Verschlüsselung von Dateien

für den Versand an die virtuelle Poststelle
via Internet

Stand 07.03.2016

Landesbetrieb Daten und Information
Valenciaplatz 6

55118 Mainz

Inhaltsverzeichnis

1 Vorbemerkung

Diese Anleitung richtet sich ausschließlich an Bürger[1] und Firmenmitarbeiter, die über die virtuelle Poststelle mit Behörden in Rheinland-Pfalz kommunizieren und Dateien per E-Mail verschlüsselt einsenden möchten. Ein weitergehender Support zu Signatur- und Verschlüsselungssoftware kann für diese Kundengruppe leider nicht übernommen werden.

Benutzer eines rheinland-pfälzischen Behördenpostfachs der virtuellen Poststelle können sich bei Fragen zu Signatur- und Verschlüsselungskomponenten an den jeweiligen Dienstleister wenden. Für kommunale Stellen ist dies die KommWis GmbH, für staatliche Stellen der Landesbetrieb Daten und Information Rheinland-Pfalz. Es gelten die bekannten Supportkontakte.
Behördenbenutzer, die Dateien per E-Mail ausschließlich über das E-Mailsystem des Landesbetriebs Daten und Information versenden (Transportweg über das sichere Behördennetz), benötigen die in dieser Anleitung gezeigte Verschlüsselung nicht.

2 Einleitung

Die virtuelle Poststelle des Landes Rheinland-Pfalz ist in der Lage, S/MIME-verschlüsselte E- Mail-Nachrichten zu entschlüsseln. Dazu muss der Absender in der Regel ein eigenes X.509 E-Mail-Zertifikat, sowie ein spezifisches X.509 E-Mail-Zertifikat für das zu adressierende virtuelle Postfach in seiner E-Mail-Software hinterlegen. Zurzeit existieren nur für wenige virtuelle Postfächer spezifische E-Mail-Zertifikate, in diesen Fällen bieten die entsprechenden Behörden das Zertifikat direkt auf ihren Internetseiten zum Download an. Mittels der S/MIME-Verschlüsselung wird die komplette Nachricht verschlüsselt, mit Ausnahme von Absender, Empfänger und Betreff.

Für alle virtuellen Postfächer besteht darüber hinaus die Möglichkeit, zumindest Dateianhänge sicher zu verschlüsseln. Bitte beachten Sie hierzu, dass im E-Mail-Text dann keine datenschutzrelevanten Informationen übermittelt werden sollten.

Zur Verschlüsselung von Nachrichtenanhängen, können beliebige Softwareprodukte zum Einsatz kommen, die eine Verschlüsselung mittels AES (bis AES256) bzw. 3-DES durchführen.

Unter Windows getestet und im Folgenden exemplarisch dargestellt wird die Nutzung der kostenlosen Software Gpg4win ab der Version 2.2.1. Gpg4win

[1] Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

unterstützt PGP/GPG- Verschlüsselung und Signatur sowie die in diesem Fall benötigte Verschlüsselung mittels S/MIME. In diesem Dokument wird ausschließlich die Verschlüsselung von Nachrichtenanhängen behandelt.

Das aktuelle Zertifikat zur Dateiverschlüsselung ist bis zum 04.02.2017 gültig. Anfang 2017 wird der Landesbetrieb Daten und Information unter http://www.rlp-service.de/RLPGateway/FVP/FV/middleware/DownloadFiles/RLP-Intermediaer.zip ein neues Zertifikat zur Verfügung stellen.

3 Herunterladen des Verschlüsselungszertifikats der virtuellen Poststelle

Um eine Datei mit dem Verschlüsselungszertifikat der virtuellen Poststelle des Landes Rheinland-Pfalz zu verschlüsseln, benötigen Sie den öffentlichen Schlüssel der virtuellen Poststelle.

Der öffentliche Schlüssel der VPS ist auf der Website www.rlp-Service.de zu finden:
http://www.rlp-service.de/RLPGateway/FVP/FV/middleware/DownloadFiles/RLP-Intermediaer.zip
Bitte speichern Sie die ZIP-Datei in einem beliebigen Ordner auf Ihrem PC und entpacken Sie sie anschließend.
Ihnen liegt nun eine Datei mit der Bezeichnung „RLP-VPS-base64.cer“ vor.
Darüber hinaus finden Sie im Archiv das Wurzelzertifkat und ggf. ein Zwischenzertifikat, beide werden im Folgenden noch benötigt. Bei zukünftigen Zertifikatswechseln werden sich die Bezeichnungen der Datei geringfügig ändern, die Anleitung gilt dann analog für die neuen Dateibezeichnungen.

4 Verschlüsselung mittels Gpg4win

Grundsätzlich können Sie zur Verschlüsselung von Dateien beliebige Programme einsetzen, die eine AES- bzw. 3DES-Verschlüsselung anhand des o.g. Zertifikats durchführen. Da viele dieser Programme kostenpflichtig sind, zeigen wir Ihnen die Verschlüsselung im Folgenden exemplarisch am Beispiel der kostenfreien
Opensource Software GPG4win. Da die Mehrzahl unserer Benutzer ein Microsoft-Betriebssystem einsetzt, zeigen wir hier die Installation der Software für Windows. Unter Linux kann GnuPG und Kleopatra analog verwendet werden. Unter Mac OS sollten die GPGTools die gleichen Funktionen bereitstellen.

4.1 Installation und Konfiguration

Gpg4win (***G****NU* ***P****rivacy* ***G****uard for* ***Win****dows*) ist ein Installationspaket für Windows und kann kostenfrei aus dem Internet (http://www.gpg4win.de/) heruntergeladen werden.

Nachrichtenanhänge für die virtuelle Poststelle können wie unten beschrieben verschlüsselt werden, die Nutzung der übrigen durch Gpg4win bereitgestellten Funktionen (insbesondere die PGP-Verschlüsselung) wird noch nicht durch die virtuelle Poststelle unterstützt.

