JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Schwickert, Axel; Schick, Lukas

Windows – Verschlüsseln, Entschlüsseln und Signieren von E-Mails

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 6 / 2019
ISSN 1613-6667

Arbeitspapiere WI Nr. 6 / 2019

Autoren: Schwickert, Axel; Schick, Lukas

Titel: Windows – Verschlüsseln, Entschlüsseln und Signieren von E-Mails

Zitation: Schwickert, Axel; Schick, Lukas: Windows – Verschlüsseln, Entschlüsseln und Signieren von E-Mails, in: Arbeitspapiere WI, Nr. 6/2019, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2019, 27 Seiten, ISSN 1613-6667.

Kurzfassung: In den beiden Arbeitspapieren WI „Verschlüsseln, Entschlüsseln und Signieren von Dateien“ (Nr. 05/2017 für macOS und 05/2018 für Windows) wurde erläutert, was unter Verschlüsselung zu verstehen ist und wie diese grundsätzlich funktioniert. Dabei wurde zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden und aufgezeigt, wie man Schlüsselpaare mithilfe einer speziellen Crypto-Software für macOS (GPG-Suite) und Gpg4Win für Microsoft Windows erstellen und verwalten kann und was der Unterschied zwischen privaten und öffentlichen Schlüsseln ist. In den beiden vorgenannten Arbeitspapieren WI erfolgte anschließend eine anwendungsorientierte Anleitung, wie Dateien mithilfe asymmetrischer Verschlüsselungsverfahren und der passenden Software geschützt werden können. Wenn Ihnen diese Grundlagen nicht (mehr) geläufig sind, sollten Sie das für Ihr Betriebssystem (Windows oder macOS) relevante Arbeitspapier WI „Verschlüsseln, Entschlüsseln und Signieren von Dateien“ durcharbeiten, bevor Sie mit dem vorliegenden Arbeitspapier WI Nr. 06/2019 fortfahren. Im vorliegenden Arbeitspapier 06/2019 wird gezeigt, wie auf Rechnern mit dem Betriebssystem Windows E-Mails verschlüsselt, entschlüsselt und signiert werden. Dazu wird die Crypto-Software „Kleopatra“ aus der Suite „GPG4win“ verwendet.

Schlüsselwörter: Verschlüsselung, Signatur, Schlüssel, Schlüsselpaar, öffentlich, privat, symmetrisch, asymmetrisch, Microsoft Windows, GPG4win, Kleopatra, E-Mail, Electronic Mail, Keychain, Widerrruf

Inhaltsverzeichnis

A Verschlüsselung von E-Mails – Warum und wie geht das?

In den beiden Arbeitspapieren WI „Verschlüsseln, Entschlüsseln und Signieren von Dateien“ (Nr. 05/2017 für macOS und 05/2018 für Windows) wurde Ihnen erläutert, was unter Verschlüsselung zu verstehen ist und wie diese grundsätzlich funktioniert. Dabei wurde zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden und aufgezeigt, wie man Schlüsselpaare mithilfe einer speziellen Crypto-Software für macOS (GPG-Suite) und Gpg4Win für Microsoft Windows erstellen und verwalten kann und was der Unterschied zwischen privaten und öffentlichen Schlüsseln ist. In den beiden o. g. Arbeitspapieren WI erfolgte anschließend eine anwendungsorientierte Anleitung, wie Dateien mithilfe asymmetrischer Verschlüsselungsverfahren und der passenden Software geschützt werden können. Wenn Ihnen diese Grundlagen nicht bekannt oder nicht mehr verständlich sind, sollten Sie das für Ihr Betriebssystem (Windows oder macOS) relevante Arbeitspapier WI „Verschlüsseln, Entschlüsseln und Signieren von Dateien“ durcharbeiten, bevor Sie mit dem vorliegenden Arbeitspapier WI Nr. 01/2019 fortfahren. Im vorliegenden Arbeitspapier 01/2019 wird gezeigt, wie auf Rechnern mit dem Betriebssystem Windows E-Mails verschlüsselt, entschlüsselt und signiert werden.

Wenn Sie sich mit dem Thema „E-Mail-Verschlüsselung“ auseinandersetzen, haben Sie sich bestimmt schon die Frage gestellt, warum man E-Mails überhaupt verschlüsseln sollte. Ein einfacher Vergleich kann Ihnen darauf eine Antwort liefern: Unverschlüsselte E-Mails sind wie Postkarten auf dem Postweg. Sie stecken nicht in einem Umschlag und können so von jedem auf dem Postweg und an den Endpunkten (Sender, Empfänger und auch der „Postbote“) gelesen werden. Eine verschlüsselte und signierte E-Mail hingegen kann mit einem Brief in einem Briefumschlag inklusive Siegel verglichen werden. Der Inhalt des Briefes kann jeweils nur vom Sender und Empfänger (solange der Briefumschlag unversehrt bleibt) gelesen werden. Das Siegel stellt außerdem sicher, dass der Brief nicht geöffnet oder verändert wurde. Im Falle der Postkarten sind wir uns bewusst, dass sie jeder lesen kann und beschriften diese zumeist ohne sensible Daten. E-Mails enthalten jedoch sehr häufig sensible Daten, wie z. B. Bankdaten, Adressen, Passwörter, vertrauliche Dokumente oder Personendaten. Wir kommunizieren heute auch mit Ärzten, Anwälten, Behörden, Versicherungen, Freunden, Familienmitgliedern u. v. m. und wollen eigentlich nicht, dass Unbefugte unsere Nachrichten lesen. Wenn wir unsere Nachrichten aber unverschlüsselt verschicken, geschieht dies zumeist im Klartext und die Nachrichten können von vielen Personen eingesehen werden. Dazu zählen Ihr E-Mail-Provider, der E-Mail-Provider Ihres Kommunikationspartners und alle Personen, die Ihre E-Mail auf dem Transportweg abfangen, mitlesen oder Zugriff auf Ihr E-Mail-Postfach erhalten. Es gibt also einen guten Grund, warum Sie Ihre E-Mails verschlüsseln sollten: Nur die von Ihnen gewünschten Empfänger sollen Ihre E-Mails lesen können.

Um E-Mails zumindest auf dem Transportweg zu schützen, versuchen die meisten E-Mail-Provider, die Verbindungen zwischen dem Mail-Server des Senders und dem Mail-Server des Empfängers zu schützen. Sie als Absender einer Nachricht verfassen dabei Ihre Nachricht im Klartext und übergeben sie an Ihren Mail-Server, der die Nachricht an den von Ihnen gewünschten Empfänger schicken soll. Ihr Mail-Server wandelt Ihren Klartext in verschlüsselten Text um und verschickt diesen an den Mail-Server des Empfängers. Dieser Mail-Server wandelt den verschlüsselten Text in lesbaren Klartext für den Empfänger um. Diese Absicherung Ihrer Mail auf dem Transportweg kann jedoch nur funktionieren, wenn Ihr eigener Mail-Server und alle anderen Mail-Server der Empfänger Ihrer Nachrichten korrekt konfiguriert sind und dass jeder Mail-Server die Verschlüsselungsverfahren jedes anderen beteiligten Mail-Servers fehlerfrei versteht. Die korrekte Mail-Server-Konfiguration und die „Verschlüsselungs-Kompatibilität" der vielen verschiedenen Mail-Server von vielen verschiedenen E-Mail-Providern sind jedoch nicht gewährleistet.

Sie dürfen also nicht davon ausgehen, dass Ihr eigener Mail-Server und die Mail-Server Ihrer Nachrichtenempfänger den Transport Ihrer Nachrichten sicher und geschützt bewerkstelligen. Damit nur Sie selbst und die von Ihnen gewünschten Empfänger Ihre Nachrichten lesen können, müssen Sie Ihre Nachrichten zunächst in Eigenregie auf Ihrem Rechner verschlüsseln. Sie geben dann Ihre verschlüsselte Nachricht an Ihren Mail-Server (E-Mail-Provider), der Ihre verschlüsselte Nachricht zum Mail-Server Ihres Nachrichtenempfängers transportiert. Der Empfänger holt sich die verschlüsselte Nachricht bei seinem Mail-Provider ab. Die Nachricht wird dann erst auf dem Rechner des Empfängers entschlüsselt und gelesen. Sie haben damit Ihre Nachricht als Sender an Ihrem eigenen „Ende" verschlüsselt und die Entschlüsselung erfolgt erst am anderen „Ende" beim Empfänger. Diese „Ende-zu-Ende"-Verschlüsselung stellt sicher, dass Ihre Nachricht an jeder Stelle des gesamten Transportwegs geschützt ist.

Der umfassende Schutz von E-Mails geht noch ein Stück weiter und lässt sich mit den Begriffen Authentizität, Vertraulichkeit und Integrität beschreiben.

- Authentizität: Die beiden Kommunikationspartner sind echt und deren Identität kann nachgeprüft werden. Für unsere E-Mails bedeutet dies, dass wir tatsächlich genau mit dem Partner kommunizieren, mit dem wir auch kommunizieren wollen.
- Vertraulichkeit: Die Information ist vor unbefugter Preisgabe geschützt. Für unsere E-Mails bedeutet dies, dass sie nur vom Sender und Empfänger gelesen werden können.
- Integrität: Die Information ist vor unbefugter Veränderung geschützt. Sender und Empfänger müssen sicher sein, dass E-Mails nicht von einem unbefugten Dritten verändert werden können (ohne dass Sender und/oder Empfänger dies bemerken).

Damit man vertrauliche E-Mails „Ende-zu-Ende“ verschlüsselt senden und empfangen kann, wird die asymmetrische Verschlüsselung genutzt (wie Sie es bei der Verschlüsselung von Dateien kennengelernt haben). Das bedeutet, das Sender und Empfänger von E-Mails je ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, besitzen müssen. Der Sender nutzt den öffentlichen Schlüssel des Empfängers, um die E-Mail zu verschlüsseln, bevor die E-Mail seinen Rechner verlässt. Ist die verschlüsselte E-Mail beim Empfänger angekommen, kann nur er diese mit seinem privaten Schlüssel entschlüsseln. Jeder Teilnehmer einer sicheren E-Mail-Kommunikation stellt also seinen öffentlichen Schlüssel zum Verschlüsseln von E-Mails bereit und hält seinen privaten Schlüssel geheim, um damit eingehende verschlüsselte E-Mails zu entschlüsseln.

Der private Schlüssel des Senders einer Nachricht wird zum Signieren einer zu verschickenden E-Mail eingesetzt. Mit der Signatur wird die Integrität einer Nachricht sichergestellt. Der öffentliche Schlüssel des Empfängers wird hingegen zur Verschlüsselung der zu verschickenden E-Mail genutzt. Mit der Verschlüsselung wird die Vertraulichkeit einer Nachricht sichergestellt. Der Sender verschlüsselt also seine Klartext-Nachricht mit dem öffentlichen Schlüssel des Empfängers. Der Sender erstellt zusätzlich mit seinem eigenen privaten Schlüssel aus seiner Klartext-Nachricht eine Signatur-Datei. Dies geschieht, indem zuerst eine Hashfunktion auf die Klartext-Nachricht angewandt wird, um einen eindeutigen „Message Digest“ (Fingerabdruck) zu generieren. Aus diesem „Message Digest“ wird anschließend mithilfe des privaten Schlüssels des Senders eine Signatur-Datei erzeugt. Die verschlüsselte Nachricht und die Signatur-Datei werden an den Empfänger geschickt. Der Empfänger entschlüsselt die Nachricht mit seinem privaten Schlüssel und erhält den Klartext der Nachricht. Der Empfänger wendet nun den öffentlichen Schlüssel des Senders auf die Signatur-Datei an und kann damit feststellen, ob der daraus entstehende „Message Digest“ aus der ursprünglichen Klartext-Nachricht erzeugt wurde.

Mit dem geschilderten Verfahren der asymmetrischen Verschlüsselung über ein Schlüsselpaar wird die Vertraulichkeit und Integrität einer Nachricht gewährleistet. Die Authentizität (die Echtheit der beiden Kommunikationspartner) ist dann sichergestellt, wenn Sender und Empfänger jeweils nachprüfbar die wahren Eigentümer ihrer Schlüsselpaare sind. Im „richtigen Leben“ in Deutschland wird die Authentizität der Bürger vom Staat gewährleistet, indem der Bürger einen Personalausweis vom Staat erhält. Der Bürger muss dafür eine staatliche Behörde persönlich aufsuchen. Die Behörde stellt den Personalausweis erst dann aus, wenn ein Behördenmitarbeiter die „Echtheit“ des Bürgers und seiner persönlichen Daten festgestellt hat. Der ausgestellte Personalausweis gehört nachprüfbar genau dem einen Bürger. Analog dazu: Wem ein Schlüsselpaar für eine asymmetrische Verschlüsselung wirklich gehört, lässt sich nur dann feststellen, wenn eine vom Sender und vom Empfänger anerkannte Autorität die Schlüsselpaare nach Prüfung der Kommunikationspartner auf Echtheit ausgegeben hat. Jeder Kommunikati-

onspartner kann dann bei der anerkannten Autorität nachfragen, wem genau ein bestimmter öffentlicher Schlüssel gehört. Die betreffenden Autoritäten für Schlüsselpaare zur asymmetrischen Verschlüsselung werden Zertifizierungsstellen, engl. Certification Authorities (CA) genannt. Eine Zertifizierungsstelle kann in Deutschland ein vom Staat zugelassenes spezielles Unternehmen sein. In Deutschland können auch öffentliche Organisationen oder Regierungsstellen als Zertifizierungsstellen dienen, zum Beispiel die Bundesnetzagentur. Die Zertifizierungsstellen geben an Unternehmen oder Personen digitale Zertifikate aus. Ein digitales Zertifikat ordnet ein bestimmtes Schlüsselpaar einer bestimmten Person oder Organisation zu. Diese Zuordnung muss von der ausgebenden staatlich zugelassenen Zertifizierungsstelle nachprüfbar garantiert werden. Es gibt allerdings viele verschiedene Zertifizierungsstellen (CA), die nicht in Deutschland ansässig und vom deutschen Staat auch nicht als CA zugelassen sind.

Die Authentizität von Sender und Empfänger einer E-Mail ist also nur dann wirklich gewährleistet, wenn Sender und Empfänger gegenseitig die jeweiligen Zertifizierungsstellen ihrer Schlüsselpaare als vertrauenswürdig anerkennen und die Zertifizierungsstellen auch die Nachprüfbarkeit der Kommunikationspartner auf deren Echtheit verlässlich ermöglichen. Erst wenn die Authentizität der Kommunikationspartner gegeben ist, ergeben also die Vertraulichkeit und Integrität einer Nachricht letztlich erst Sinn.

