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

Schwickert, Axel; Schick, Lukas

macOS – Verschlüsseln, Entschlüsseln und Signieren von Dateien

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 5 / 2017
ISSN 1613-6667

Arbeitspapiere WI Nr. 5 / 2017

Autoren: Schwickert, Axel; Schick, Lukas

Titel: macOS – Verschlüsseln, Entschlüsseln und Signieren von Dateien

Zitation: Schwickert, Axel; Schick, Lukas: macOS – Verschlüsseln, Entschlüsseln und Signieren von Dateien, in: Arbeitspapiere WI, Nr. 5/2017, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2017, 14 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 Apple-Rechnern mit dem Betriebssystem macOS Dateien verschlüsselt, entschlüsselt und signiert werden. Dazu wird die Crypto-Software „GPG Suite“ vom Hersteller GPGTools verwendet.

Schlüsselwörter: Verschlüsselung, Signatur, Schlüssel, Schlüsselpaar, öffentlich, privat, symmetrisch, asymmetrisch, macOS, GPG Suite, GPGTools

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).

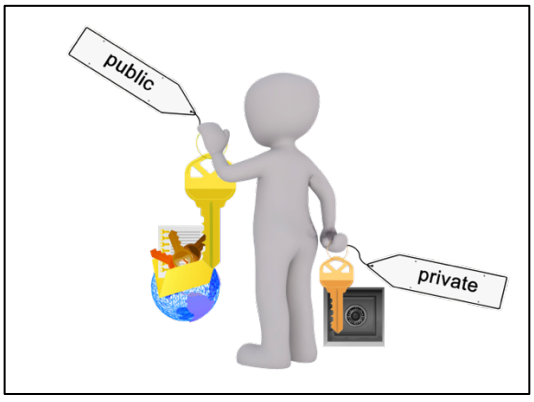

Abb. 1: Jeder hat ein eigens Schlüsselpaar mit Public und mit Private Key

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 „GPG Suite“ 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.

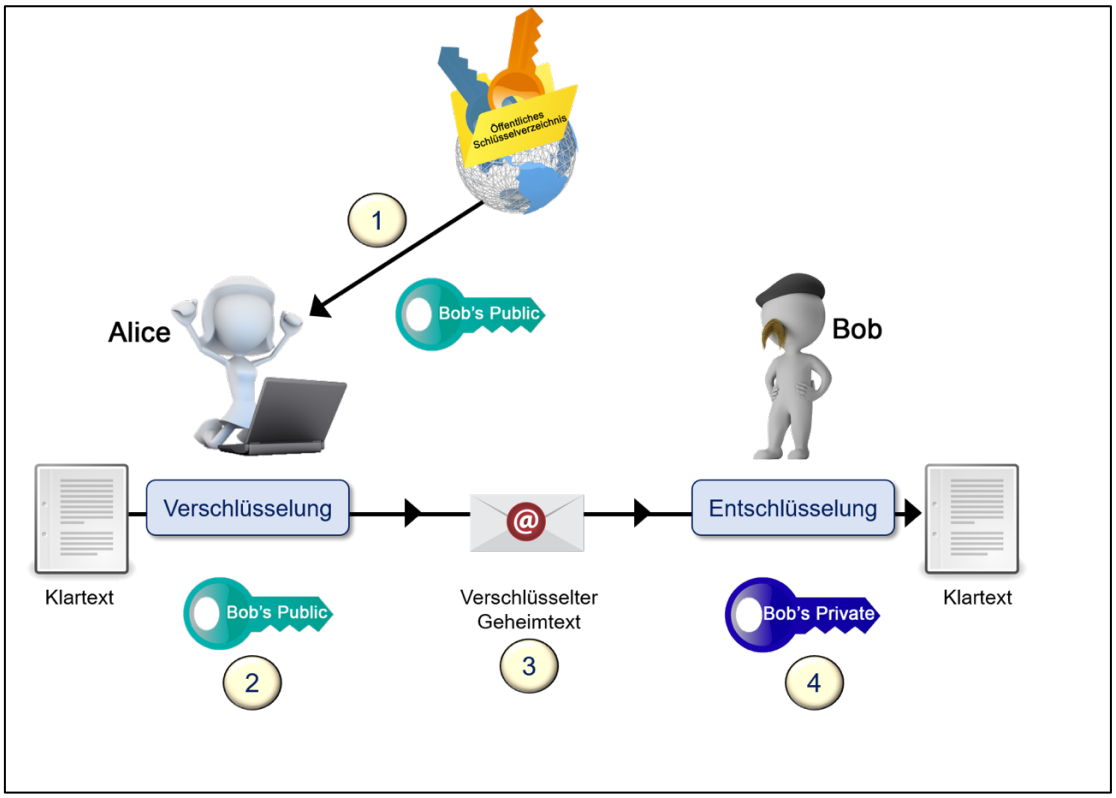

Abb. 2: Funktionsprinzip der asymmetrisch verschlüsselten Kommunikation

(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 von Apple wie z. B. einen iMac oder ein MacBook mit der neuesten Version des Betriebssystems macOS. Ihr Rechner braucht eine Internet-Anbindung.

Web-Browser: Auf Ihrem Rechner muss ein Web-Browser in neuester Version installiert sein wie z. B. Safari, 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 die „GPG Suite“ vom Hersteller GPGTools.

