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

Schwickert, Axel; Schick, Lukas

macOS – Verschlüsseln, Entschlüsseln und Signieren von E-Mails

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 4 / 2019
ISSN 1613-6667

Arbeitspapiere WI Nr. 4 / 2019

Autoren: Schwickert, Axel; Schick, Lukas

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

Zitation: Schwickert, Axel; Schick, Lukas: macOS – Verschlüsseln, Entschlüsseln und Signieren von E-Mails, in: Arbeitspapiere WI, Nr. 4/2019, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2019, 23 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. 04/2019 fortfahren. Im vorliegenden Arbeitspapier 04/2019 wird gezeigt, wie auf Apple-Rechnern mit dem Betriebssystem macOS E-Mails 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, E-Mail, Electronic Mail, Keychain, Widerruf

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 Apple-Rechnern mit dem Betriebssystem macOS 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 seinen Klartext mit dem öffentlichen Schlüssel des Empfängers. Der Sender erstellt zusätzlich mit seinem eigenen privaten Schlüssel aus seinem Klartext 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 Kommunikationspartner 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 Thunderbird auf macOS verwenden, müssen Sie neben der Verschlüsselungs-Software „GPGSuite" noch ein Thunderbird-Plugin mit dem Namen „Enigmail" installieren. Die GPGSuite übernimmt die Schlüsselverwaltung übernimmt und liefert die Schlüssel bei Bedarf an das Plugin Enigmail. Enigmail selbst ist für das Verschlüsseln, Entschlüsselung und Signieren von E-Mails im E-Mail-Client „Thunderbird" zuständig. Nutzen Sie hingegen Apple Mail unter macOS, benötigen Sie nur die GPG-Suite. Bei der Installation der GPGSuite auf Ihrem Apple-Rechner wird automatisch ein Plugin für Apple Mail mitinstalliert, das das Verschlüsseln, Entschlüsseln und Signieren von E-Mails in Apple Mail übernimmt. 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 Apple-Rechner mit dem Betriebssystem macOS E-Mails verschlüsseln, entschlüsseln und signieren können. Sie brauchen dafür folgendes Equipment:

<u>Das Wissen aus dem Arbeitspapier:</u> 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.

<u>Rechner:</u> 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.

<u>Web-Browser:</u> Auf Ihrem Rechner muss ein Web-Browser in neuester Version installiert sein wie z. B. Safari, Chrome oder Firefox.

<u>E-Mail-Client-Software:</u> Apple Mail

<u>Crypto-Software:</u> Auf Ihrem Rechner muss eine Software installiert sein, mit welcher Sie Ihre Schlüssel erstellen, beziehen und verwalten können. Wir verwenden als Crypto-Software die „GPG Suite“ vom Hersteller GPGTools.

<u>PGP Plugin für die E-Mail-Client-Software:</u> GPG Mail

C Installation des PGP Plugins

Laden Sie zunächst, wenn nicht bereits schon installiert, auf https://gpgtools.org die neueste Version von GPG Suite herunter. Star- ten Sie die Installation, indem Sie die heruntergeladene .dmg-Datei doppelklicken. Folgen Sie den Installationsanweisungen. Nach erfolgter Installation können Sie die .dmg-Installationsda- tei in den Papierkorb legen.

Die GPG Suite enthält neben dem Programm GPG Keychain noch weitere Programme, die bei der Installation automatisch mitinstalliert werden: GPG Mail 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.

Öffnen Sie nun Apple Mail. Sie sehen zunächst den Startbildschirm von GPG Mail im Vordergrund. Wenn Sie GPG Mail erwerben möchten, klicken Sie auf den blauen Button „Buy Now". Um GPG Mail zuerst testen zu können, klicken Sie auf den Button „Continue Trial".