E-Mails lassen sich mit verschiedenen Software-Lösungen verschlüsseln, entschlüsseln und signieren. Zum einen kann dies im Web-Browser mithilfe von Browser-Erweiterungen (z. B. Mailvelope) ablaufen, zum anderen mithilfe von lokal installierten E-Mail-Clients. Im vorliegenden Arbeitspapier wird vorgestellt, wie die Verschlüssellungsprozesse und die Schlüsselverwaltung in lokaler E-Mail-Software (E-Mail-Clients) vonstatten geht, die als eigenständige Applikation auf Ihrem Rechner installiert wird. Auf Apple-Rechnern mit dem Betriebssystem macOS ist z. B. die E-Mail-Software „Apple Mail“ vorinstalliert. Auf Windows-Rechnern nutzen viele Anwender die E-Mail-Clients „Outlook“ oder „Thunderbird“ (diese beiden E-Mail-Clients gibt es auch in Versionen für Apple-Rechner mit dem Betriebssystem macOS).

Nicht jeder E-Mail-Client bringt jedoch alle notwendigen Software-Bestandteile zum sicheren E-Mail-Verkehr mit. Wenn Sie z. B. die E-Mail-Client-Software Outlook auf Windows verwenden, müssen Sie das Plugin „GpgOL“ der Verschlüsselungs-Software „Gpg4win“ nutzten. Gpg4win übernimmt die Schlüsselverwaltung und liefert die Schlüssel bei Bedarf an das Plugin GpgOL. GpgOL selbst ist für das Verschlüsseln, Entschlüsselung und Signieren von E-Mails im E-Mail-Client „Outlook“ zuständig. Nutzen Sie hingegen Thunderbird unter Windows, benötigen Sie zusätzlich ein Plugin mit dem Namen „Enigmail“. Das Setup Ihrer Verschlüsselungslösung ist also von Ihrem eingesetzten E-Mail-Client abhängig.

B Was brauchen Sie?

In diesem Dokument wird Ihnen erklärt, wie Sie auf einem Personal Computer mit dem Betriebssystem Windows E-Mails verschlüsseln, entschlüsseln und signieren können. Sie brauchen dafür folgendes Equipment:

Das Wissen aus dem Arbeitspapier: Schwickert, Axel; Schick, Lukas: Windows – Verschlüsseln, Entschlüsseln und Signieren von Dateien, in: Arbeitspapiere WI, Nr. 5/2018, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2018.

Rechner: Sie brauchen einen persönlichen Rechner mit der neuesten Version des Betriebssystems Windows. Ihr Rechner braucht eine Internet-Anbindung.

Web-Browser: Auf Ihrem Rechner muss ein Web-Browser in neuester Version installiert sein wie z. B. Chrome oder Firefox.

E-Mail-Client-Software: Outlook

Crypto-Software: Auf Ihrem Rechner muss eine Software installiert sein, mit welcher Sie Ihre Schlüssel erstellen, beziehen und verwalten können. Wir verwenden als Crypto-Software „Kleopatra“, enthalten in der Suite „Gpg4win“ von den Herstellern Intevation GmbH und g10 Code GmbH.

PGP Plugin für die E-Mail-Client-Software: GpgOL (in der „Gpg4win“-Suite enthalten)

C Installation des PGP Plugins

Laden Sie zunächst auf https://www.gpg4win.de die neueste Version von Gpg4win herunter. Starten Sie die Installation, indem Sie die heruntergeladene .exe-Datei doppelklicken. Folgen Sie den Installationsanweisungen. Nach erfolgter Installation können Sie die .exe-Installationsdatei in den Papierkorb legen.

Durch diese Installation wurde auf Ihrem Rechner das Programm „Kleopatra“ installiert. Den Startbildschirm davon sehen Sie in Abbildung 1.

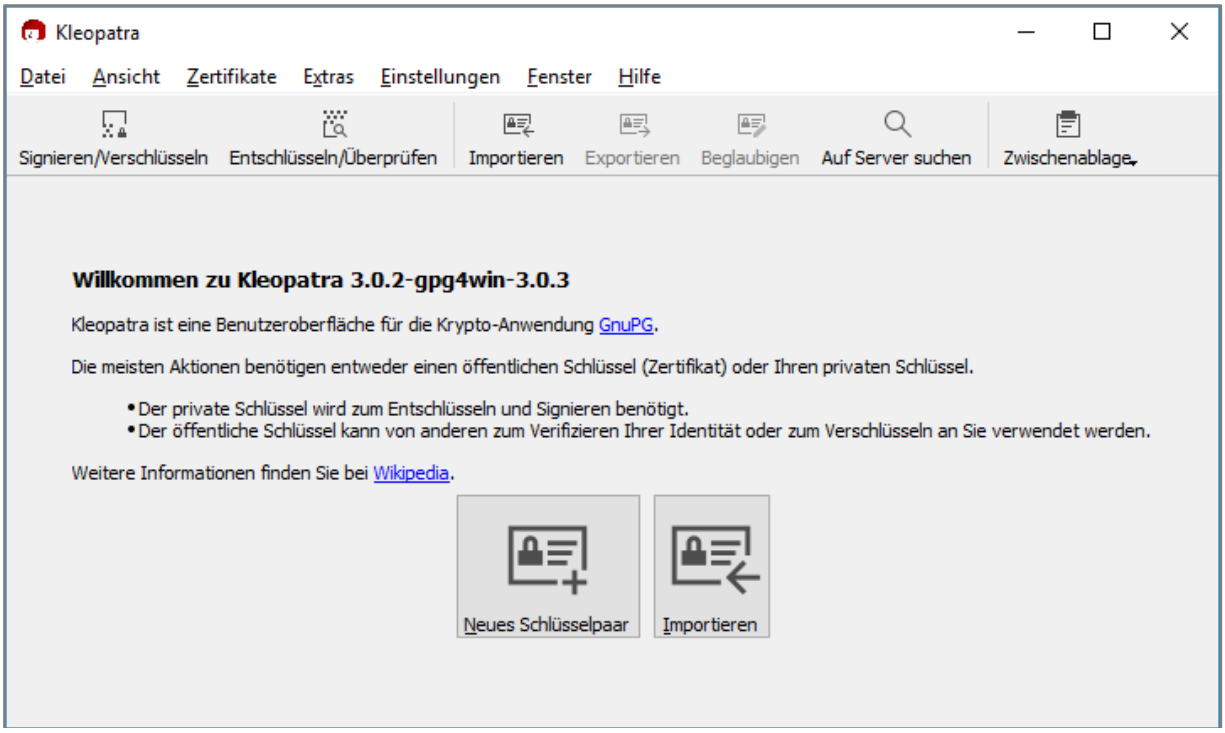

Abb. 1: Der Start-Bildschirm von Kleopatra

Gpg4win enthält neben dem Programm Kleopatra noch weitere Programme, die bei der Installation automatisch mitinstalliert werden: GnuPG ist das Kernstück der Software Gpg4win und führt die mathematischen Verschlüsselungsoperationen durch. GnuPG ist weiterhin eine Anwendung für die Kommandozeile und richtet sich an fortgeschrittene Nutzer von Gpg4win oder an Nutzer die keine grafische Benutzeroberfläche benötigen. GpgOL ist eine Funktionserweiterung für Microsoft Outlook und ermöglicht es Ihnen, Ihre E-Mails bei Bedarf mit wenigen Klicks zu verschlüsseln. GpgEX ist ein Plugin, welches Gpg4win-Funktionalitäten in andere Anwendungen integriert. Zum Beispiel stellt GpgEX sicher, dass Sie notwendige neue Funktionen zur Verfügung gestellt bekommen, wenn Sie in Ihrem Windows Explorer per Rechtsklick auf eine Datei klicken.

Überprüfen Sie nun zunächst in den Einstellungen Ihres Outlook-Mail-Programms, ob das Plugin GpgOL der Gpg4win-Suite voll funktionstüchtig installiert wurde. Klicken Sie dazu während Outlook geöffnet ist in der oberen Menüleiste von Outlook auf „Datei“ und anschließend auf „Optionen“.

Wechseln Sie im sich öffnenden Fenster „Outlook-Optionen“ in den Reiter „Add-Ins“. Die Liste unterhalb von „Add-Ins“ zeigt ihnen die installieren Add-Ins in Outlook an und sortiert diese nach ihrem Status. Wenn das Add-In „GpgOL – The GnuPG Outlook Plugin“ in der Liste der „Aktiven Anwendungs-Add-Ins“ aufgeführt ist, wurde es erfolgreich installiert und in Outlook aktiviert.

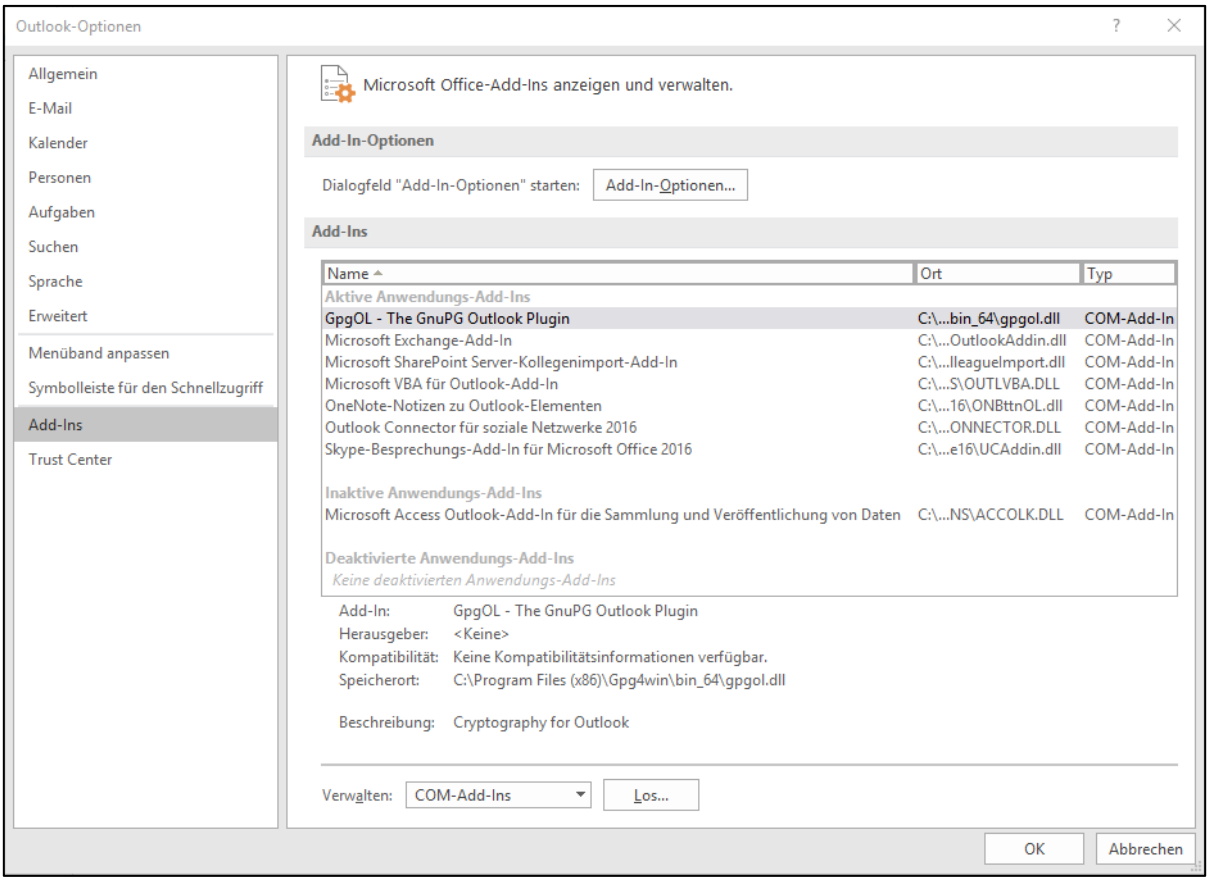

Abb. 2: Outlook – Installation des Plugins GpgOL überprüfen

D Ein Schlüsselpaar erstellen

Über die Funktion „Datei“ und „Neues Schlüsselpaar“ in der Menüleiste oder über den Button „Neues Schlüsselpaar“ im Start-Bildschirm von Kleopatra erstellen Sie für sich ein neues Schlüsselpaar (siehe Abbildung 3).

Geben Sie Ihren Namen und Ihre Uni-E-Mail-Adresse ein. Wenn Sie auf „Erweiterte Einstellungen ...“ klicken, sehen Sie, dass standardmäßig ein RSA-Schlüsselpaar mit 2048 Bit Länge erstellt wird, welches kein Verfallsdatum hat. Setzten Sie daher einen Haken bei „Gültig bis:“ und wählen Sie ein Datum aus, an dem Ihr Schlüssel verfallen soll (i. d. R. 2-3 Jahre; siehe Abbildung 4).

