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

Schwickert, Axel; Schick, Lukas

Windows – Verschlüsseln, Entschlüsseln und Signieren von Dateien

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 5 / 2018
ISSN 1613-6667

Arbeitspapiere WI Nr. 5 / 2018

Autoren: Schwickert, Axel; Schick, Lukas

Titel: Windows – Verschlüsseln, Entschlüsseln und Signieren von Dateien

Zitation: 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, 18 Seiten, ISSN 1613-6667.

Kurzfassung: Der Überlieferung nach verschlüsselte der römische Feldherr Caesar seine militärischen Nachrichten für die geheime Kommunikation mit seinen Soldaten. Caesar nutze dafür eine Verschiebung des Alphabets um drei Buchstaben. Dieser Schlüssel musste natürlich vor den Feinden geheim gehalten werden. Damit nur Caesars Offiziere seine Nachrichten von Geheimtext in Klartext umwandeln konnten, musste Caesar den Offizieren vorher den geheimen Schlüssel mitgeteilt haben. Caesar konnte das noch recht einfach bewerkstelligen. Bevor er mit seinem Heer in den Krieg zog, teilte er seinen Offizieren in Rom den geheimen Schlüssel im persönlichen Gespräch mit. Die symmetrische Verschlüsselung hilft jedoch nicht, wenn im heutigen Internet zwei Personen miteinander geheim kommunizieren wollen, die sich nicht kennen und auch keine Gelegenheit haben, vor ihrer Kommunikation einen gemeinsamen („symmetrischen“) geheimen Schlüssel auszutauschen. Im Internet spielen heute zur Verschlüsselung von Nachrichten zwischen anonymen Kommunikationspartnern sog. „asymmetrische“ Verschlüsselungsverfahren eine zentrale Rolle. Dabei herrscht „Schlüssel-Asymmetrie“ – die Verschlüsselung einer Nachricht erfolgt mit einem anderen Schlüssel als die Entschlüsselung der Nachricht. Bei den asymmetrischen Verfahren besitzt jeder Kommunikationsteilnehmer ein eigenes Schlüsselpaar. Das Schlüsselpaar besteht aus einem öffentlichen Schlüssel (public key) und einem privaten Schlüssel. Im vorliegenden Arbeitspapier wird gezeigt, wie auf Rechnern mit dem Betriebssystem Microsoft Windows Dateien verschlüsselt, entschlüsselt und signiert werden. Dazu wird die Crypto-Software „Gpg4win“ verwendet.

Schlüsselwörter: Verschlüsselung, Signatur, Schlüssel, Schlüsselpaar, öffentlich, privat, symmetrisch, asymmetrisch, Microsoft Windows, Gpg4win

Inhaltsverzeichnis

A Asymmetrische Verschlüsselung – Was ist das?

Der Überlieferung nach verschlüsselte der römische Feldherr Caesar seine militärischen Nachrichten für die geheime Kommunikation mit seinen Soldaten. Caesar nutze dafür eine Verschiebung des Alphabets um drei Buchstaben.

klar	**a**	b	**c**	d	**e**	f	g	h	i	j	k	l	m	n	o	p	q	**r**	**s**	t	u	v	w	x	y	z
geheim	**D**	E	**F**	G	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	**U**	**V**	W	X	Y	Z	A	B	C

Aus dem Klartext „caesar“ wird der verschlüsselte Text „FDHVDU“. Dies ist ein Beispiel für eine sog. „symmetrische“ Verschlüsselung. Zur Verschlüsselung und zur Entschlüsselung nutzen Sender und Empfänger der Nachricht den gleichen Schlüssel („Schlüssel-Symmetrie“).

Der Schlüssel im Caesar-Beispiel lautet „Verschiebe um 3 Buchstaben.“ Dieser Schlüssel musste natürlich vor den Feinden geheim gehalten werden. Damit nur Caesars Offiziere seine Nachrichten von Geheimtext in Klartext umwandeln konnten, musste Caesar den Offizieren vorher den geheimen Schlüssel mitgeteilt haben. Caesar konnte das noch recht einfach bewerkstelligen. Bevor er mit seinem Heer in den Krieg zog, teilte er seinen Offizieren in Rom den geheimen Schlüssel im persönlichen Gespräch mit.

Die symmetrische Verschlüsselung hilft jedoch nicht, wenn im heutigen Internet zwei Personen miteinander geheim kommunizieren wollen, die sich nicht kennen und auch keine Gelegenheit haben, vor ihrer Kommunikation einen gemeinsamen („symmetrischen“) geheimen Schlüssel auszutauschen. Im Internet spielen heute zur Verschlüsselung von Nachrichten zwischen anonymen Kommunikationspartnern sog. „asymmetrische“ Verschlüsselungsverfahren eine zentrale Rolle. Dabei herrscht „Schlüssel-Asymmetrie“ – die Verschlüsselung einer Nachricht erfolgt mit einem anderen Schlüssel als die Entschlüsselung der Nachricht.

Bei den asymmetrischen Verfahren besitzt jeder Kommunikationsteilnehmer ein eigenes Schlüsselpaar. Das Schlüsselpaar besteht aus einem öffentlichen Schlüssel (public key) und einem privaten Schlüssel (private key; siehe Abbildung 1).

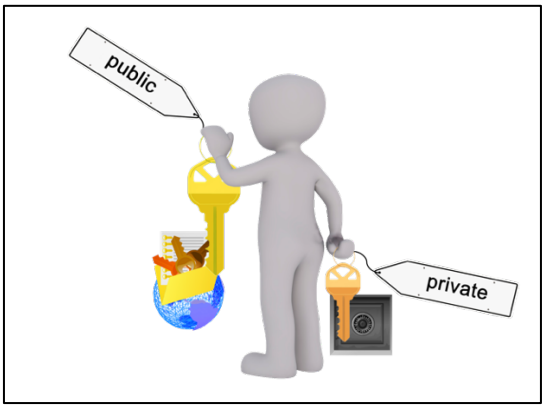

Abb. 1: Jeder hat ein eigens Schlüsselpaar mit Public und mit Private Key

Der öffentliche und der private Schlüssel sind über ein kompliziertes mathematisches Verfahren eindeutig miteinander verbunden. In Kapitel D dieses Dokuments werden Sie sehen, wie Sie sich selbst ein ganz persönliches Schlüsselpaar mit Hilfe der Crypto-Software „Gpg4win“ erstellen. Jedes Schlüsselpaar wird absolut individuell für eine bestimmte einzelne Person erstellt. Aus technischer Sicht ist jeder einzelne Schlüssel eine eigenständige Datei, die eine bestimmte Zeichenfolge enthält.

Jeder Kommunikationsteilnehmer gibt seinen eigenen öffentlichen Schlüssel bekannt. Dies erfolgt häufig durch das Einstellen seiner Datei mit dem öffentlichen Schlüssel in Schlüssel-Listen, die im Internet jeder offen einsehen kann. Im Gegensatz dazu muss jeder Kommunikationsteilnehmer seinen privaten Schlüssel geheim halten. Nur Sie kennen also ihren privaten Schlüssel aus Ihrem persönlichen Schlüsselpaar. Die Datei Ihres privaten Schlüssels ist auf Ihrem persönlichen Rechner gespeichert. Sie sollten also auf Ihren Rechner und die Datei mit Ihrem privaten Schlüssel gut aufpassen.

Ihren privaten Schlüssel halten Sie also geheim, Ihren öffentlichen Schlüssel posaunen Sie bewusst offen hinaus. Jeder, der mit Ihnen asymmetrisch verschlüsselt kommunizieren will, muss Ihren öffentlichen Schlüssel kennen. Abbildung 2 zeigt, wie eine solche Kommunikation funktioniert. Der Sender (Alice) will eine Nachricht an den Empfänger (Bob) schicken. Alice und Bob verfügen jeweils über ein Schlüsselpaar mit eigenem öffentlichen und privaten Schlüssel. Bob hat seinen öffentlichen Schlüssel in einer Schlüssel-Liste im Internet bekannt gemacht.