C Installation der Crypto-Software „GPG Suite“

Laden Sie zunächst auf https://gpgtools.org die neueste Version von GPG Suite herunter. Starten Sie die Installation, indem Sie die heruntergeladene .dmg-Datei doppelklicken. Folgen Sie den Installationsanweisungen. Nach erfolgter Installation können Sie die .dmg-Installationsdatei in den Papierkorb legen.

Durch diese Installation wurde auf Ihrem Rechner das Programm „GPG Keychain“ installiert. Den Startbildschirm davon sehen Sie in Abbildung 3.

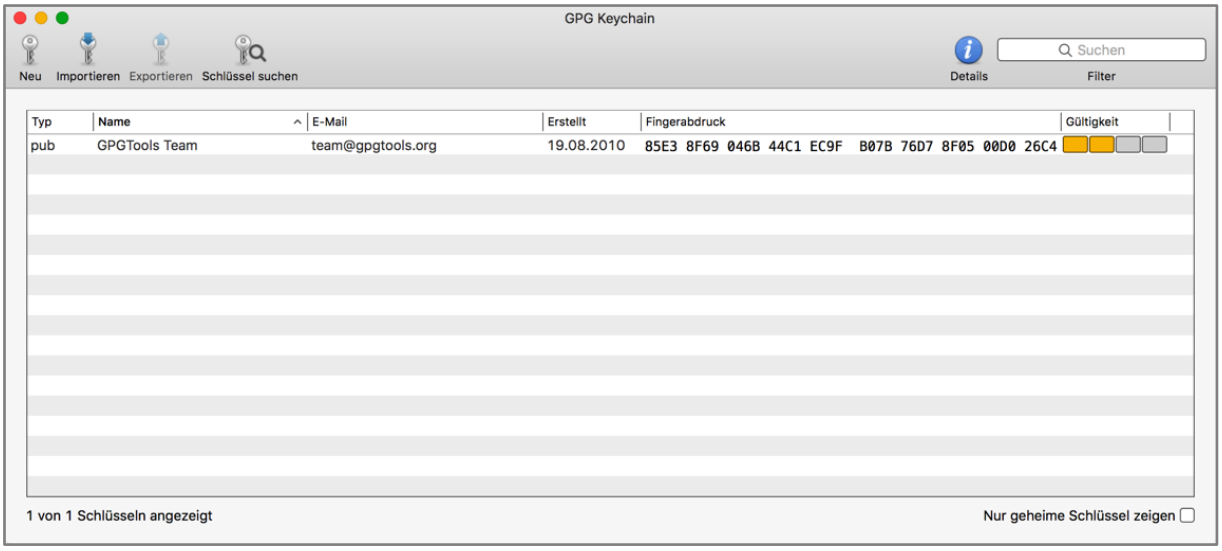

Abb. 3: Der Start-Bildschirm von GPG Keychain

Die GPG Suite enthält neben dem Programm GPG Keychain noch weitere Programme, die bei der Installation automatisch mitinstalliert werden: GPGMail ist eine Funktionserweiterung für Apple Mail und ermöglicht es Ihnen, Ihre E-Mails bei Bedarf mit wenigen Klicks zu verschlüsseln. MacGPG ist eine Anwendung für die Kommandozeile und richtet sich an fortgeschrittene Nutzer der GPG Suite oder an Nutzer, die keine grafische Benutzeroberfläche benötigen. GPG Services ist ein Plugin, welches GPG Suite-Funktionalitäten in andere Anwendungen integriert. Zum Beispiel stellt GPG Services sicher, dass Sie notwendige neue Funktionen zur Verfügung gestellt bekommen, wenn Sie in Ihrem Finder per Rechtsklick auf eine Datei klicken.

D Ein Schlüsselpaar erstellen

Über die Funktion „Neu“ im Start-Bildschirm von GPG Keychain links oben erstellen Sie für sich ein neues Schlüsselpaar (siehe Abbildung 4).

Geben Sie Ihren Namen, Ihre Uni-E-Mail-Adresse und ein starkes Passwort ein. Wenn Sie „Erweiterte Optionen“ ausklappen, sehen Sie, dass standardmäßig ein RSA-Schlüsselpaar mit 4096 Bit Länge erstellt wird, das ein Verfallsdatum hat.

Mit Klick auf den Button „Schlüssel erstellen“ beginnt das Programm, Ihr Schlüsselpaar zu errechnen und zeigt anschließend den Bildschirm aus Abbildung 5. Sie sehen die etwas irreführende Meldung „Ihr Schlüssel wurde erfolgreich erstellt“. Es müsste richtigerweise heißen „Ihr Schlüsselpaar wurde erfolgreich erstellt.“ Denn genau das hat GPG Keychain gerade gemacht. Das Programm hat eine Datei für einen öffentlichen und eine Datei für einen privaten Schlüssel erzeugt und diese beiden Dateien auf Ihrem Rechner mit Ihrem gewählten Passwort verschlüsselt abgespeichert.