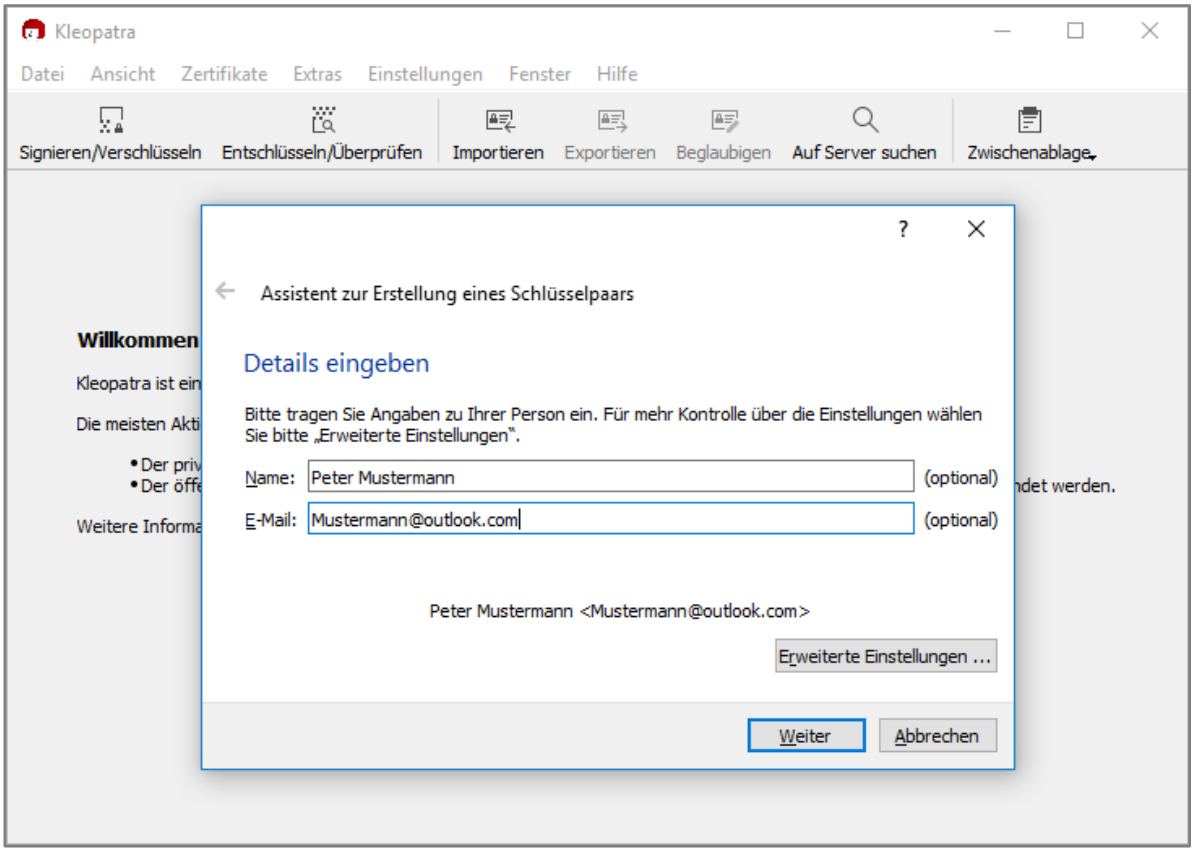

Abb. 3: Ein neues Schlüsselpaar erstellen

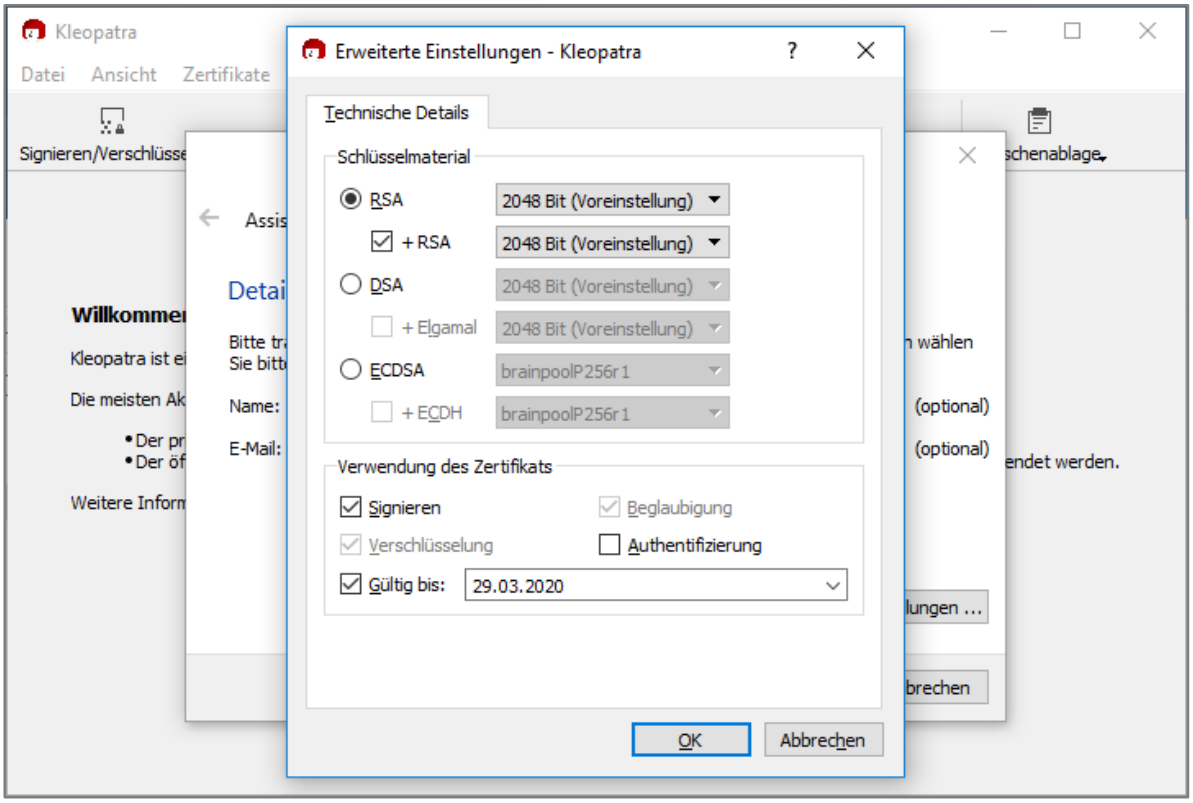

Abb. 4: Ein neues Schlüsselpaar erstellen – Erweiterte Einstellungen

Bestätigen Sie Ihre Anpassungen mit „OK“ und klicken Sie auf „Weiter“. Mit Klick auf den Button „Erstellen“ beginnt das Programm, Ihr Schlüsselpaar zu errechnen und zeigt anschließend den Bildschirm aus Abbildung 5. Kleopatra benötigt eine Passphrase (Passwort), um Ihr Schlüsselpaar geschützt auf Ihrer Festplatte speichern zu können. Wählen Sie ein starkes Passwort und notieren Sie es an geeigneter Stelle. Sollten Sie es verlieren, haben Sie keinen Zugriff mehr auf Ihr Schlüsselpaar.

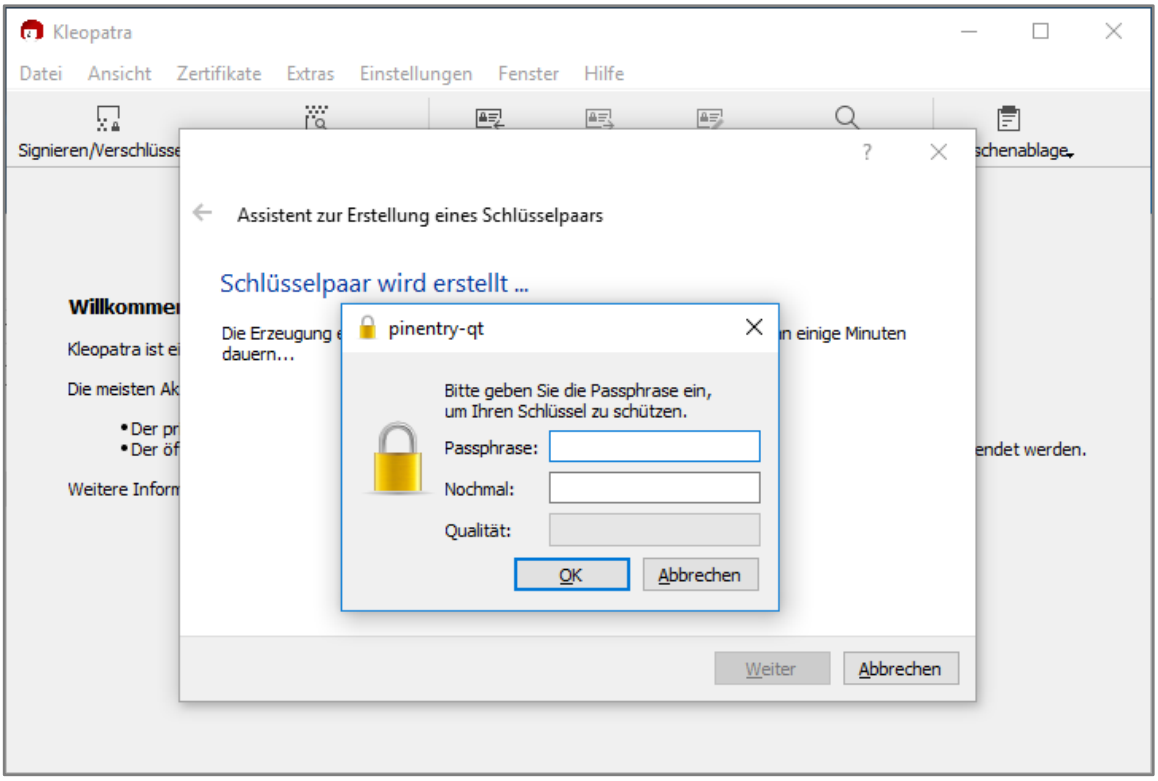

Abb. 5: Ein neues Schlüsselpaar erstellen – Passphrase festlegen

Nach Klick auf „OK“ und „Weiter“ wird Ihr Schlüsselpaar erstellt. Das Programm Kleopatra hat nun je eine Datei für einen öffentlichen und einen privaten Schlüssel erzeugt und diese beiden Dateien auf Ihrem Rechner mit Ihrem gewählten Passwort verschlüsselt abgespeichert.

Mithilfe des Buttons „Sicherheitskopie Ihres Schlüsselpaares erstellen...“ können Sie Ihr Schlüsselpaar an einem weiteren Ort ablegen. Kleopatra bietet Ihnen weiterhin an, Ihren öffentlichen Schlüssel auf einen Öffentlichen-Schlüssel-Server hochzuladen (siehe Kapitel A; eine Schlüssel-Liste, die im Internet jeder offen einsehen kann). Nutzen Sie dieses Angebot zunächst nicht und klicken Sie auf den Button „Abschließen“ (siehe Abbildung 6). Sie können jederzeit später aus dem Programm Kleopatra heraus Ihre öffentlichen Schlüssel auf Schlüssel-Server hochladen.

Abbildung 7 zeigt die Liste der Schlüssel, die Kleopatra für Sie auf Ihrem Rechner vorhält und verwaltet. Sie sehen zunächst nur das gerade von Ihnen erzeugte Schlüsselpaar.

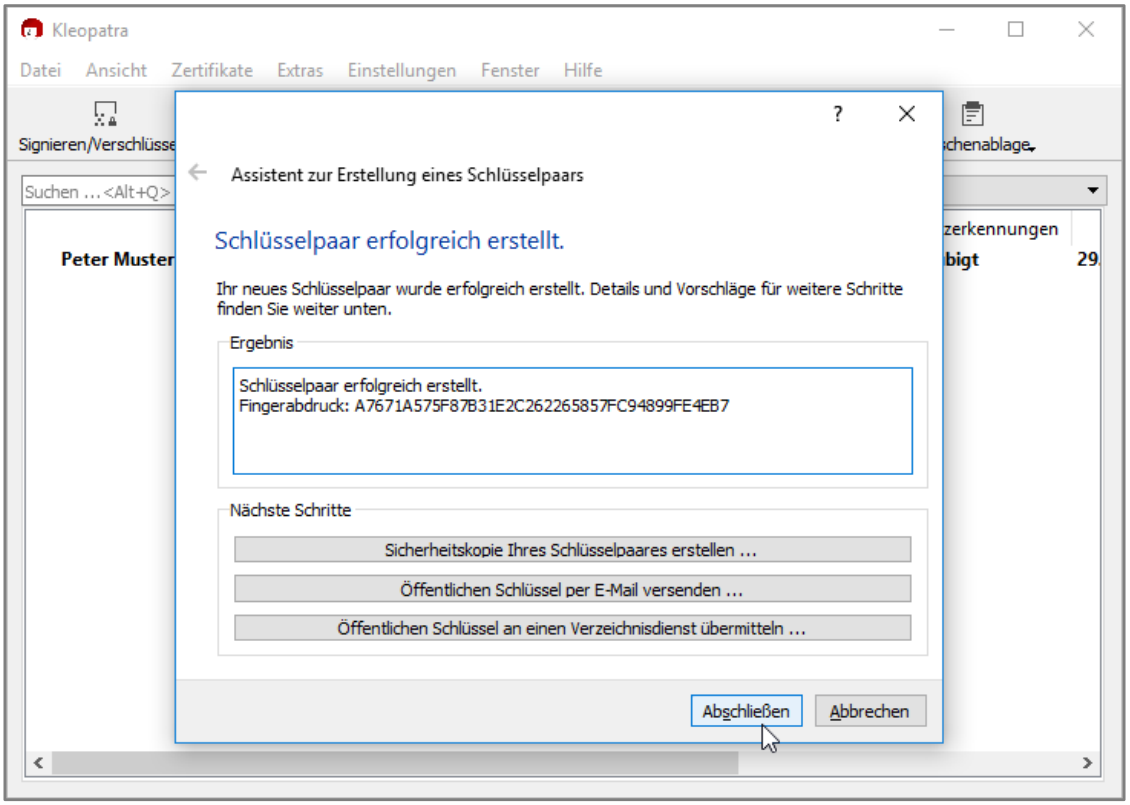

Abb. 6: Ihr Schlüsselpaar wurde erfolgreich erstellt.

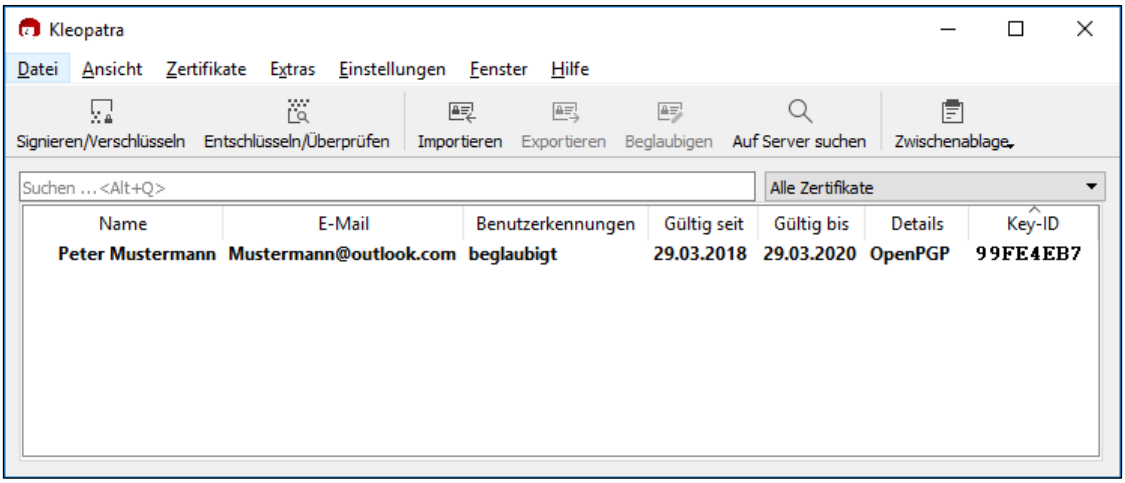

Abb. 7: Ihre Schlüssel in Kleopatra

Das Programm Kleopatra fungiert als Behälter und Verwalter aller Ihrer Schlüssel-/paare auf Ihrem Rechner. Die Software Gpg4win übernimmt auf Ihrem Rechner weitere Funktionen: Bei der Installation von Gpg4win wurde bereits erwähnt (siehe oben Kapitel C), dass in Outlook automatisch eine Funktionserweiterung für die Verschlüsselung von E-Mails installiert wird. Auch in Ihrem Windows Explorer wird eine Funktionserweiterung installiert, die es Ihnen erlaubt, einzelne Dateien oder ganze Verzeichnisse zu verschlüsseln. Im folgenden Kapitel E. erfahren Sie, wie Sie mithilfe von GpgOL E-Mails verschlüsseln und signieren können.