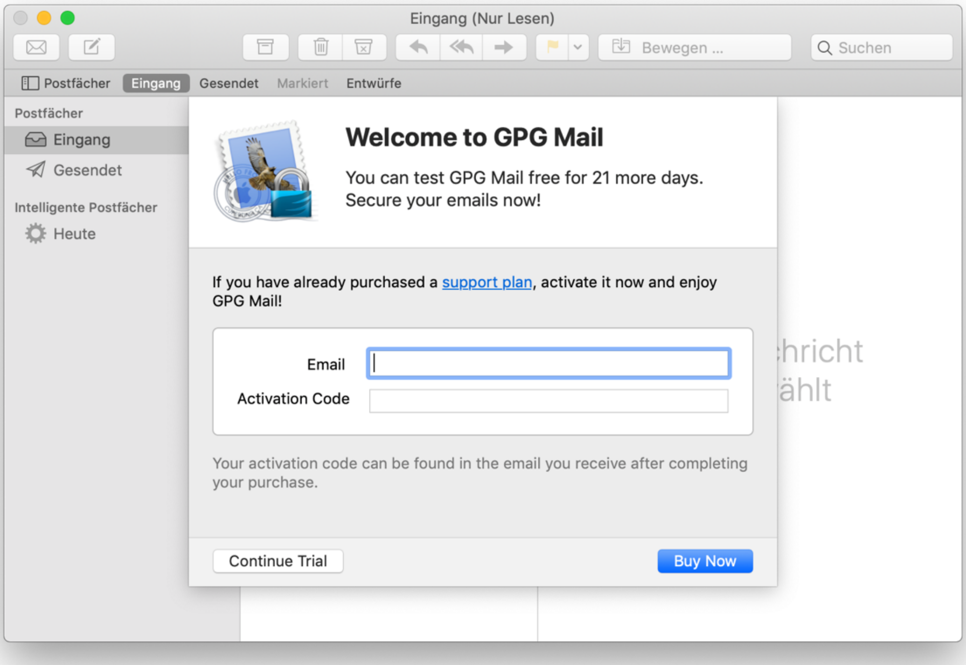

Abb. 1: Apple Mail – Welcome to GPG Mail

Überprüfen Sie nun zunächst in den Einstellungen Ihres Apple-Mail-Programms, ob das GPG Mail Plugin voll funktionstüchtig installiert wurde. Klicken Sie dazu, während Apple Mail geöffnet ist, in der oberen Menüleiste von macOS auf „Mail" und anschließend auf „Einstellungen".

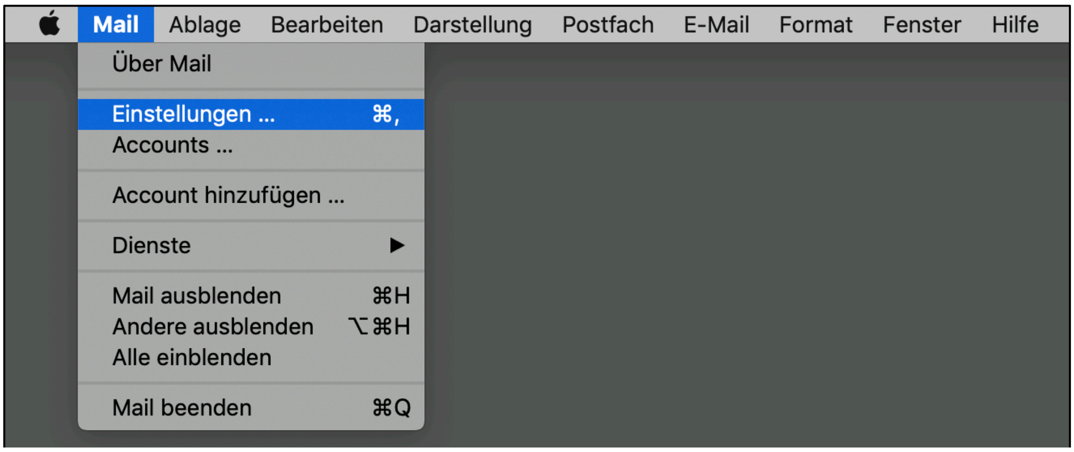

Abb. 2: GPG Mail – Einstellungen überprüfen

Wechseln Sie im sich öffnenden Fenster „GPGMail“ in den Reiter „GPGMail“. Der grüne Kreis in der ersten Zeile zeigt Ihnen den aktiven Status von GPGMail an. Sie können weiterhin zusätzliche Einstellungen zum Standardvorgehen bei der Verschlüsselung und dem Signieren neuer E-Mails vornehmen.