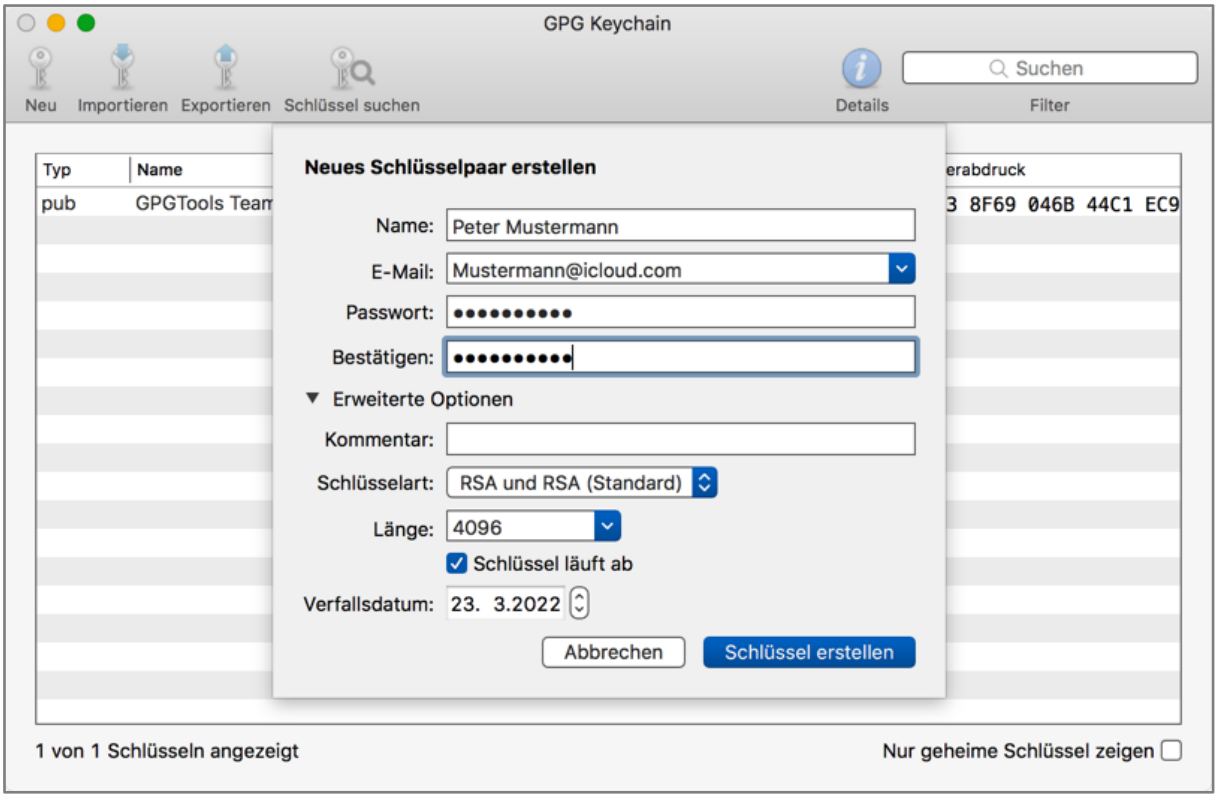

Abb. 4: Ein neues Schlüsselpaar erstellen

Abb. 5: Ihr Schlüsselpaar wurde erfolgreich erstellt.

GPG Keychain bietet Ihnen 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 auf den Button „Nein, danke!“. Sie können jederzeit später aus dem Programm GPG Keychain heraus Ihre öffentlichen Schlüssel auf Schlüssel-Server hochladen.

Abbildung 6 zeigt die Liste der Schlüssel, die GPG Keychain für Sie auf Ihrem Rechner vorhält und verwaltet. Sie sehen den öffentlichen Schlüssel des GPGTools-Teams, der automatisch bei der Installation des Programms geladen wurde. Sie sehen weiterhin das gerade von Ihnen erzeugte Schlüsselpaar, dessen Typ in der linken Spalte mit „sec/pub“ angegeben wird („secure“ für den privaten Schlüssel und „public“ für den öffentlichen Schlüssel).

