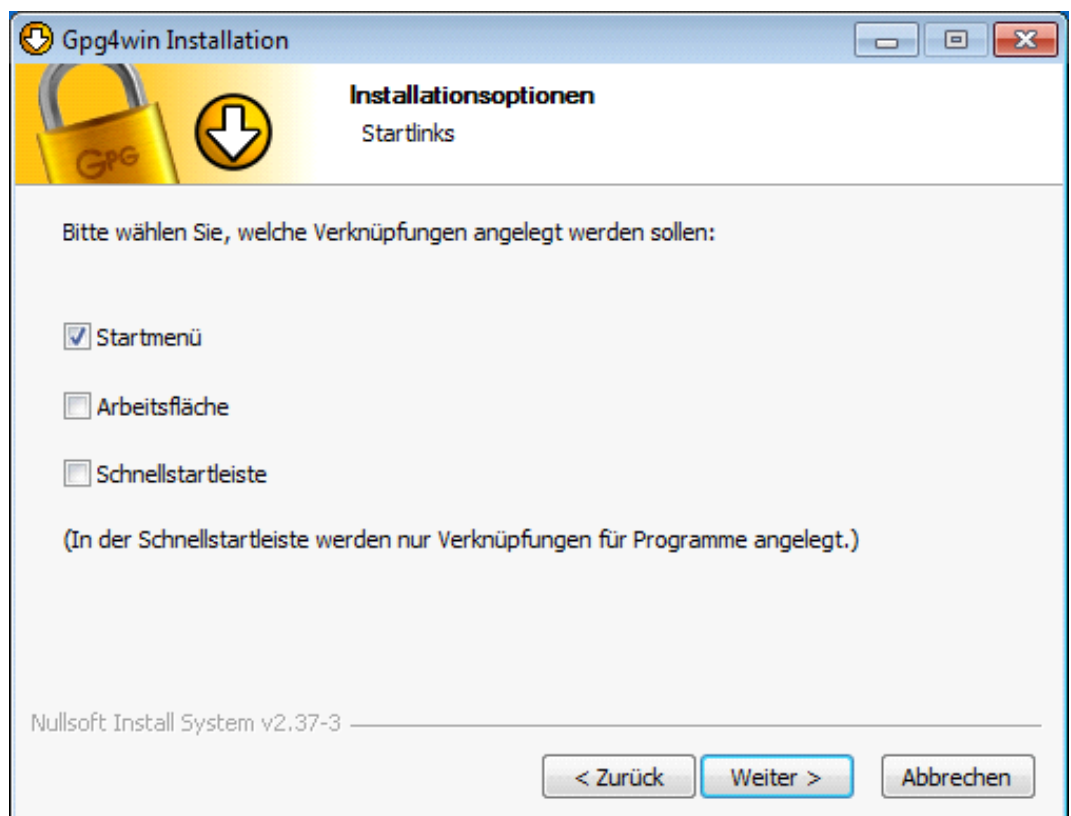
Bestätigen Sie die Lizenzbedingungen.

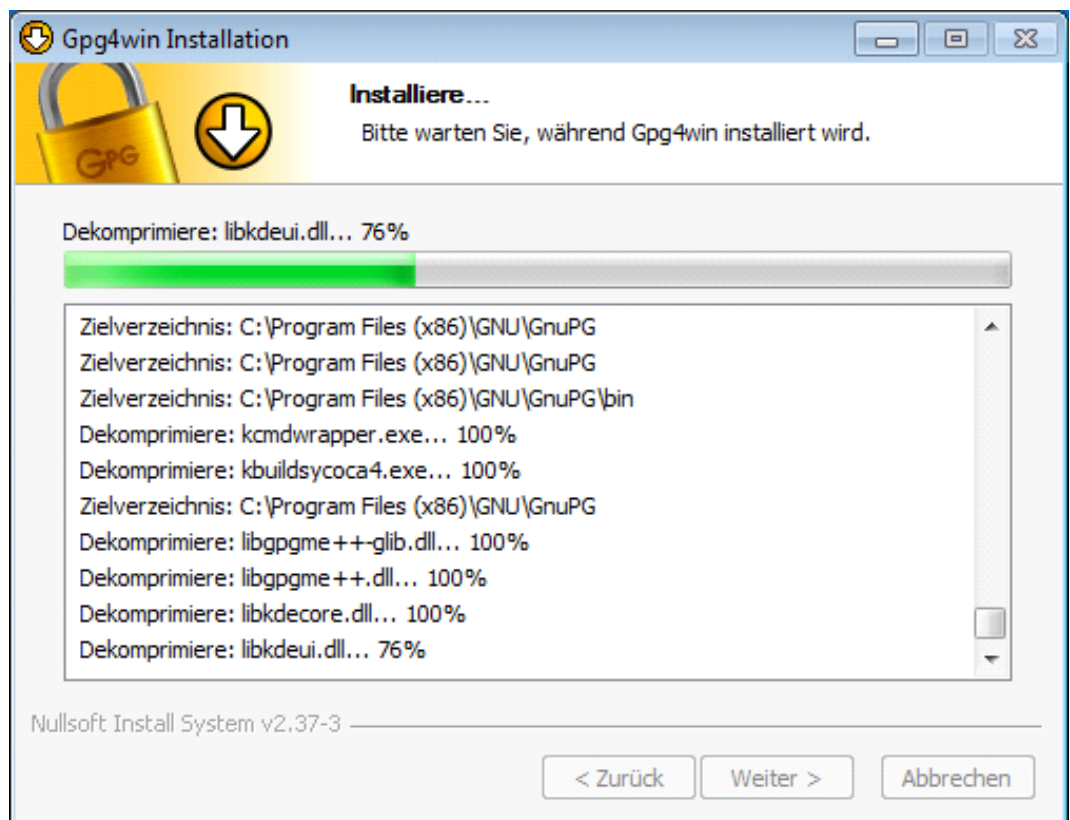
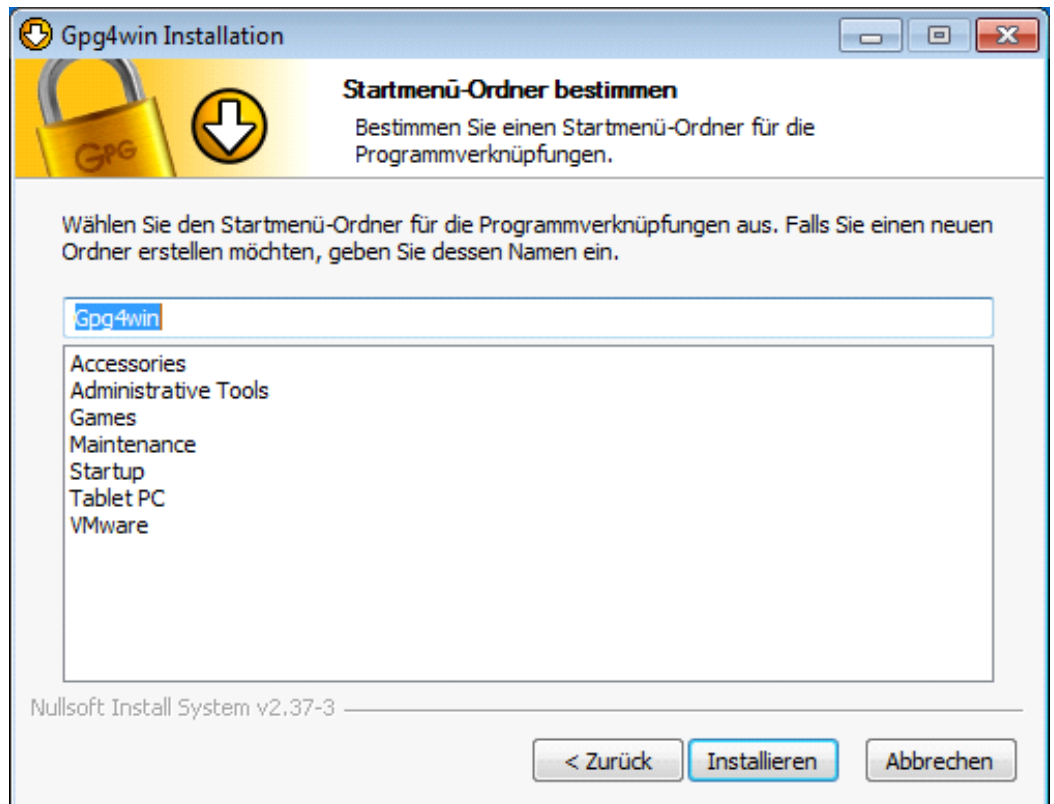