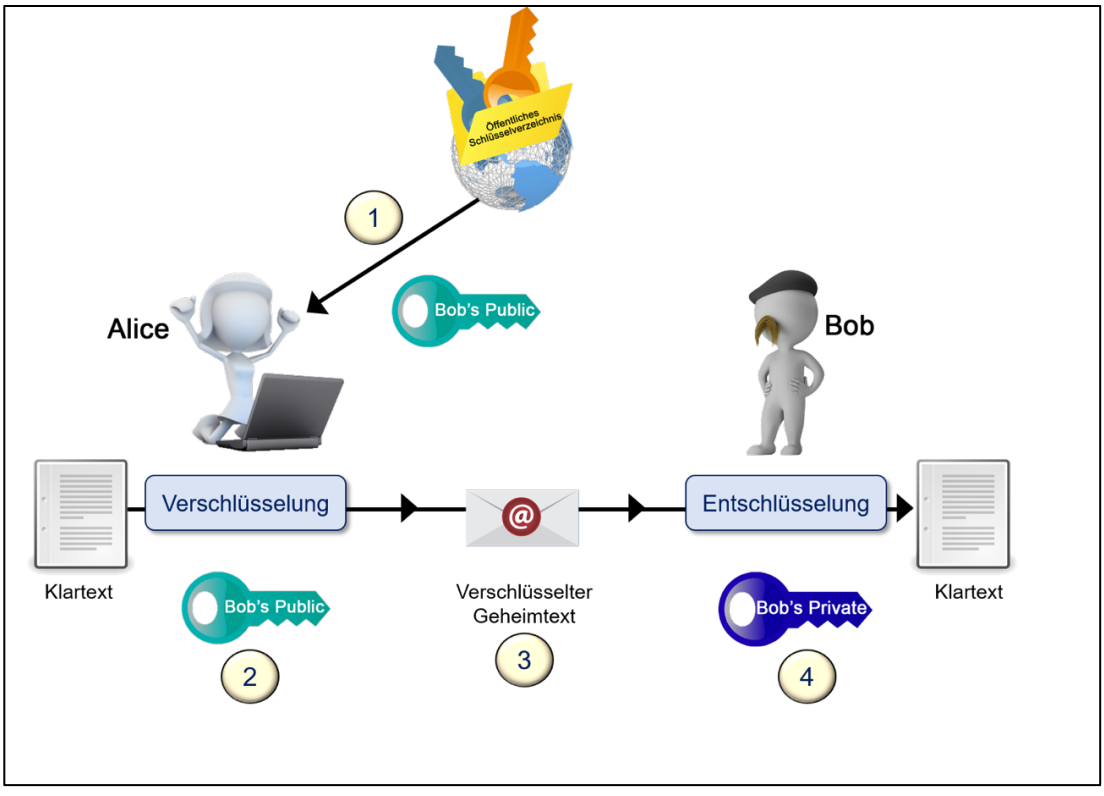

Abb. 2: Funktionsprinzip der asymmetrisch verschlüsselten Kommunikation

(1) Alice holt sich den öffentlichen Schlüssel von Bob aus der öffentlichen Schlüssel-Liste.

(2) Alice schreibt den Klartext ihrer Nachricht „Klartext“ und verschlüsselt ihn mit dem öffentlichen Schlüssel von Bob. Es entsteht eine Nachricht mit dem Geheimtext.

(3) Alice schickt die Datei mit dem Geheimtext per E-Mail an Bob. Wenn jemand unterwegs die Datei abgreift und öffnet, findet er nur den unverständlichen Geheimtext.

(4) Nur Bob kann die Geheimtext-Datei mit seinem privaten Schlüssel in Klartext umwandeln.

B Was brauchen Sie?

In diesem Dokument wird Ihnen erklärt, wie Sie auf einem Apple-Rechner mit dem Betriebssystem macOS Dateien verschlüsseln, entschlüsseln und signieren können. Sie brauchen dafür folgendes Equipment:

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. Internet Explorer, Microsoft Edge, Chrome oder Firefox.

Crypto-Software: Auf Ihrem Rechner muss eine Software installiert sein, die Dateien verschlüsselt, entschlüsselt und signieren kann. Wir verwenden als Crypto-Software „Gpg4win“ der Gpg4win-Initiative.

C Installation der Crypto-Software „Gpg4win“

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 3.

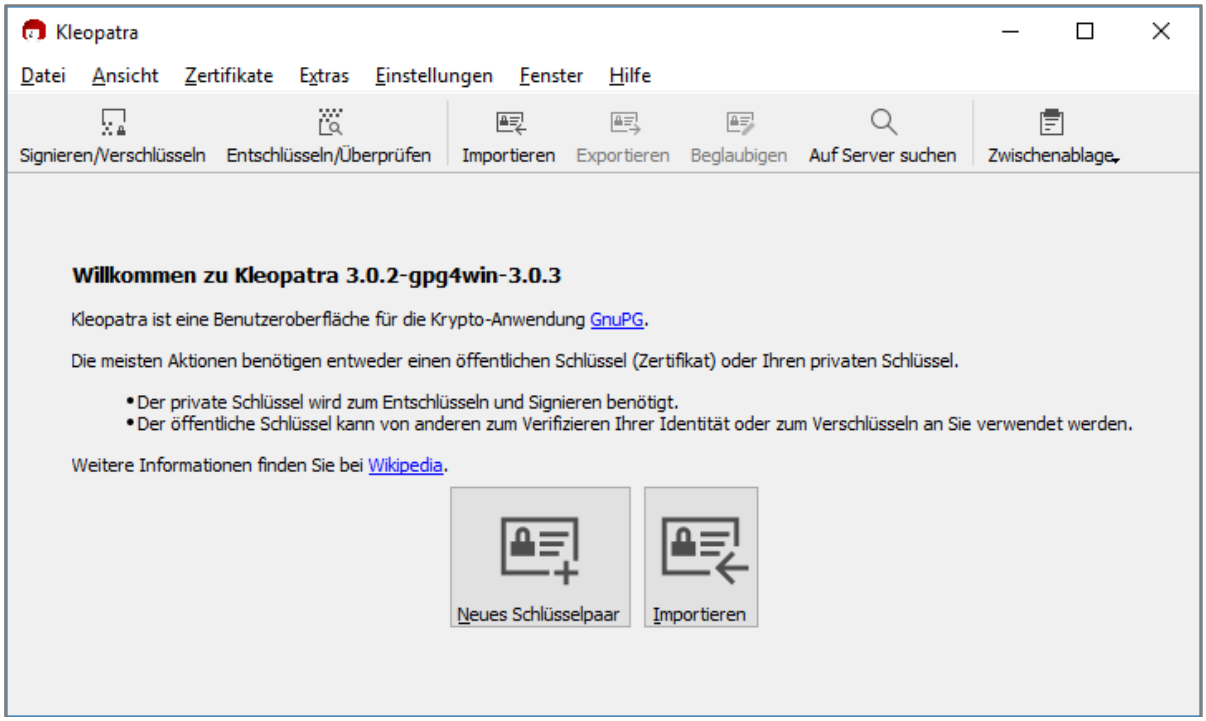

Abb. 3: Der Start-Bildschirm von Kleopatra

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.

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 4).

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 5).