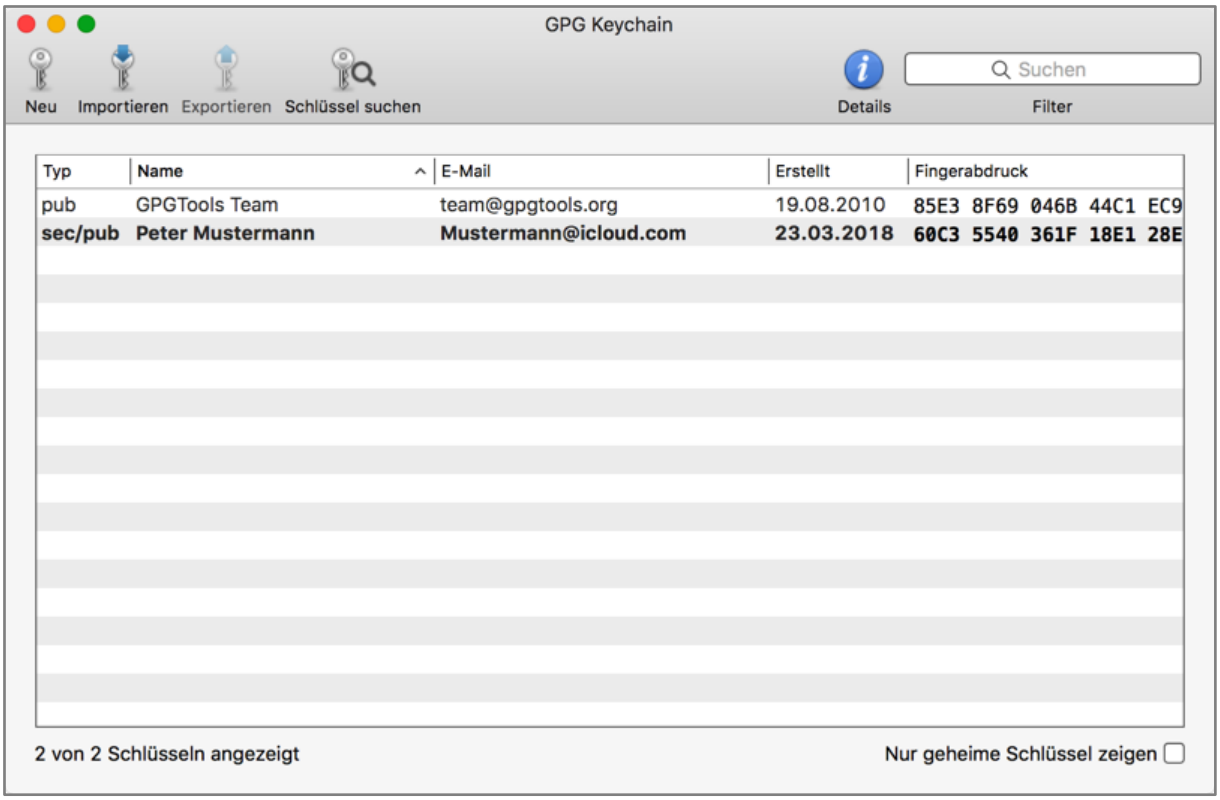

Abb. 6: Ihre Schlüssel in GPG Keychain

Das Programm GPG Keychain fungiert als Behälter und Verwalter aller Ihrer Schlüssel-/paare auf Ihrem Rechner. Die GPG Suite übernimmt auf Ihrem Rechner weitere Funktionen: Bei der Installation der GPG Suite wurde bereits erwähnt (siehe oben Kapitel C), dass in Apple Mail automatisch eine Funktionserweiterung für die Verschlüsselung von E-Mails installiert wird. Auch in Ihrem Finder 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, soweit 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 Finder 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 Finder auf diese Datei können Sie unter dem Eintrag „Dienste“ verschiedene Funktionen der GPG Services (Funktionserweiterung des Finders durch die GPG Suite) auswählen. Um eine Datei zu verschlüsseln, wählen Sie unter „Dienste“ den Eintrag „OpenPGP: Encrypt File“ (siehe Abbildung 7).