Wählen Sie die wichtigen Komponenten „Kleopatra“ und „GpgEX“ aus.



Das Programm legt automatisch einen neuen Ordner im Verzeichnis „Programme“ an, wenn Sie nicht selbst ein vorhandenes Verzeichnis vorgeben.





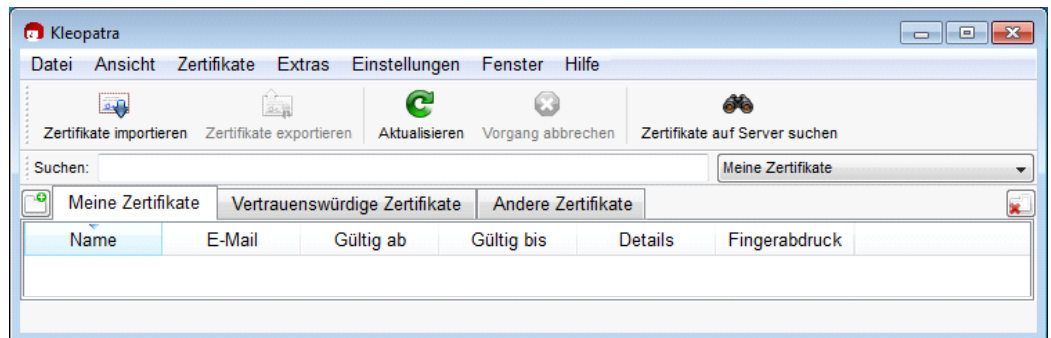
Warten Sie bis die Installation fertiggestellt ist.



Schritt 2

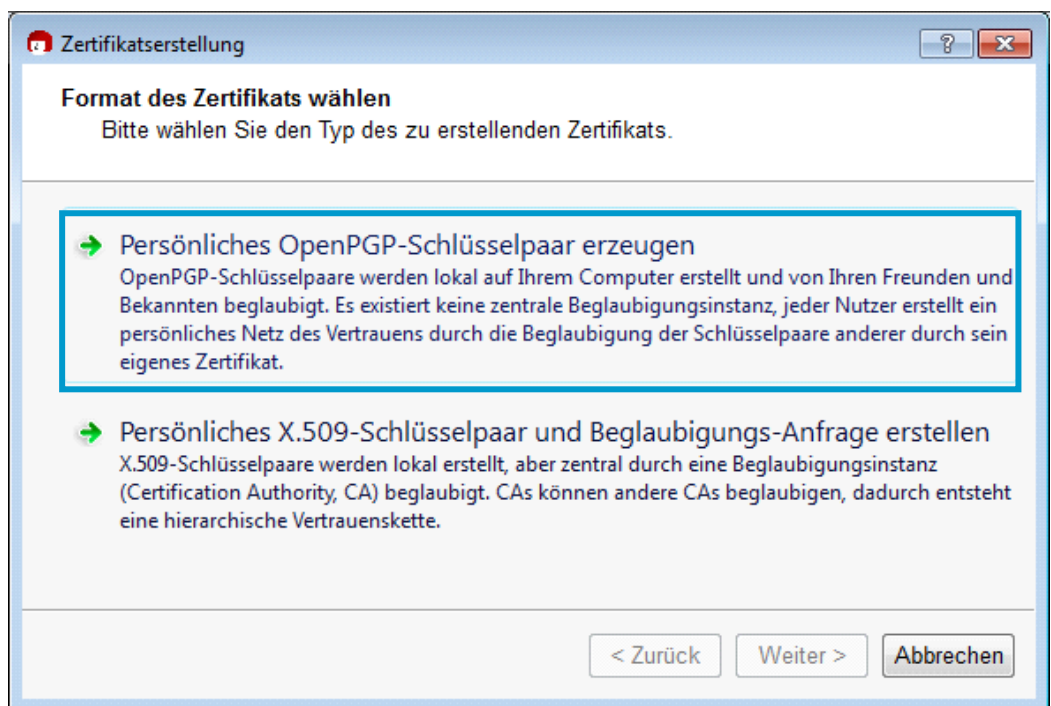
Import bzw. Erstellung eines eigenen Zertifikats

Zur Verifizierung ist es nötig, dass Sie über ein eigenes PGP-Zertifikat verfügen. Sie können nun entweder ein schon vorhandenes Zertifikat importieren oder ein neues erstellen. In beiden Fällen müssen Sie zunächst das zuvor installierte Programm „Kleopatra“ öffnen.