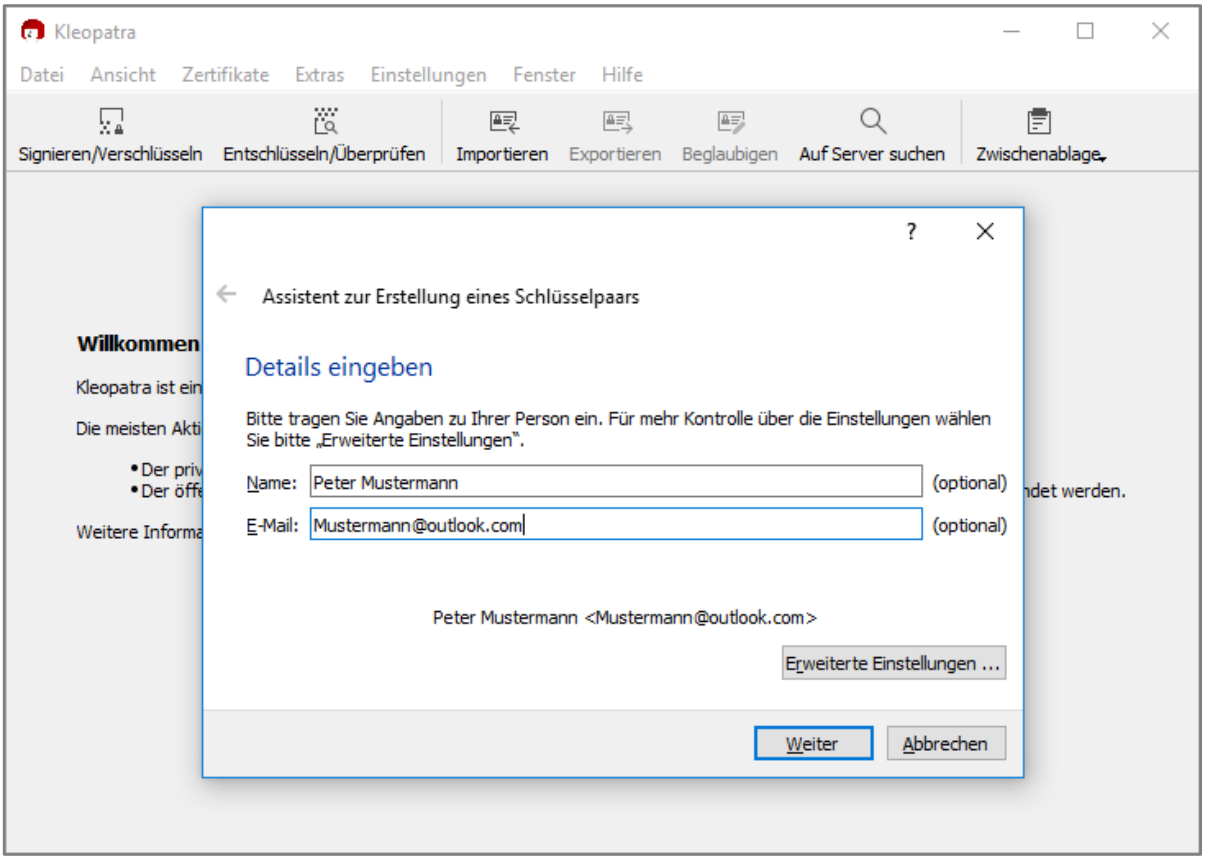

Abb. 4: Ein neues Schlüsselpaar erstellen

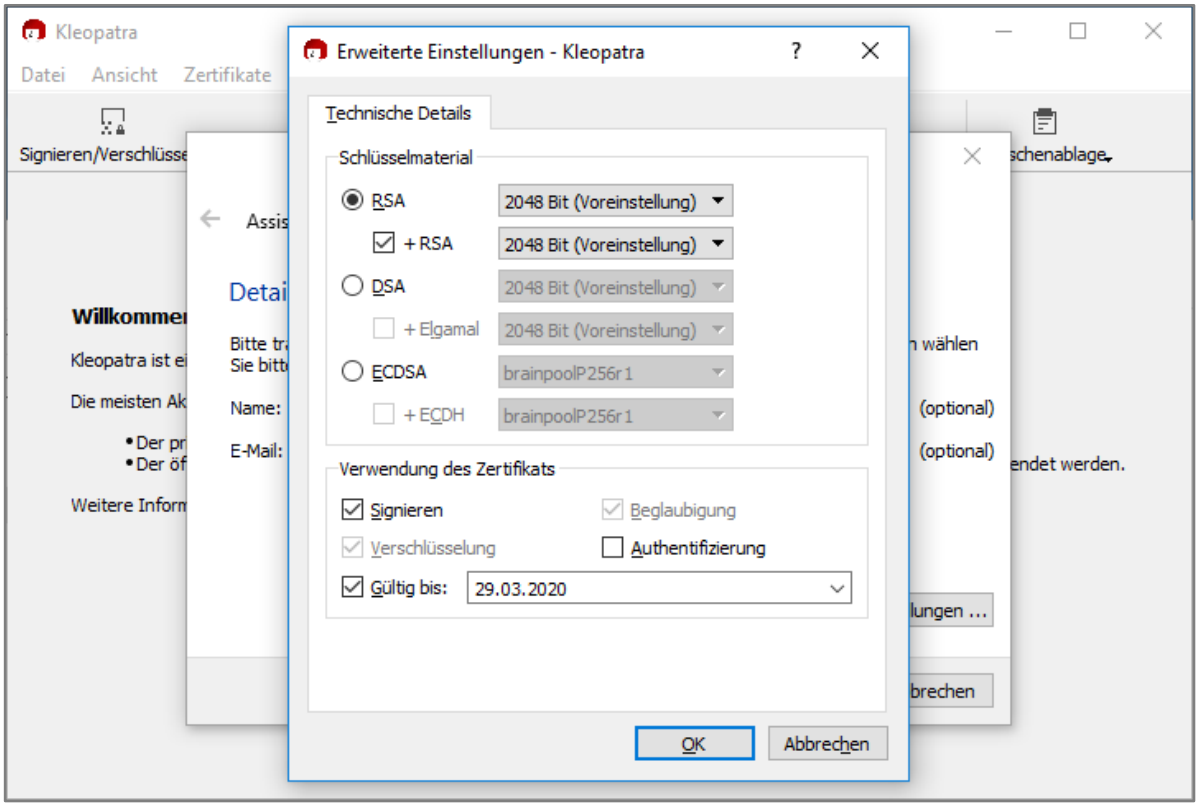

Abb. 5: Ein neues Schlüsselpaar erstellen – Erweiterte Einstellungen

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 6. Kleopatra benötigt eine Passphrase, 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.

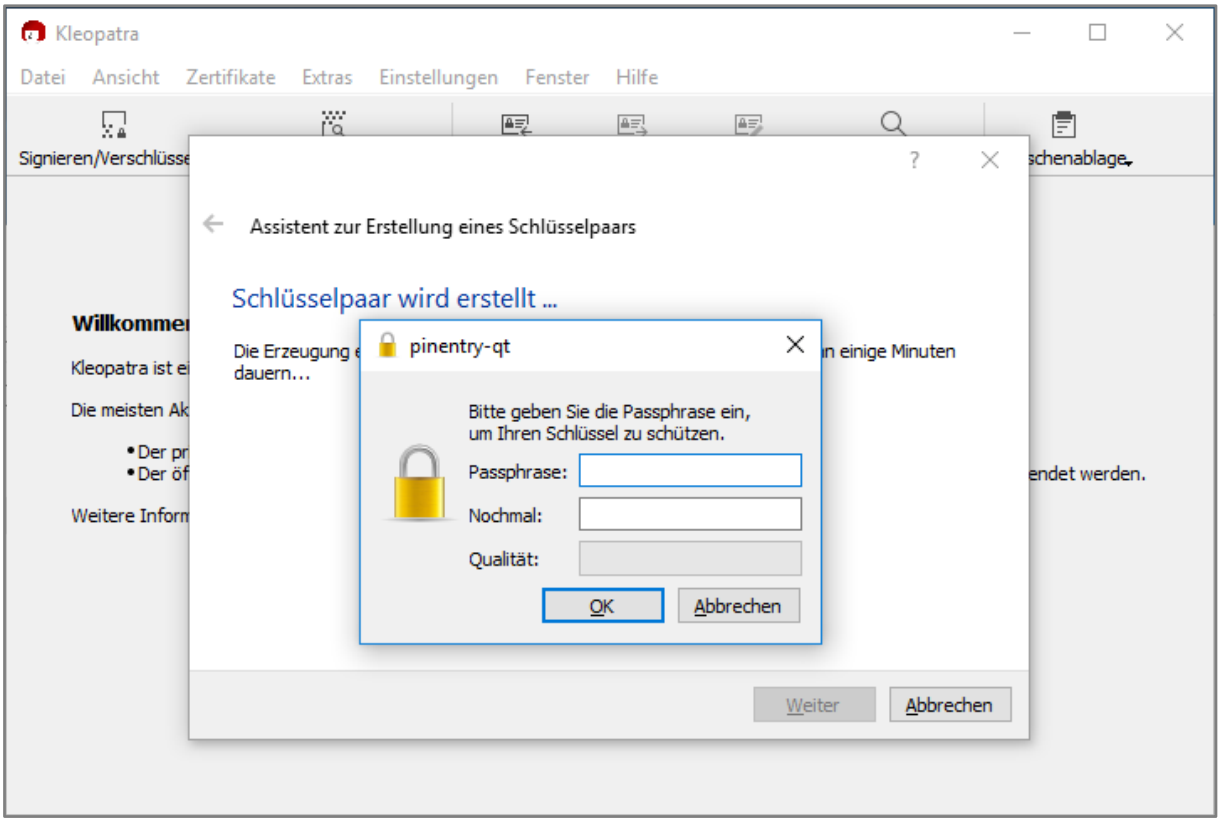

Abb. 6: Ein neues Schlüsselpaar erstellen – Passphrase festlegen

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 7). Sie können jederzeit später aus dem Programm Kleopatra heraus Ihre öffentlichen Schlüssel auf Schlüssel-Server hochladen.