Nach dem Download von Gpg4win wird die Installation durch Doppelklick auf die Datei gpg4winX.X.exe (X.X= die jeweils aktuelle Versionsnummer) und Klick auf den Button „Ausführen“ gestartet:

Abbildung 1

Während der Installation kann die gewünschte Sprache ausgewählt werden:

Abbildung 2

Es erscheint der Begrüßungsbildschirm:

Abbildung 3

In der folgenden Maske werden die Lizenzinformationen angezeigt:


Gpg4win Installation
Lizenzabkommen
Diese Software ist unter der GNU General Public License (GPL) lizensiert.
Drücken Sie die Bild-nach-unten Taste, um den Rest des Abkommens zu sehen.
Gpg4win consist of several independent developed packages, available under different license conditions. Most of these packages however are available under the GNU General Public License (GNU GPL). Common to all is that they are free to use without restrictions, may be modified and that modifications may be distributed. If the source files (i.e. gpg4win-src-x.y.z.exe) are distributed along with the binaries and the use of the GNU GPL has been pointed out, distribution is in in all cases possible.
What follows are the terms of the GNU GPL; for a list of individual copyright and license notices please see the installed README file.
In aller Kürze: Sie haben das Recht, die Software zu jedem Zweck einzusetzen. Sie können die Software weitergeben, sofern Sie dem Empfänger dieselben Rechte einräumen, die auch Sie erhalten haben.
Nullsoft Install System v2,46-7
< Zurück
Weiter >
Abbrechen

Abbildung 4

Die Betätigung des Weiter-Buttons führt zur Komponentenauswahl:

Abbildung 5

Hier kann die Standardvorbelegung übernommen werden. In jedem Fall aber muss Kleopatra (Ein Zertifikatsmanager für OpenPGP und X.509 (S/MIME)) mit ausgewählt sein. Ein Klick auf den Weiter-Button schließt die Komponentenauswahl ab.

Nun ist das Zielverzeichnis für die zu installierenden Komponenten festzulegen:

Abbildung 6

In der Maske „Installationsoptionen“ wird die gewünschte Verknüpfung ausgewählt:

Abbildung 7

Schließlich wird der Startmenü-Ordner bestimmt:

Abbildung 8

Damit ist die Installation vollständig:

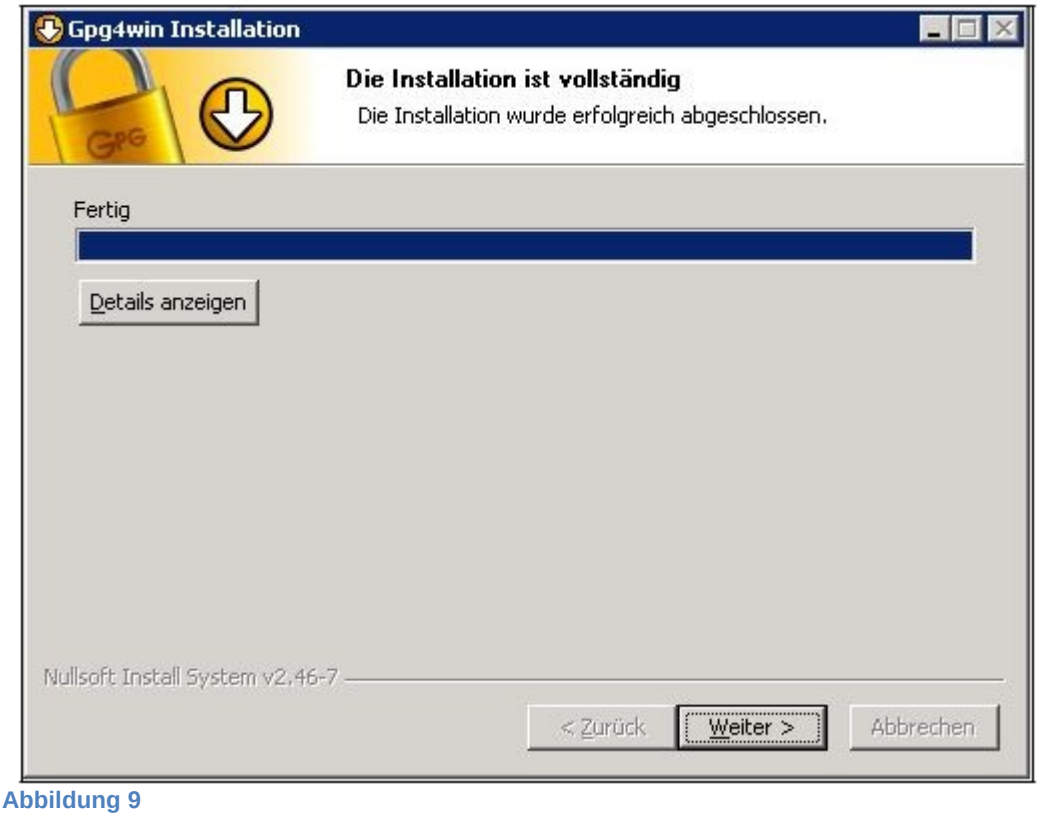

Abbildung 9

Zum Abschluss muss der Rechner neu gestartet werden:

Abbildung 10

4.2 Basiskonfiguration Kleopatra

Als nächstes muss die Anwendung Kleopatra konfiguriert werden. Dazu muss Kleopatra gestartet, in der Menüleiste die Auswahl „Einstellungen“ und anschließend „Kleopatra einrichten“ gewählt werden.

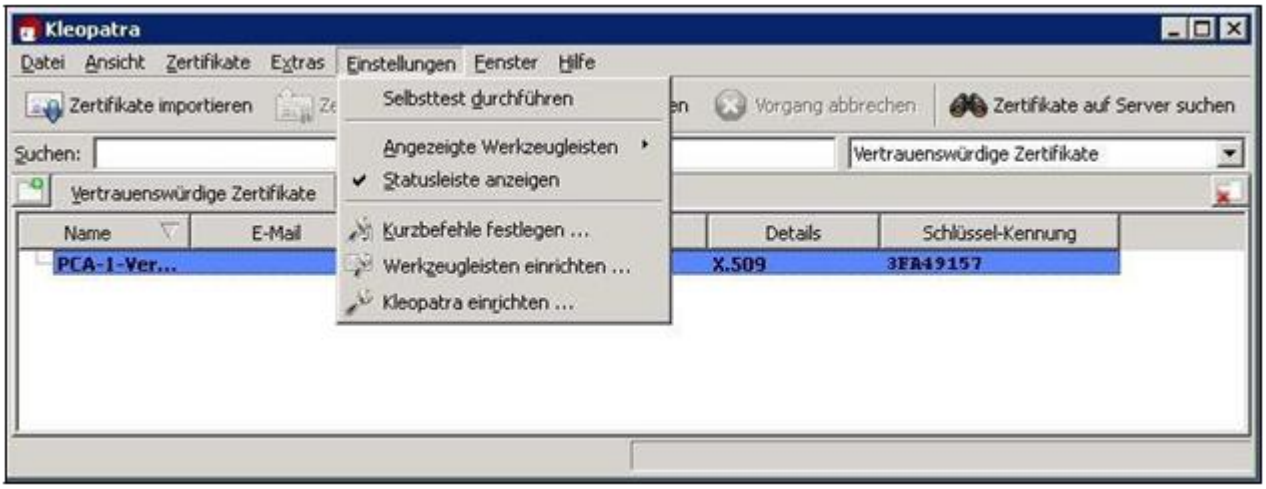

Abbildung 11

Hier ist es wichtig, darauf zu achten, dass unter „GnuPG-System“ auf der Registerkarte „GPG for S/MIME“ in jedem Fall als Verschlüsselungsverfahren AES oder 3DES eingetragen ist.