Wenn Sie bereits ein PGP-Zertifikat besitzen, dann können Sie dieses über die Schaltfläche „Zertifikate importieren“ hinzufügen.

Falls Sie noch kein Zertifikat besitzen, erstellen Sie jetzt Ihr eigenes Zertifikat. Über „Datei“ -> „Neues Zertifikat...“ erreichen Sie den Erstellungsassistenten:



Wählen Sie die obere Option „Persönliches OpenPGP-Schlüsselpaar erzeugen“.

Zertifikatserstellung

Details angeben
Bitte tragen Sie Ihre persönliche Angaben ein. Für mehr Kontrolle über die Zertifikateinstellungen bitte "Erweiterte Einstellungen" wählen.

Name: (benötigt)

E-Mail: (benötigt)

Kommentar: (optional)

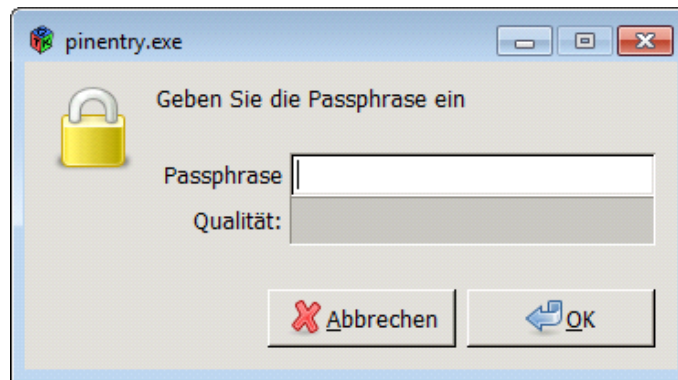
Füllen Sie den Dialog mit Ihren Daten.

Zertifikatserstellung

Zertifikateinstellungen prüfen
Bitte überprüfen Sie vor der Zertifikatserstellung nochmals Ihre Angaben.

Name: Tim Steufmehl
E-Mail-Adresse: steufmehl@enet.eu

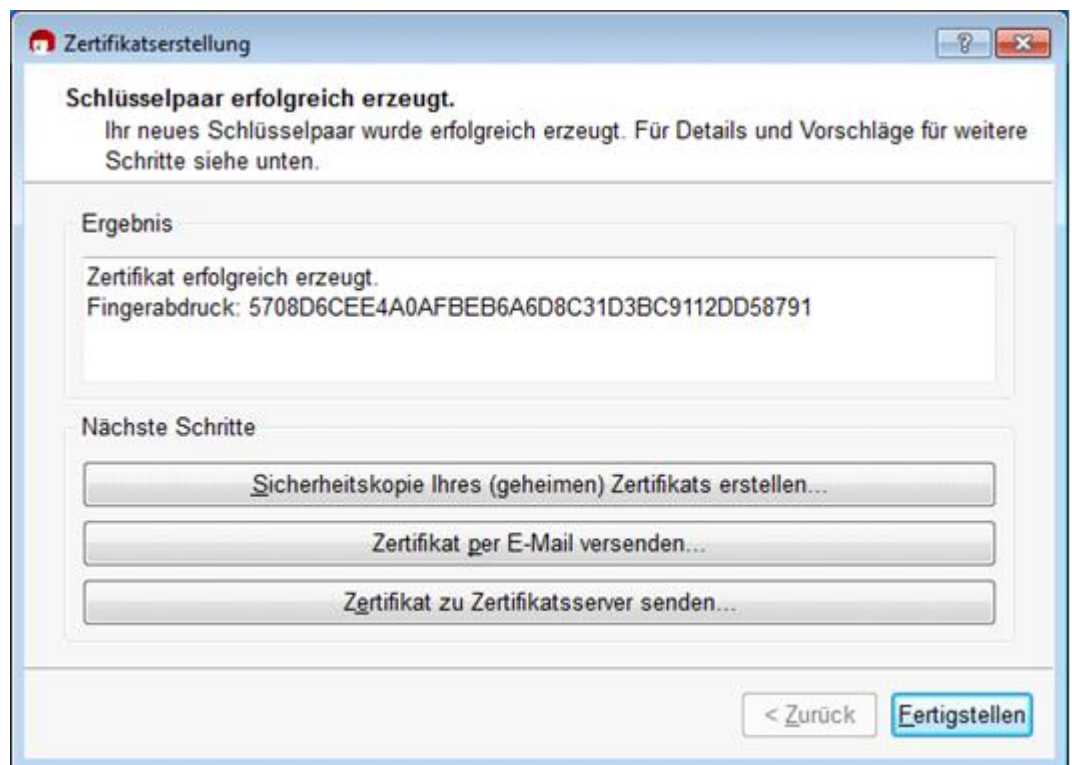
Alle Details



ACHTUNG: Dieses Fenster kann sich in den Hintergrund verschieben, so dass es nicht mehr sichtbar ist.

Ihr Passwort sollte möglichst eine Qualität von 100% besitzen. Mit einer Zusammensetzung aus Buchstaben und Zahlen sowie /oder Sonderzeichen können Sie ein ziemlich sicheres Passwort erzeugen.

Bei der Erstellung muss das Passwort noch ein zweites Mal eingegeben werden.



Wurde Ihr Schlüsselpaar erfolgreich erstellt, können Sie den Assistenten über „Fertigstellen“ beenden.

Schritt 3

Importieren des ene't Zertifikats

Zur Verifizierung der ene't Dateien benötigen Sie unseren öffentlichen Schlüssel, den Sie zunächst von einem Schlüsselservers importieren müssen.

Kleopatra ermöglichen diesen Import direkt von einem Schlüsselservers aus.