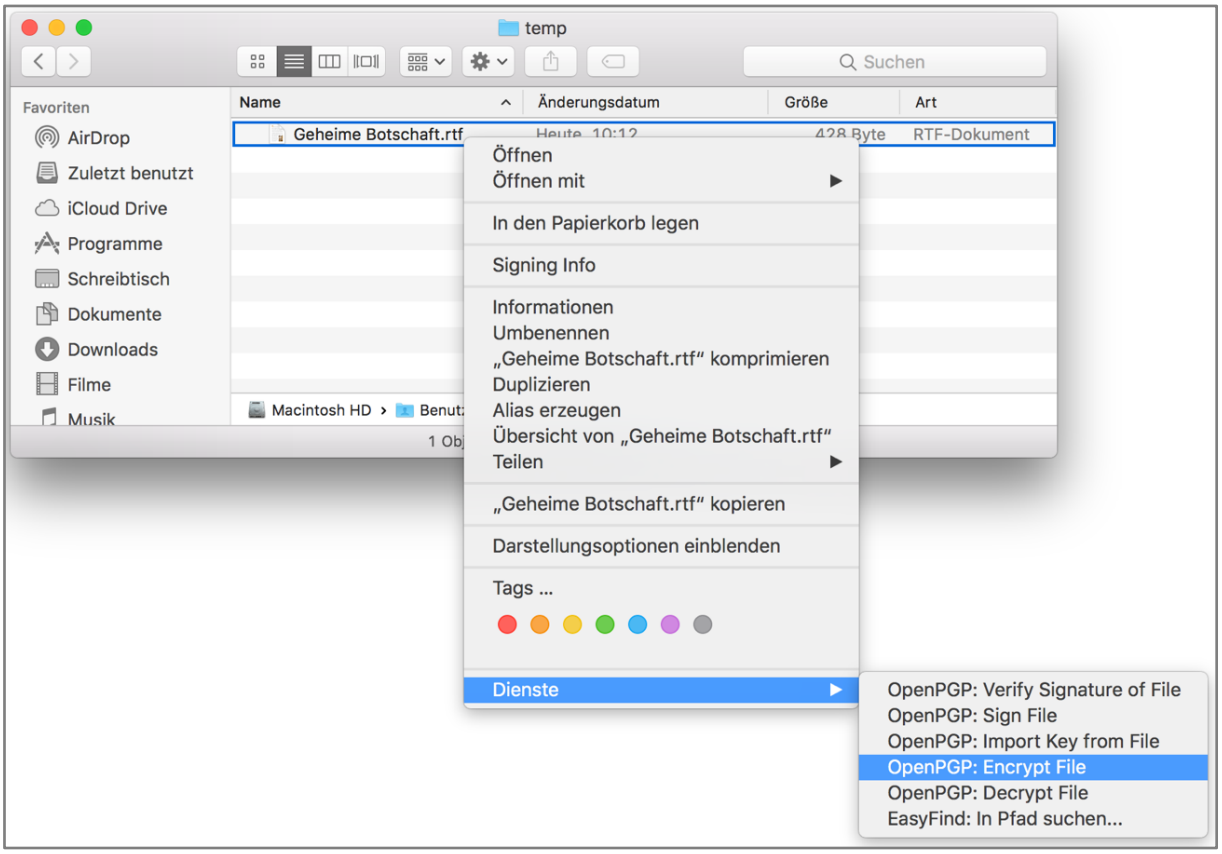

Abb. 7: GPG Services – GPG-Suite-Erweiterung im Finder

Nach Klick auf den Eintrag „OpenPGP: Encrypt File“ öffnet sich ein Fenster der GPG Services. 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 aus der Liste aus. Wählen Sie weiterhin unter „Dein Schlüssel:“ ebenfalls Ihren Schlüssel aus. Bestätigen Sie mit „OK“ (siehe Abbildung 8). Eine abschließende Meldung bestätigt Ihnen, ob der Verschlüsselungsprozess erfolgreich war. Die neu entstandene Datei mit der Endung „.gpg“ beinhaltet nun Ihre Datei in verschlüsselter Form. Diese Datei kann nun nur noch mit Ihrem privaten Schlüssel entschlüsselt werden.

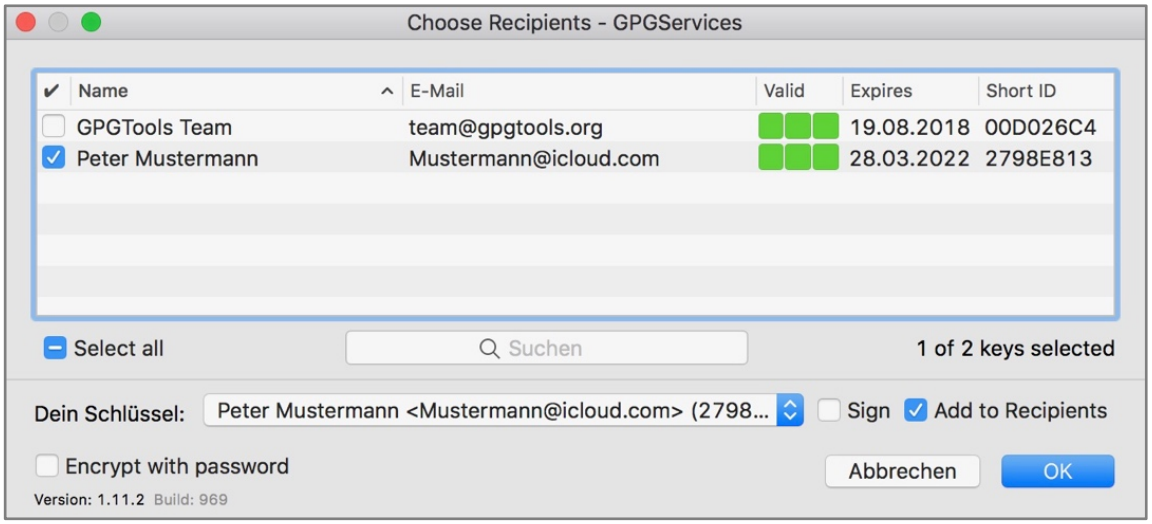

Abb. 8: GPG Services – Schlüsselauswahl

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 öffentluichen 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 Finder zur verschlüsselten Datei aus Kapitel E. Per Rechtsklick auf diese Datei können Sie unter „Dienste“ die Option „OpenPGP: Decrypt File“ auswählen (siehe Abbildung 9).

Nach Klick auf „OpenPGP: Decrypt File“ öffnet sich ein Fenster der GPG Services Erweiterung (siehe Abbildung 10).