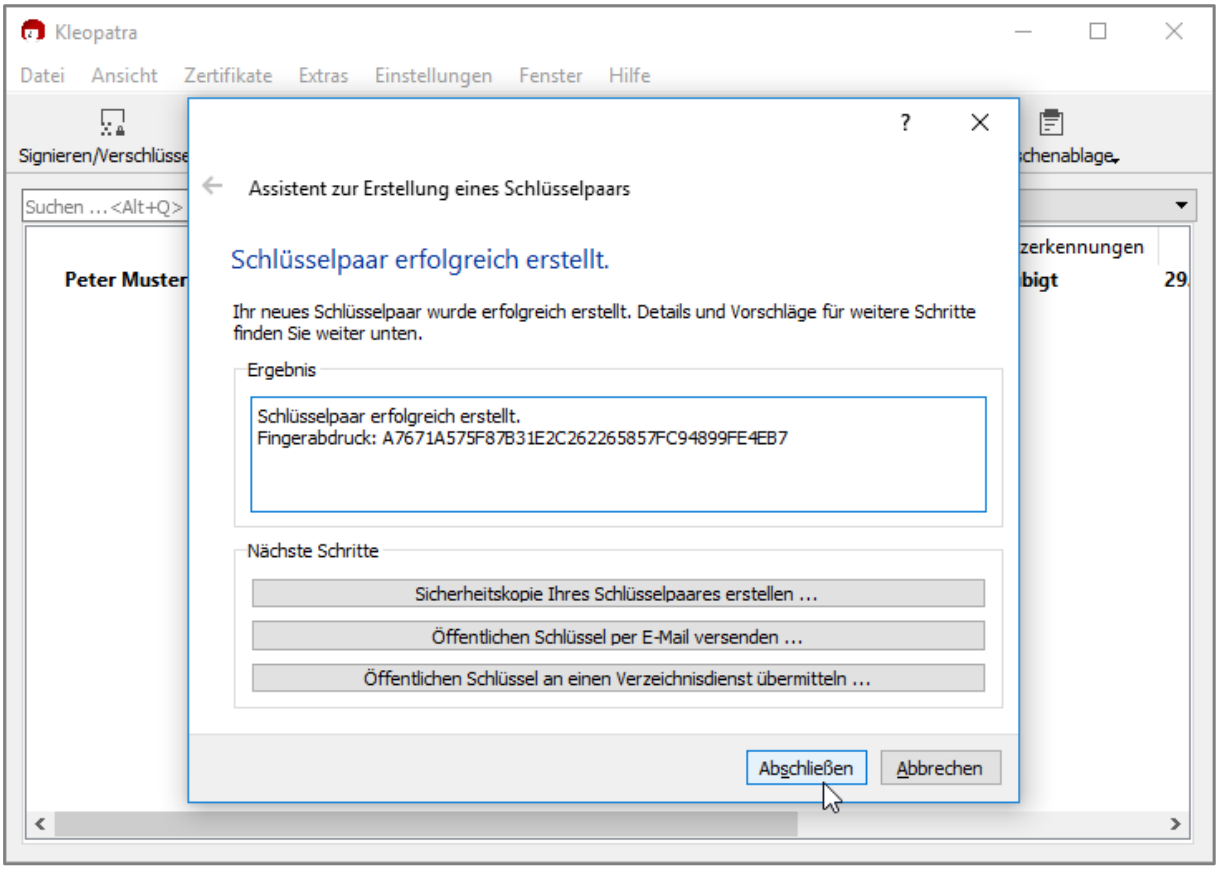

Abb. 7: Ihr Schlüsselpaar wurde erfolgreich erstellt.

Abbildung 8 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.

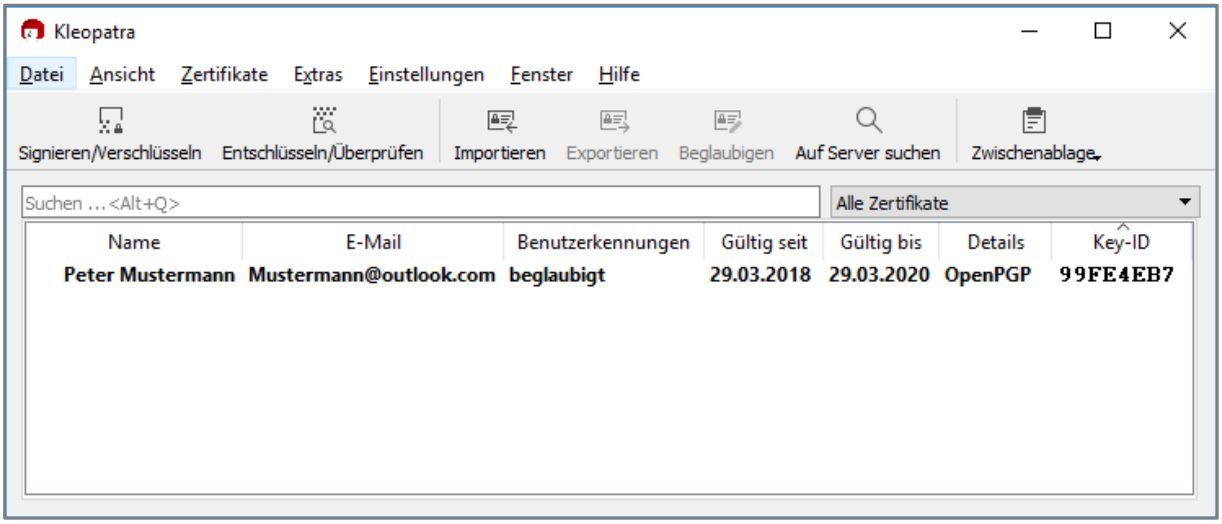

Abb. 8: Ihre Schlüssel in Kleopatra

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 dies funktioniert.

E Verschlüsseln einer Datei

Eine Verschlüsselung von Dateien stellt sicher, dass niemand außer dem gewünschten Adressaten, die Inhalte der Datei lesen kann (Vertraulichkeit). Um eine Datei zu verschlüsseln, benötigen Sie, wie in Kapitel D beschrieben, einen öffentlichen Schlüssel. Sie können also für jeden Empfänger Dateien, E-Mails oder Texte verschlüsseln, wenn Sie den öffentlichen Schlüssel des Empfängers besitzen. In diesem Kapitel verschlüsseln Sie eine Datei mit Ihrem eigenen Schlüssel, damit Sie diese Datei testweise in Kapitel F entschlüsseln können. Bedenken Sie: Sie können nur diejenigen Dateien entschlüsseln, die mit Ihrem eigenen öffentlichen Schlüssel verschlüsselt wurden.

Navigieren Sie mit Ihrem Windows Explorer zu einer beliebigen Datei, welche Sie gerne schützen möchten. Sie können jede beliebige Art von Datei verschlüsseln. Es kann sich dabei um ein Word-Dokument, eine PDF-Datei, eine ZIP-Datei oder jede beliebige andere Datei handeln. Per Rechtsklick im Explorer auf diese Datei können Sie unter dem Eintrag „Mehr GpgEX Optionen“ verschiedene Funktionen der GpgEX (Funktionserweiterung des Windows Explorers durch Gpg4win) auswählen. Um eine Datei zu verschlüsseln, wählen Sie den Eintrag „Verschlüsseln“ (siehe Abbildung 9).

Nach Klick auf den Eintrag „Verschlüsseln“ öffnet sich ein Fenster von Kleopatra. Wählen Sie nun den öffentlichen Schlüssel aus, mit dem Sie Ihre Datei verschlüsseln möchten. In diesem Fall sollte es Ihr öffentlicher Schlüssel sein, da Sie diese Datei in Kapitel F wieder entschlüsseln möchten. Wählen Sie Ihren öffentlichen Schlüssel per Klick auf die Checkbox „Für mich verschlüsseln:“ aus und entfernen Sie in den jeweils anderen Zeilen die Haken. Im unteren Bereich des Fensters wird Ihnen der Ausgabeort der verschlüsselten Datei angezeigt. Bestätigen Sie mit „Verschlüsseln“ (siehe Abbildung 10). Eine abschließende Meldung bestätigt Ihnen, ob der Verschlüsselungsprozess erfolgreich war. Die neu entstandene Datei mit der Endung „.gpg“ beinhaltet nun Ihre schützenswerte Datei in einem verschlüsselten Format. Diese Datei kann nun nur noch mit Ihrem privaten Schlüssel entschlüsselt werden.

