Verschlüsselung von Dateien

mittels

SecCommerce SecSigner
und
Gpg4win

Stand 03.02.2014

Landesbetrieb Daten und Information
Valenciaplatz 6
55118 Mainz

Inhaltsverzeichnis

1. 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 3-DES durchführen.

Unter Windows getestet und exemplarisch im Folgenden dargestellt wird die Nutzung der kostenlosen Software SecCommerce SecSigner ab Version 3.5.0 und Gpg4win ab der Version 2.2.1.
SecSigner kann sowohl zur qualifizierten elektronischen Signatur von Dateien als auch zur Verschlüsselung von Dateien verwendet werden. Gpg4win 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 mit dem Algorithmus Triple-DES (3DES) behandelt.

Das Zertifikat zur Dateiverschlüsselung ist bis zum 04.02.2017 gültig. Anfang 2017 werden wir unter http://www.rlp-service.de/RLPGateway/FVP/FV/middleware/DownloadFiles/RLP-Intermediaer.zip ein neues Zertifikat zur Verfügung stellen.

2. Verschlüsselung mittels SecSigner

2.1. Installation und Konfiguration

Die Software SecSigner ist über die Seite des Hersteller zu beziehen:
https://www.seccommerce.de/de/products/secsigner/download.html
Bzw. Direktlink:
https://www.seccommerce.de/de/public-downloads/file/1-windows-setup.html

Die Installationsdatei muss heruntergeladen (ca. 4,7 MB) und installiert werden:

Abbildung 1: Speichern des Setup-Programms

Speichern Sie die Installationsdatei bitte zunächst auf Ihrem Rechner.

Abbildung 2: Ausführen des Setup-Programms

Starten Sie nun das soeben heruntergeladene Setup-Programm durch Doppelklick auf die Datei „Setup-3-5-0.exe“. Eine etwaige Sicherheitswarnung bestätigen Sie bitte mit „Ausführen“.

Abbildung 3: Startbildschirm des Setup-Programms

Nun erscheint der Startbildschirm des Setup-Programms. Mit „Weiter“ gelangen Sie zur nächsten Seite.

Abbildung 4: Bestätigung der Lizenzbedingungen

Prüfen und bestätigen Sie nun bitte den Lizenzvertrag durch Setzen des Häkchens bei „Ich stimme den Bedingungen zu.“. Klicken Sie anschließend bitte auf „Weiter“.

Abbildung 5: Einstellung der Installationsoptionen

Die Installationsoptionen können Sie unverändert lassen. Benötigt werden in jedem Fall: SecCommerce SecSigner und CSP für Windows-Anwendungen. Der Installationsordner kann bei Bedarf geändert werden. Durch Klick auf „Installieren“ wird die Software installiert.

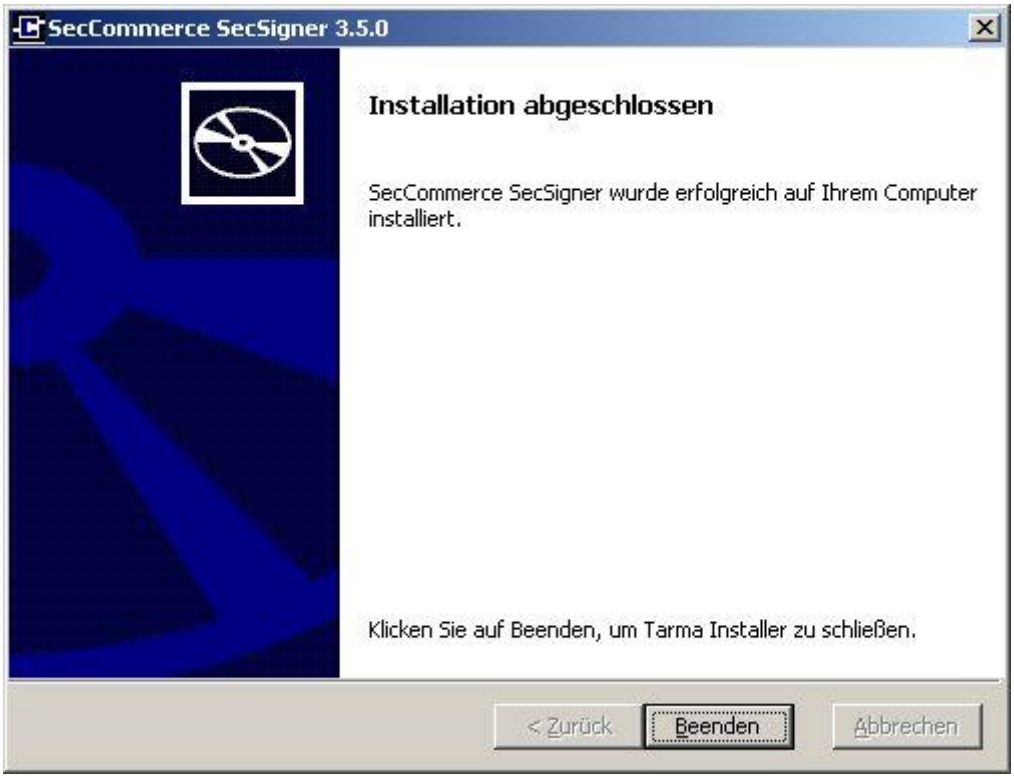

Abbildung 6: Abschluss des Setup-Programms

Das Abschlussfenster des Setup-Programms schließen Sie bitte durch Klick auf „Beenden“.

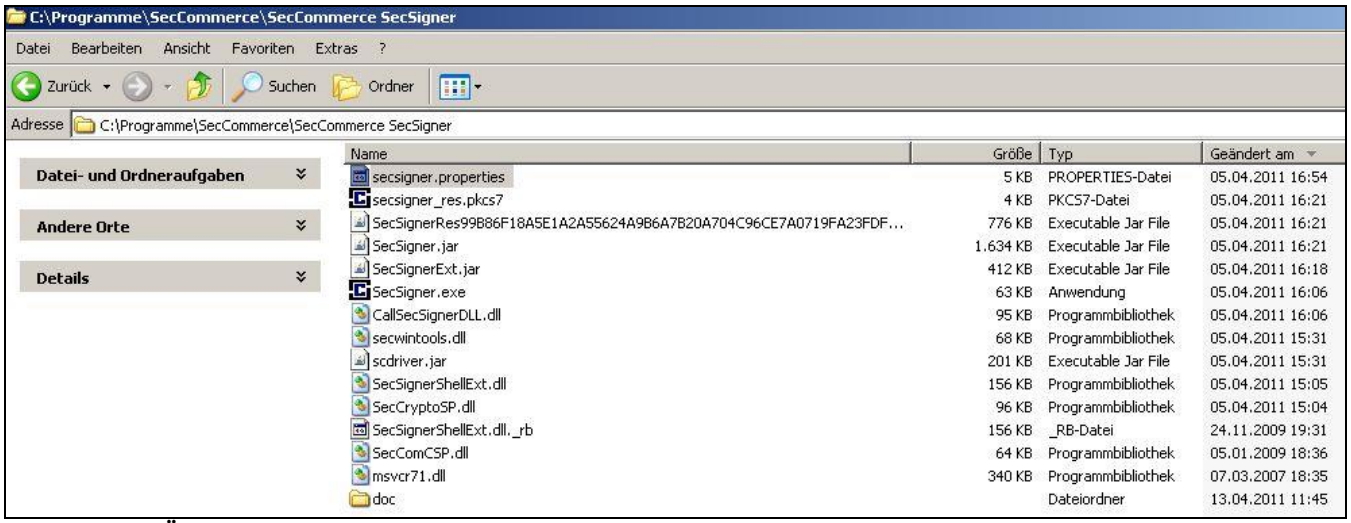

Abbildung 7: Öffnen der Konfigurationsdatei „secsigner.properties“

Im Nachgang ist noch eine Konfigurationsänderung erforderlich, um die Software mit der virtuellen Poststelle des Landes Rheinland-Pfalz verwenden zu können.
Wechseln Sie dazu bitte in das Installationsverzeichnis der Anwendung (Standardmäßig: „C:\Programme\SecCommerce\SecCommerce\SecSigner“).