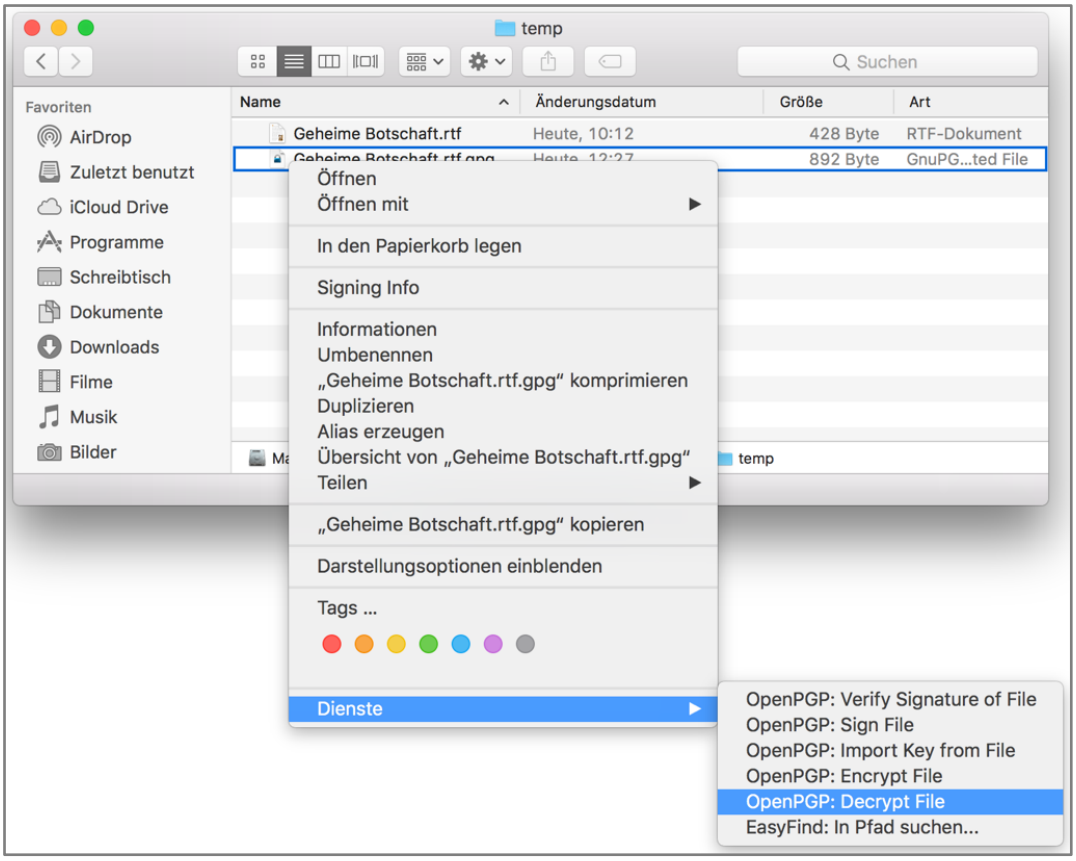

Abb. 9: GPG Services – GPG-Suite-Erweiterung im Finder

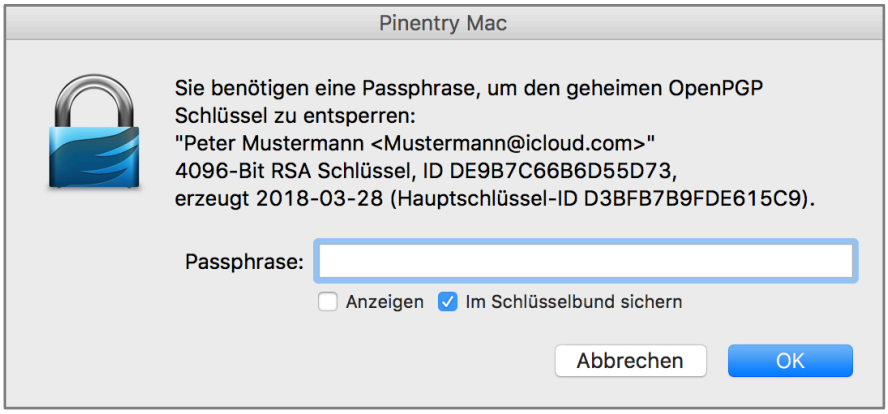

Abb. 10: GPG Services – Entsperren Ihres privaten Schlüssels

Wie bereits in Kapitel D beschrieben, schützt die GPG Keychain 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. Bestätigen Sie anschließend mit „OK“. Ein letztes Fenster zeigt Ihnen an, ob die Datei erfolgreich entschlüsselt wurde. Wenn der Prozess erfolgreich war, erhalten Sie Ihre ursprüngliche Datei im unverschlüsselten Format zurück.

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 Finder-Erweiterung GPG Services. Vergleichen Sie dazu Abbildung 8: Setzen Sie zum Verschlüsseln UND Signieren ein Haken bei „Sign“ in der Zeile zur Auswahl Ihres eigenen Schlüssels und bestätigen Sie anschließend mit „OK“.

Wenn Sie eine nicht verschlüsselte Datei beliebigen Formats oder eine bereits verschlüsselte Datei nachträglich signieren möchten, hilft Ihnen ebenfalls die Finder-Erweiterung GPG Services. Navigieren Sie dazu in Ihrem Finder zur verschlüsselten Datei aus Kapitel E. Wie gewohnt können die Funktionen der GPG Services per Rechtsklick auf die Datei aufgerufen werden. Wählen Sie den Eintrag „OpenPGP: Sign File“ (siehe Abbildung 11).