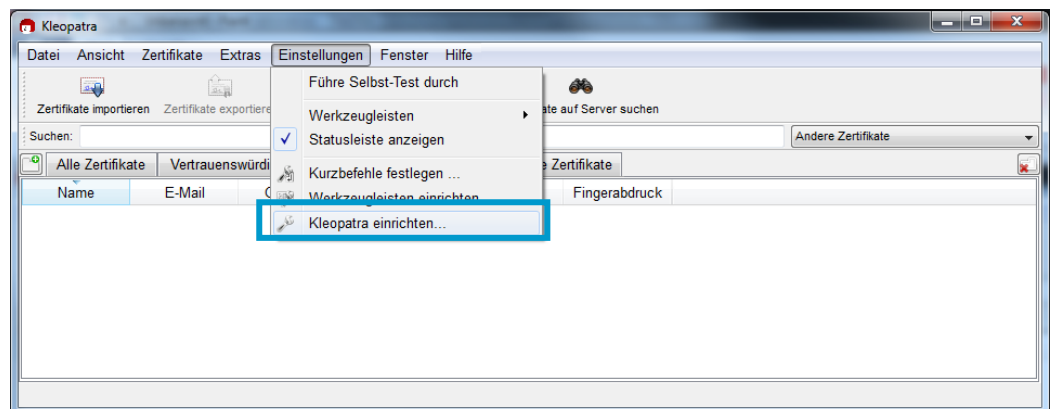
HINWEIS:

Der Import des Zertifikates über Kleopatra erfolgt über den Port 11371 (HKP-Protokoll), der in Ihrem Unternehmen unter Umständen gesperrt sein könnte.

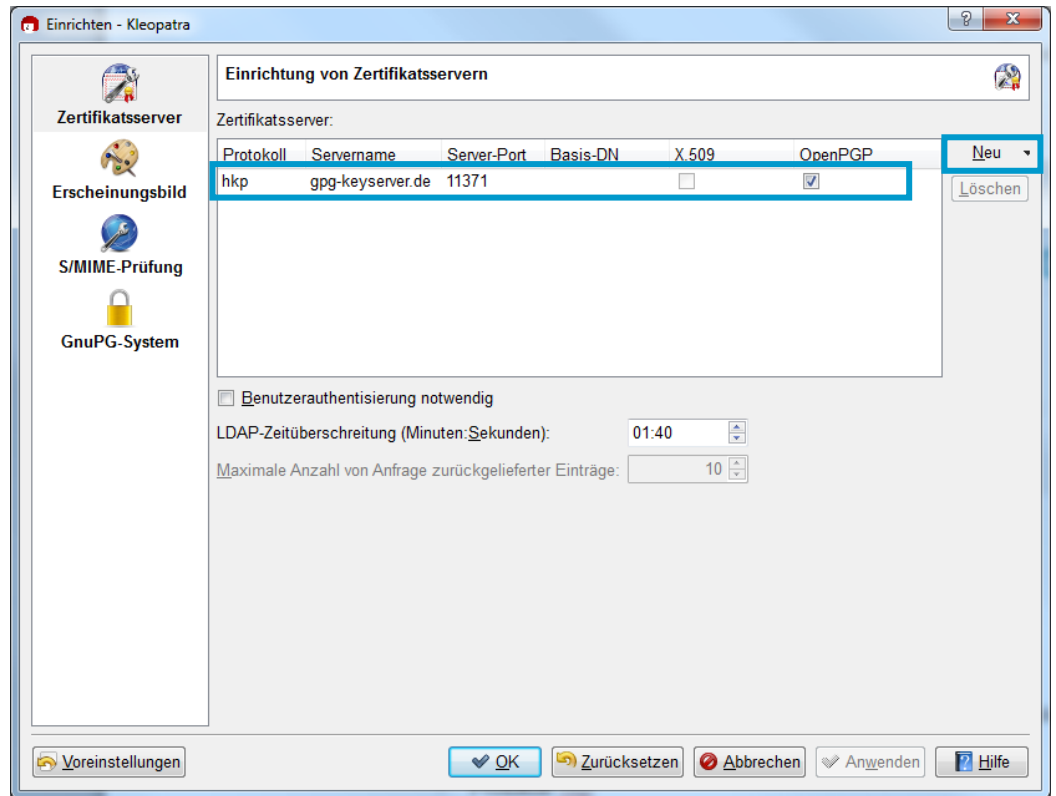
Sollte dies der Fall sein, so kontaktieren Sie uns bitte, damit die Schlüssel-Übermittlung auf anderem Weg schnellstmöglich stattfinden kann oder erkundigen Sie sich bei Ihrem Systemadministrator, ob der betroffene Port 11371 für diesen Zweck freigeschaltet werden kann.

Der Import über Kleopatra sollte allerdings bevorzugt verwendet werden, sofern dies möglich ist.

Um mit Kleopatra den Schlüsselservers erreichen zu können, muss dieser zuvor unter „Einstellungen“ -> „Kleopatra einrichten ...“ eingetragen werden:

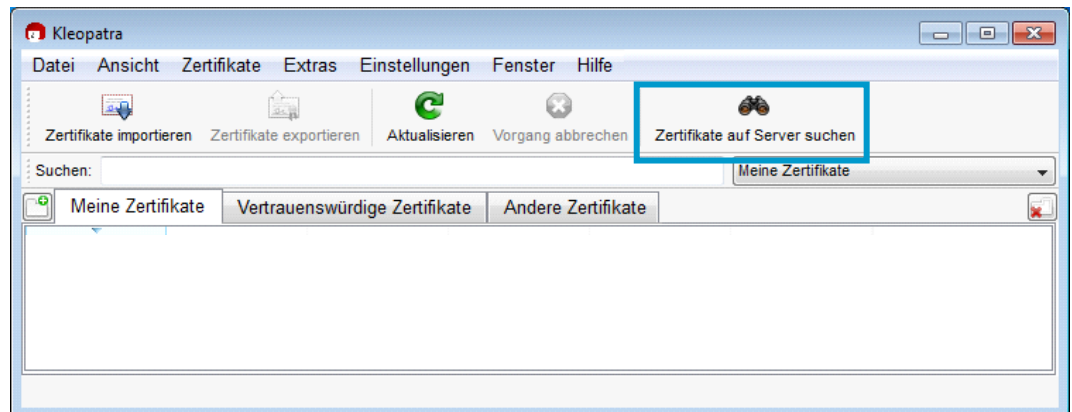


Im erscheinenden Fenster „Einrichtung von Zertifikatsservern“ fügen Sie mit einem Klick auf „Neu“ einen neuen Server ein.