Öffnen Sie dort bitte die Datei secsigner.properties (z.B. mit Wordpad) und fügen Sie am Ende der Datei bitte folgende Zeile (ohne Anführungszeichen) ein:
„seccommerce.secsigner.encryption.cipherid=0“

```
seccommerce.secsigner.showattributecertoption=on
seccommerce.secsigner.disableselectwhensigning=off
seccommerce.secsigner.resetkeyuponprevinit=off
seccommerce.cert.requirequalified=off
seccommerce.secsigner.certstackdownload.url=https
\://www.seccommerce.de/dev/certs-secsigner/cgi-bin/getCertStack.py
seccommerce.secsigner.certstackdownload.name=https
\://www.seccommerce.de/dev/certs-secsigner/cgi-
bin/getCertStackName.py
seccommerce.secsigner.certstackdownload.confirm=on
seccommerce.secsigner.certstackdownload.enabled=on
seccommerce.secsigner.displayhelp=off
seccommerce.secsigner.savedocument=on
seccommerce.secsigner.encryption.mandatory=off
seccommerce.secsigner.softcertautoselect=off
seccommerce.secsigner.encryption.cipherid=0
```

Abbildung 8: Ergänzung der Datei secsigner.properties

Nachdem Sie die Zeile ergänzt haben speichern Sie bitte Änderungen.

2.2. 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.

2.3. Verschlüsselung einer Datei

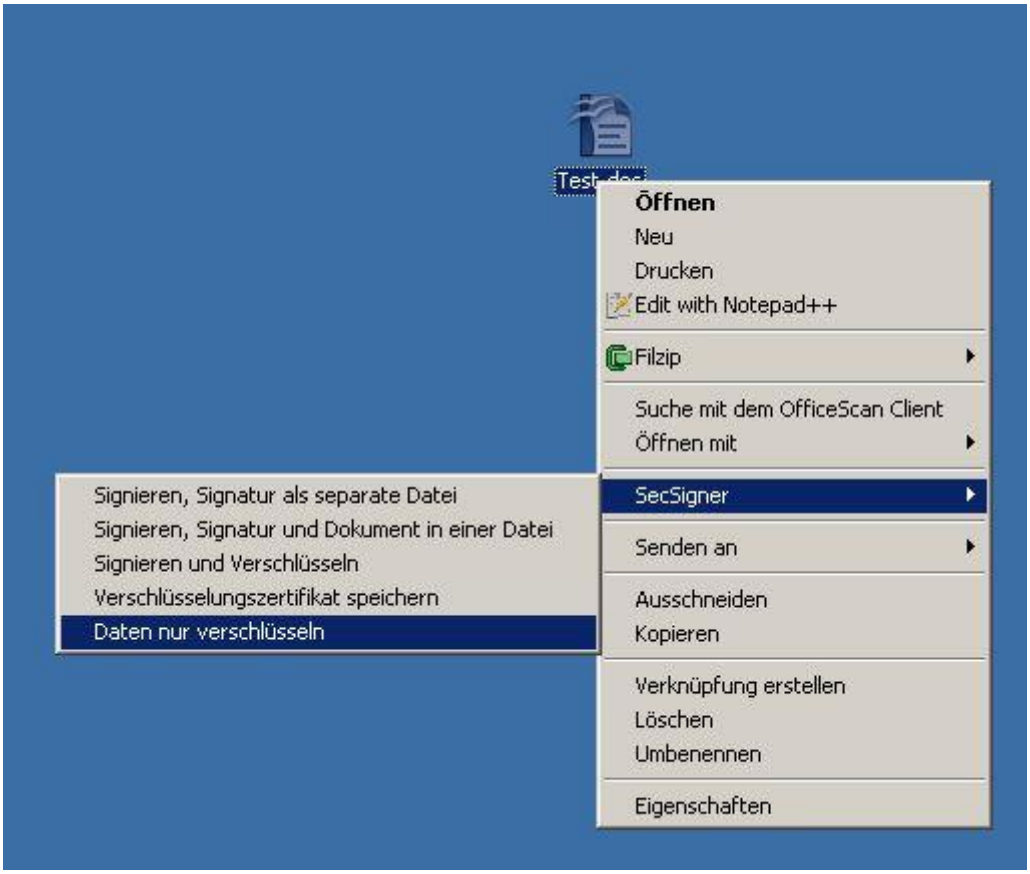

Abbildung 9: Zu verschlüsselnde Datei auswählen

Nach der Installation von SecSigner finden Sie bei Verwendung der rechten Maustaste auf die zu verschlüsselnde Datei einen Menupunkt "SecSigner", der wiederum als untersten Menupunkt "Daten nur verschlüsseln" anbietet.

Abbildung 10: Bestätigungsfenster zur Auswahl des Verschlüsselungszertifikats

Das nun folgende Bestätigungsfenster können Sie durch einfachen Klick auf „OK“ bestätigen.

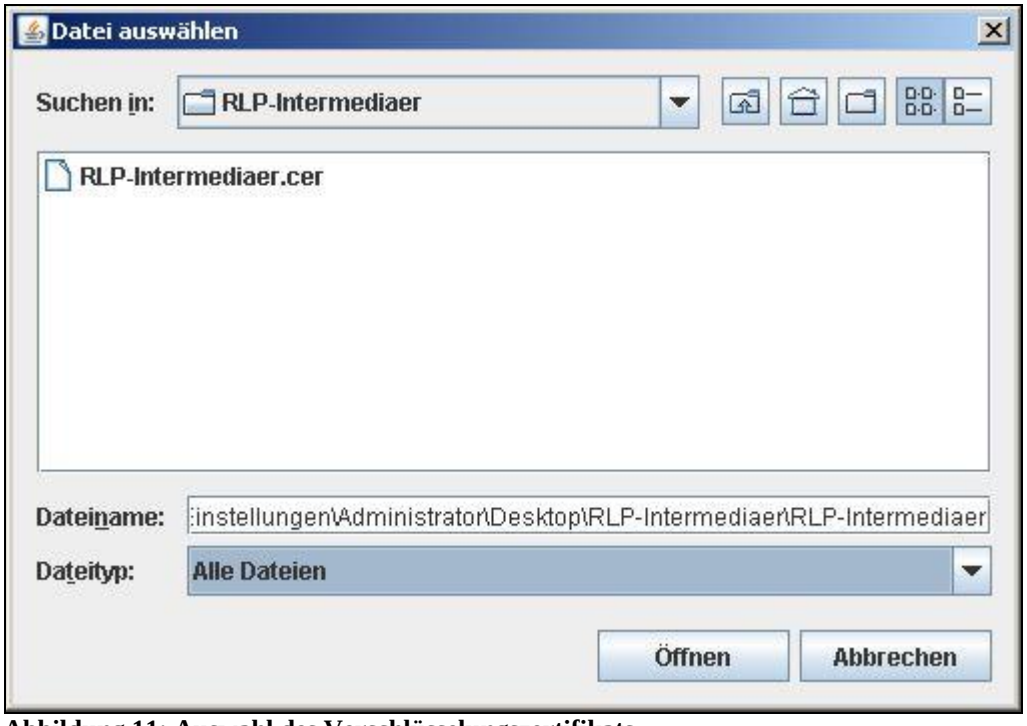

Abbildung 11: Auswahl des Verschlüsselungszertifikats

Nach der Auswahl "Daten nur verschlüsseln" haben Sie noch den Speicherort des öffentlichen Schlüssels der virtuellen Poststelle auf Ihrem PC anzugeben. Achten Sie darauf bei Dateityp

„Alle Dateien“ auszuwählen. Navigieren Sie zu der im Vorfeld heruntergeladenen Datei „RLP-VPS-base64.cer“, wählen Sie diese aus und klicken Sie anschließend auf „Öffnen“.