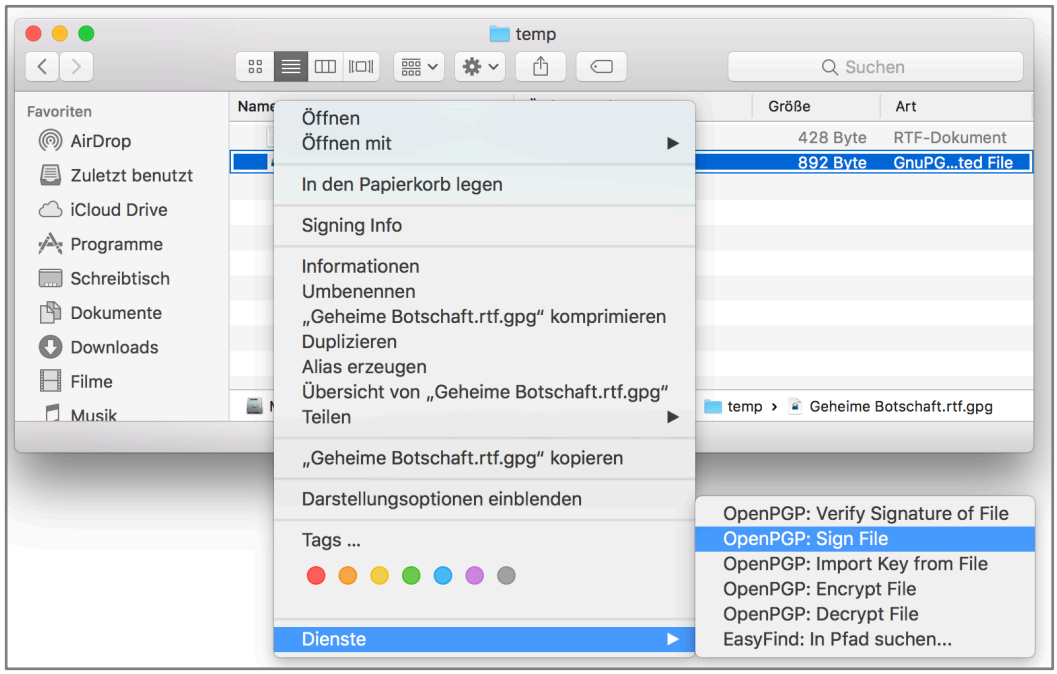

Abb. 11: GPG Services – GPG-Suite-Erweiterung im Finder

Nach Klick auf „OpenPGP: Sign File“ öffnet sich ein Fenster der GPG Services. An dieser Stelle müssen Sie den GPG Services nun mitteilen, welcher Ihrer privaten Schlüssel zum Signieren der ausgewählten Datei verwendet werden soll. Wählen Sie Ihren in Kapitel D erstellten privaten Schlüssel aus und klicken Sie anschließend auf „Auswählen“ (siehe Abbildung 12).

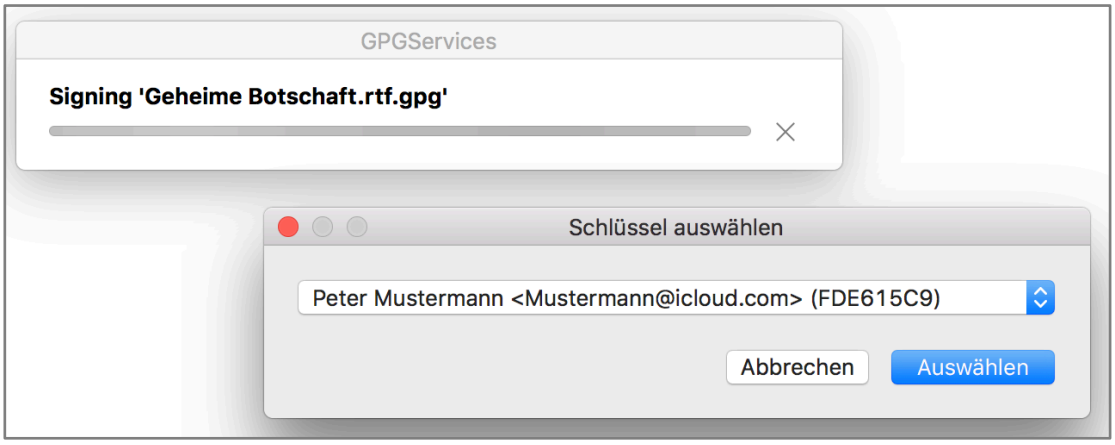

Abb. 12: GPG Services – Auswahl des signierenden Schlüssels

Unter Umständen sehen Sie nach Klick auf den „Auswählen“-Button erneut Abbildung 10. Dies kann vorkommen, wenn Sie längere Zeit nicht an Ihrem Rechner eingeloggt waren oder Ihre Passphrase nicht im macOS-Schlüsselbund hinterlegt haben. In diesem Fall geben Sie Ihre Passphrase erneut ein und bestätigen mit „OK“. Eine letzte Meldung zeigt Ihnen an, dass der Signaturprozess erfolgreich war. GPG Services 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 Ihre eigene GPG Keychain 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 Sie nicht mit seinen privaten Schlüssel entschlüsseln. Zur Sicherstellung der Echtheit von Schlüsseln gibt es zwei Möglichkeiten in der GPG Suite: 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 bereits das Gegenteil bewiesen. Eine Kontrolle ausschließlich auf Basis der Schlüssel-ID reicht daher nicht aus (in Abbildung 13 sehen Sie eine Beispiel-Schlüssel-ID: `2798E813`). 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. In Abbildung 13 sehen Sie einen Beispiel-Fingerabdruck: `9873 F2E1 9F5E 0AE5 E45F BC85 B40F D256 2798 E813`

In Ihrer GPG Keychain können Sie sich per Doppelklick auf den entsprechenden Schlüssel oder über den blauen „Details“-Button in der Menü-Leiste die Details eines Schlüssels anzeigen lassen (siehe Abbildung 13).