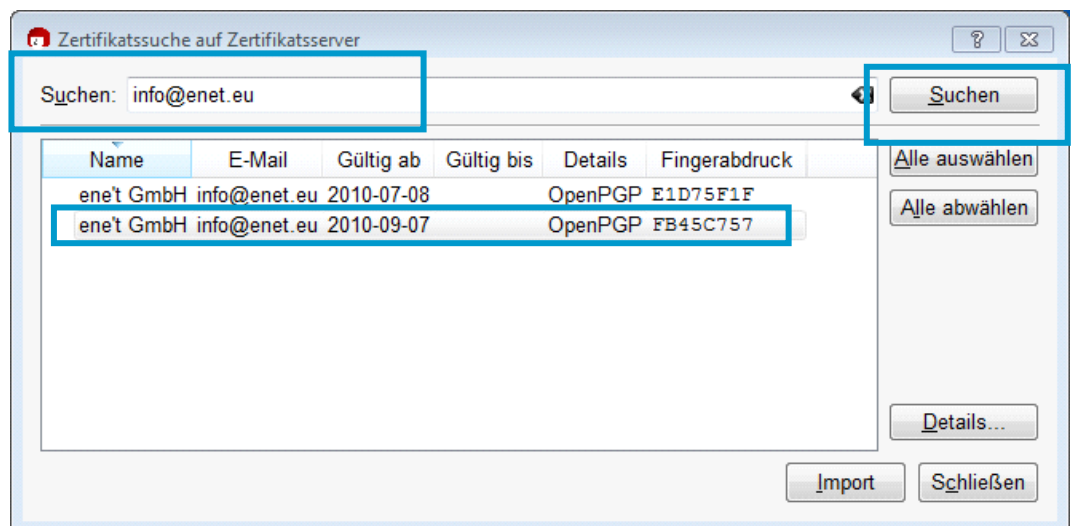


In der neuen Zeile müssen folgende Informationen eingetragen werden (alle anderen Einträge können gelöscht werden):

- **Protokoll:** hkp
- **Servername:** gpg-keyserver.de
- **Server-Port:** 11371
- Haken bei „OpenPGP“ setzen
- Bestätigung mit Klick auf „OK“



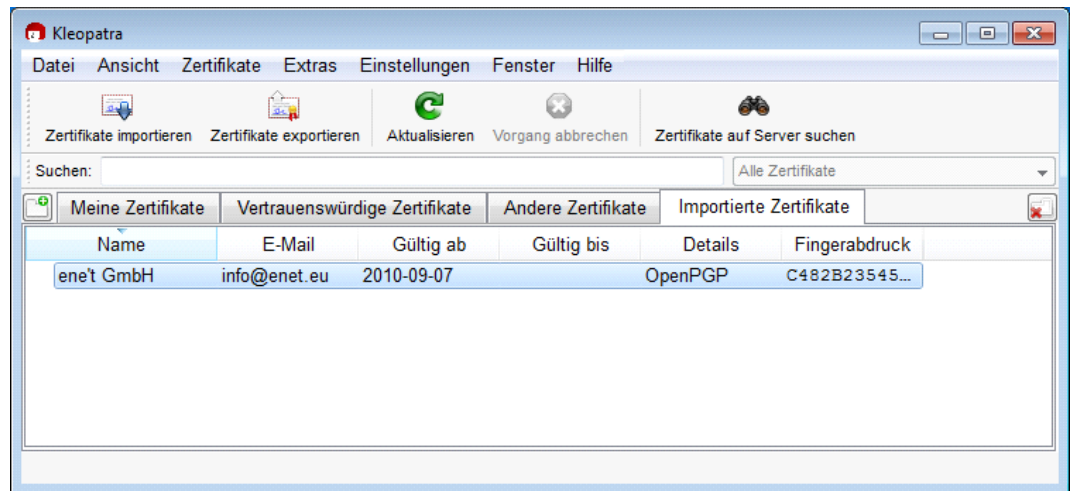
Über die Schaltfläche „Zertifikat auf Server suchen“ erreichen Sie das folgende Fenster:



Geben Sie in das Suchfeld „info@enet.eu“ ein und klicken die Schaltfläche „Suchen“ an.

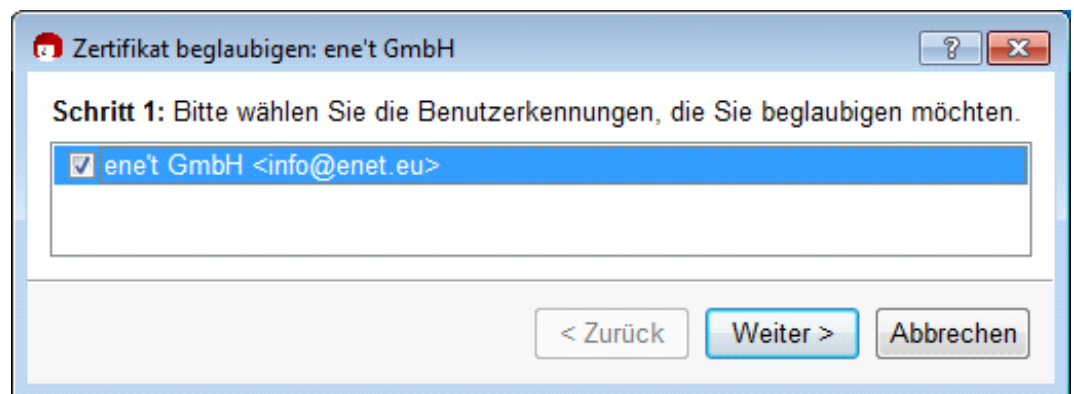
Wählen Sie nun das Zertifikat vom „07.09.2010“ mit dem Fingerabdruck „FB45C757“ aus und klicken auf die Schaltfläche „Import“.

Öffnen Sie die Registerkarte „Importierte Zertifikate“.