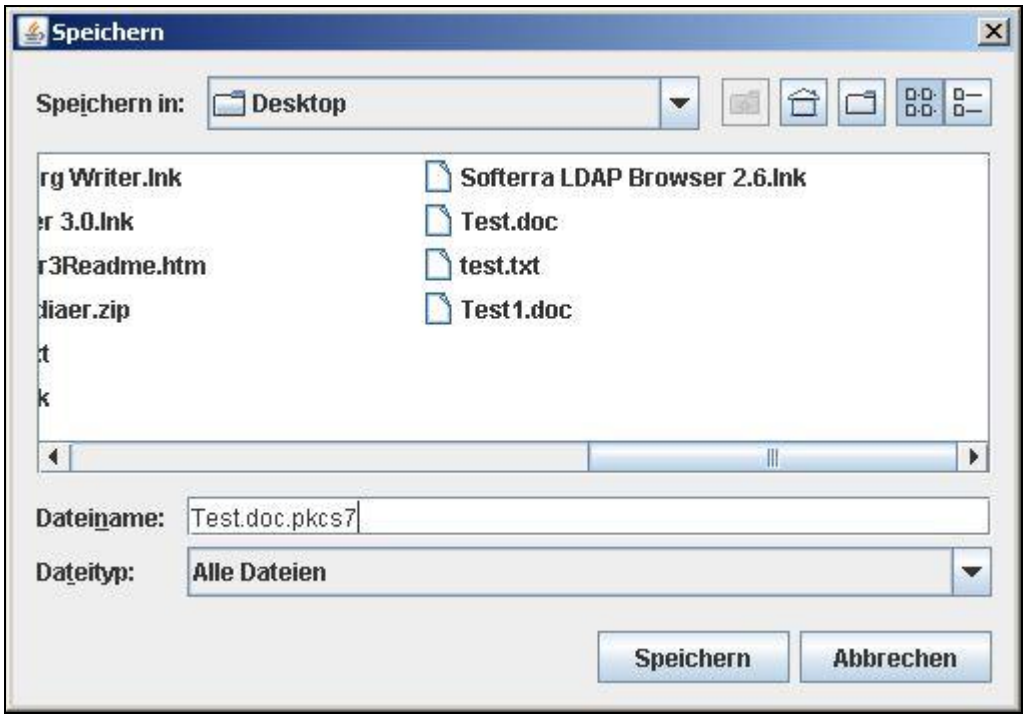

Abbildung 12: Speichern der verschlüsselten Datei

Sie erhalten nun die Möglichkeit auszuwählen, wo die neue verschlüsselte Datei gespeichert werden soll. Standardmäßig wird der ursprüngliche Dateiname um die Endung „.pkcs7“ ergänzt, dies sollten Sie beibehalten. Ihre Ursprungsdatei wird dann nicht verändert.

Die verschlüsselte Datei mit der Endung „.pkcs7“ können Sie nun an eine E-Mail anhängen, die Sie an eine virtuelle Postfachadresse des Landes Rheinland-Pfalz senden möchten.

3. Verschlüsselung mittels Gpg4win

3.1. 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.

Bitte beachten Sie, dass die aktuelle Version der virtuellen Poststelle Nachrichten mit angehängten PGP/GPG-Zertifikaten nicht verarbeiten kann. D.h. Nachrichtenanhänge für die virtuelle Poststelle können wie unten beschrieben verschlüsselt werden, die Nutzung der übrigen durch Gpg4win bereitgestellten Funktionen wird in diesem Kontext noch nicht 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 13: Installation 1

Während der Installation kann man die gewünschte Sprache auswählen:

Abbildung 14: Installation 2

Es erscheint der Begüßungsbildschirm:

Abbildung 15: Installation 3

Im Folgenden werden die Lizenzinformationen angezeigt:

Abbildung 16: Installation 4

Die Betätigung der Weiter-Buttons führt zur Komponentenauswahl:

Abbildung 17: Installation 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 18: Installation 6

Im Bildschirm „Installationsoptionen“ wird die gewünschte Verknüpfung hinterlegt:

Abbildung 19: Installation 7

Schließlich wird der Startmenü-Ordner bestimmt:

Abbildung 20: Installation 8

Damit ist die Installation vollständig:

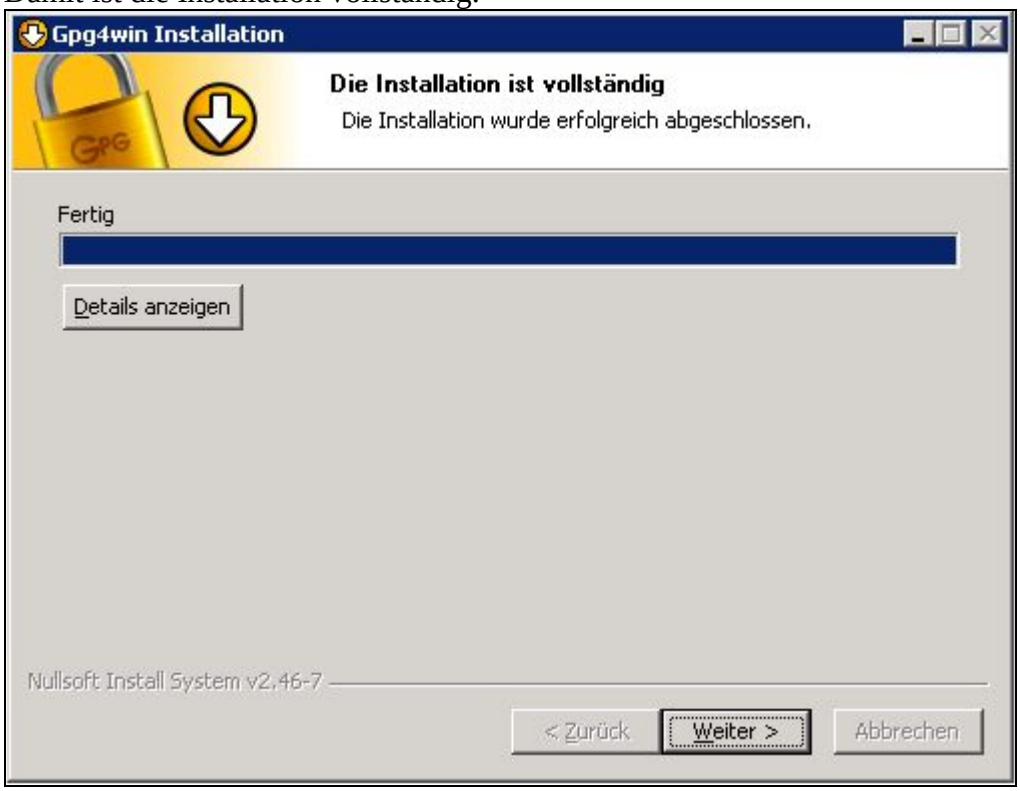

Abbildung 21: Installation 9

Und abgeschlossen:

Abbildung 22: Installation 10

Im Folgenden ist die Einstellung von Kleopatra vorzunehmen bzw. zu kontrollieren. Dazu muss Kleopatra gestartet und in der Menüleiste die Auswahl „Einstellungen“ und anschließend „Kleopatra einrichten“ gewählt werden.

Abbildung 23: Kleopatra Einrichtung 1

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

Falls der Rechner, auf dem die Verschlüsselung durchgeführt wird, keinen Zugriff auf das Internet hat, ist es notfalls hier auch möglich, die Option „Niemals eine CRL konsultieren“ auszuwählen. Das hat zur Folge, dass keine Prüfung auf zurückgezogene Zertifikate erfolgen kann.