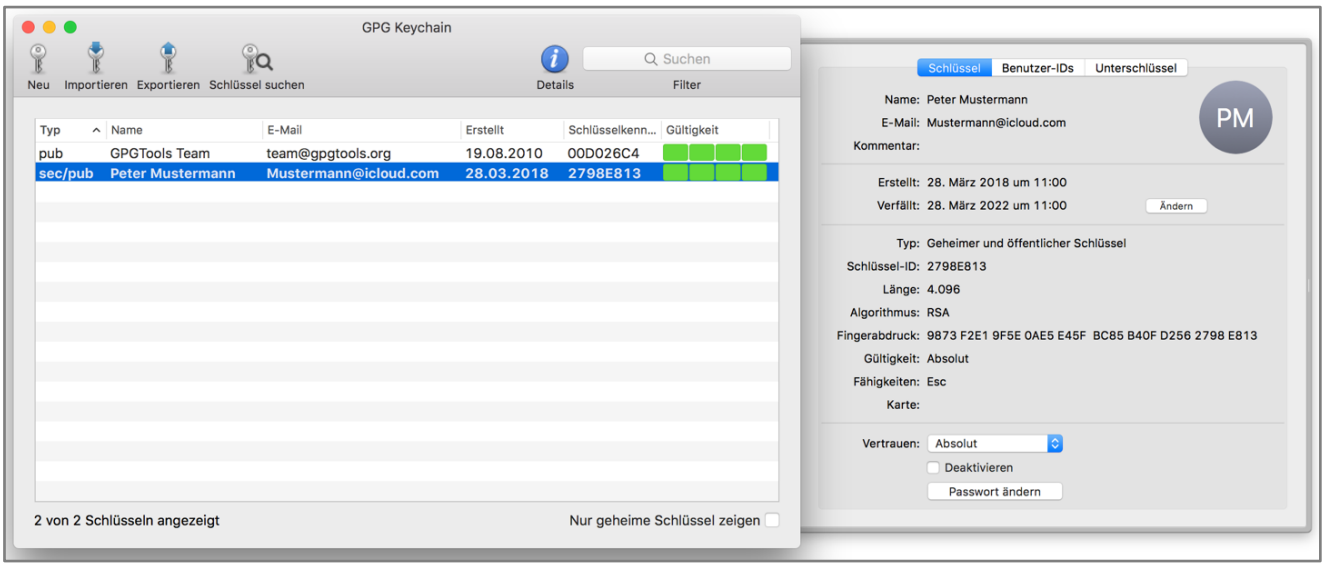

Abb. 13: GPG Keychain – Details eines Schlüsselpaars

Auf der rechten Seite sehen Sie das Detail-Fenster des Schlüssels von Peter Mustermann. In diesem Bereich sehen Sie ebenfalls die zugehörige Schlüssel-ID und den Fingerabdruck. Im Dropdown-Feld „Vertrauen“ können Sie Ihr Vertrauen gegenüber diesem Schlüssel festlegen. Selbst erstellte Schlüssel haben standardmäßig ein „absolutes“ Vertrauen. Importierte Schlüssel müssen dieses Vertrauen durch Sie erst erlangen. Wenn Sie einen neuen Schlüssel in Ihre GPG Keychain aufnehmen, sollten Sie daher zuerst den Fingerabdruck des Schlüssels überprüfen. Erst nach Überprüfung legen Sie Ihr Vertrauen gegenüber dem Schüssel fest.

Möchten Sie einen neuen Schlüssel z. B. eines Geschäftspartners in Ihre GPG Keychain aufnehmen, können Sie dies über den „Schlüssel 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 in Ihre GPG Keychain importieren. Fortgeschrittene Nutzer können den öffentlichen Schlüssel des Kommunikationspartners auch über die Kommandozeile importieren.

Um nun einen öffentlichen Schlüssel zu importieren, klicken Sie in Ihrer GPG-Keychain auf den „Schlüssel 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 Kommunikationspartners in das Suchfeld eingeben, sollten Sie nur einen einzigen Schlüssel finden. Markieren Sie diesen Schlüssel per Checkbox am Anfang der Ergebniszeile und bestätigen Sie den Import mit „Schlüssel holen“ (siehe Abbildung 14). Der importierte Schlüssel sollte nun in Ihrer GPG Keychain 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.

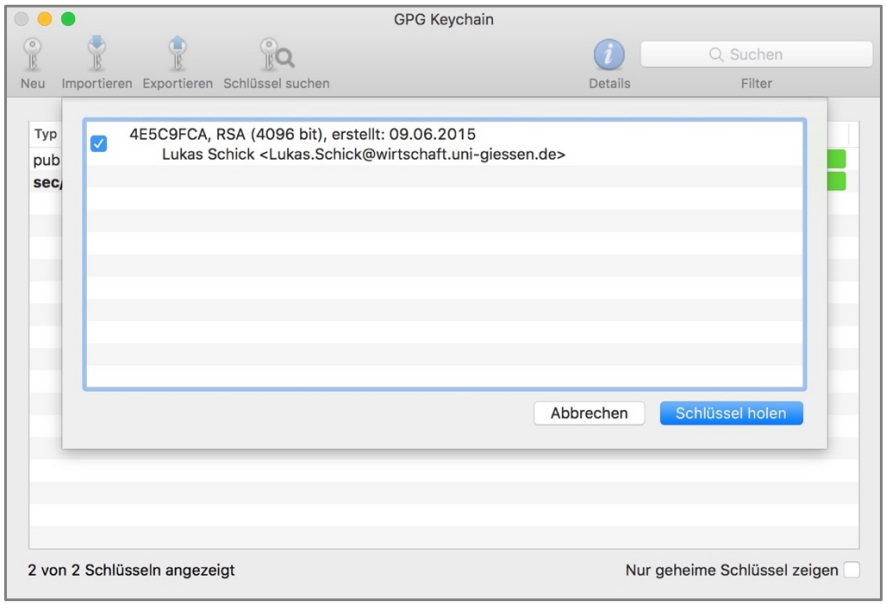

Abb. 14: GPG Keychain – Importieren eines Schlüssels

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.