E Verschlüsseln und Signieren einer E-Mail

Eine Verschlüsselung von E-Mails stellt sicher, dass niemand außer dem gewünschten Adressaten, die Inhalte der E-Mail lesen kann (Vertraulichkeit). Um eine E-Mail zu verschlüsseln, benötigen Sie, wie in Kapitel D beschrieben, einen öffentlichen Schlüssel. Sie können also für jeden Empfänger Dateien, E-Mails oder Texte verschlüsseln, soweit Sie dessen öffentlichen Schlüssel besitzen. Damit weiterhin sichergestellt werden kann, dass eine bestimmte E-Mail von Ihnen und niemand anderem stammt (Authentizität) und nicht manipuliert wurde (Integrität), sollten Sie E-Mails signieren. Signaturen für E-Mails werden mit privaten Schlüsseln erstellt. In diesem Kapitel verschlüsseln Sie eine E-Mail mit dem öffentlichen Schlüssel Ihres Kommunikationspartners und signieren die E-Mail mit Ihrem privaten Schlüssel.

Öffnen Sie zunächst in Windows das Programm „Kleopatra“, um zu überprüfen, ob Sie über den öffentlichen Schlüssel Ihres Kommunikationspartners verfügen (siehe Abbildung 8). Zusätzlich sollten Sie Ihr eigenes Schlüsselpaar sehen. In unserem Fall hat Robin Schmidt in Kleopatra ein eigenes Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, und den öffentlichen von Anna Fröhlich. Mit diesen Schlüsseln ist Robin in der Lage, eine verschlüsselte E-Mail an Anna zu schreiben und diese zu signieren. Des Weiteren kann er sämtliche E-Mails entschlüsseln, welche mit seinem öffentlichen Schlüssel verschlüsselt wurden.

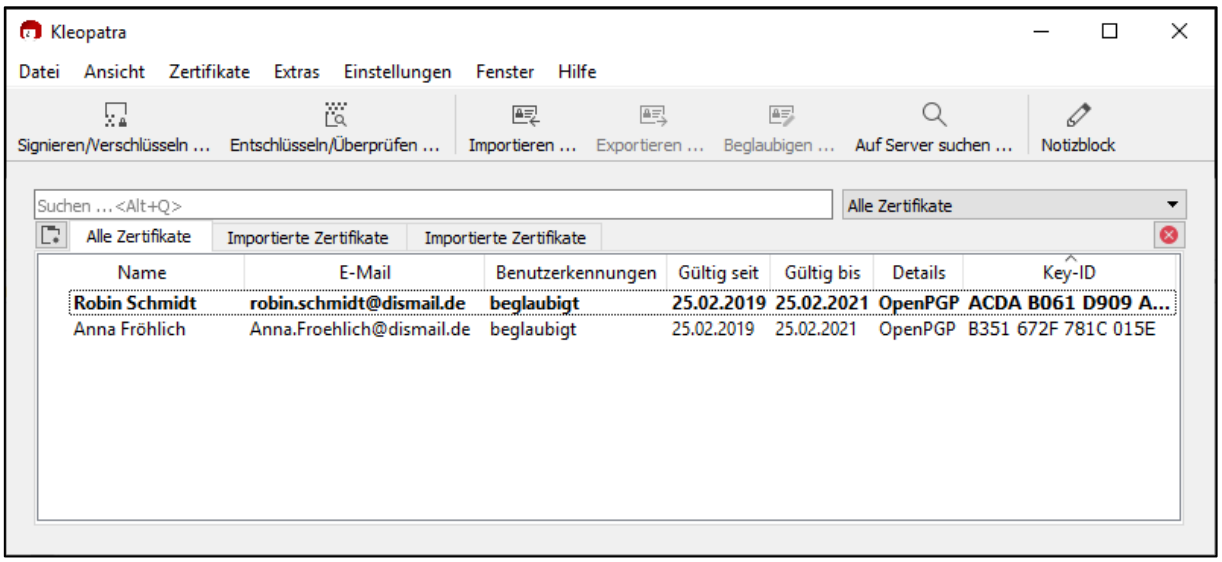

Abb. 8: GPG Keychain – Vorhandene kryptographische Schlüsselpaare

Öffnen Sie nun Outlook und klicken Sie auf den entsprechenden Button, um eine neue E-Mail zu verfassen (siehe Abbildung 9).

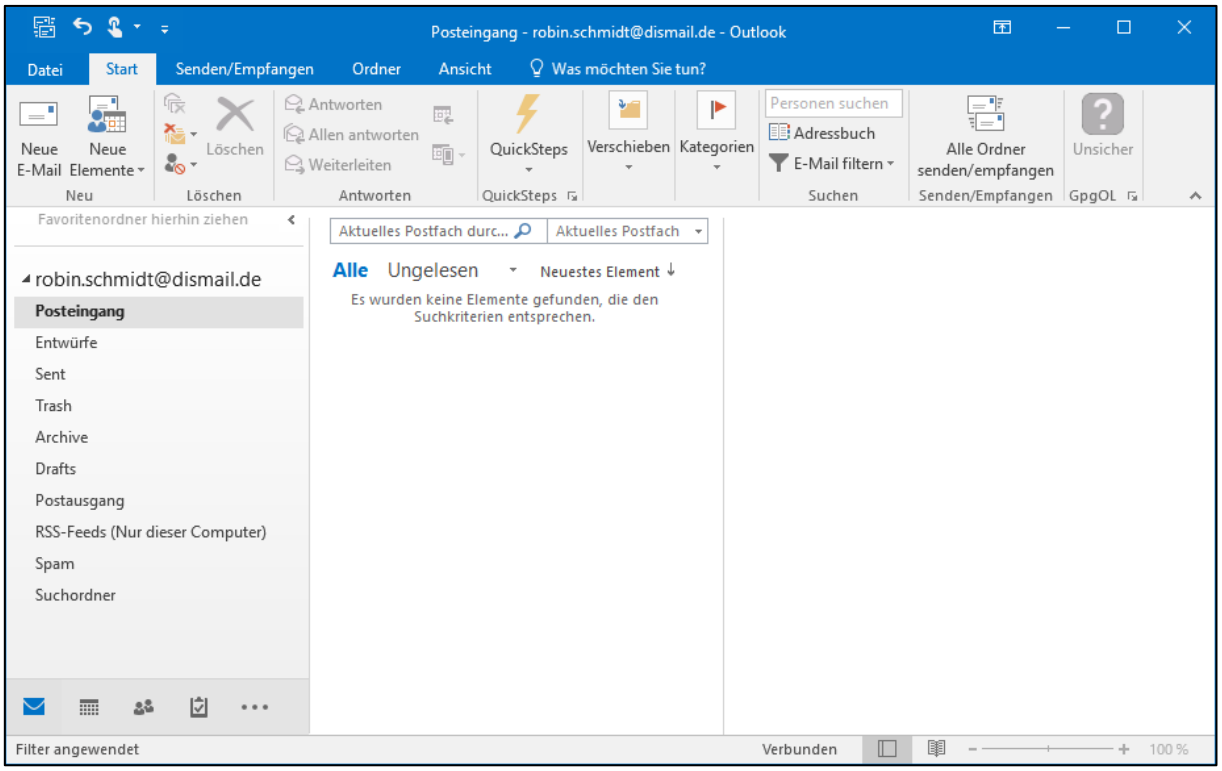

Abb. 9: Microsoft Outlook – Startbildschirm

Werfen Sie zuerst einen Blick in die obere rechte Ecke des E-Mail-Verfassen-Fensters. Wenn Sie dort einen Button mit einem Fragezeichen und der Beschriftung „Unsicher“ in der Kategorie „GpgOL“ sehen, wurde das Gpg4win Plugin erfolgreich in Outlook installiert.

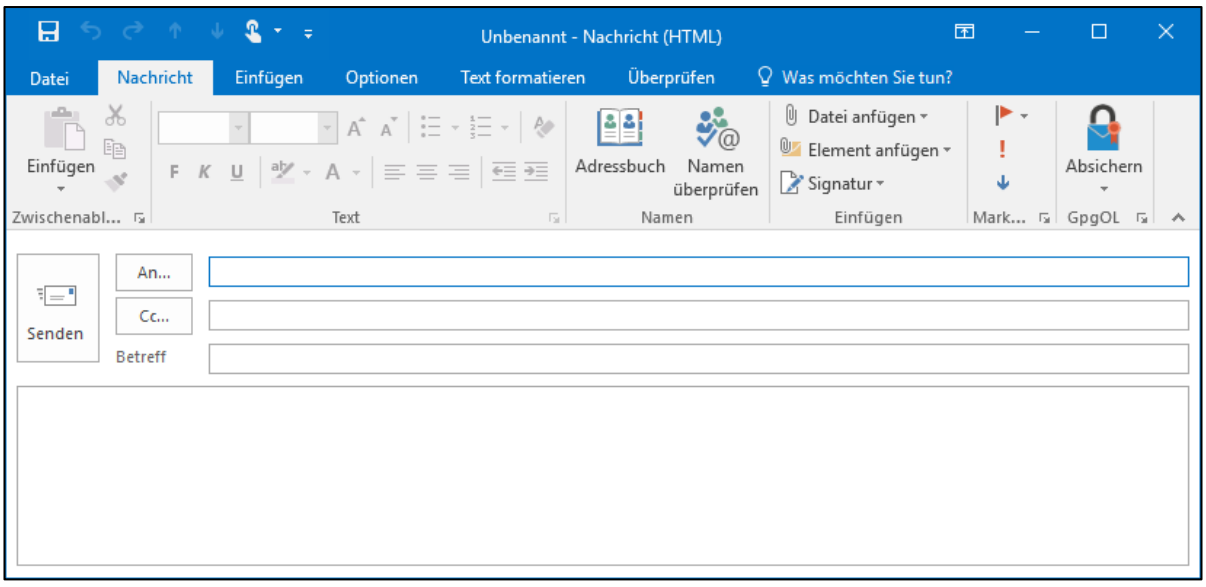

Abb. 10: Microsoft Outlook – Neue E-Mail verfassen

Geben Sie in der Zeile „An:“ die E-Mail des Kommunikationspartners ein, dem Sie eine verschlüsselte E-Mail zusenden möchten. In unserem Fall gibt Robin die E-Mail-Adresse von Anna Fröhlich ein (siehe Abbildung 11) . Das GpgOL Plugin in Outlook erkennt automatisch, dass für diese E-Mail (Anna.Froehlich@dismail.de) ein öffentlicher Schlüssel in Kleopatra hinterlegt wurde. GpgOL verwendet diesen, um die zu sendende E-Mail an Anna zu verschlüsseln. GpgOL verwendet zusätzlich Ihren privaten Schlüssel, um die zu versendende Nachricht zu signieren. Bedenken Sie: GpgOL kann Ihre E-Mails nur Signieren, wenn Sie über einen privaten Schlüssel passend zu Ihrer E-Mail-Adresse verfügen. Ob GpgOL Ihre zu versendende E-Mail automatisch verschlüsseln und signieren kann, können Sie anhand des grau hinterlegten „Absichern“-Buttons in der oberen rechten Ecke des Verfassen-Fensters erkennen. Wenn Sie auf diesen Button klicken, so dass dieser nicht mehr in der Farbe Grau erscheint, wird Ihre E-Mail nicht verschlüsselt oder signiert. Sie können also mithilfe dieser Buttons die Verschlüsselung und das Signieren von zu sendenden E-Mails manuell deaktivieren. Wenn Sie auf den kleinen Pfeil unterhalb des Buttons klicken, können Sie jeweils die Verschlüsselung oder Signatur der zu versendenden E-Mail deaktivieren.

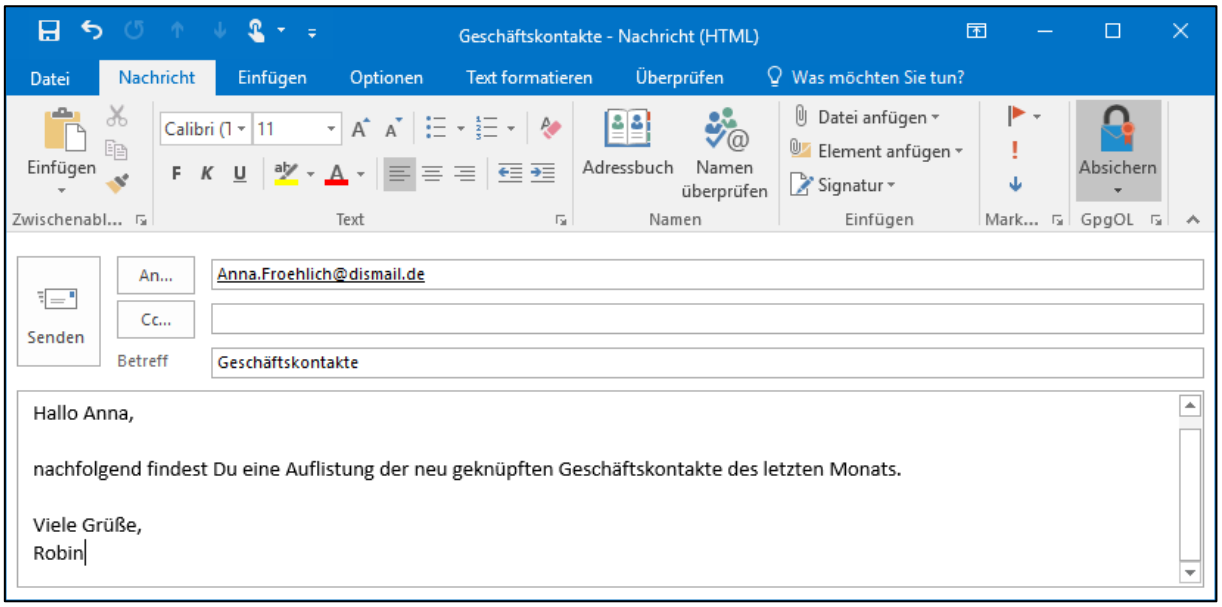

Abb. 11: Microsoft Outlook – Verschlüsselte und signierte E-Mail versenden

GpgOL wird nun auf Ihren privaten Schlüssel in Kleopatra zugreifen, um die zu versendende E-Mail zu signieren. Weiterhin wird GpgOL den öffentlichen Schlüssel von Anna Fröhlich aus Kleopatra verwenden, um die zu versendende E-Mail zu verschlüsseln. Wie bereits in Kapitel D beschrieben, schützt Kleopatra Ihre Schlüsselpaare mit dem jeweils von Ihnen bei der Erstellung vergebenen Passwort. Dieses Passwort wird nach Erstellung des Schlüsselpaars als „Passphrase“ bezeichnet. Geben Sie daher im Feld „Passphrase:“ das Passwort ein, das Sie zum Erstellen den Schlüsselpaars verwendet haben (siehe Abbildung 12). Bestätigen Sie anschließend

mit „OK“. Sollten Sie diese Passphrasen-Abfrage nicht sehen, kann das daran liegen, dass Sie diese erst vor kurzem eingegeben haben.