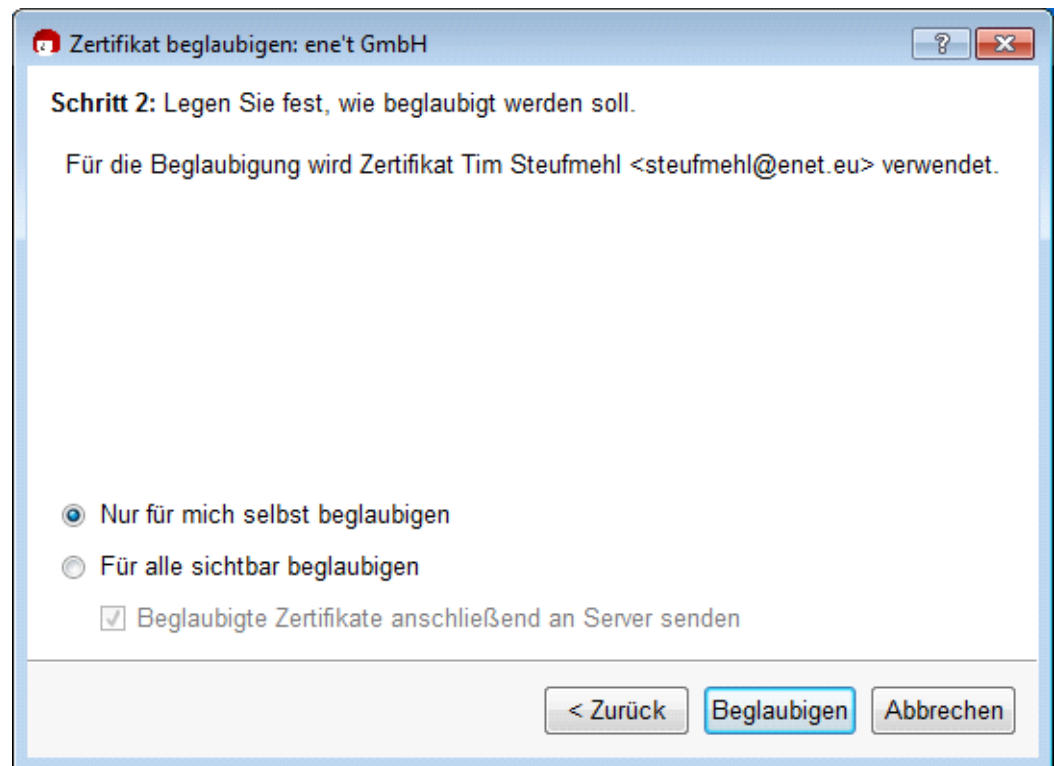


Mit einem Rechtsklick auf das Zertifikat öffnen Sie im Kontextmenü „Zertifikat beglaubigen...“.

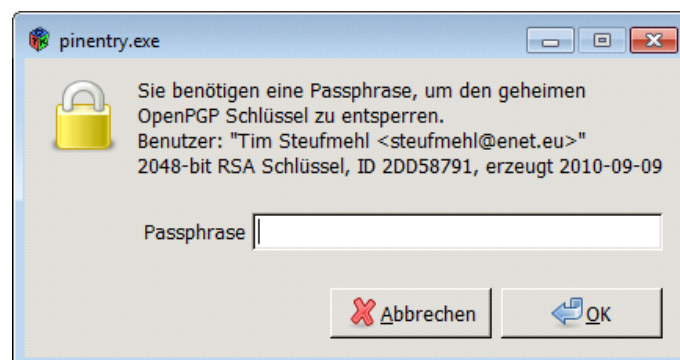
Der nun folgende Dialog führt Sie durch den Prozess:



Wählen Sie das Zertifikat „ene't GmbH <info@enet.eu>“ aus und klicken Sie auf „Weiter >“.

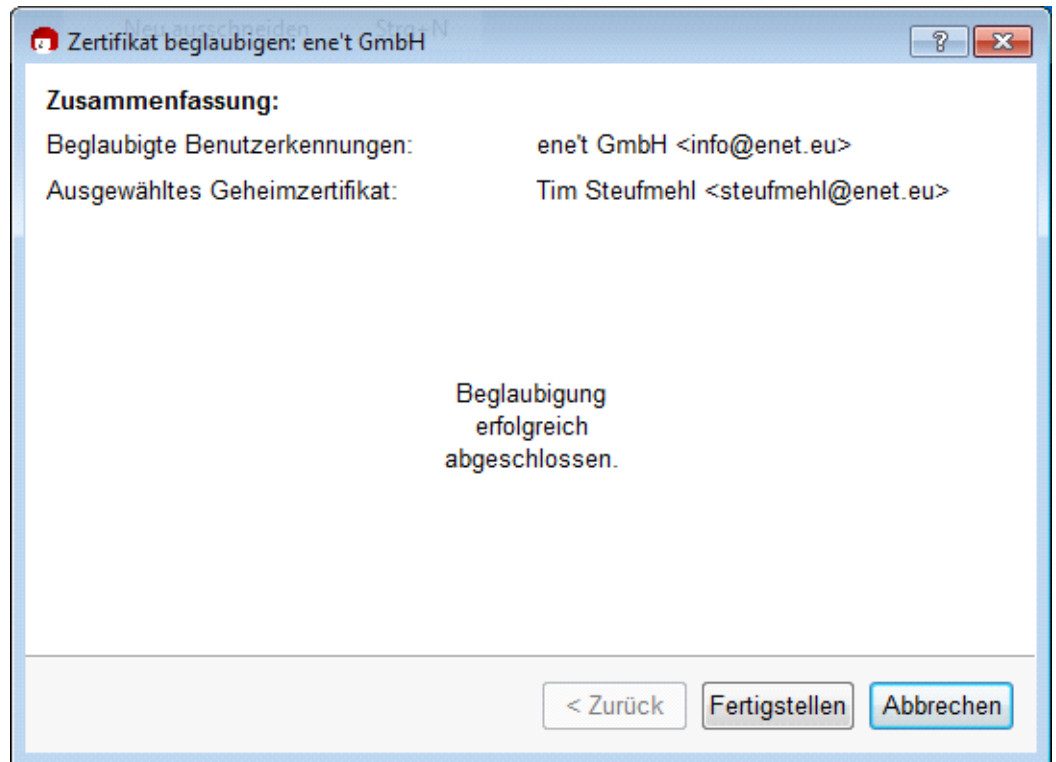


Wenn Sie Ihr Vertrauen zu ene't öffentlich kundtun möchten, dann wählen Sie „Für alle sichtbar beglaubigen“. Dies trägt zum PGP-Prinzip des „Web of Trust“ bei. Mehr Informationen finden Sie hier: http://de.wikipedia.org/wiki/Web_of_Trust



ACHTUNG: Dieses Fenster kann sich in den Hintergrund verschieben, so dass es nicht mehr sichtbar ist.

Geben Sie das Kennwort (Passphrase) Ihres zuvor generierten Zertifikats ein und bestätigen Sie mit OK.



Sie haben unser Zertifikat erfolgreich beglaubigt und „vertrauen“ ab sofort den korrekt signierten Dateien der ene't GmbH.