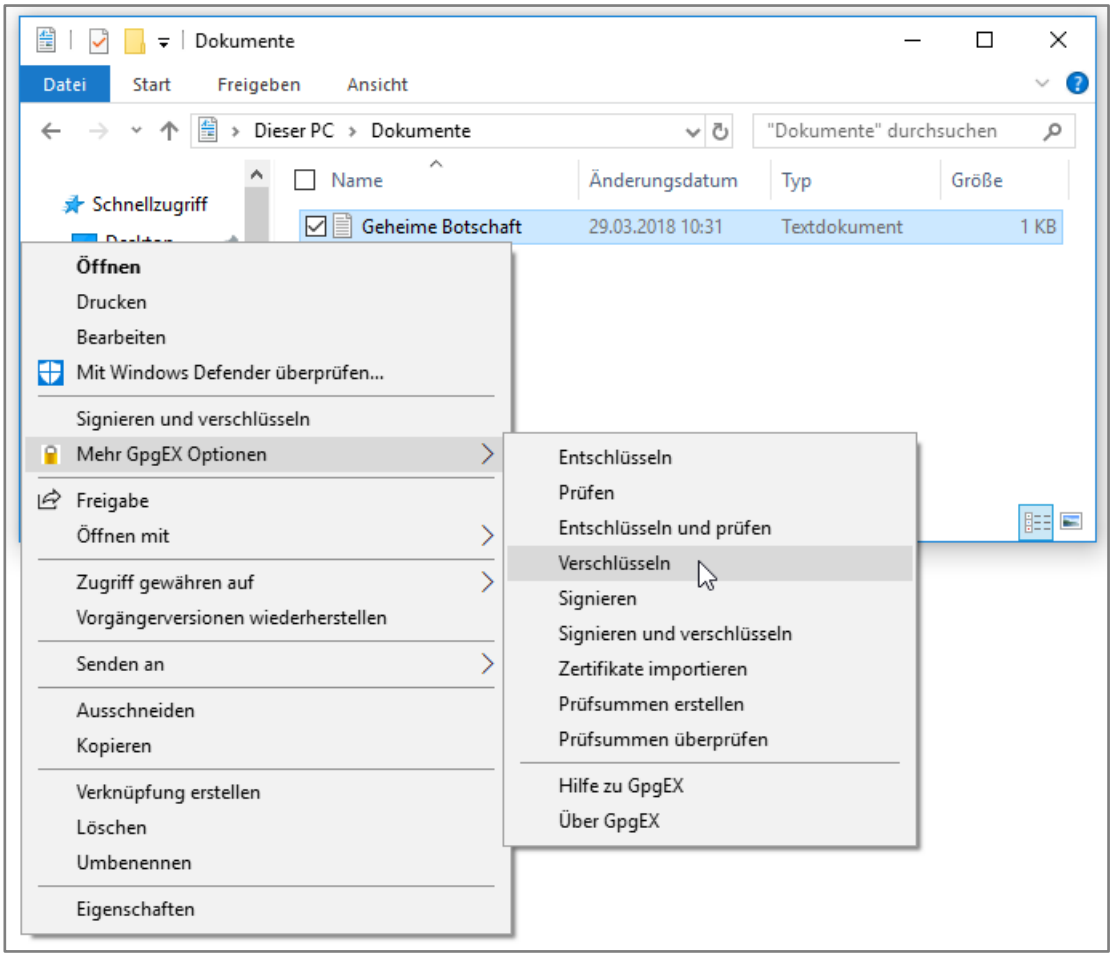

Abb. 9: GpgEX – Gpg4win-Erweiterung im Windows Explorer

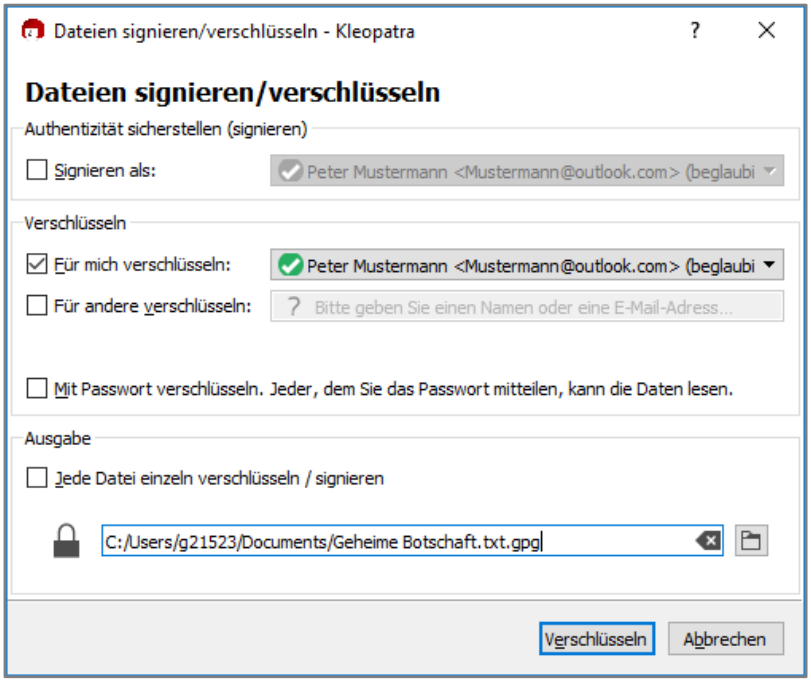

Abb. 10: Kleopatra – Schlüsselauswahl zur Verschlüsselung

F Entschlüsseln einer Datei

Wie Ihnen bereits im vorangegangen Kapitel erläutert wurde, benötigen Sie zum Verschlüsseln von Dateien, Texten oder E-Mails den öffentlichen Schlüssel des Empfängers, dem Sie Ihre Datei schicken wollen. Zum Entschlüsseln von verschlüsselten Dateien 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 verschlüsselt wurden.

Um nun eine Datei zu entschlüsseln, navigieren Sie in Ihrem Windows Explorer zur verschlüsselten Datei aus Kapitel E. Per Rechtsklick auf diese Datei können Sie unter „Mehr GpgEX Optionen“ die Option „Entschlüsseln“ auswählen (siehe Abbildung 11).

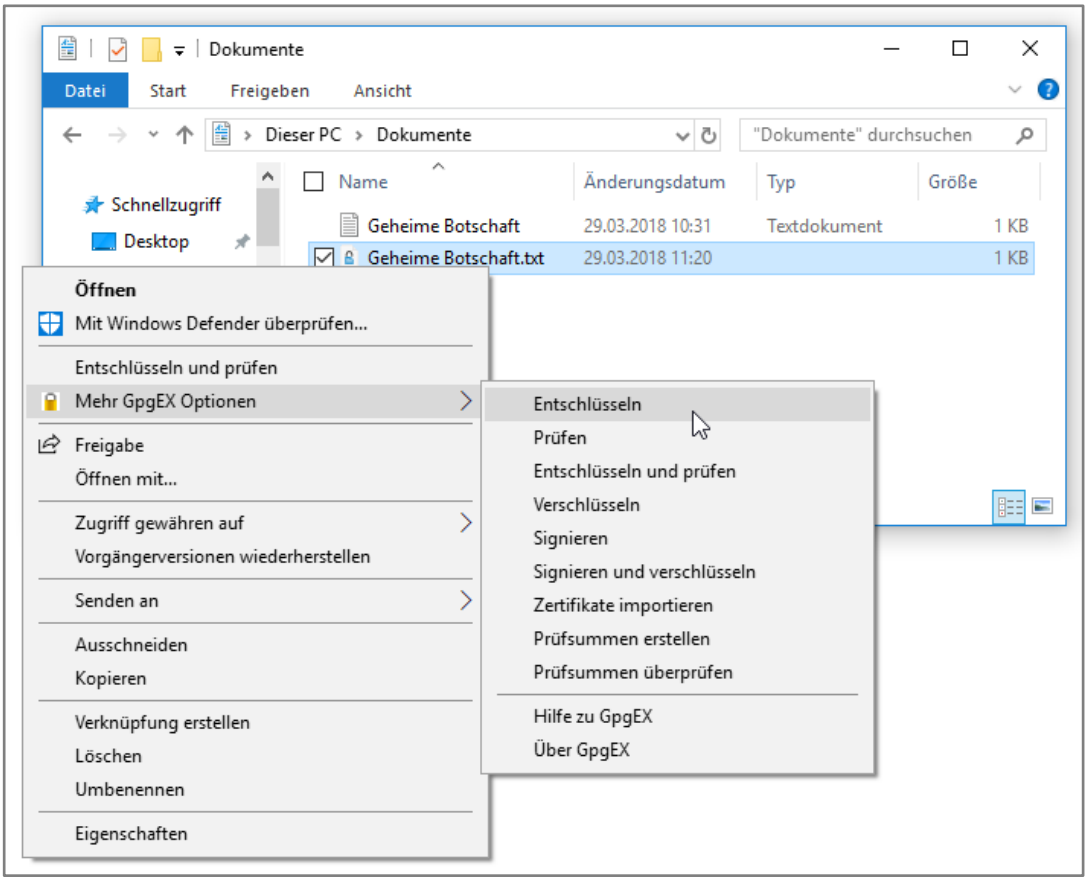

Abb. 11: GpgEX – Gpg4win-Erweiterung im Windows Explorer

Nach Klick auf „Entschlüsseln“ öffnet sich ein Fenster von Kleopatra (siehe Abbildung 12). Wie bereits in Kapitel D beschrieben, schützt Kleopatra Ihre Schlüsselpaare mit dem jeweils von Ihnen bei der Erstellung vergebenen Passphrase. Geben Sie daher nun im Feld „Passphrase:“ die Passphrase ein, die Sie zum Erstellen den Schlüsselpaars verwendet haben. Bestätigen Sie anschließend mit „OK“. Ein letztes Fenster zeigt Ihnen an, ob die Datei erfolgreich ent-

schlüsselt wurde. Abschließend müssen Sie mithilfe des Button „Alles speichern“ Ihre entschlüsselten Daten auf Ihre Festplatte speichern (siehe Abbildung 13). Wenn der Prozess erfolgreich war, erhalten Sie Ihre ursprüngliche Datei im unverschlüsselten und lesbarem Format zurück.