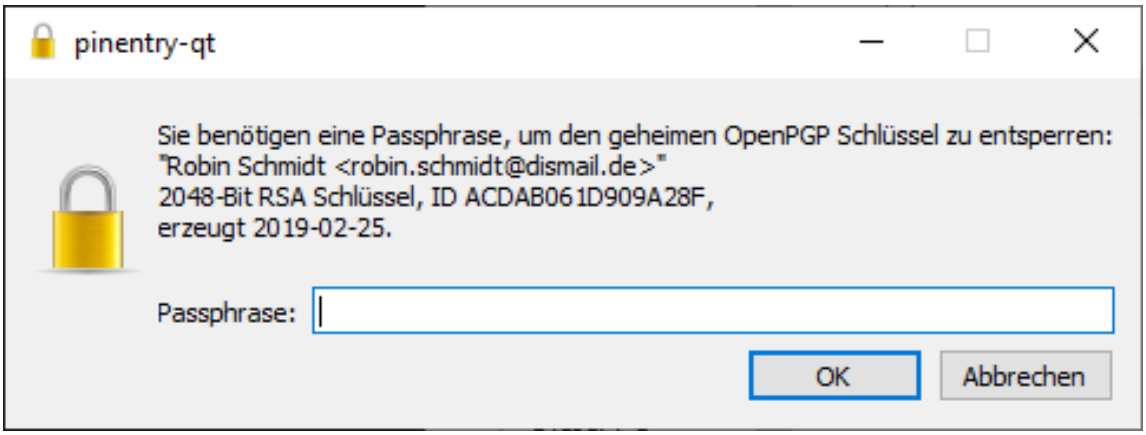

Abb. 12: Kleopatra – Entsperren Ihres privaten Schlüssels

Wenn Sie einen Blick in Ihr Postfach „Sent“ werfen, sehen Sie die von Ihnen verschlüsselte und signierte versendete E-Mail (siehe Abbildung 13).

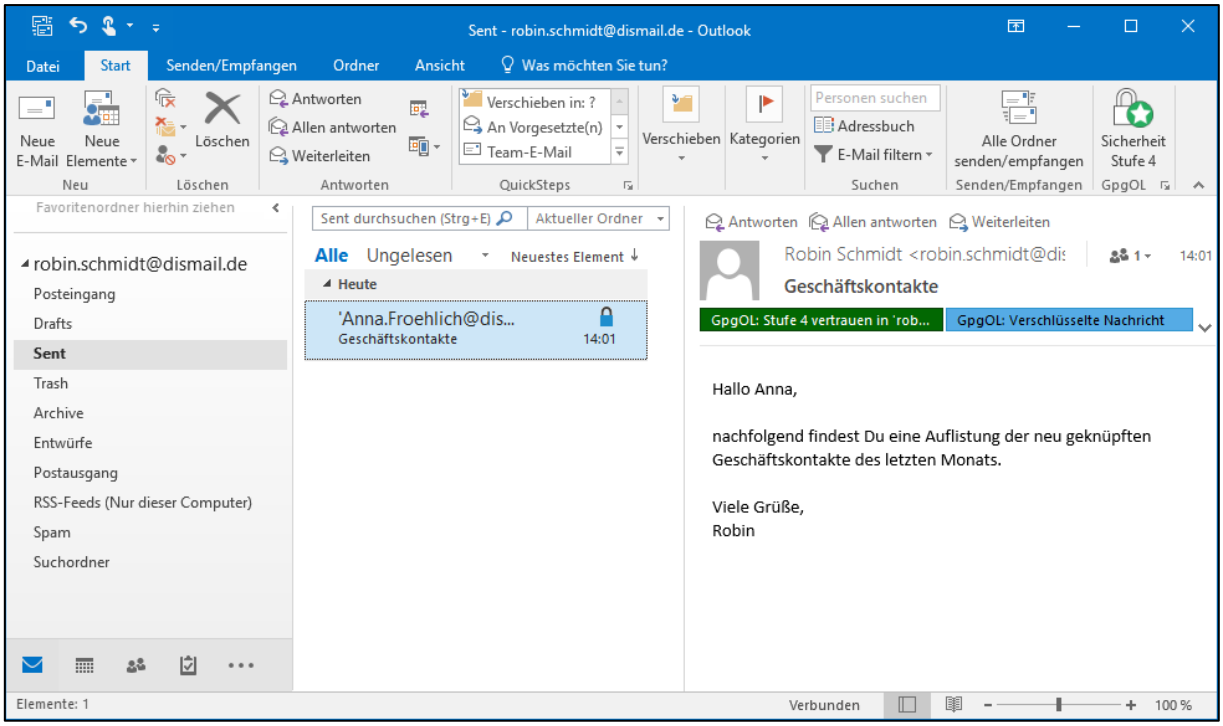

Abb. 13: Microsoft Outlook – Verschlüsselte und signierte E-Mail versendet

F Entschlüsseln einer E-Mail

Wie Ihnen bereits im vorangegangen Kapitel erläutert wurde, benötigen Sie zum Verschlüsseln von Dateien, Texten oder E-Mails den öffentlichen Schlüssel des Empfängers. Zum Entschlüsseln von verschlüsselten Dateien oder E-Mails benötigen Sie den zum öffentlichen Schlüssel passenden privaten Schlüssel. Passend meint, dass der private Schlüssel aus dem gleichen Schlüsselpaar stammen muss, wie der öffentliche Schlüssel, mit welchem die Dateien oder E-Mails verschlüsselt wurden. Bedenken Sie: Sie können nur diese E-Mails entschlüsseln, die mit Ihrem öffentlichen Schlüssel verschlüsselt wurden.

Um nun eine E-Mail zu entschlüsseln, können Sie sich entweder selbst eine verschlüsselte Nachricht zukommen lassen oder erhalten eine verschlüsselte E-Mail von ihrem Kommunikationspartner. Öffnen Sie Outlook und klicken Sie auf die erhaltene verschlüsselte E-Mail. In unserem Fall erhält Robin von Anna eine verschlüsselte Antwort-E-Mail (siehe Abbildung14).

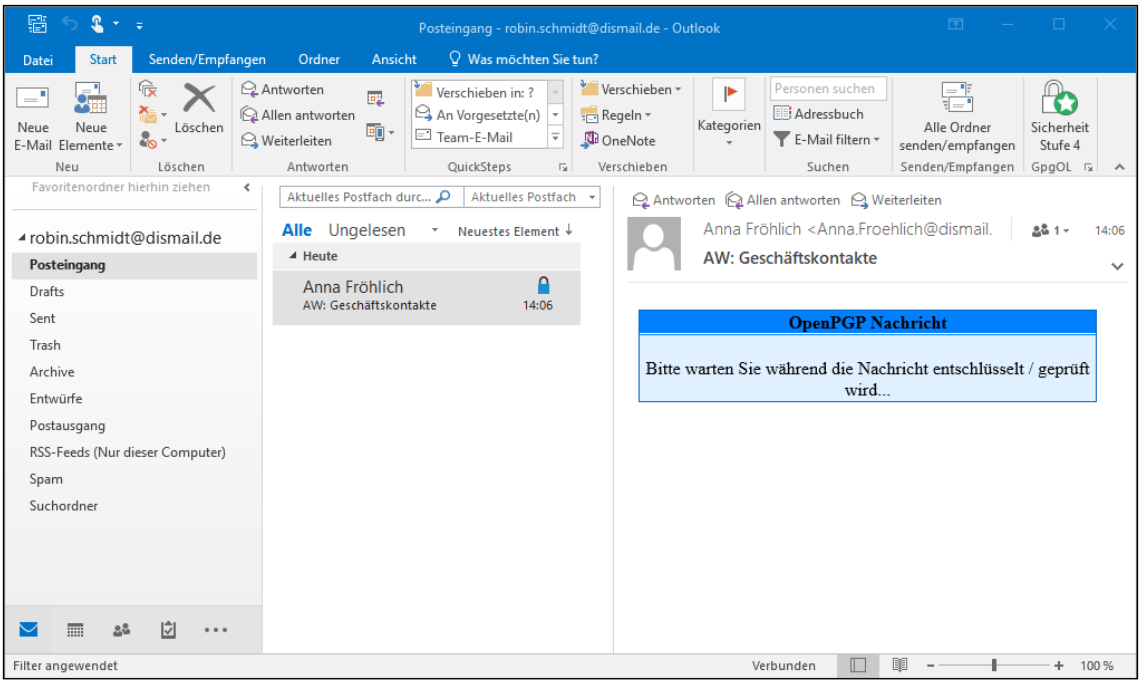

Abb. 14: Microsoft Outlook – Posteingang mit verschlüsselter E-Mail

Outlook wird nun auf Ihren privaten Schlüssel in Kleopatra zugreifen, um die empfangene verschlüsselte E-Mail zu entschlüsseln. Wie bereits in Kapitel D beschrieben, schützt Kleopatra Ihre Schlüsselpaare mit dem jeweils von Ihnen bei der Erstellung vergebenen Passwort. Dieses Passwort wird nach Erstellung des Schlüsselpaars als „Passphrase“ bezeichnet. Geben Sie daher im Feld „Passphrase:“ das Passwort ein, das Sie zum Erstellen des Schlüsselpaars verwendet haben (siehe Abb. 15). Bestätigen Sie anschließend mit „OK“. Sollten Sie diese Passphrasen-Abfrage nicht sehen, kann das daran liegen, dass Sie diese erst vor kurzem eingegeben haben.

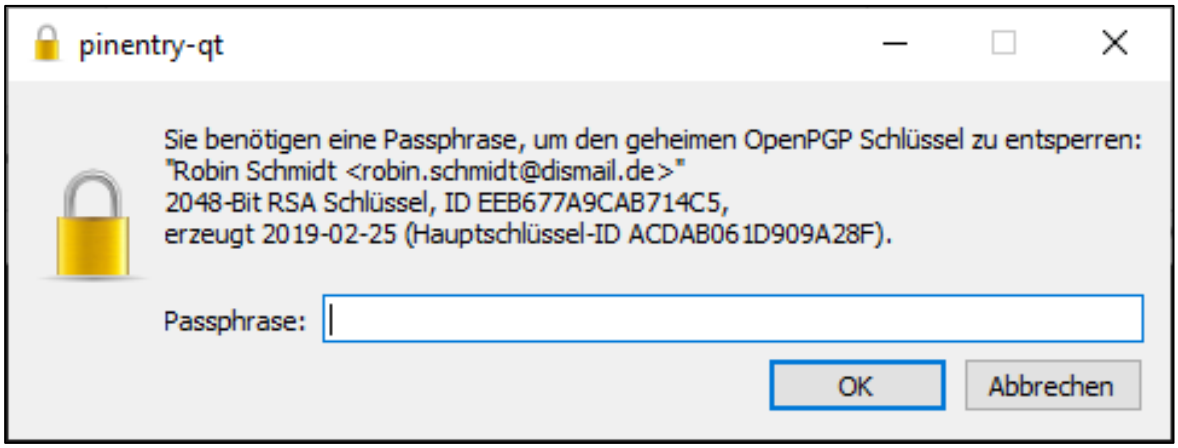

Abb. 15: Kleopatra – Entsperren Ihres privaten Schlüssels

GpgOL wird nun unter Zuhilfenahme Ihres privaten Schlüssels die verschlüsselte E-Mail automatisch entschlüsseln. Wenn der Prozess erfolgreich war, wird Ihnen die empfangene E-Mail im Klartext dargestellt. Die Zeile unterhalb des Empfängernamens zeigt Ihnen zusätzlich an, ob die E-Mail signiert wurde (siehe Abbildung 16).

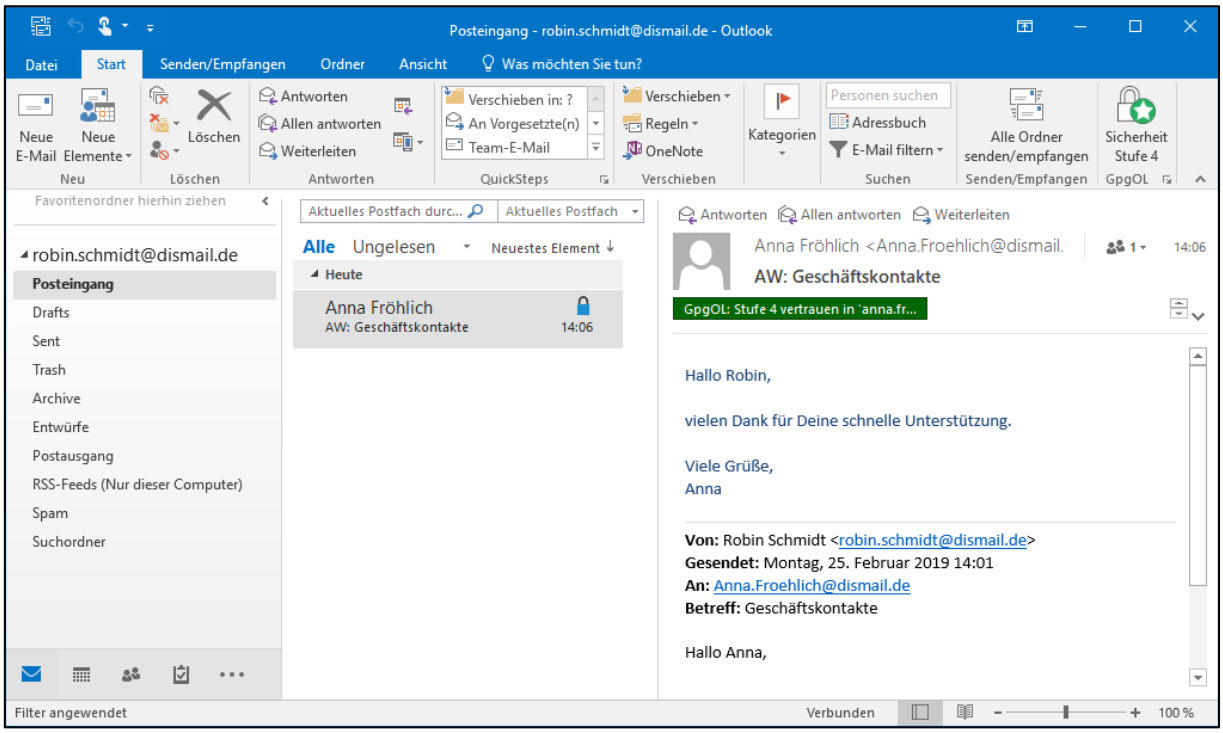

Abb. 16: Microsoft Outlook – Posteingang mit entschlüsselter E-Mail

G Gültigkeit und Bezug von öffentlichen Schlüsseln

Wie bereits in den vorangegangenen Kapiteln erläutert, benötigen Sie mindestens einen öffentlichen Schlüssel, um Dateien oder E-Mails zu verschlüsseln. In Kapitel E haben Sie bereits eine E-Mail verschlüsselt. Dieses Kapitel soll Ihnen erläutern, wie Sie neue öffentliche Schlüssel weiterer Kommunikationspartner in Kleopatra importieren und beglaubigen können.