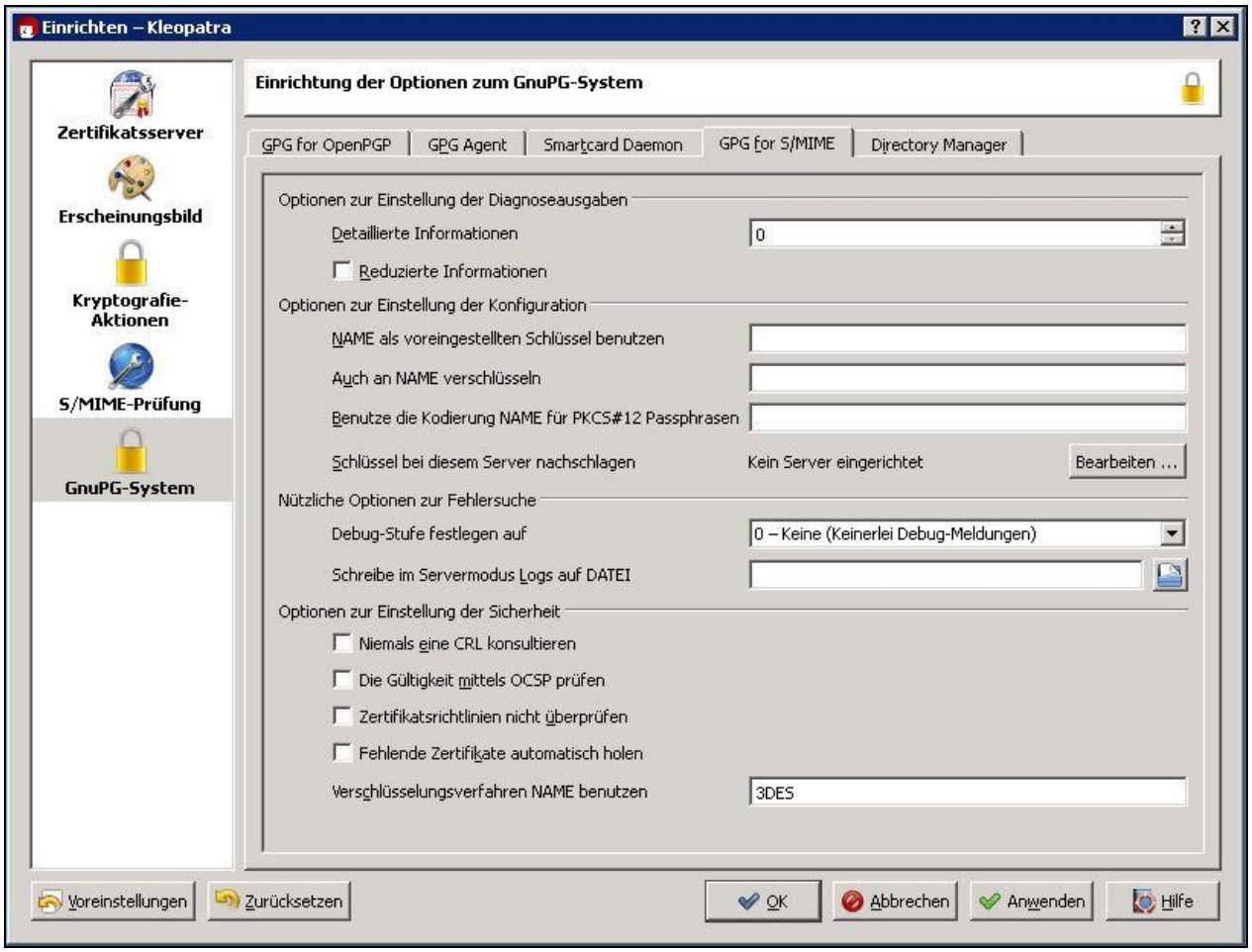

Abbildung 24: Kleopatra Einrichtung 2

3.2. Import der Verschlüsselungszertifikate

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

Abbildung 25: Kleopatra starten

Abbildung 26: Kleopatra Startbildschirm

Zur Auswahl der zu importierenden Zertifikate klickt man auf den Button „Zertifikate importieren“:

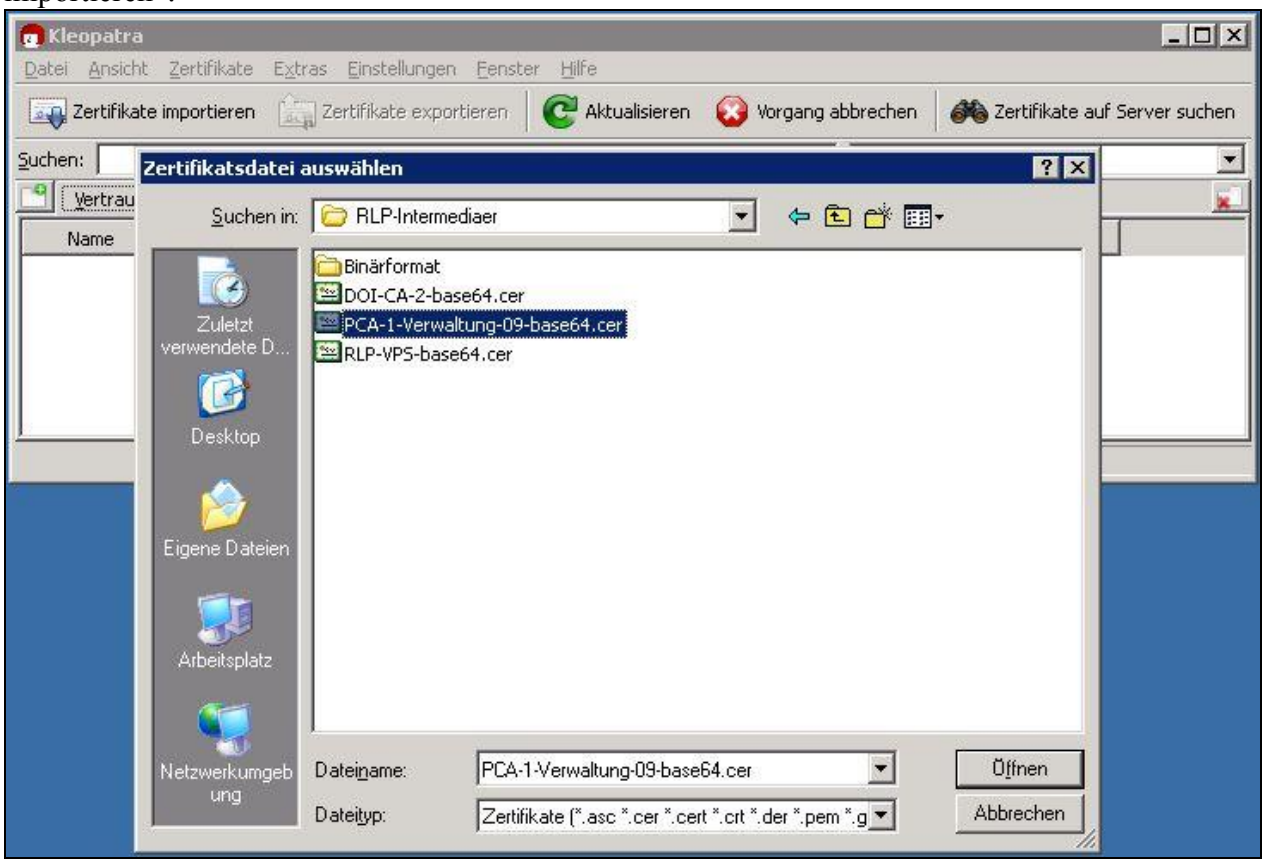

Abbildung 27: Zertifikatsauswahl

Zunächst wird das Rootzertifikat PCA-1-Verwaltung-09-base64.cer ausgewählt:

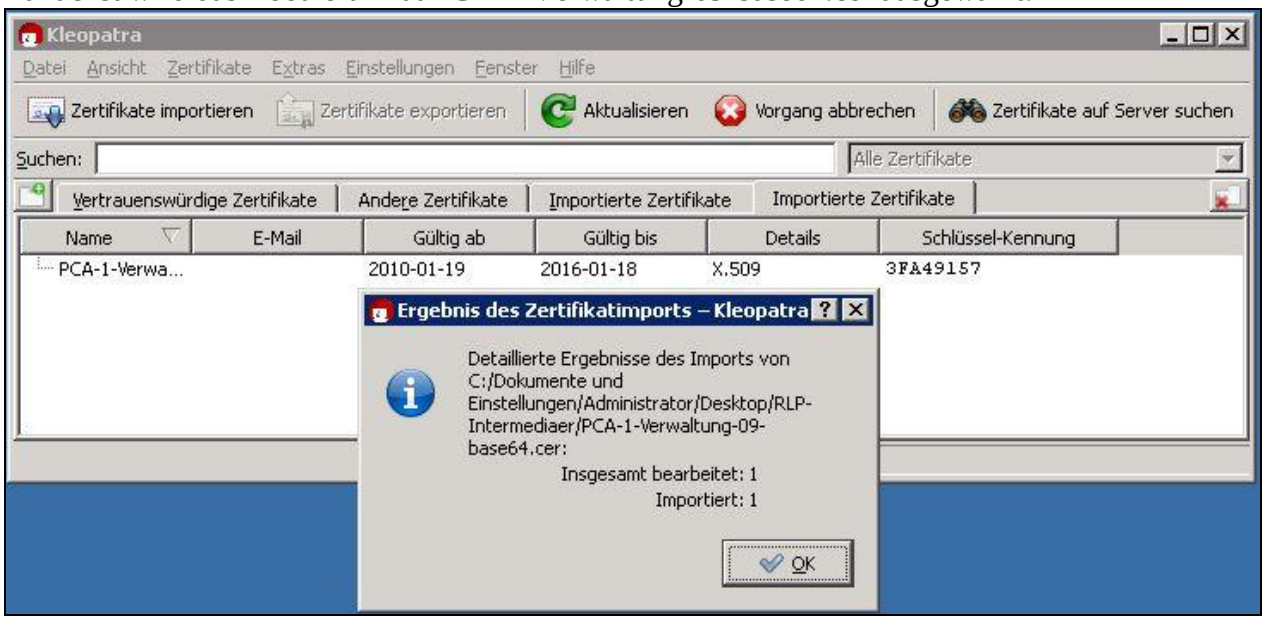

Abbildung 28: Import des Rootzertifikats

Ein Rechtsklick auf das Rootzertifikat ermöglicht es, diesem Zertifikat das erforderliche Vertrauen zu erteilen:

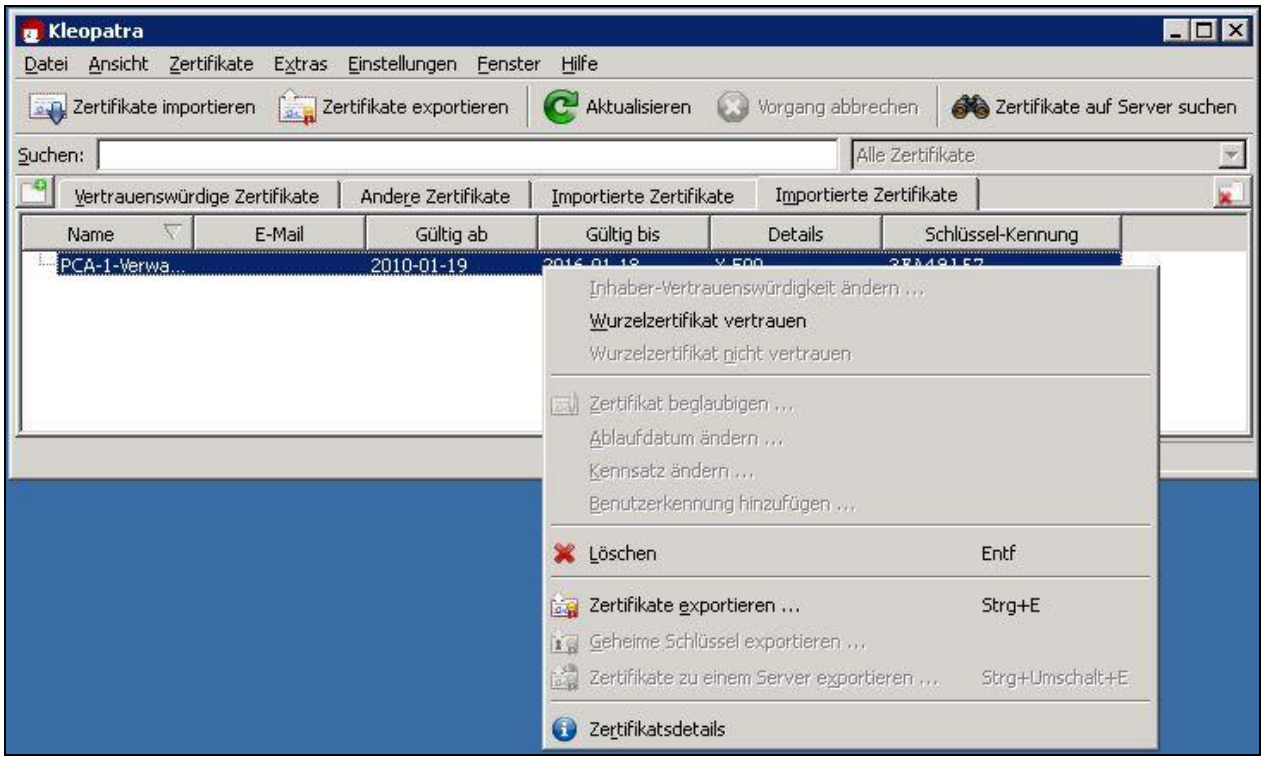

Abbildung 29: Wurzelzertifikat vertrauen

Anschließend ist das Wurzelzertifikat blau hinterlegt:

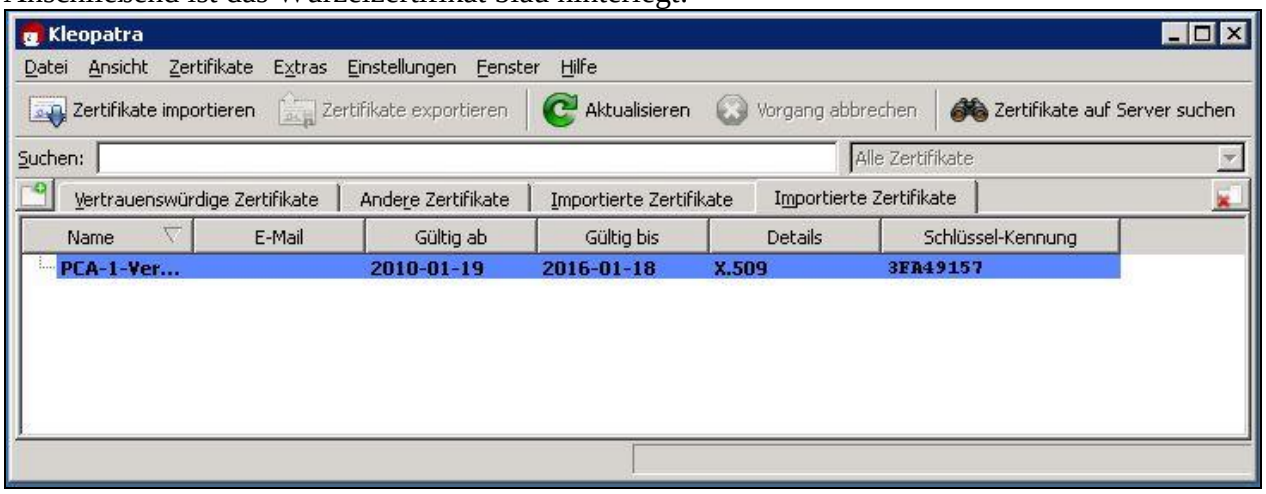

Abbildung 30: Darstellung vertrauenswürdiges Wurzelzertifikat

Nun wird auf dem gleichen Weg das Zwischenzertifikat DOI-CA-2 importiert:

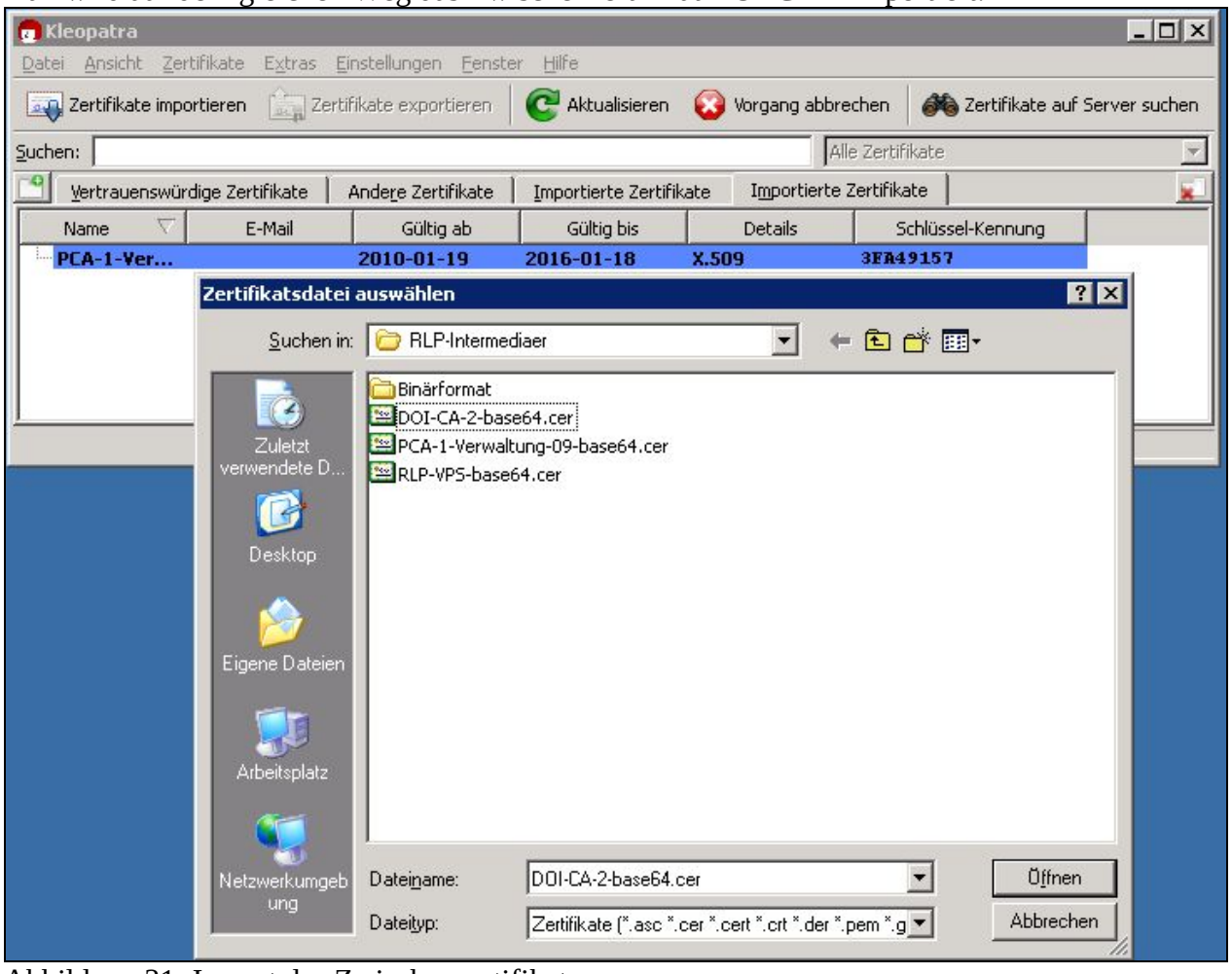

Abbildung 31: Import des Zwischenzertifikats

Der erfolgreiche Import des Zwischenzertifikats wird wie folgt bestätigt:

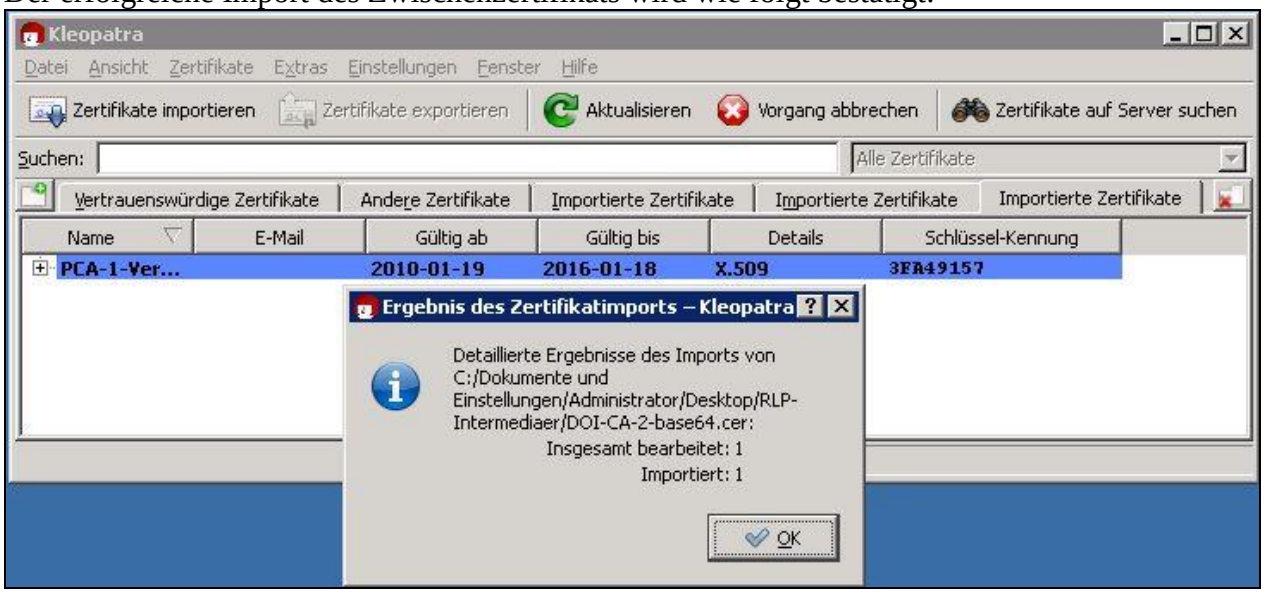

Abbildung 32: Ergebnis des Zwischenzertifikat-Imports

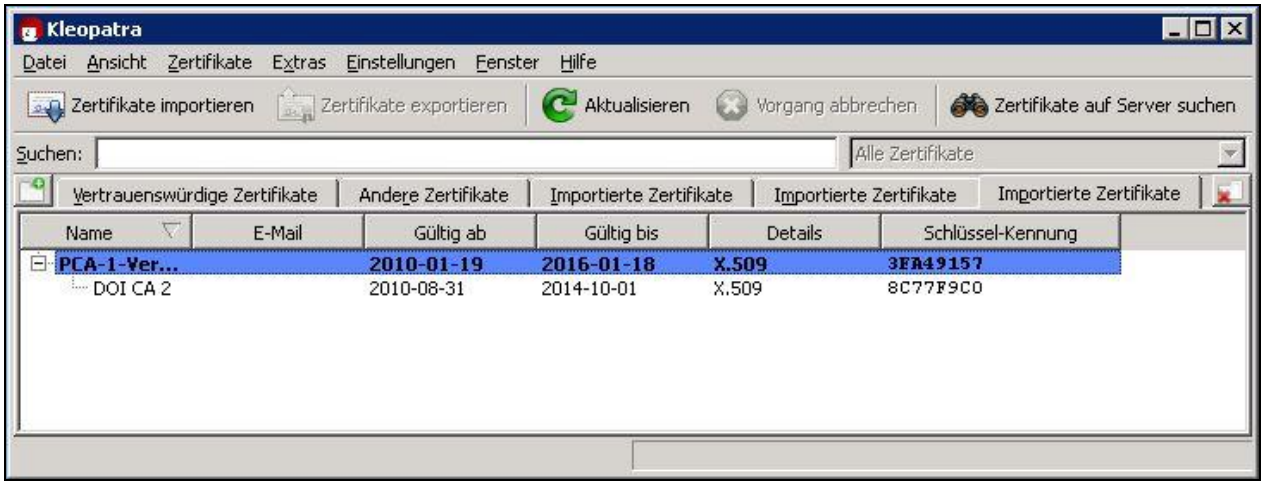

Abbildung 33: Ausgeklapptes Zwischenzertifikat

Jetzt wird das eigentliche Zertifikat, RLP-VPS, importiert:

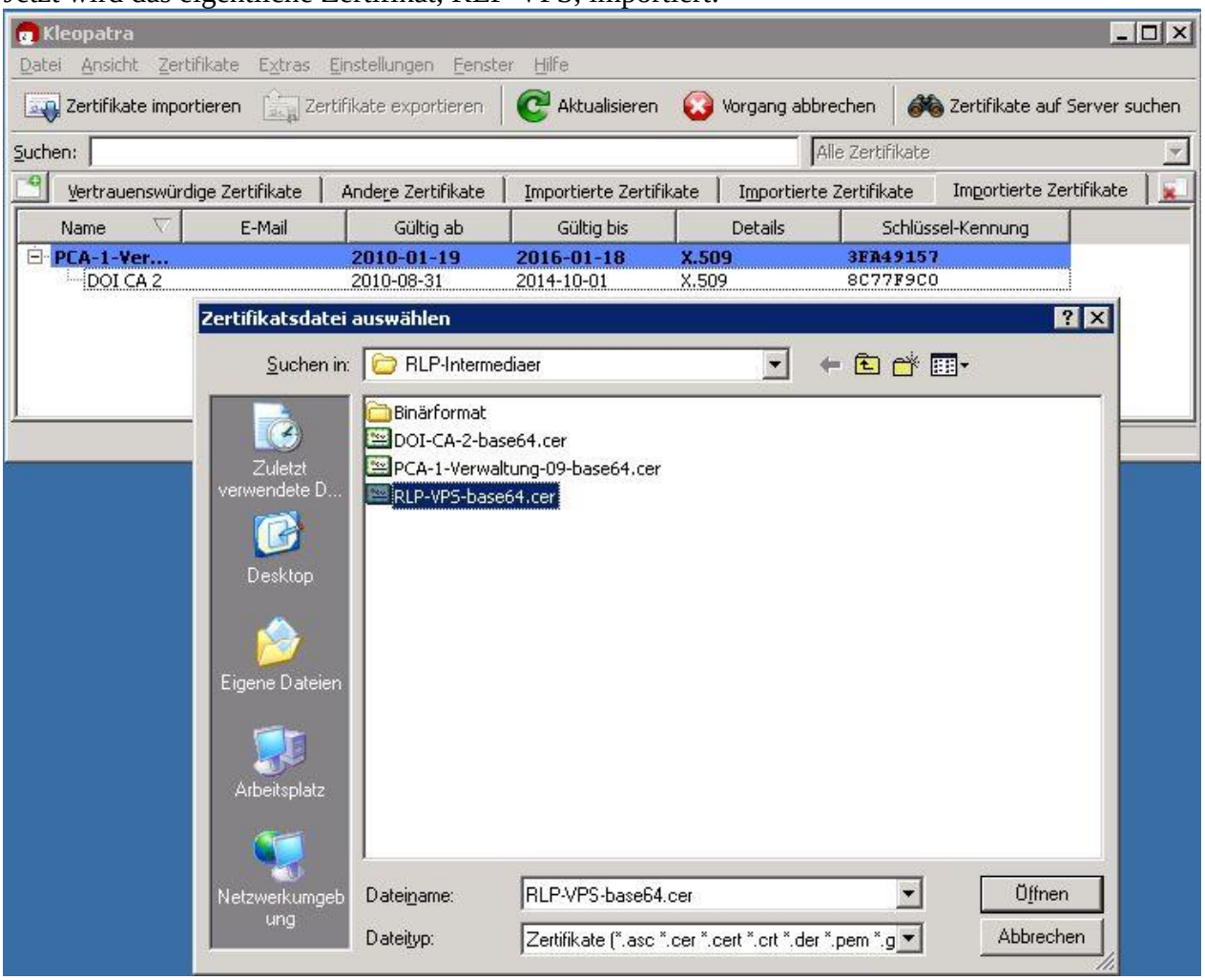

Abbildung 34: Import des Zertifikats RLP-VPS

Der erfolgreiche Import des Zertifikats wird wie folgt bestätigt:

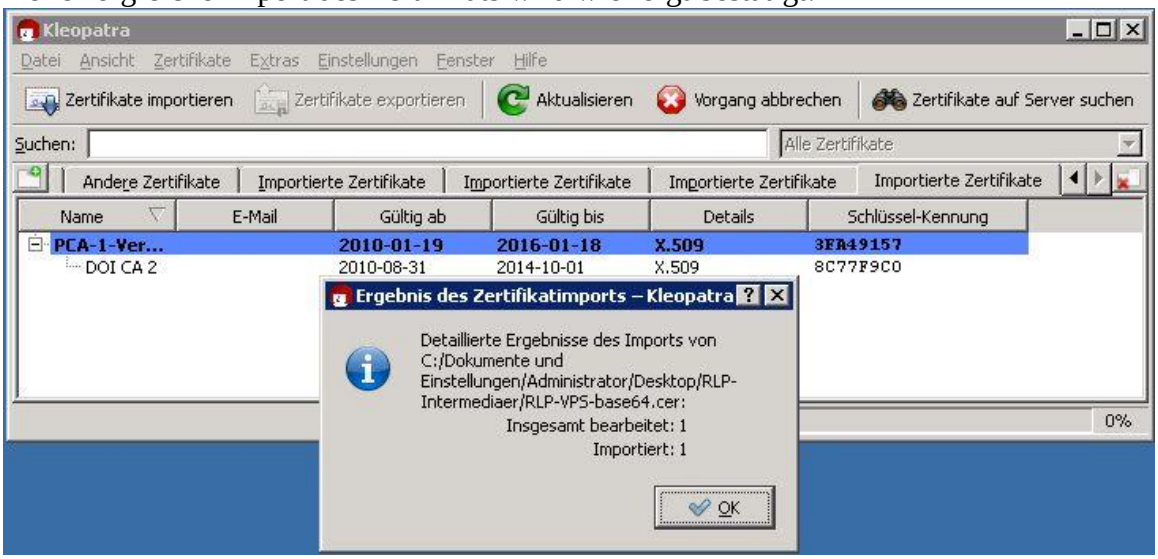

Abbildung 35: Importergebnis für das Zertifikats RLP-VPS

3.3. Verschlüsseln einer Datei

Es liegt eine zu verschlüsselnde Datei vor:

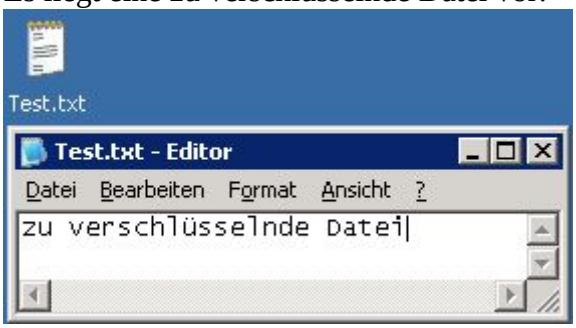

Abbildung 36: Zu verschlüsselnde (Text) Datei

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

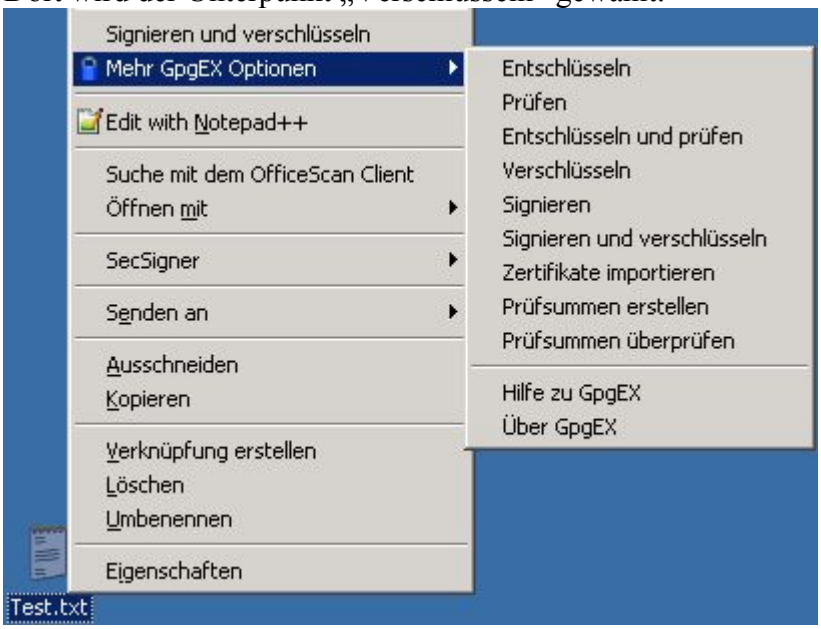

Abbildung 37: Mehr GpgEX Optionen

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

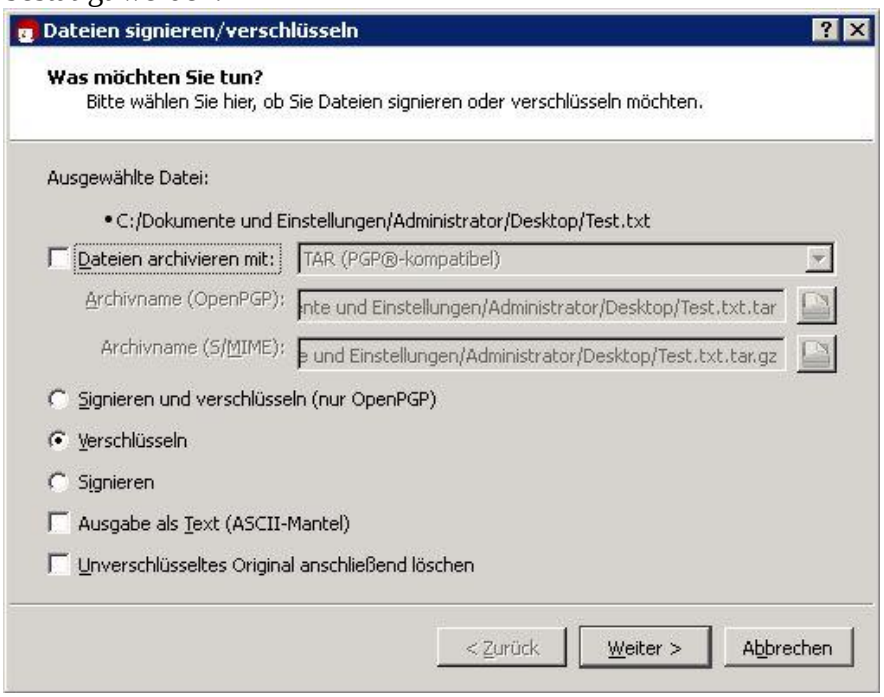

Abbildung 38: Auswahl „Verschlüsseln

Jetzt wird das Zertifikat hinzugefügt und „Verschlüsseln“ angeklickt:

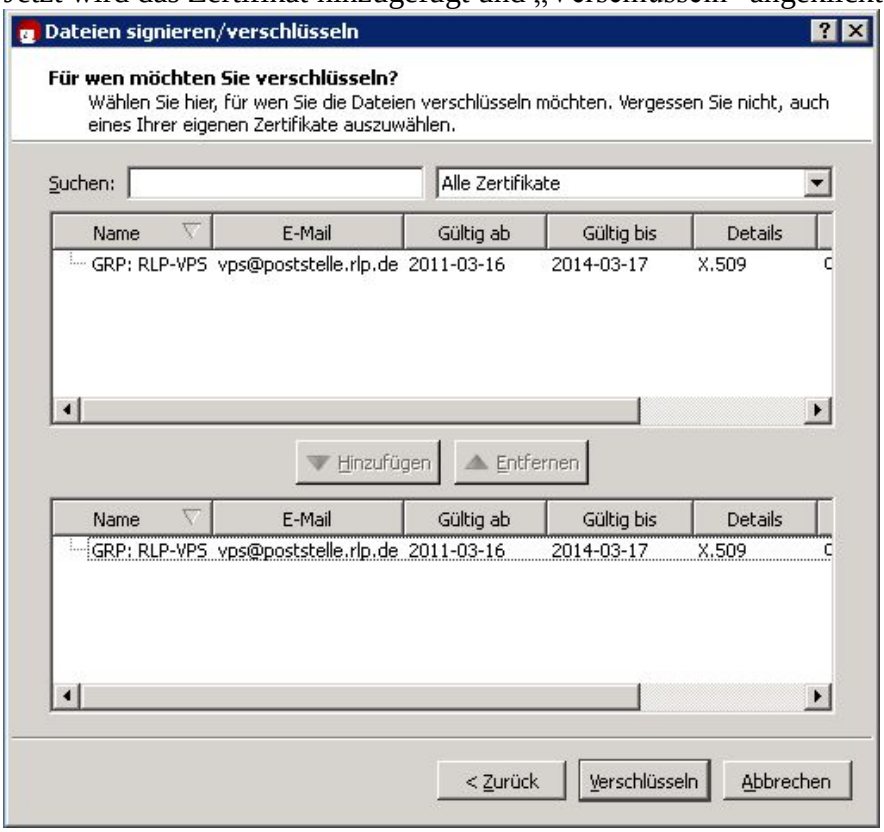

Abbildung 39: Zertifikat hinzufügen und Verschlüsseln

Dieser Hinweis kann mit „Fortsetzen“ ignoriert werden:

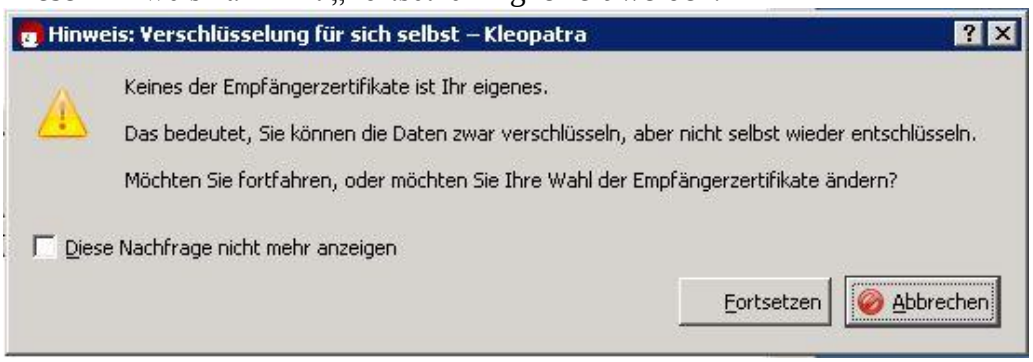

Abbildung 40: Hinweis

Bei Bedarf kann hier auch die Option „Diese Nachfrage nicht mehr anzeigen“ aktiviert werden.

Das Ergebnis wird im folgenden Bildschirm dargestellt:

Abbildung 41: Ergebnisdarstellung

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.

Abbildungsverzeichnis