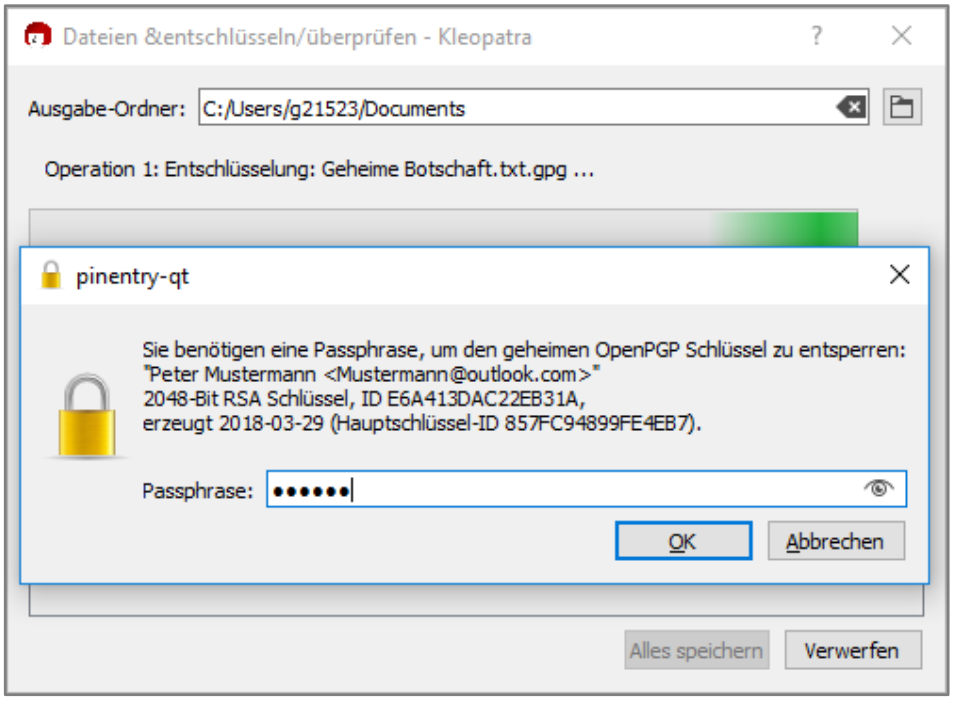

Abb. 12: Kleopatra – Entsperren Ihres privaten Schlüssels

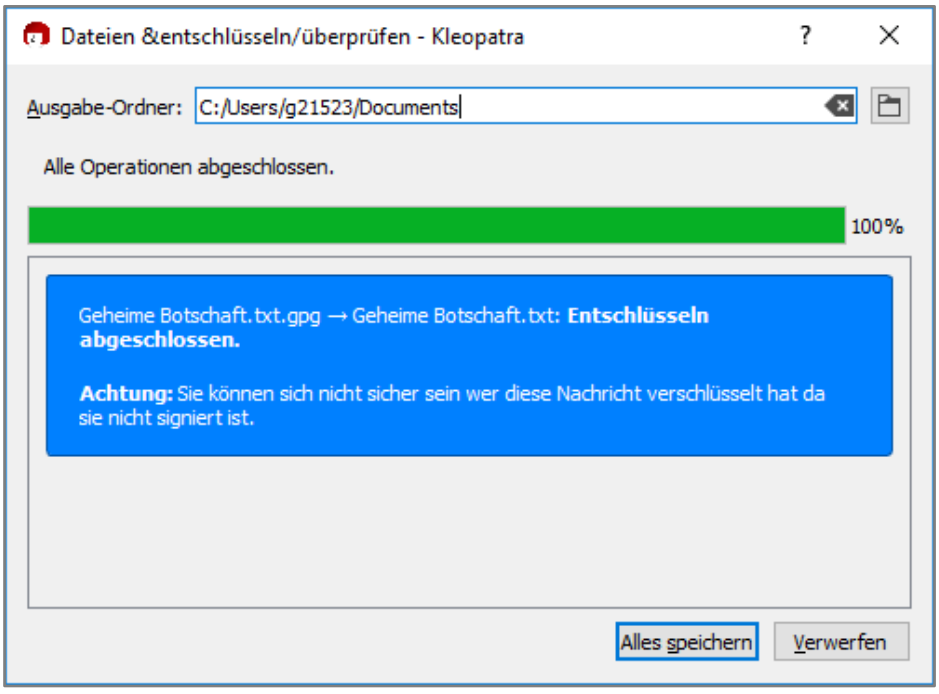

Abb. 13: Kleopatra – Speichern der entschlüsselten Datei

G Signieren einer Datei

Damit sichergestellt werden kann, dass eine bestimmte Datei von Ihnen und niemand anderem stammt (Authentizität) und nicht manipuliert wurde (Integrität), sollten Sie die betreffende Datei signieren. Signaturen für Dateien werden mit privaten Schlüsseln erstellt. Sie können jede Art von Dateien signieren, es muss nicht zwingend eine verschlüsselte Datei sein. So können Sie Word-, PowerPoint-, PDF-, ZIP-, TXT-Dateien oder jede andere beliebige Datei signieren.

Wenn Sie eine Datei in einem Schritt verschlüsseln und signieren möchten, hilft Ihnen die Windows-Explorer-Erweiterung GpgEX. Vergleichen Sie dazu Abbildung 10 und 11. Klicken Sie zum Verschlüsseln und Signieren auf den Eintrag „Signieren und verschlüsseln“.

Wenn Sie eine nicht verschlüsselte Datei beliebigen Formats oder eine bereits verschlüsselte Datei nachträglich signieren möchten, hilft Ihnen ebenfalls die Windows Explorer-Erweiterung GpgEX. Navigieren Sie dazu in Ihrem Windows Explorer zur verschlüsselten Datei aus Kapitel E. Wie gewohnt können die Funktionen von GpgEX per Rechtsklick auf die Datei aufgerufen werden. Wählen Sie den Eintrag „Signieren“ (siehe Abbildung 14).