Vorab ist zu sagen, dass es bei der Verschlüsselung mithilfe von PGP gewisse „Problempunkte" gibt, die man als Anwender „aus dem Weg räumen muss": Grundsätzlich ist es jedem Nutzer möglich, Schlüsselpaare auf beliebige E-Mail-Adressen zu erstellen. Es wird nicht sichergestellt, dass der Ersteller des Schlüsselpaars auch der Eigentümer der zugehörigen E-Mail-Adresse ist. Daher ist es wichtig, dass Sie die „richtigen" öffentlichen Schlüssel importieren und verwenden. Importieren Sie den falschen öffentlichen Schlüssel und verschlüsseln damit eine Datei, die Sie Ihrem Gegenüber senden möchten, kann dieser Sie nicht entschlüsseln. Zur Sicherstellung der Echtheit von Schlüsseln gibt es zwei Möglichkeiten in Kleopatra: Eine flüchtige, nicht sichere Kontrolle kann über ein Schlüssel-ID-Vergleich erfolgen. Die sicherere Kontrolle erfolgt mit Hilfe eines Fingerabdruck-Vergleichs.

Die Schlüssel-ID ist ein 32-Bit-Wert, welcher in hexadezimaler Darstellung bereitgestellt wird. Diese Schlüssel-ID sollte für jedes Schlüsselpaar eindeutig sein. Hier sehen Sie eine Beispiel-Schlüssel-ID: `99FE4EB7`. Im Jahr 2014 wurde jedoch das Gegenteil bewiesen. Eine Kontrolle ausschließlich auf Basis der Schlüssel-ID reicht daher nicht aus. Vielmehr muss auf die Kontrolle über Fingerabdrücke zurückgegriffen werden.

Der Fingerabdruck ist einzigartig und stellt eine Art Quersumme dar, welche aus dem Schlüsselpaar errechnet wurde. Dieser Fingerabdruck hat eine entsprechende Länge und passt weltweit nur auf ein einziges Schlüsselpaar. Hier sehen Sie einen Beispiel-Fingerabdruck:

```
A767 1A57 5F87 B31E 2C26 2265 857F C948 99FE 4EB7
```

In Kleopatra können Sie sich per Doppelklick auf den entsprechenden Schlüssel oder über Rechtsklick auf den Schlüssel und dem Eintrag „Details" die Details eines Schlüssels anzeigen lassen (siehe Abbildung 17).

Im unteren Bereich des Fensters sehen Sie die Zertifikatsdetails des Schlüssels von Peter Mustermann. In diesem Bereich sehen Sie ebenfalls den zugehörigen Fingerabdruck. Über den Button „Beglaubigungen" können Sie sehen, wer diesem Schlüssel bereits sein Vertrauen zugesichert hat. Ihr Vertrauen gegenüber einem Schlüssel können Sie in der Schlüsselübersicht von Kleopatra festlegen: Rechtsklicken Sie dazu auf einen Schlüssel und wählen Sie den Eintrag „Beglaubigen...". Eigens erstellte Schlüssel haben standardmäßig ein „ultimatives" Vertrauen. Importierte Schlüssel müssen dieses Vertrauen durch Sie erst erlangen. Wenn Sie einen neuen

Schlüssel in Kleopatra aufnehmen, sollten Sie daher zuerst den Fingerabdruck des Schlüssels überprüfen. Erst nach Überprüfung legen Sie Ihr Vertrauen gegenüber der Schüssel fest.

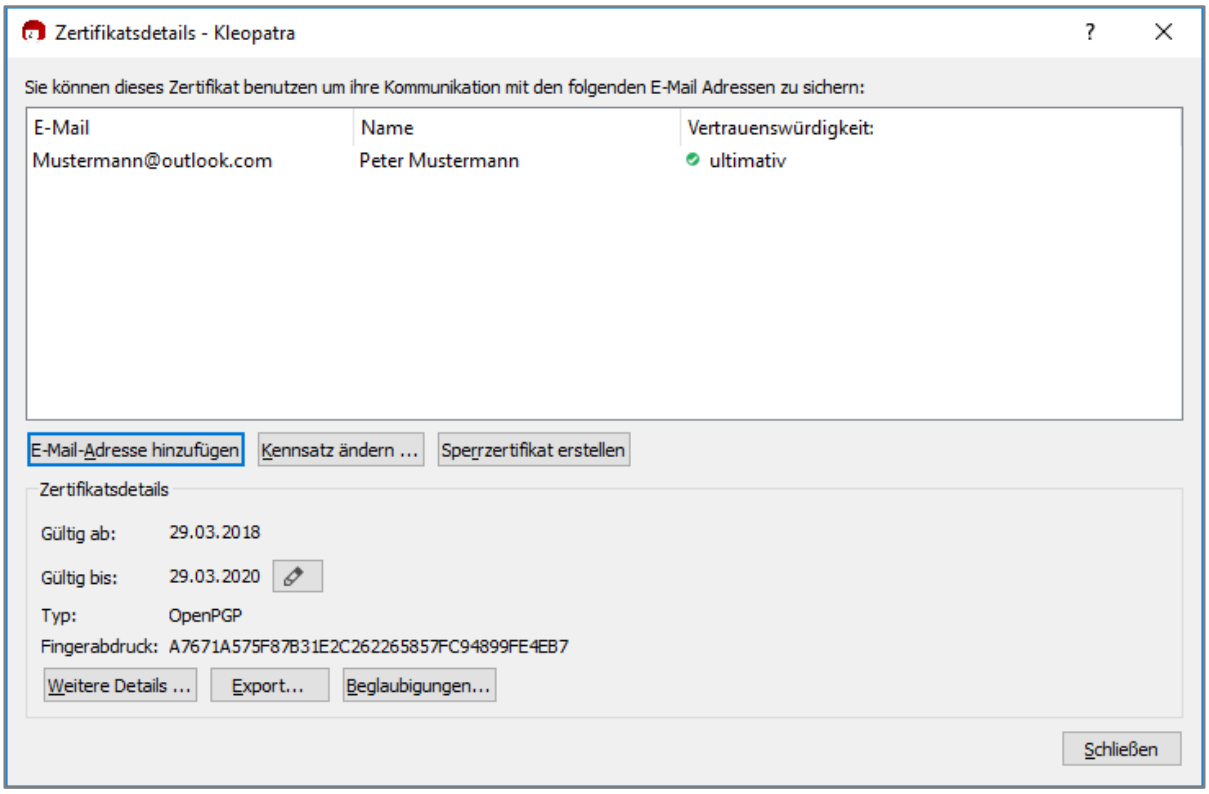

Abb. 17: Kleopatra – Details eines Schlüsselpaars

Möchten Sie einen neuen Schlüssel z. B. eines Geschäftspartners oder Freundes in Kleopatra aufnehmen, können Sie dies über den „Auf Server suchen"-Button in der Menüleiste durchführen. Wahlweise kann Ihr Kommunikationspartner Ihnen den öffentlichen Schlüssel seines Schlüsselpaars auch als Datei zukommen lassen, die Sie dann über den „Importieren"-Button in der Menüleiste von Kleopatra importieren. Fortgeschrittene Nutzer können den öffentlichen Schlüssel des Kommunikationspartners auch über die Kommandozeile importieren.

Um nun einen öffentlichen Schlüssel zu importieren, klicken Sie in Kleopatra auf den „Auf Server suchen"-Button in der Menüleiste. Geben Sie im vorgesehenen Feld entweder den Namen, die E-Mail oder den Fingerabdruck Ihres Kommunikationspartners ein. Je präziser Ihre Anfrage, desto weniger Schlüssel werden Ihnen zum Import angeboten. Wenn Sie den Fingerabdruck Ihres Gesprächspartners in das Suchfeld eingeben, sollten Sie nur einen einzigen Schlüssel finden. Klicken Sie diesen Schlüssel an und bestätigen Sie den Import mit „Importieren" (siehe Abbildung 18).

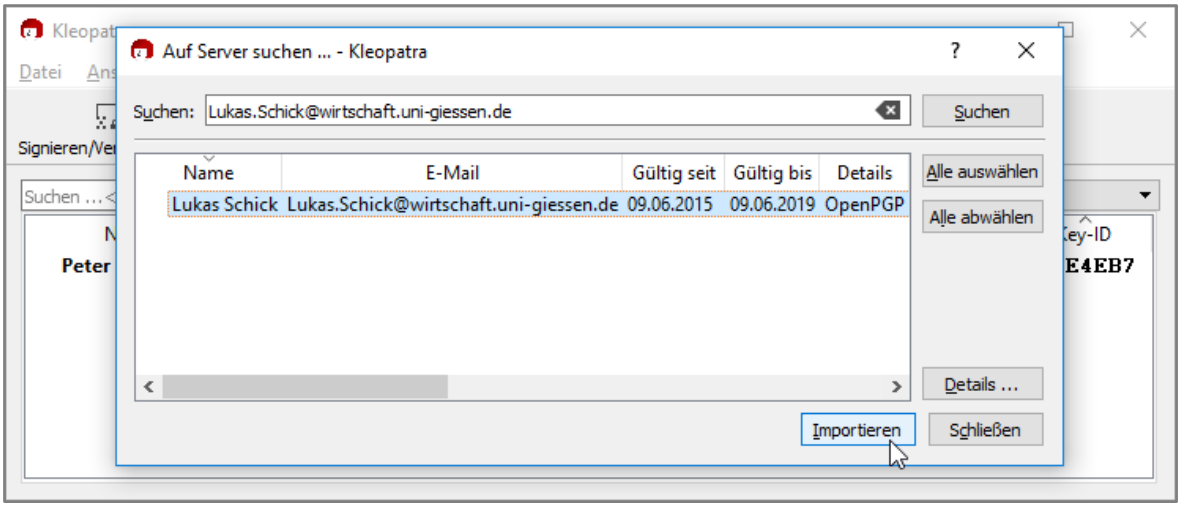

Abb. 18: Kleopatra – Importieren eines Schlüssels

Direkt nach Klicken des „Importieren“-Buttons öffnet sich ein Assistenzfenster von Kleopatra zum Festlegen des Vertrauens gegenüber dem importieren Schlüssel (siehe Abbildung 19).

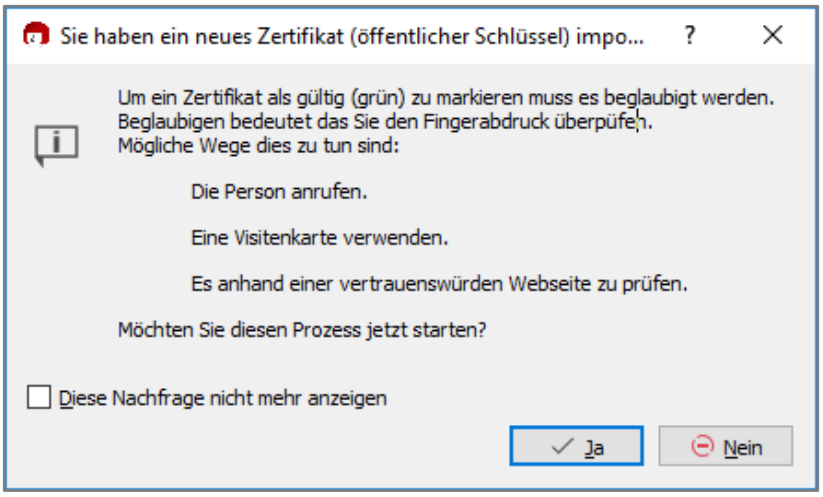

Abb. 19: Kleopatra – Beglaubigen eines Schlüssels nach Import (1)

Klicken Sie auf „Ja“, um den Beglaubigungsprozess zu starten. Das nächste Fenster (Abbildung 20) zeigt Ihnen den zu beglaubigenden Schlüssel und darunter den Fingerabdruck des Schlüssels an. Sobald Sie diesen Fingerabdruck verglichen und damit überprüft haben, setzten Sie einen Haken bei „Ich habe den Fingerabdruck überprüft“ und klicken Sie auf „Weiter“. Der Fingerabdruck sollte Ihnen von Ihrem Kommunikationspartner auf einem alternativen Weg (E-Mail, Telefon, SMS etc.) übermittelt werden, so dass Sie diesen hier vergleichen können.

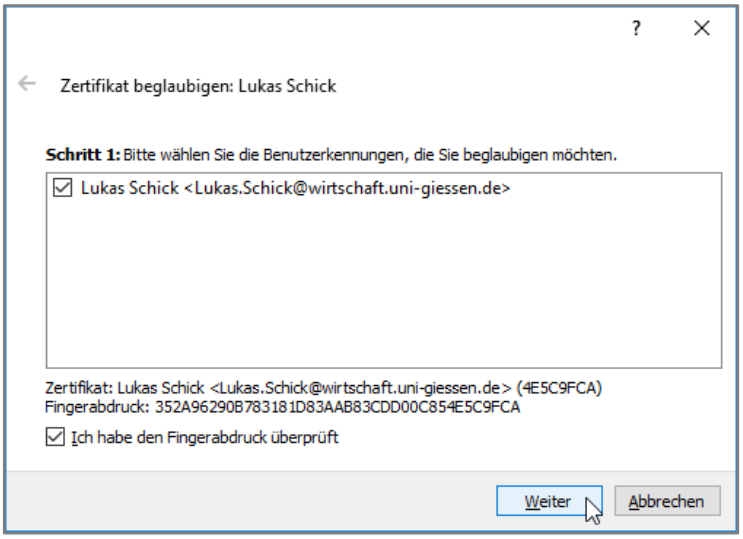

Abb. 20: Kleopatra – Beglaubigen eines Schlüssels nach Import (2)

Im darauffolgenden Fenster wählen Sie aus, wie dieser Schlüssel beglaubigt werden soll (siehe Abbildung 21). Wenn Sie „Nur für mich selbst beglaubigen“ wählen, wird der Schlüssel nur in Ihrem Kleopatra-Schlüsselverzeichnis als beglaubigt angegeben. Wenn Sie „Für alle sichtbar beglaubigen“ wählen, wird dieser Schlüssel mit Ihrem Schlüssel signiert und an einen öffentlichen Schlüsselserver gesandt. An dieser Stelle reicht es aus, wenn Sie den Schlüssel nur für sich selbst beglaubigen. Klicken Sie anschließend auf „Beglaubigen“.