Falls der Rechner, auf dem die Verschlüsselung durchgeführt wird, keinen Zugriff auf das Internet hat, ist es hier notfalls auch möglich, die Option „Niemals eine CRL konsultieren“ auszuwählen. Das hat zur Folge, dass keine Prüfung auf zurückgezogene Zertifikate erfolgen kann. Wählen Sie diese Option daher bitte nur, wenn Sie selbst keine Signaturen und Zertifikate prüfen möchten und tatsächlich kein Internetzugang besteht.

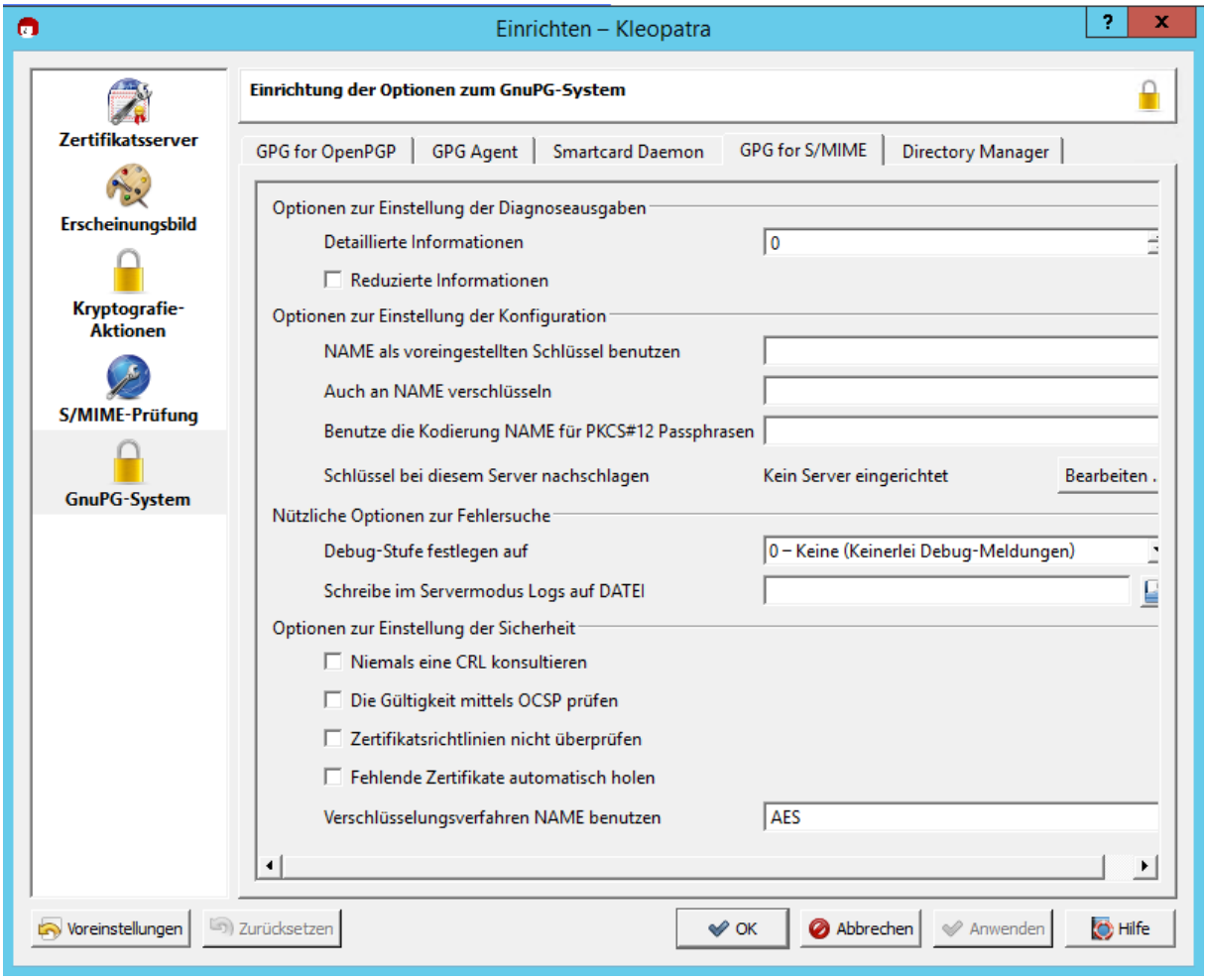

Abbildung 12

4.3 Import der Verschlüsselungszertifikate

Um das Verschlüsselungszertifikat der virtuellen Poststelle inklusive Herausgeberzertifikat und Zwischenzertifikat zu importieren, wird zunächst Kleopatra gestartet:

Abbildung 13

Der Startbildschirm zeigt zunächst keine Zertifikate:

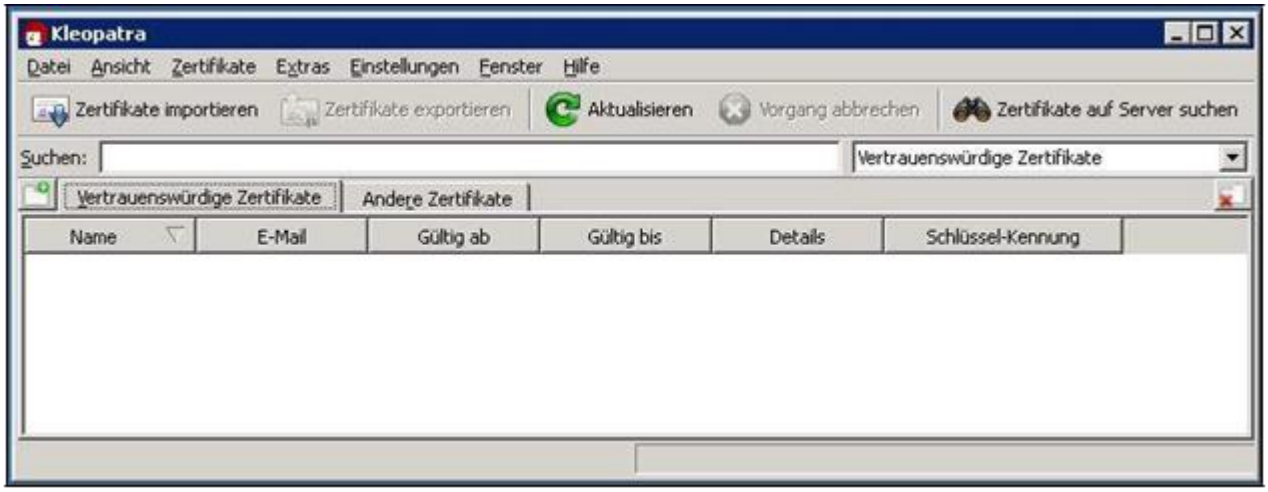

Abbildung 14

Zur Auswahl der zu importierenden Zertifikate ist zunächst der Button „Zertifikate importieren“ anzuklicken:

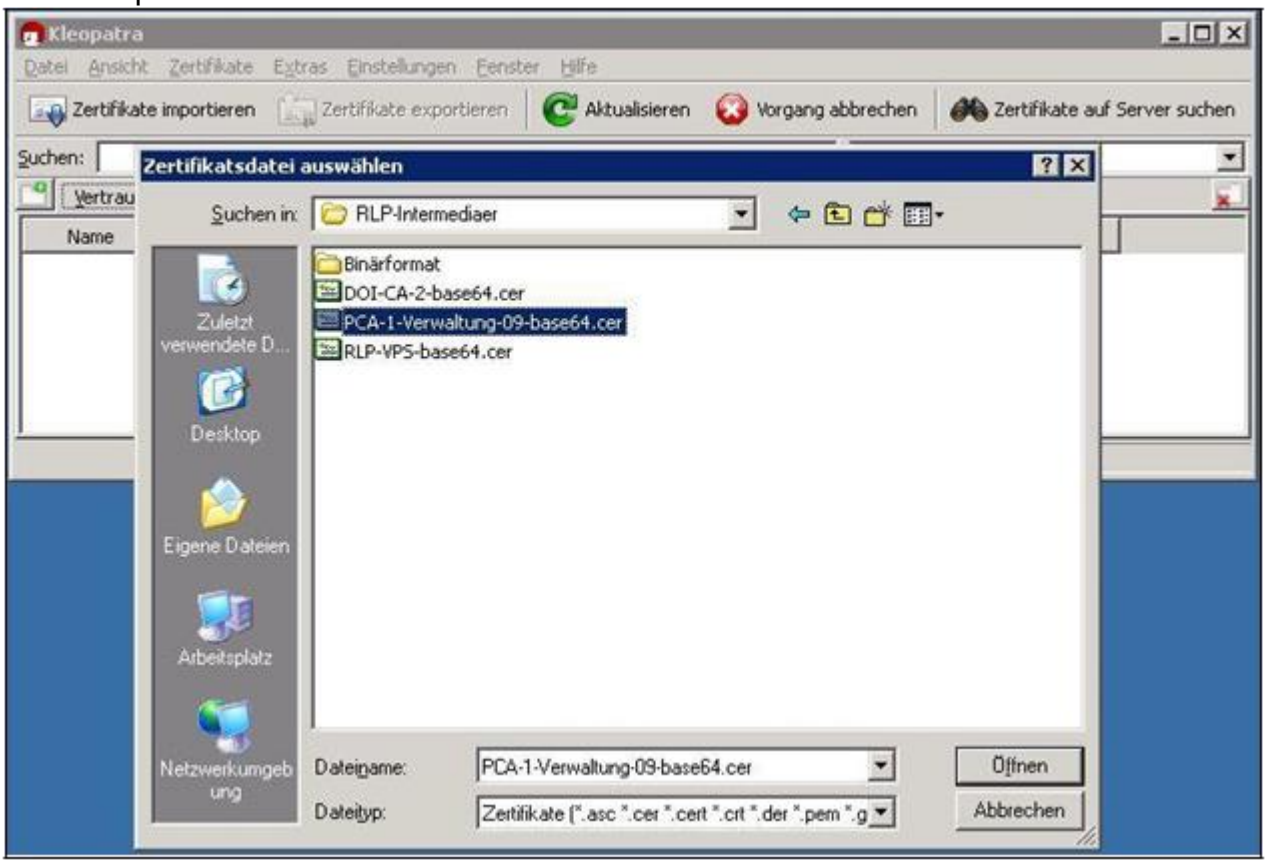

Abbildung 15

Zunächst wird das Rootzertifikat PCA-1-Verwaltung-14-base64.cer ausgewählt (die Nummerierung ändert sich mit dem Austausch der Zertifikate auf unserer Seite, verwenden Sie immer die Dateien, die Sie wie unter Kapitel 3 beschrieben heruntergeladen haben):

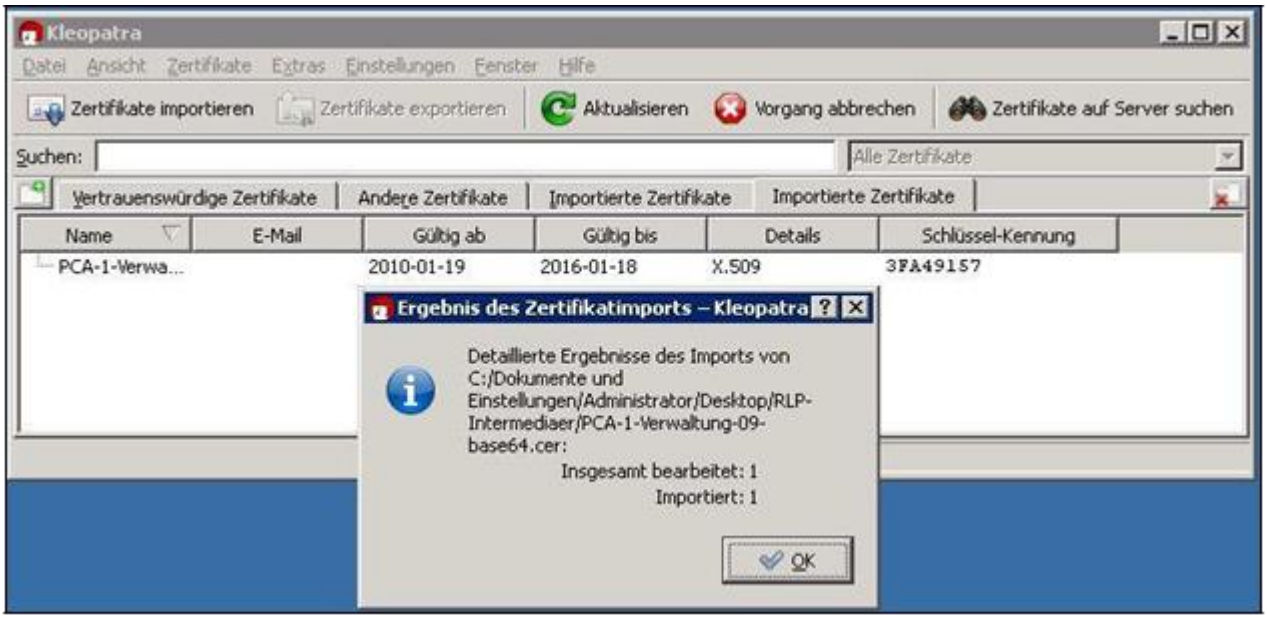

Abbildung 16

Ein Rechtsklick auf dieses „Root“-Zertifikat ermöglicht es, dem Zertifikat über „Wurzelzertifikat vertrauen“ das erforderliche Vertrauen auszusprechen:

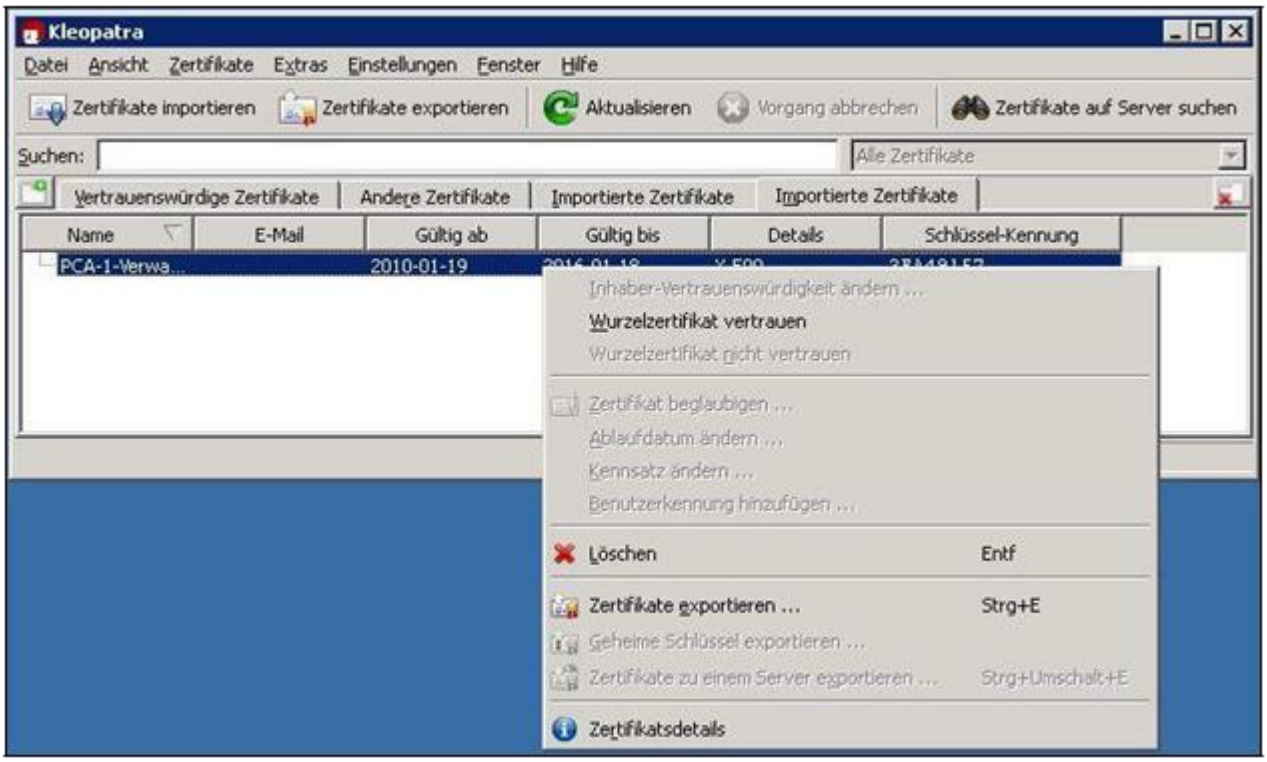

Abbildung 17

Als Resultat ist das Wurzelzertifikat anschließend blau hinterlegt:

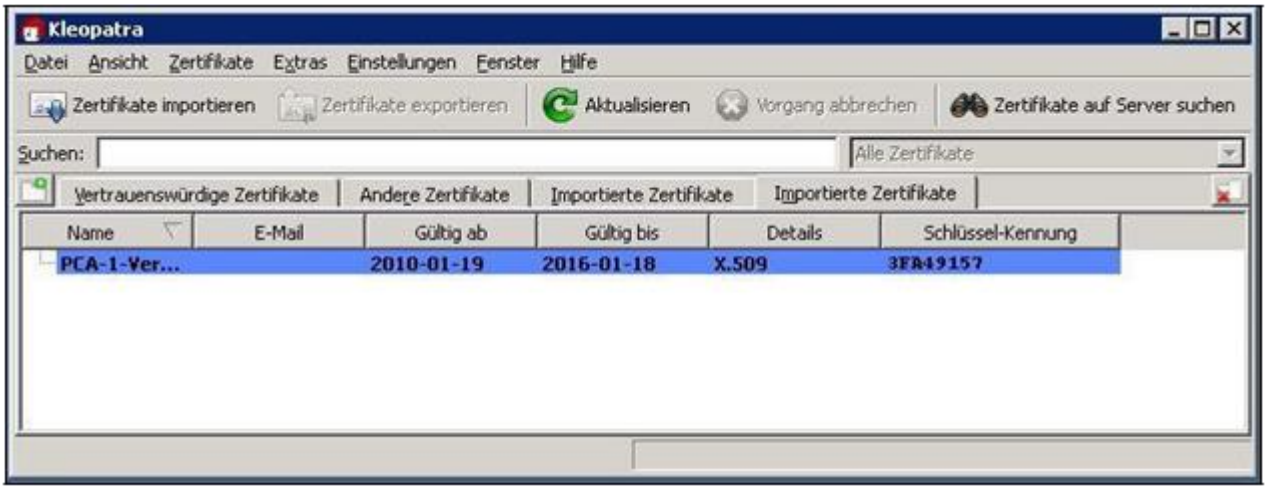

Abbildung 18

Nun wird auf dem gleichen Weg das Zwischenzertifikat DOI-CA Zertifikat importiert:

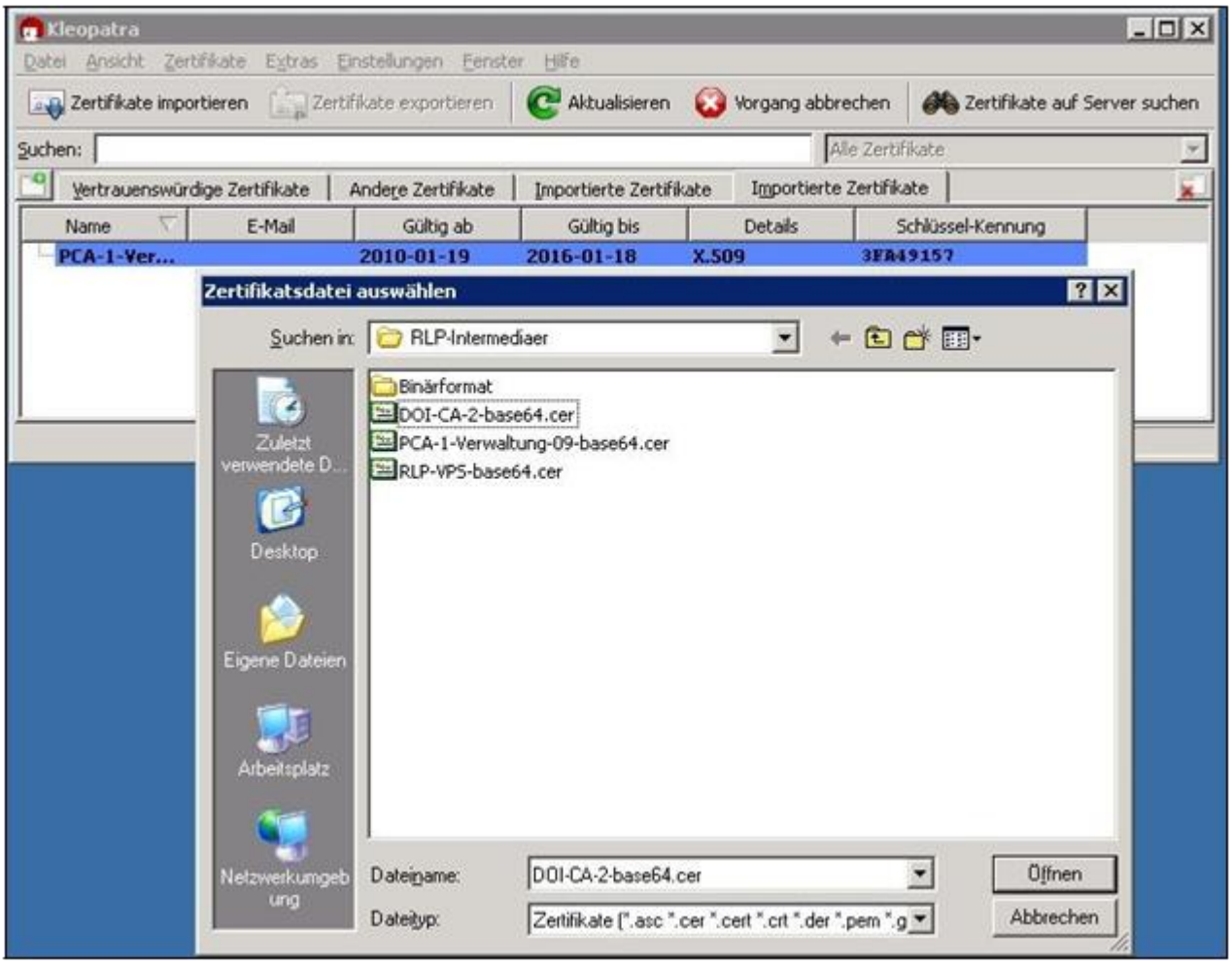

Abbildung 19

Der erfolgreiche Import des Zwischenzertifikats wird wie folgt bestätigt:

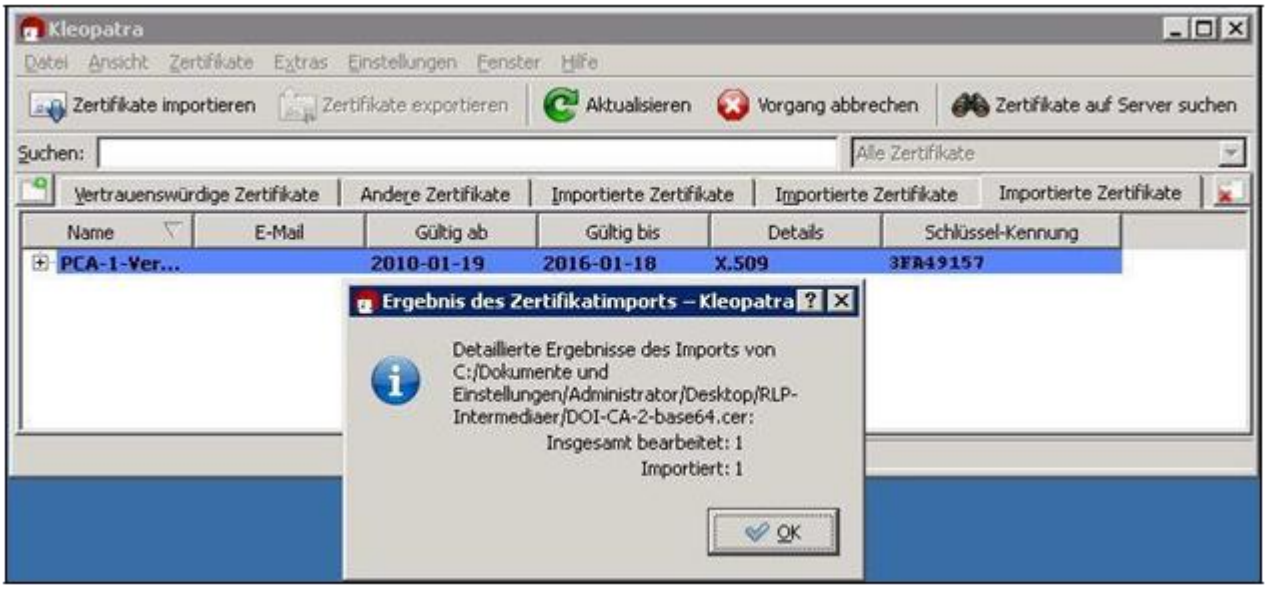

Abbildung 20

Durch Klick auf das Pluszeichen vor dem Wurzelzertifikat kann die bisherige Zertifikatskette angezeigt werden:

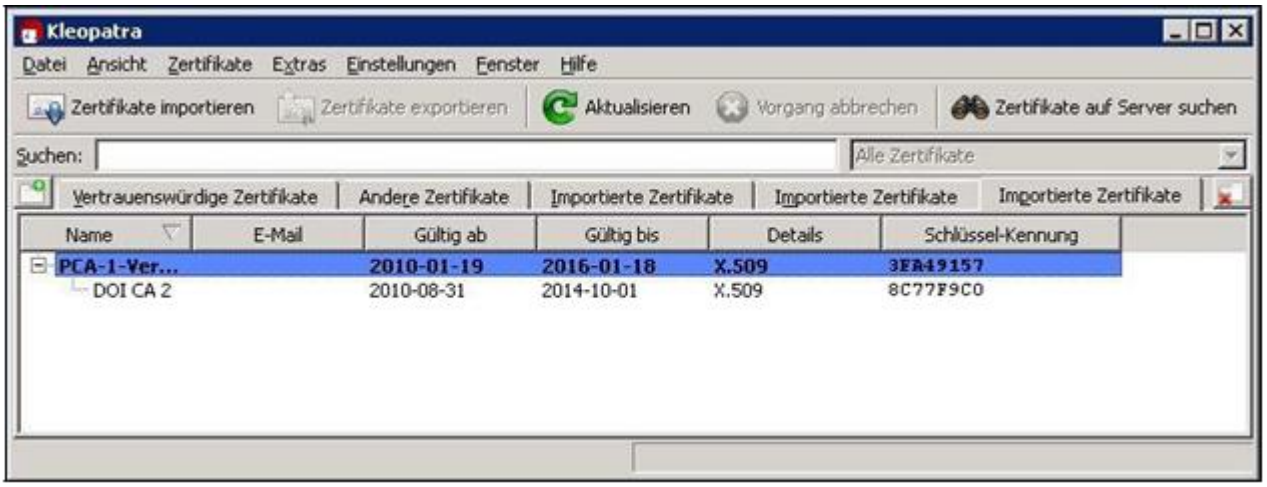

Abbildung 21

Jetzt wird, wie gehabt, das eigentliche Zertifikat „RLP-VPS“ importiert:

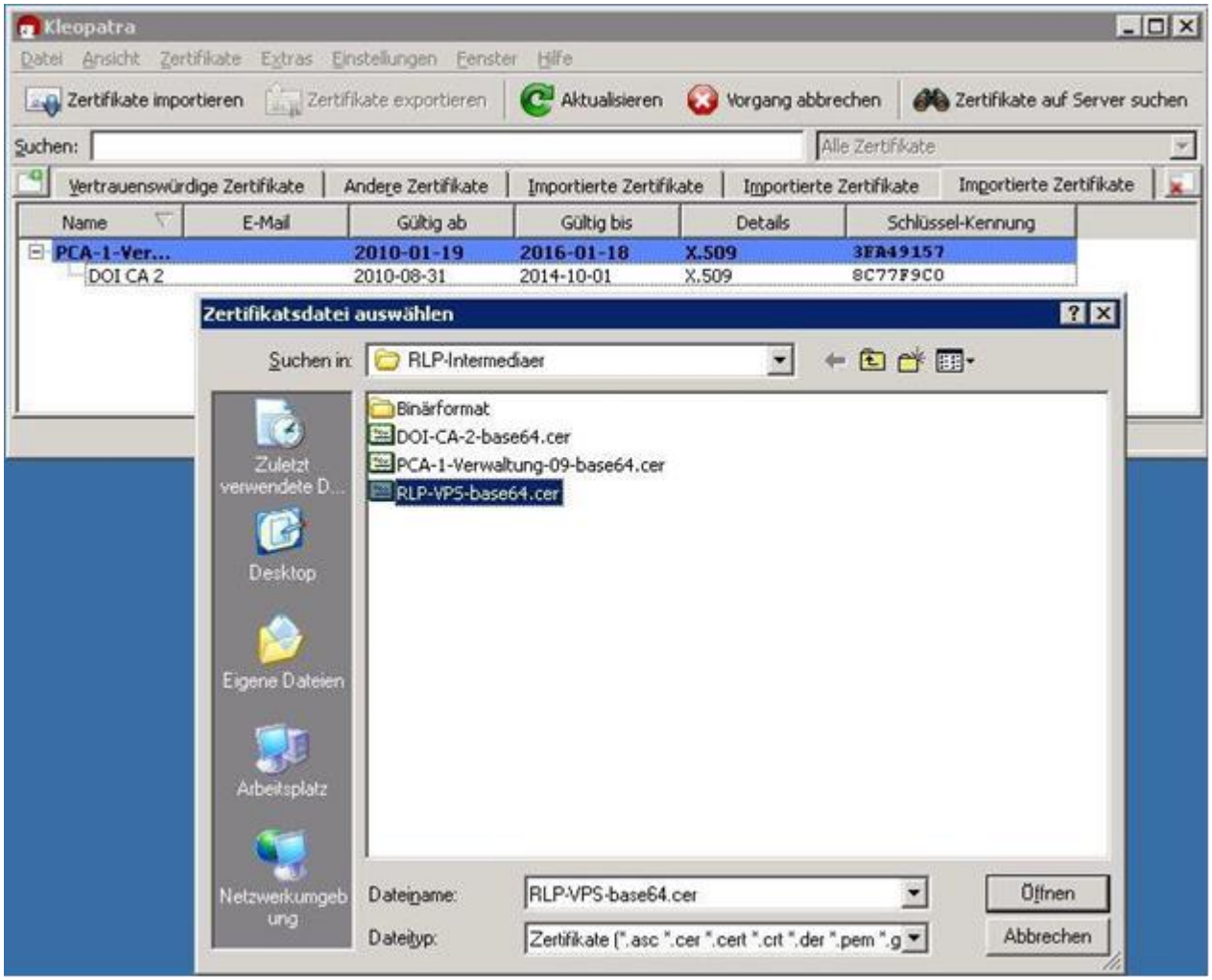

Abbildung 22

Der erfolgreiche Import des Zertifikats wird wieder bestätigt:

Abbildung 23

4.4 Verschlüsseln einer Datei

Ausgangslage: Es liegt eine zu verschlüsselnde Datei vor:

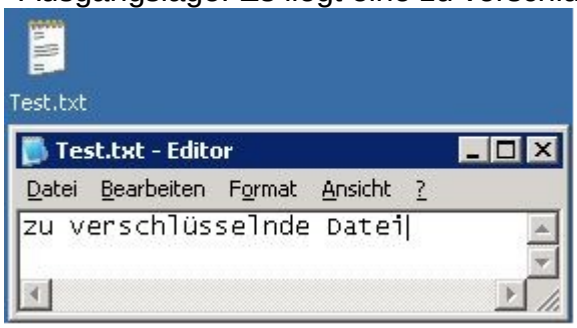

Abbildung 24

Ein Rechtsklick auf die Datei ermöglicht die Auswahl „Mehr GpgEX Optionen“: Dort wird der Unterpunkt „Verschlüsseln“ gewählt:

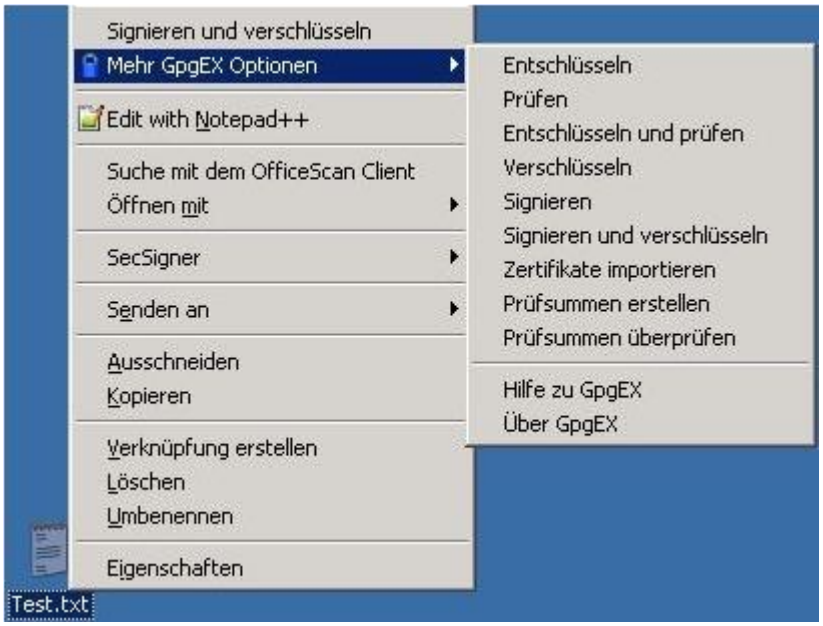

Abbildung 25

Im folgenden Bildschirm muss die Option „Verschlüsseln“ gewählt sein und mit „Weiter“ bestätigt werden:

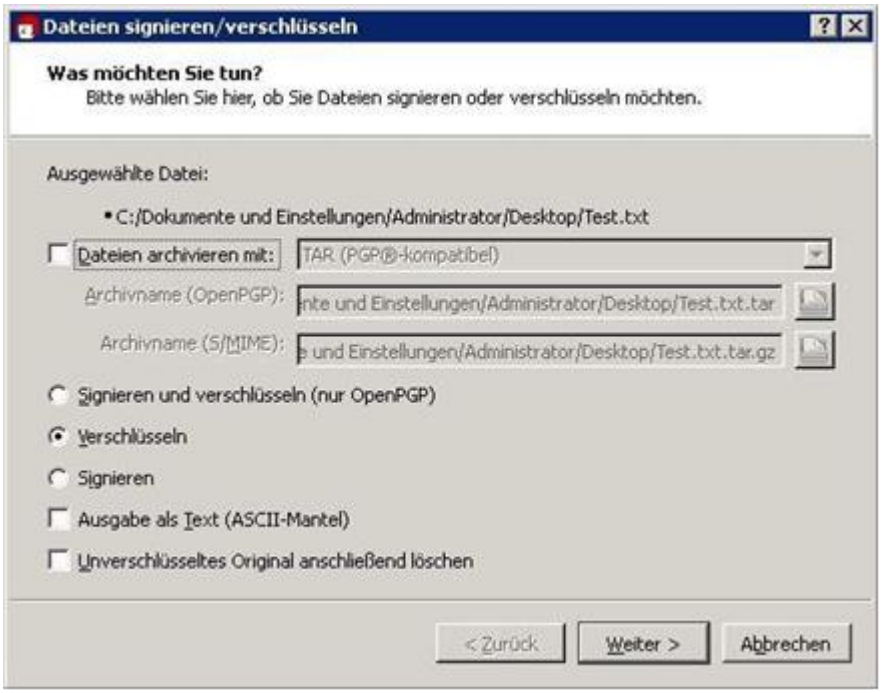

Abbildung 26

Jetzt wird das Zertifikat ausgewählt und „Verschlüsseln“ angeklickt:

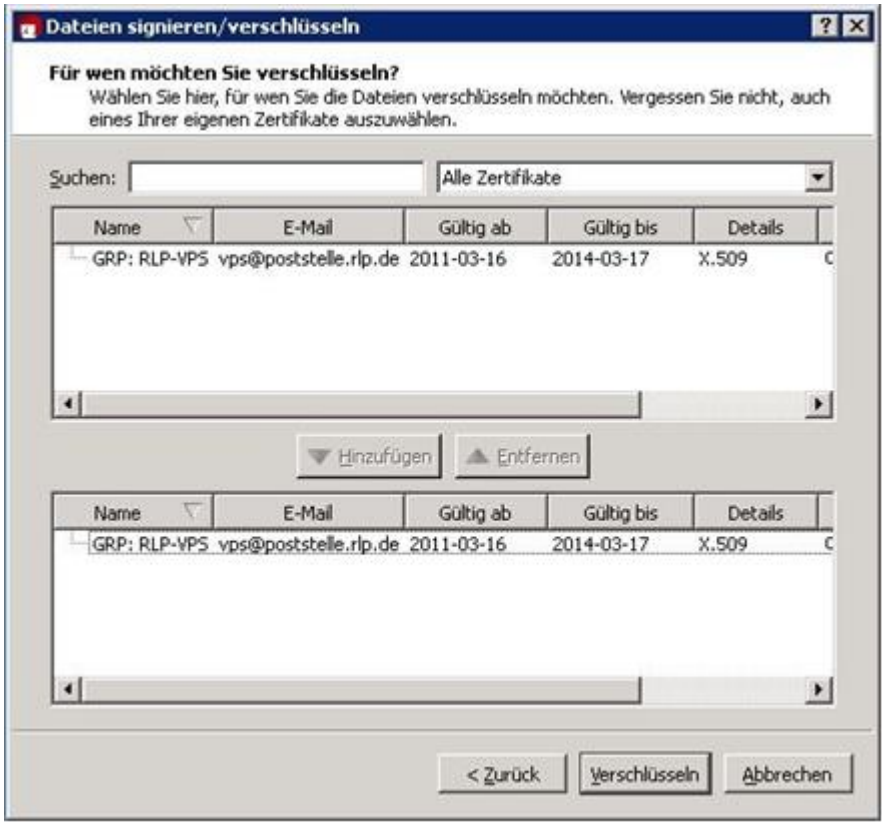

Abbildung 27

Es erfolgt ein Hinweis, den Sie jedoch ignorieren können (Hier können Sie auch die Option „Diese Nachfrage nicht mehr anzeigen“ wählen):

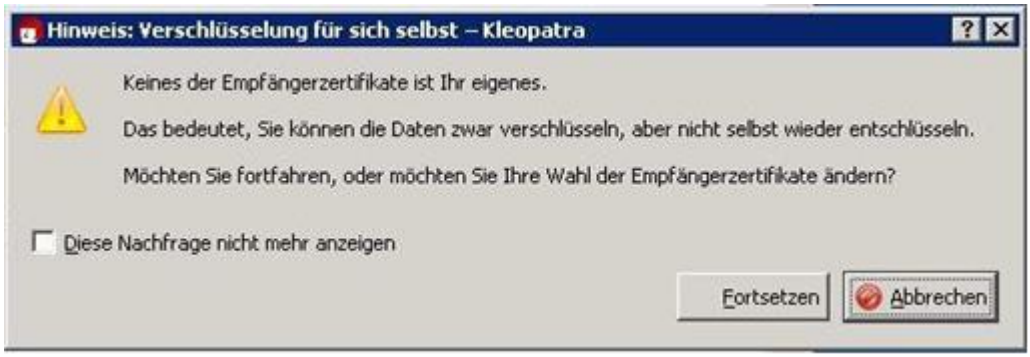

Abbildung 28

Das Ergebnis der Verschlüsselung wird im folgenden Bildschirm dargestellt:

Abbildung 29

Mit einem Klick auf „Fertigstellen“ wird der Vorgang abgeschlossen.

Die verschlüsselte Datei mit der Endung „.p7m“ können Sie nun an eine E-Mail anhängen, die Sie an eine virtuelle Postfachadresse des Landes Rheinland-Pfalz senden möchten.