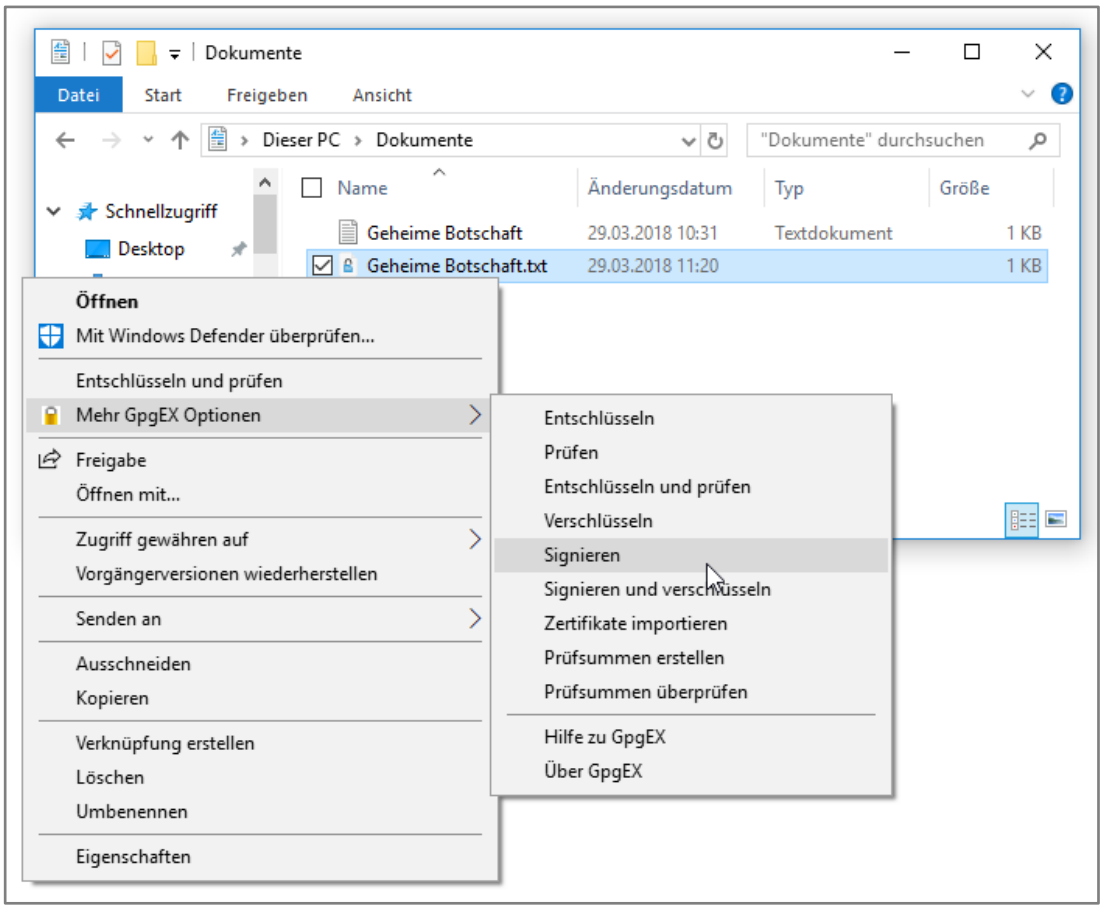

Abb. 14: GpgEX – Gpg4win-Erweiterung im Windows Explorer

Nach Klick auf „Signieren“ öffnet sich ein Fenster von Kleopatra. An dieser Stelle müssen Sie Kleopatra nun mitteilen, welcher Ihrer privaten Schlüssel zum Signieren der ausgewählten Datei verwendet werden soll. Wählen Sie Ihren in Kapitel D erstellten privaten Schlüssel in der Zeile „Signieren als:“ aus. Unter Ausgabe sehen Sie den Pfad, in dem die Signatur-Datei gespeichert wird. Klicken Sie anschließend auf „Signieren“ (siehe Abbildung 15).

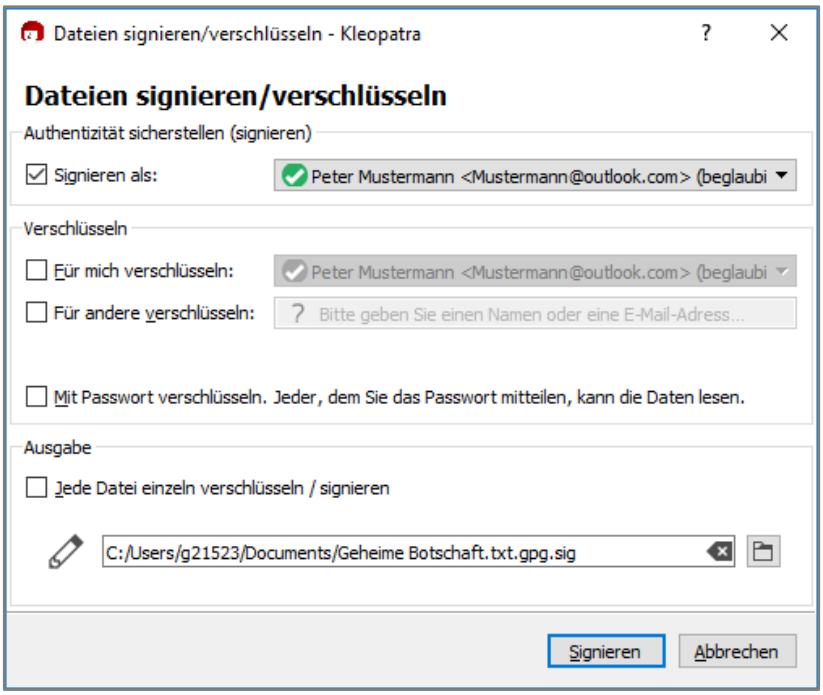

Abb. 15: Kleopatra – Auswahl des signierenden Schlüssels

Unter Umständen sehen Sie nach Klick auf den „Signieren“-Button erneut Abbildung 12. Dies kann vorkommen, wenn Sie längere Zeit nicht an Ihrem Rechner eingeloggt waren oder Ihre Passphrase nicht gespeichert wurde. In diesem Fall geben Sie Ihre Passphrase erneut ein und bestätigen Sie mit „OK“. Eine letzte Meldung zeigt Ihnen an, dass der Signaturprozess erfolgreich war. Kleopatra hat für Sie eine Datei mit gleichem Dateinamen wie die verschlüsselte Datei, aber mit einer anderen Endung erstellt. Die Endung „.sig“ zeigt an, dass es sich um eine Datei mit Signaturdaten handelt. Diese Datei enthält keine Inhaltsdaten der ursprünglichen verschlüsselten Datei, sondern dient lediglich zum Verifizieren der Echtheit der verschlüsselten Datei. Wenn die „.sig“-Datei und die zugehörige verschlüsselte Datei in einem Ordner liegen, kann per Doppelklick auf die .sig-Datei überprüft werden, ob die verschlüsselte Datei von demjenigen signiert wurde, der die Datei auch verschlüsselt hat.

Wenn Sie also möchten, dass der Empfänger Ihrer Datei deren Herkunft prüfen kann, senden Sie die von Ihnen erstellte .sig-Datei mit der von Ihnen verschlüsselten Datei an den Empfänger. Der kann dann mithilfe der .sig-Datei sicherstellen, dass genau Sie diese Datei verschlüsselt und signiert haben.

H Gültigkeit und Bezug von öffentlichen Schlüsseln

Wie bereits in den vorangegangen Kapiteln erläutert, benötigen Sie mindestens einen öffentlichen Schlüssel, um Dateien beliebiger Art zu verschlüsseln. In Kapitel E haben Sie bereits eine Datei verschlüsselt. Dies erfolgte jedoch mit Ihrem eigenen öffentlichen Schlüssel – der Bezug des öffentlichen Schlüssels eines Kommunikationspartners entfiel damit. Da das Verschlüsseln von Dateien mit dem eigenen öffentlichen Schlüssel jedoch nicht der Regelfall ist, soll Ihnen dieses Kapitel erläutern, wie Sie öffentliche Schlüssel Ihrer Kommunikationspartner in Kleopatra importieren und beglaubigen.

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 die Datei 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. 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. Hier sehen Sie eine Beispiel-Schlüssel-ID: `99FE4EB7`