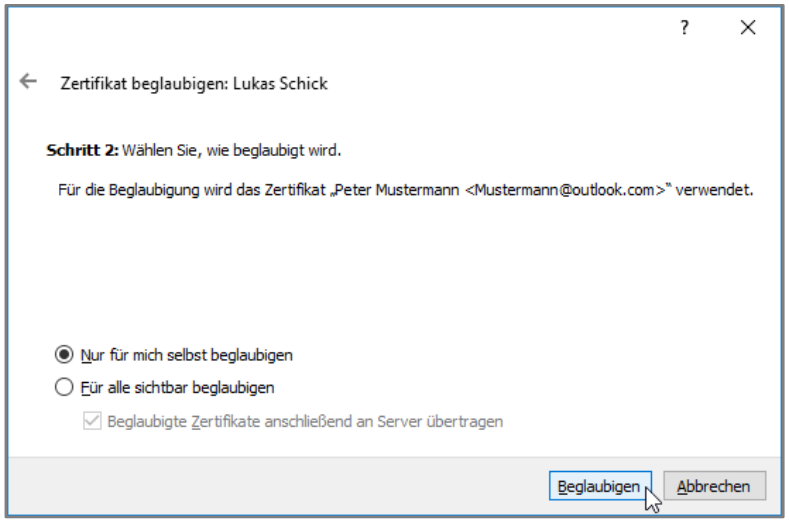

Abb. 21: Kleopatra – Beglaubigen eines Schlüssels nach Import (3)

Ein letztes Fenster gibt Ihnen noch einmal aus, ob der Beglaubigungsprozess erfolgreich war. Der importierte Schlüssel sollte nun in Kleopatra auftauchen. Per Doppelklick auf diesen Schlüssel erhalten Sie alle weiteren Details und können so noch einmal den Fingerabdruck überprüfen und anschließend Ihr Vertrauen gegenüber dem Schlüssel anpassen.

H Schlüssel widerrufen

Es gibt verschiedene Gründe, warum es notwendig sein kann, erstellte oder veröffentlichte Schlüsselpaare zu widerrufen. Ein Grund kann zum Beispiel sein, dass private Schlüssel kompromittiert wurden. Kompromittiert meint, dass der Schlüsselersteller die Kontrolle über seinen privaten Schlüssel verloren hat und dieser (möglicherweise) Unberechtigten zugänglich ist. In der Regel äußert sich dies durch nicht mehr geheime Passphrasen, „verlorene" private Schlüssel oder „verlorene" Widerrufszertifikate. Unberechtigte könnten dann private E-Mails oder Dateien entschlüsseln und ausgehende E-Mails, Dateien oder weitere Schlüssel mit dem kompromittierten privaten Schlüssel signieren. Das Vertrauen in das kompromittierte Schlüsselpaar ist dadurch verloren. Das Widerrufen eines Schlüssels soll unter anderem diesen Vertrauensverlust gegenüber Ihren Kommunikationspartner signalisieren.

Grundsätzlich sollten kompromittierte Schlüssel immer widerrufen werden, auch wenn diese nicht in ein öffentliches Schlüsselverzeichnis kopiert wurden. Ihre Kommunikationspartner wissen dann, dass sie zur Verschlüsselung von Dateien oder E-Mails auf andere öffentliche Schlüssel zurückgreifen müssen. Haben Sie Ihren öffentlichen Schlüssel in ein öffentliches Schlüsselverzeichnis kopiert, müssen Sie, nachdem Sie den Schlüssel lokal widerrufen haben, einem öffentlichen Schlüsselverzeichnis diesen Widerruf mitteilen. Das Schlüsselverzeichnis zeigt Ihren öffentlichen Schlüssel dann als widerrufen an. Die Entfernung eines öffentlichen Schlüssels aus einem Schlüsselverzeichnis ist nicht möglich. Einmal veröffentlicht, können Schlüssel nur widerrufen aber nicht mehr aus Schlüsselverzeichnissen gelöscht werden. Bedenken Sie: Das Widerrufen eines Schlüssels ist unumkehrbar und endgültig.

Um nun ein Schlüsselpaar zu widerrufen, müssen Sie zuerst auf die Kommandozeile zurückgreifen, da Kleopatra keine Widerrufsfunktion mit graphischer Benutzeroberfläche bereitstellt. Öffnen Sie in Windows die Eingabeaufforderung (siehe Abb. 22) und gehen Sie wie folgt vor:

1. Die Zeichen vor Ihrem blinkenden Cursor zeigen Ihnen an, in welchem Ordner Sie sich auf Ihrem PC befinden. In unserem Fall auf Laufwerk Z:\.
2. Geben Sie per Tastatur folgenden Befehl ein, um alle Keys aus Kleopatra samt ID anzuzeigen: „gpg --list-keys" (ohne Anführungszeichen). Bestätigen Sie Ihre Eingabe mit Hilfe des Enter-Buttons.
3. Notieren Sie die ID Ihres zu widerrufenden Schlüssels. In unserem Fall ist die ID des Schlüssels von Robin Schmidt folgende: A1A77...
4. Geben Sie folgenden Befehl ein, um ein Widerrufszertifikat für den entsprechenden Schlüssel zu erstellen: „gpg --output revoke.asc --gen-revoke A1A77...." (ohne Anführungszeichen). Bestätigen Sie die Eingabe mithilfe des Enter-Buttons.
5. Geben Sie in den nächsten zwei Dialogen den Grund für den Widerruf sowie eine optionale Beschreibung ein und bestätigen Sie wieder beide Schritte mit Enter.

6. Ihr Widerrufszertifikat für den entsprechenden Schlüssel wurde im derzeit befindlichen Ordner gespeichert (in unserem Fall auf Laufwerk Z:\).

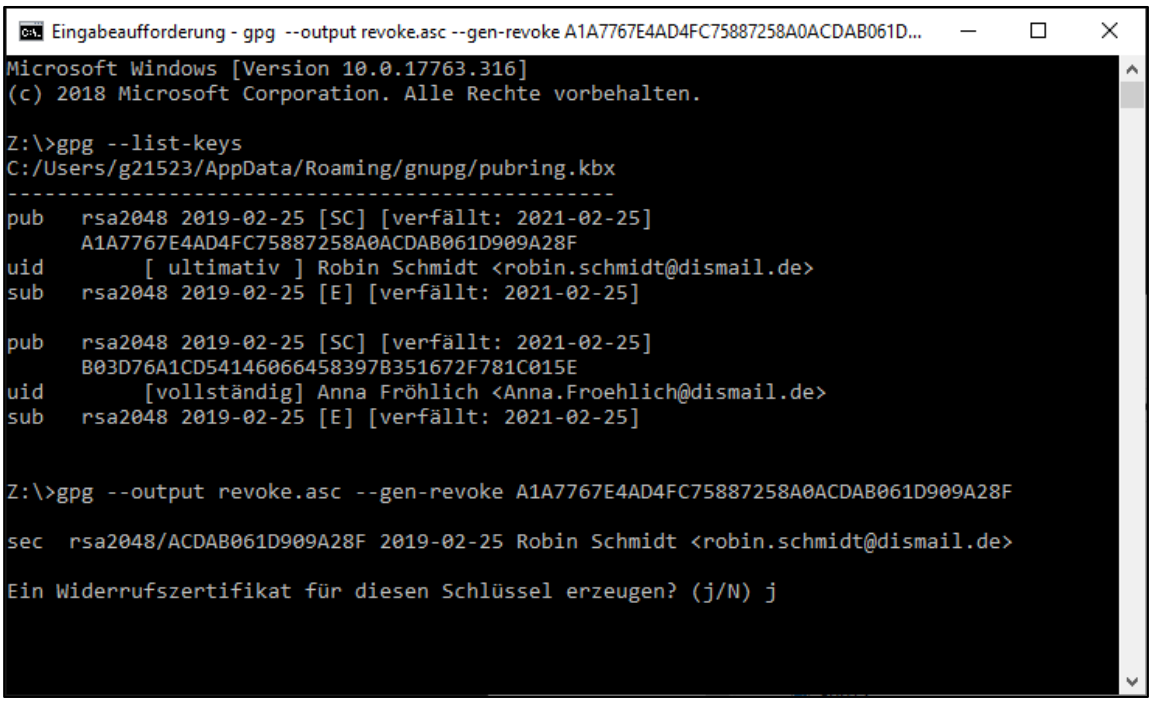

Abb. 22: Windows Eingabeaufforderung – Widerrufszertifikat erstellen

Sie werden abschließend von Kleopatra aufgefordert Ihre Passphrase passend zu dem zu widerrufenden Zertifikat anzugeben. Geben Sie dieses ein und bestätigen Sie mit „OK“.

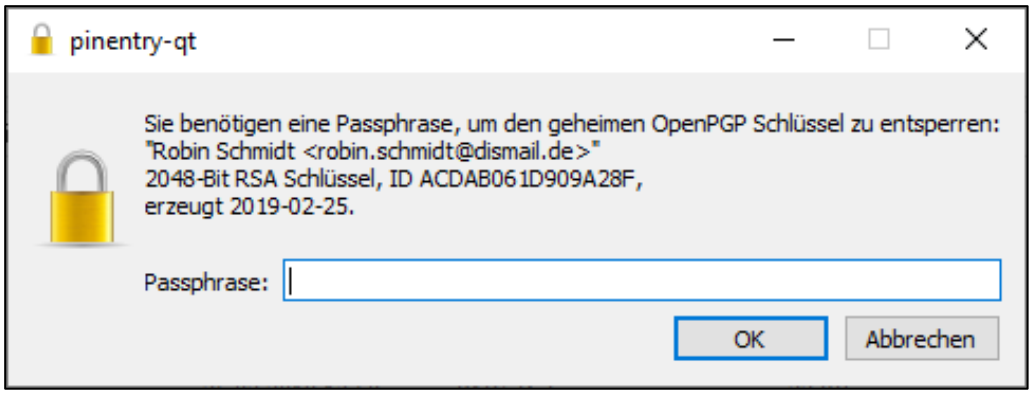

Abb. 23: Kleopatra – Passphrase eingeben

Das Widerrufszertifikat wurde erfolgreich erstellt und unter Z:\ abgelegt (siehe Abbildung 24). Bitte lesen Sie sich die abschließende Mitteilung aufmerksam durch und bewahren Sie das Zertifikat an einem sicheren Ort auf. Öffnen Sie nun Kleopatra und importieren Sie die Datei „revoke.asc“ über den „Importieren...“-Button in der Menüzeile (siehe Abbildung 25).