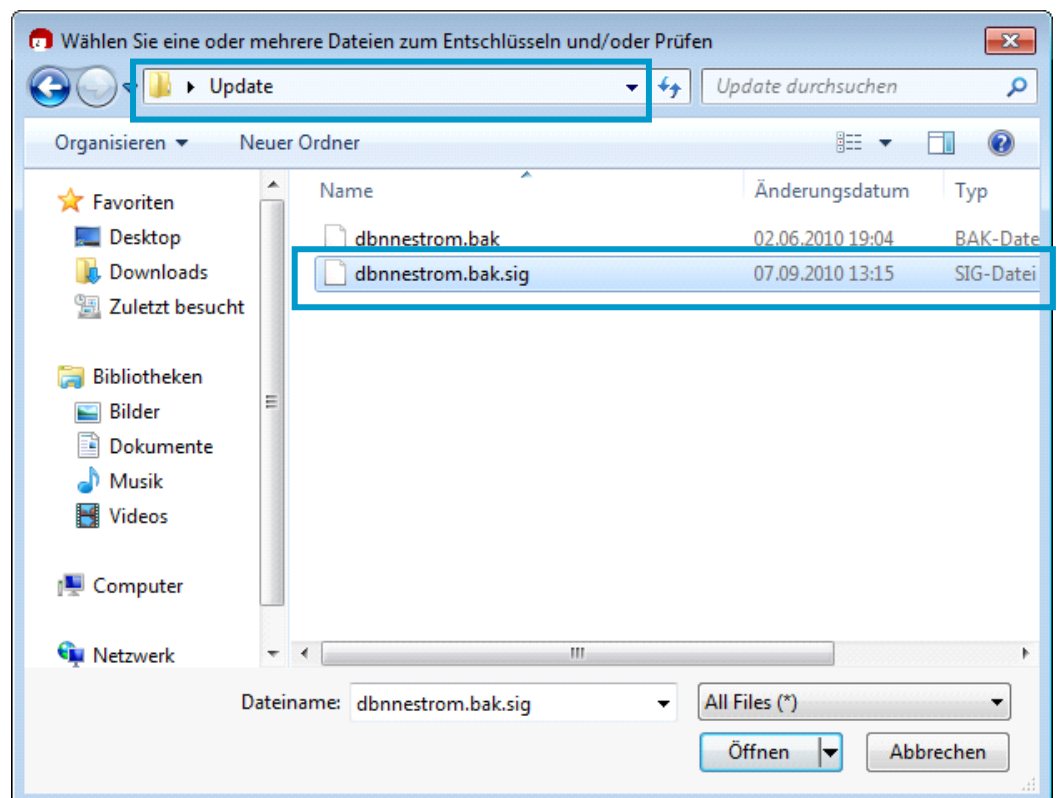
Schritt 4

Dateien manuell verifizieren

Sie haben die Möglichkeit, Dateien quasi „manuell“ zu verifizieren, Hierzu benötigen Sie die von uns mitgelieferte Datei mit der Endung „.sig“. Diese können Sie über das Programm „Kleopatra“ öffnen.

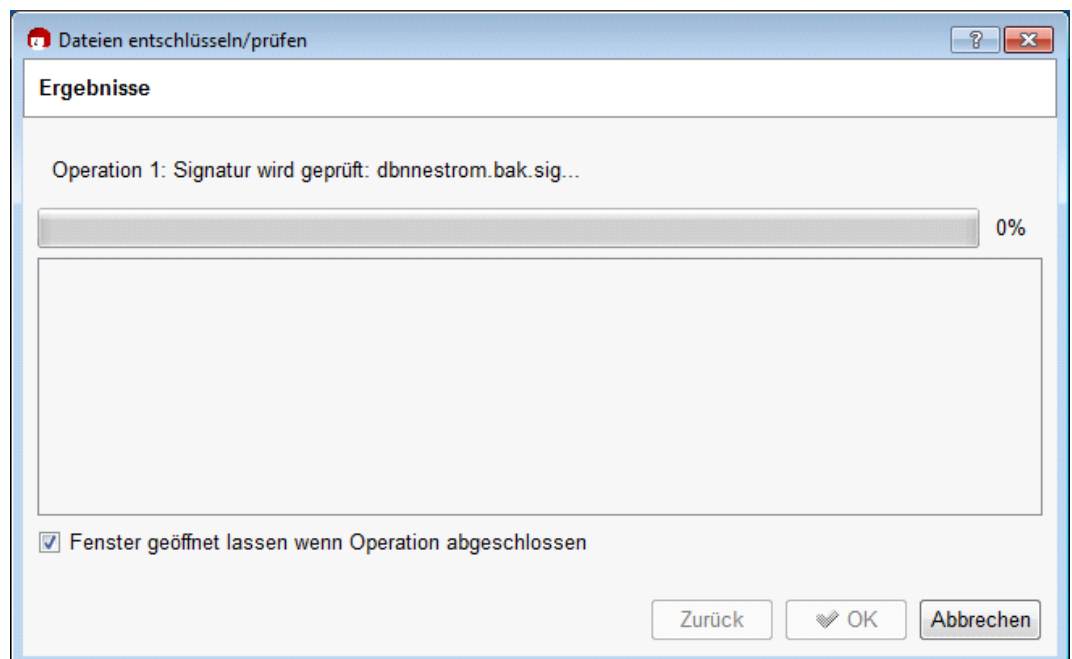
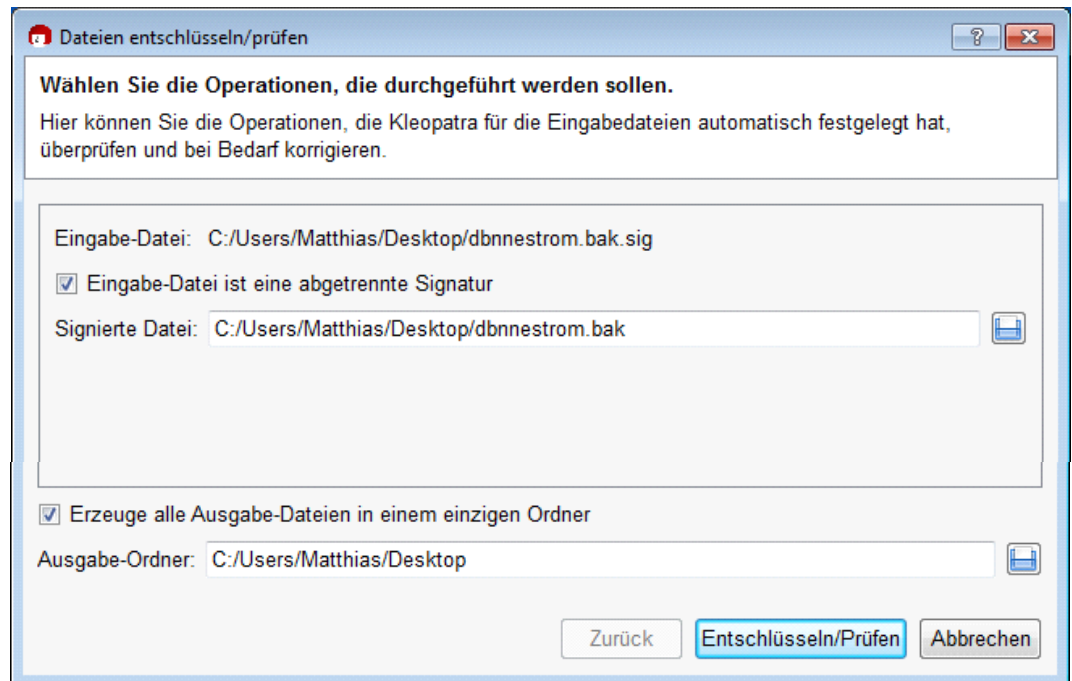
(Nur wenn Gpg4win auf einem Rechner mit einem 32-Bit Betriebssystem installiert ist, bietet Ihnen das Programm zusätzlich den Weg über das Kontextmenü an, das nach einem Rechtsklick auf die „.sig“-Datei sichtbar wird.)