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 ein Beispiel-Fingerabdruck (siehe auch Abbildung 16):

```
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 16). 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: Klicken Sie dazu per Rechtsklick auf einen Schlüssel und wählen Sie den Eintrag „Beglaubigen...“. Selbst 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 dem Schüssel fest.

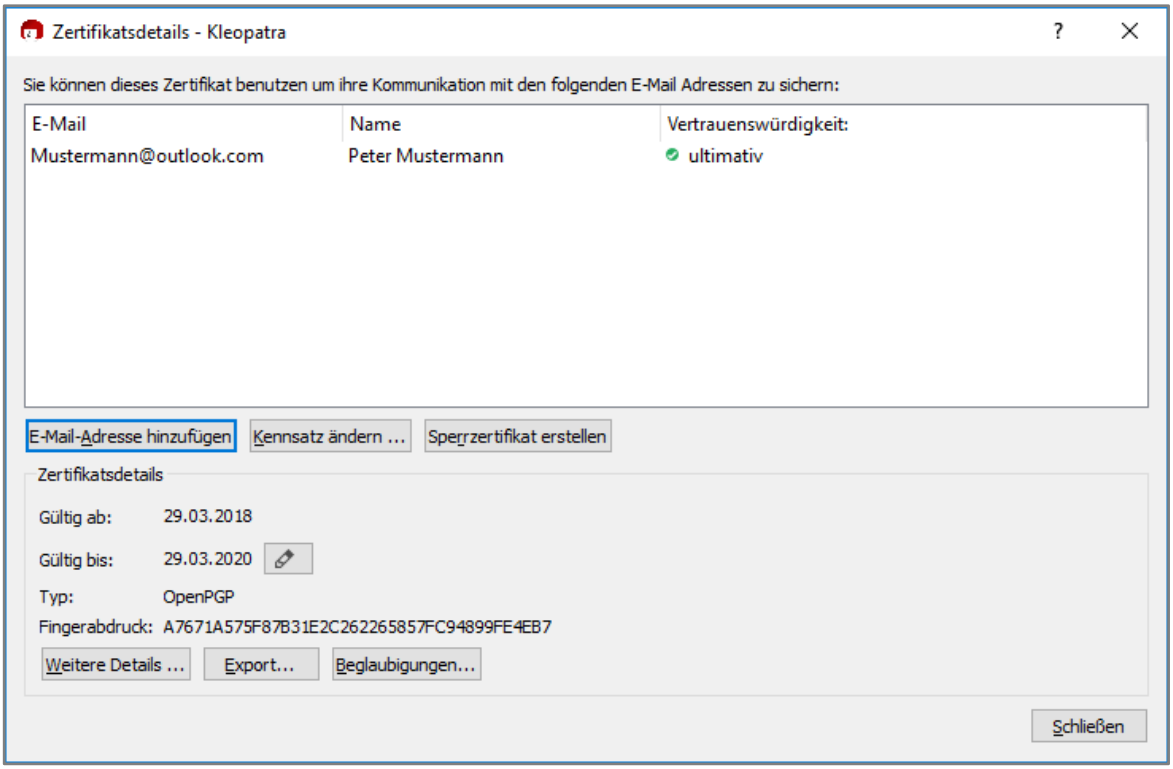

Abb. 16: Kleopatra – Details eines Schlüsselpaars

Möchten Sie einen neuen Schlüssel z. B. eines Geschäftspartners 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 17).

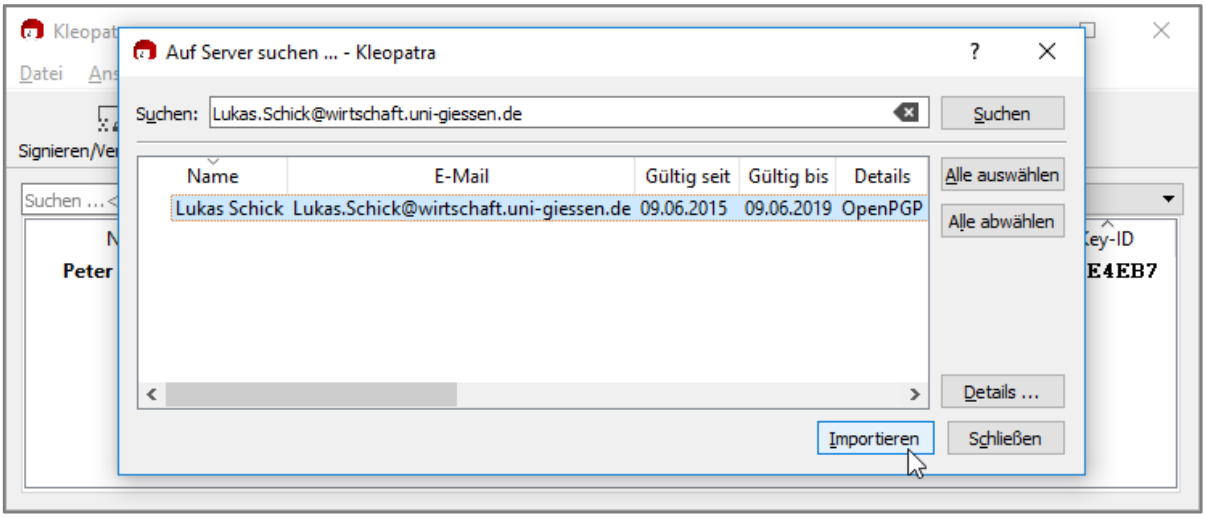

Abb. 17: Kleopatra – Importieren eines Schlüssels

Direkt nach Klicken des „Importieren“-Buttons öffnet sich ein Assistenzfenster von Kleopatra zum Festlegen des Vertrauens gegenüber dem importieren Schlüssel (siehe Abbildung 18).

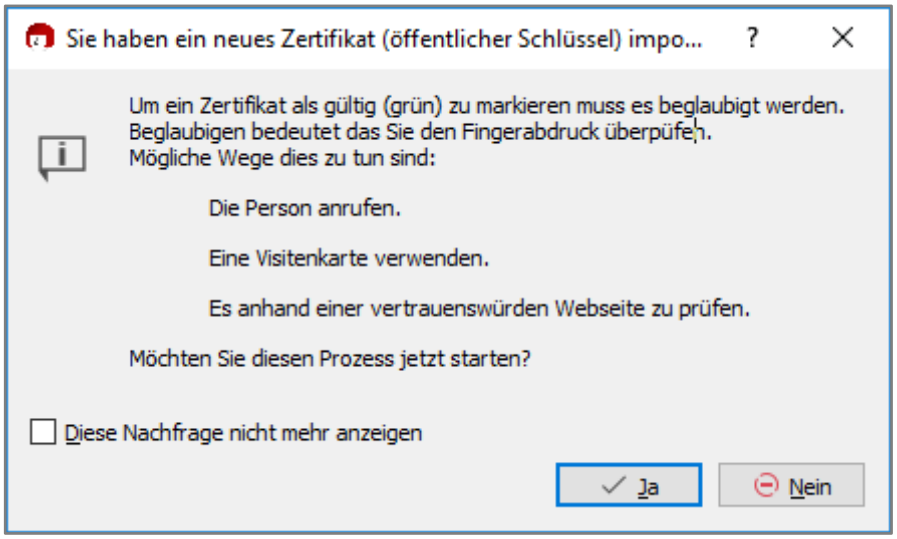

Abb. 18: Kleopatra – Beglaubigen eines Schlüssels nach Import (1)

Klicken Sie auf „Ja“, um den Beglaubigungsprozess zu starten. Das nächste Fenster (Abbildung 19) zeigt Ihnen den zu beglaubigenden Schlüssel an. Unterhalb sehen Sie den Fingerabdruck des Schlüssel. 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 anderen Weg (E-Mail, Telefon, Kurznachricht etc.) übermittelt worden sein.

Im darauf folgenden Fenster (siehe Abbildung 20) wählen Sie aus, wie dieser Schlüssel beglaubigt werden soll. 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“ (siehe Abbildung 20).

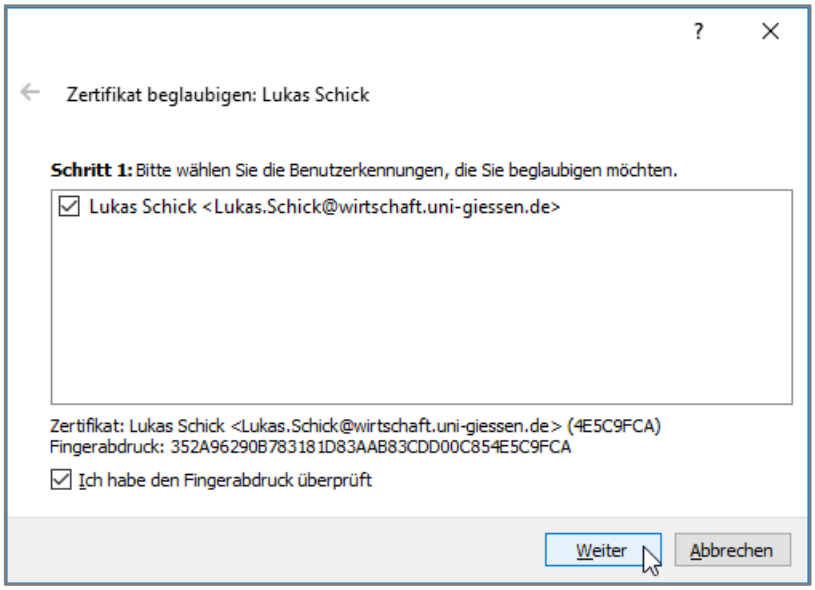

Abb. 19: Kleopatra – Beglaubigen eines Schlüssels nach Import (2)

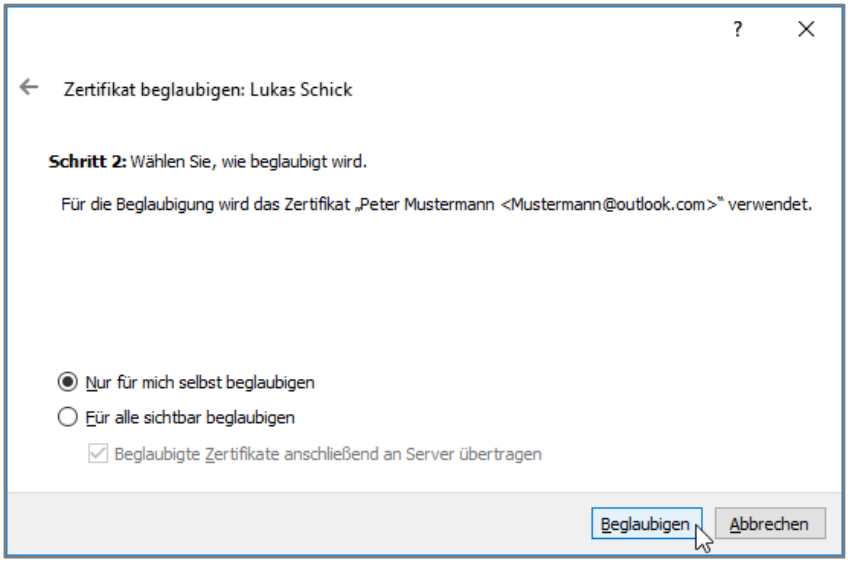

Abb. 20: Kleopatra – Beglaubigen eines Schlüssels nach Import (3)

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.

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 Forschungsarbeiten, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr- und Vortragsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Univ. Prof. Dr. Axel C. Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen und Kritik 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 dem Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Adresse http://wi.uni-giessen.de.