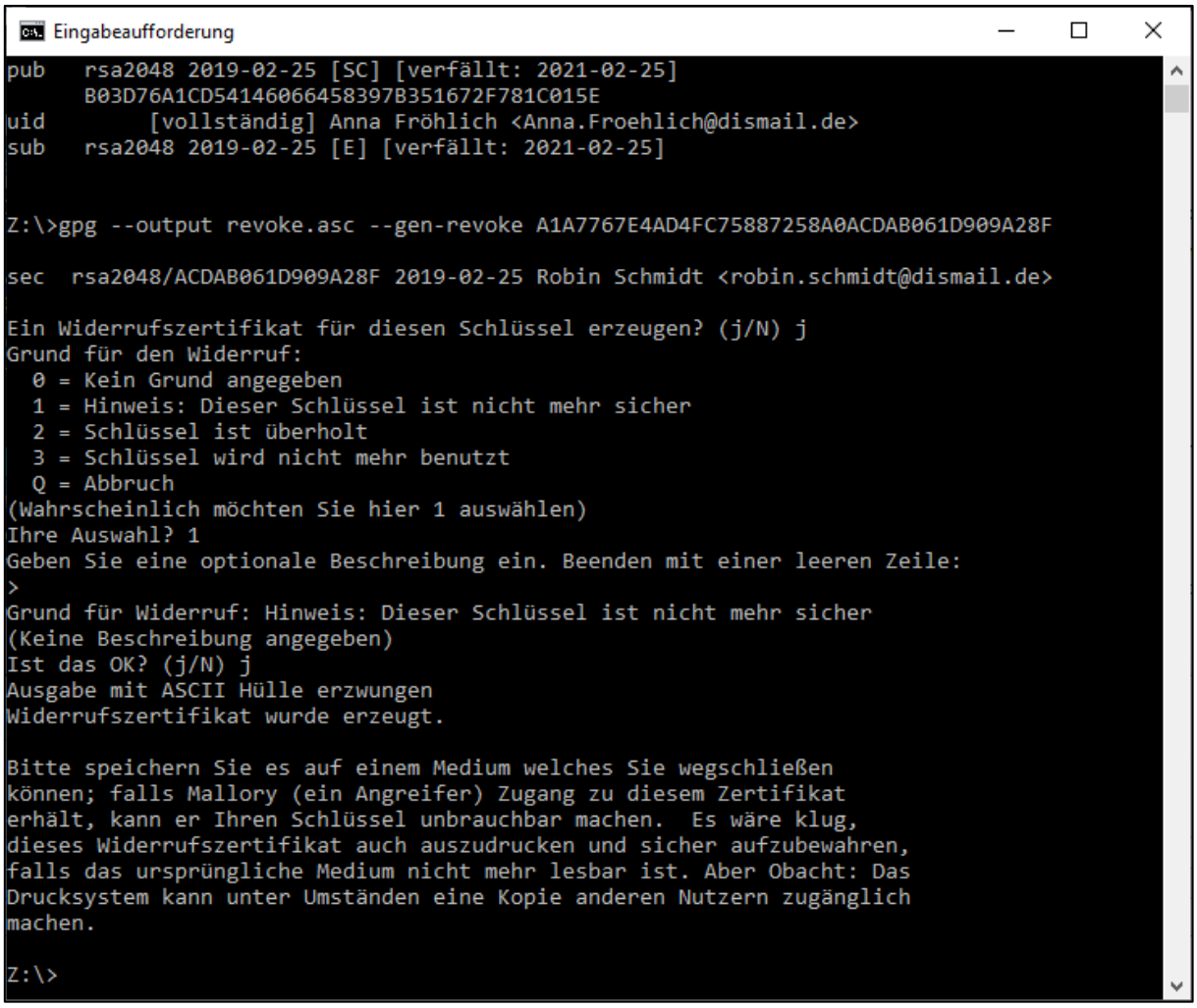

Abb. 24: Windows Eingabeaufforderung – Schlüsselpaar widerrufen

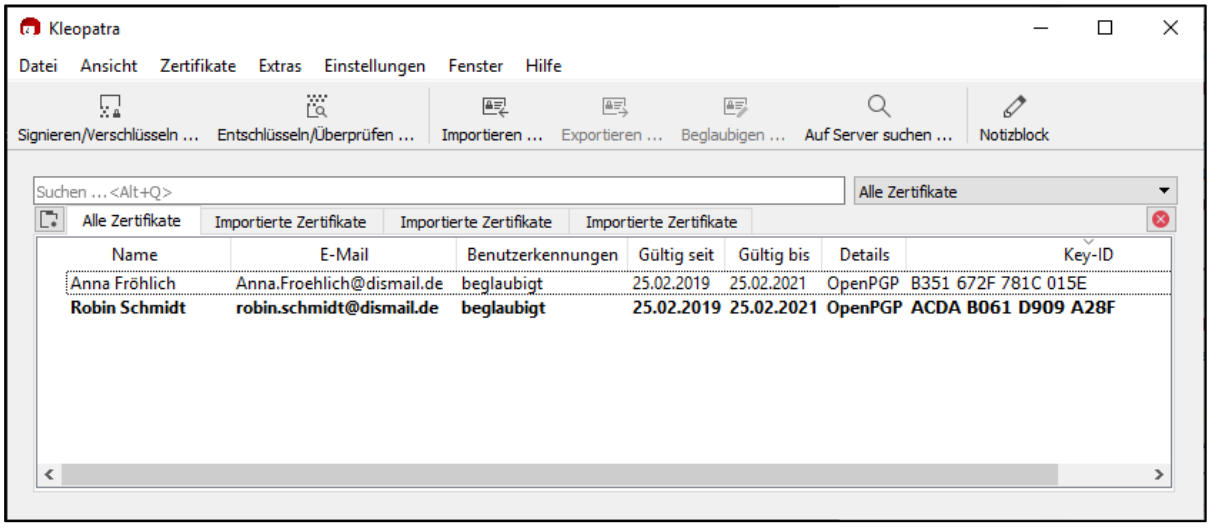

Abb. 25: Kleopatra – Widerrufszertifikat importieren

Navigieren Sie nun zum Speicherort des Widerrufszertifikats (Iin diesem Fall wurde die Datei „revoke.asc“ aus Komfortgründen zum Desktop bewegt). Wählen Sie die „revoke.asc“-Datei aus und bestätigen Sie Ihre Auswahl mithilfe des „Öffnen“-Buttons (siehe Abbildung 26).

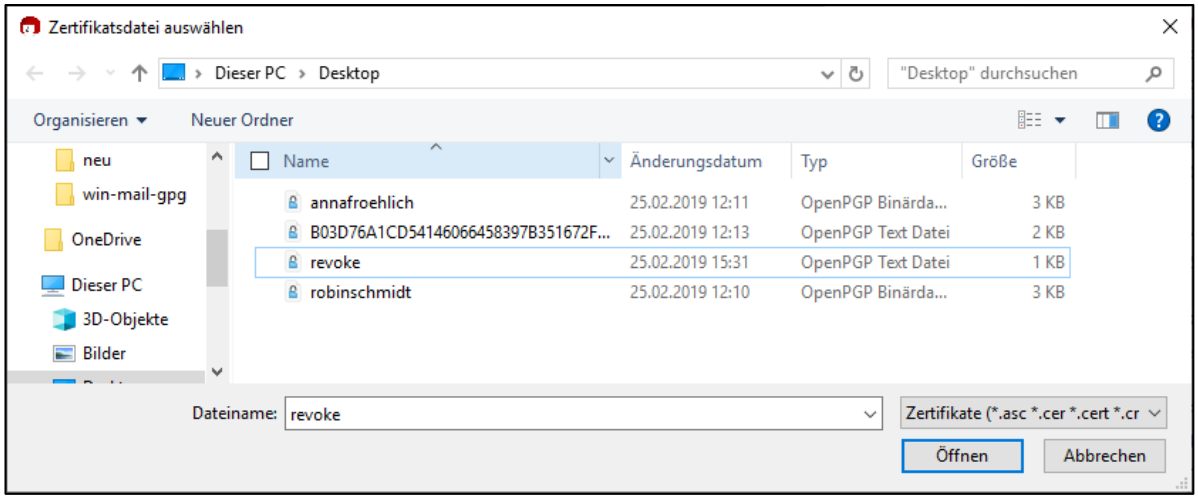

Abb. 26: Kleopatra – Widerrufszertifikat auswählen

Kleopatra importiert nun das Widerrufszertifikat aus der Datei „revoke.asc“ und gibt Ihnen eine entsprechende Ergebnismeldung. Bestätigen Sie den Vorgang mit „OK“ (siehe Abbildung 27).

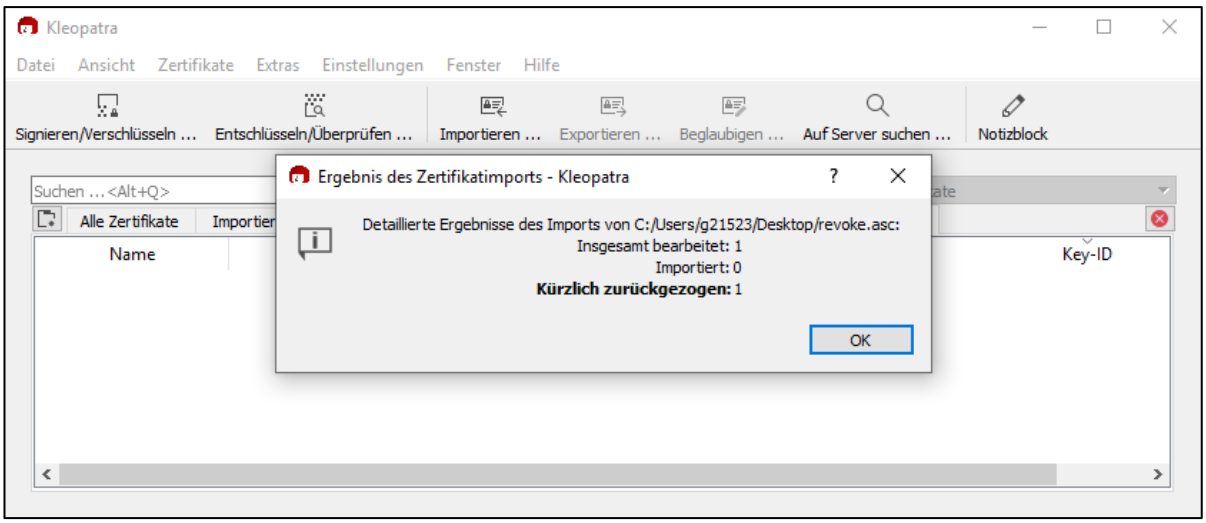

Abb. 27: Kleopatra – Schlüsselpaar erfolgreich widerrufen

Um nun sicherstellen zu können, dass das Widerrufszertifikat erfolgreich angewendet wurde, navigieren Sie in Kleopatra zu Ihrer Schlüsselpaar-Liste. War der Vorgang erfolgreich, wurde der Eintrag „beglaubigt“ in der Spalte „Benutzerkennung“ der entsprechenden Zeile in den Wert „nicht beglaubigt“ abgeändert (vergleichen Sie die Abbildungen 25 und 28).

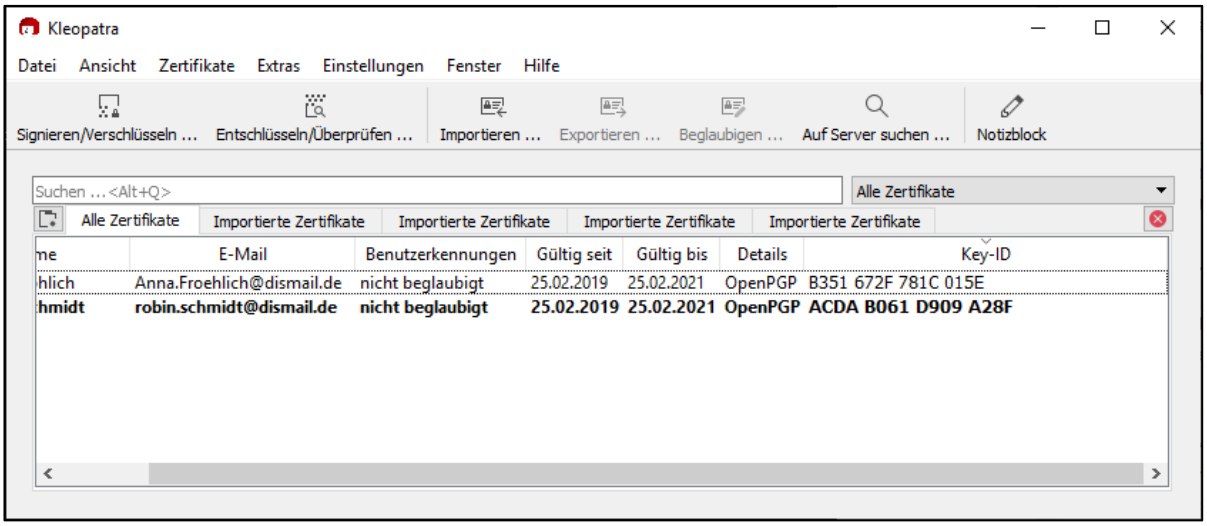

Abb. 28: Kleopatra – Schlüsselpaar-Liste

Sie erhalten weitere Details zum Schlüsselpaar, wenn Sie es per Doppelklick in der Zeile anklicken oder per Rechtsklick auf „Details“ klicken. In der Spalte „Vertrauenswürdigkeit“ (siehe Abbildung 29) können Sie sehen, dass der Wert „zurückgerufen“ eingetragen wurde. Sie haben damit Ihr Zertifikat erfolgreich widerrufen.

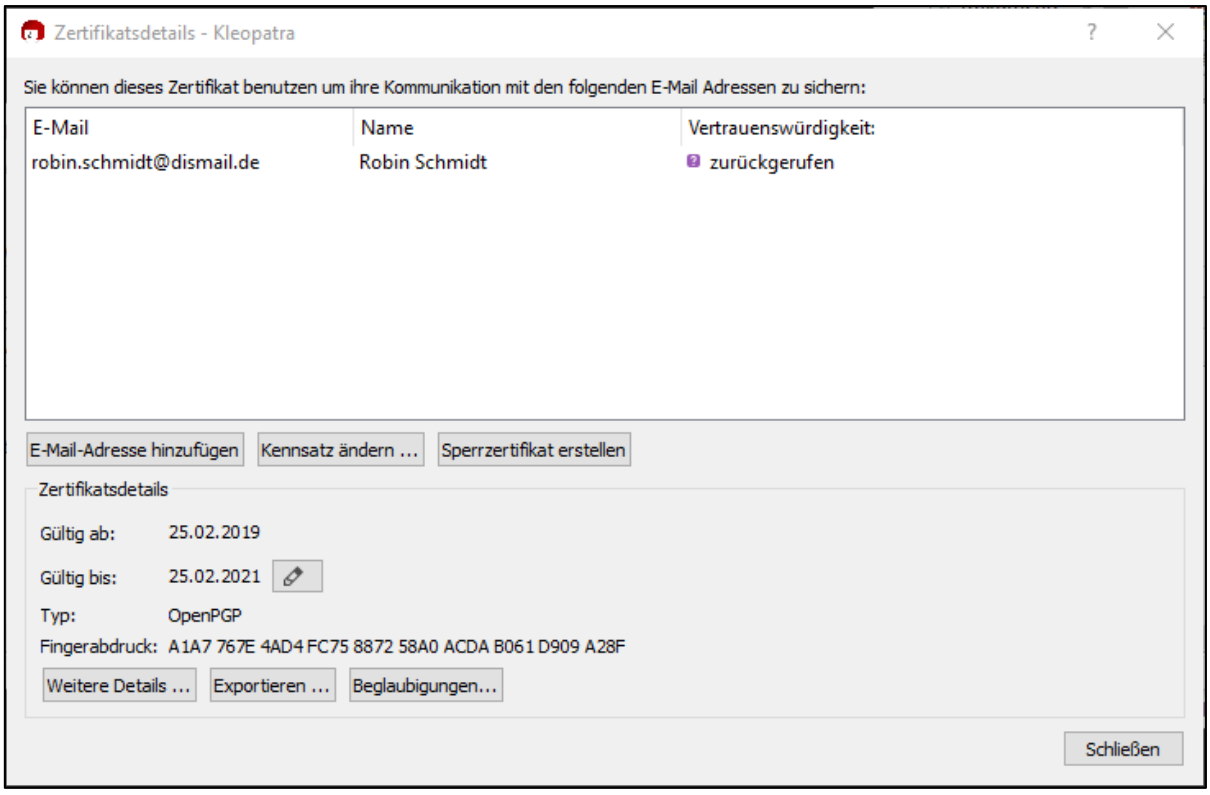

Abb. 29: Kleopatra – Details zum Schlüsselpaar

Kleopatra konnte diesen Widerruf nur für Sie durchführen, weil Sie im Besitz des Schlüsselpaares (öffentlicher und privater Schlüssel) und der dazugehörigen Passphrase sind. Wenn Sie bei der Erstellung Ihres Schlüsselpaares ein Widerrufszertifikat erstellt haben, kann dies Ihnen helfen, das Schlüsselpaar zu widerrufen, auch wenn Sie über keine Kopie Ihres privaten Schlüssels mehr verfügen oder die Passphrase vergessen haben. Das Widerrufszertifikat dient daher oftmals als „Handbremse“, wenn Sie nicht mehr über alle Mittel zum Widerruf verfügen. Jedoch muss dieses mächtige Widerrufszertifikat nach der Schlüsselerstellung außerhalb von Kleopatra auf Ihrer Festplatte abgelegt werden. Sie müssen dann eigenständig der Aufgabe des Schützens und Sicherns dieses Zertifikats nachkommen.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: http://wiwi.uni-giessen.de/home/Schwickert/arbeitspapiere/

Herausgeber: Prof. Dr. Axel C. Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse http://wiwi.uni-giessen.de/home/ Schwickert/arbeitspapiere/.