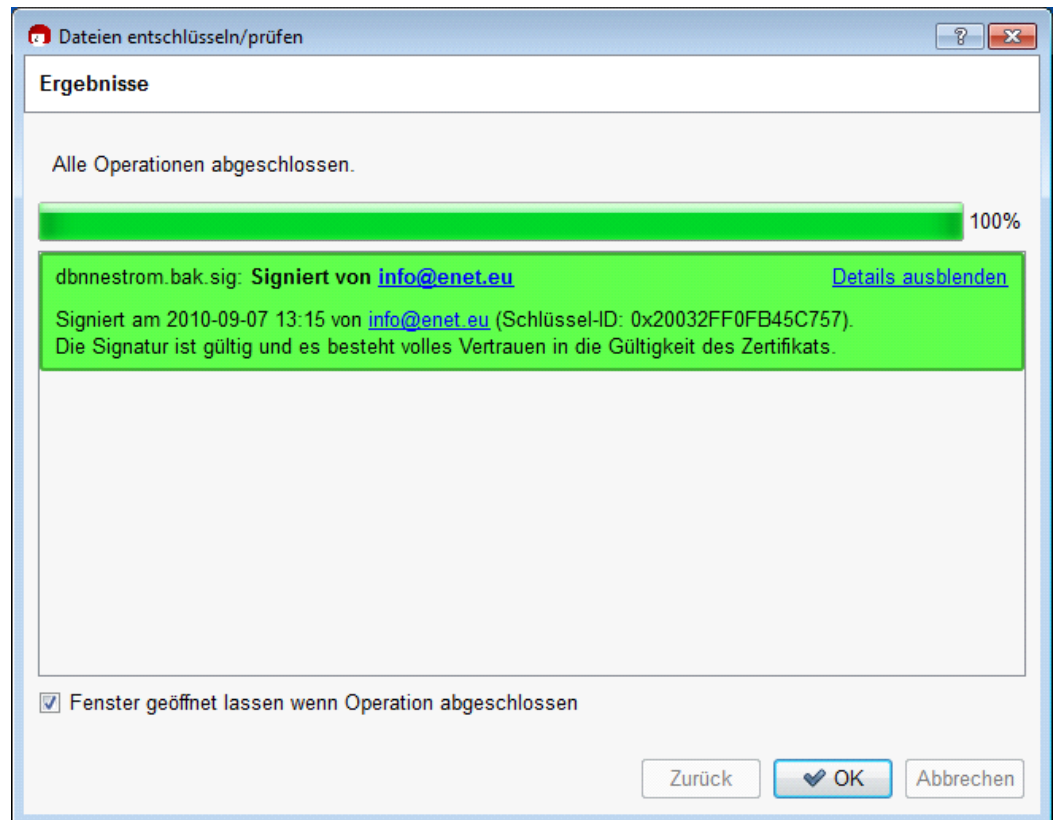
In Kleopatra öffnen Sie über den Menüpunkt „Datei“ -> „Dateien entschlüsseln/prüfen...“ den folgenden Dialog:



Navigieren Sie in das Verzeichnis, in dem Sie die ene't Dateien abgelegt haben. Wählen Sie die Signaturdatei mit der Endung „.sig“ aus.

Die folgenden Abbildungen dokumentieren die weiteren Schritte. Zusätzliche Eingaben Ihrerseits sind in der Regel nicht erforderlich:





Hier erhalten Sie genaue Informationen zum Verlauf der Überprüfung. Hieraus lässt sich schließen, ob die Verifizierung erfolgreich verlaufen ist.

Die Seite für Systemadministratoren

Dateien automatisiert verifizieren

Neben der manuellen Verifizierung besteht die Möglichkeit diese – beispielsweise per Batch-Job – zu automatisieren. Auch hier ist Voraussetzung die Installation der schon oben genannten Werkzeuge „Kleopatra“ und „GpgEx“.

Der Befehl zur Verifizierung der SIG-Datei lautet:

```
gpg --verify "<Pfad zur Datei>"
```

Im oben verwendeten Beispiel wäre die Syntax demnach:

```
gpg --verify "C:\Users\Matthias\Desktop\dbnnestrom.bak.sig"
```

Die darauffolgende Meldung informiert darüber, ob die Signatur korrekt oder falsch ist. Außerdem lässt sich durch das zugehörige errorlevel auch automatisiert ermitteln, ob die Verifizierung erfolgreich (errorlevel = 0) oder fehlerhaft (errorlevel > 0) verlaufen ist.

Support und weitere Informationen

Sollten Sie Schwierigkeiten mit der Zertifikaterstellung, dem Import unseres Zertifikates oder der Verifizierung haben, so stehen wir gerne für Auskünfte zur Verfügung.

Weitergehende Informationen über Elektronische / Digitale Signaturen, PGP und Web of Trust, erhalten Sie über folgende Links:

http://de.wikipedia.org/wiki/Elektronische_Signatur

http://de.wikipedia.org/wiki/Digitale_Signatur

http://de.wikipedia.org/wiki/Pretty_Good_Privacy

<http://de.wikipedia.org/wiki/OpenPGP>

http://de.wikipedia.org/wiki/Web_of_Trust