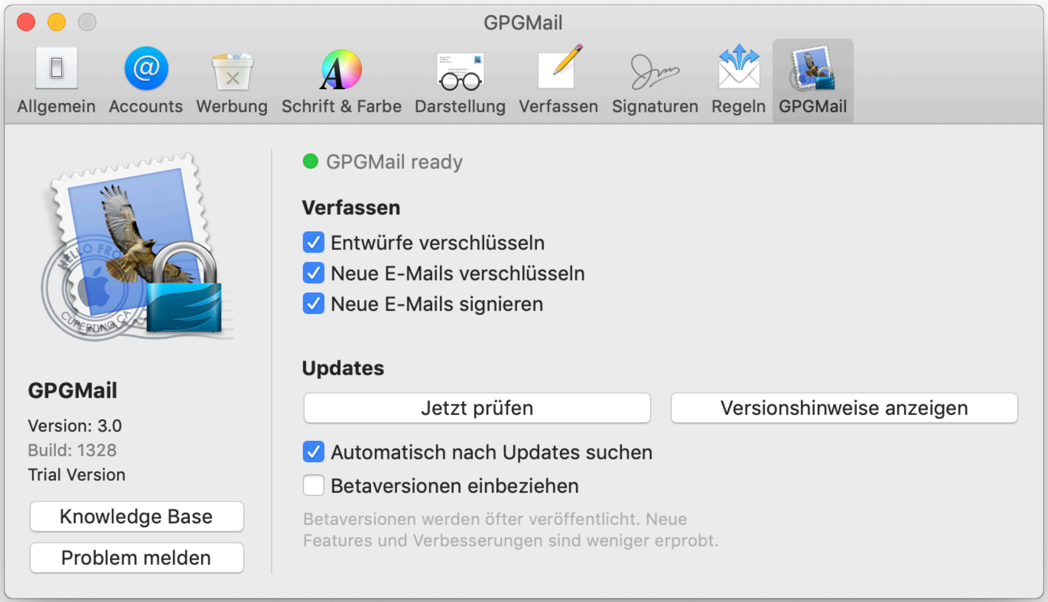

Abb. 3: Apple Mail – Einstellungen von GPGMail überprüfen

Überprüfen Sie zuletzt, ob sich die GPG Suite auf dem neuesten Stand befindet. Klicken Sie dazu auf den Button „Jetzt prüfen“. Das sich öffnende Fenster zeigt Ihnen den Update-Status der GPG Suite an.

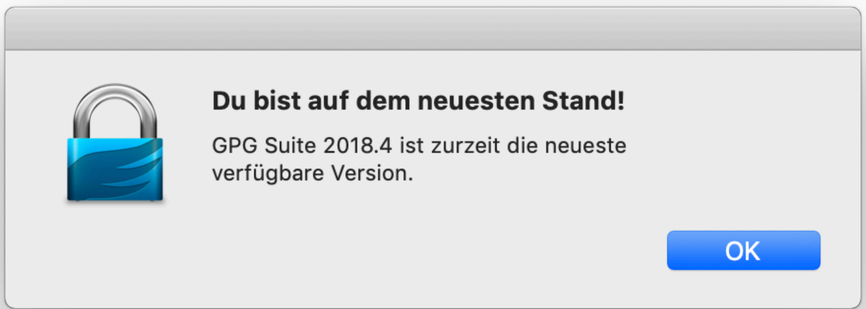

Abb. 4: Update-Status der GPG Suite

D Ein Schlüsselpaar erstellen

Öffnen Sie zuerst das Programm „GPG Keychain“. Die GPG Keychain ist ein Programm innerhalb der GPG Suite und wird eingesetzt, um sämtliche kryptographische Schlüsselpaare auf Ihrem persönlichen Computer sicher aufzubewahren.

Solange Sie noch keine eigenen Schlüsselpaare erstellt oder öffentliche Schlüssel Ihrer Kommunikationspartner importiert haben, sehen Sie eine leere Liste in Ihrer GPG Keychain. Über die Funktion „Neu“ im Start-Bildschirm von GPG Keychain links oben erstellen Sie für sich ein neues Schlüsselpaar (siehe Abbildung 6).

Geben Sie Ihren Namen, Ihre 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 6. 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 je eine Datei für einen öffentlichen und einen privaten Schlüssel erzeugt und diese beiden Dateien auf Ihrem Rechner mit Ihrem gewählten Passwort verschlüsselt abgespeichert.

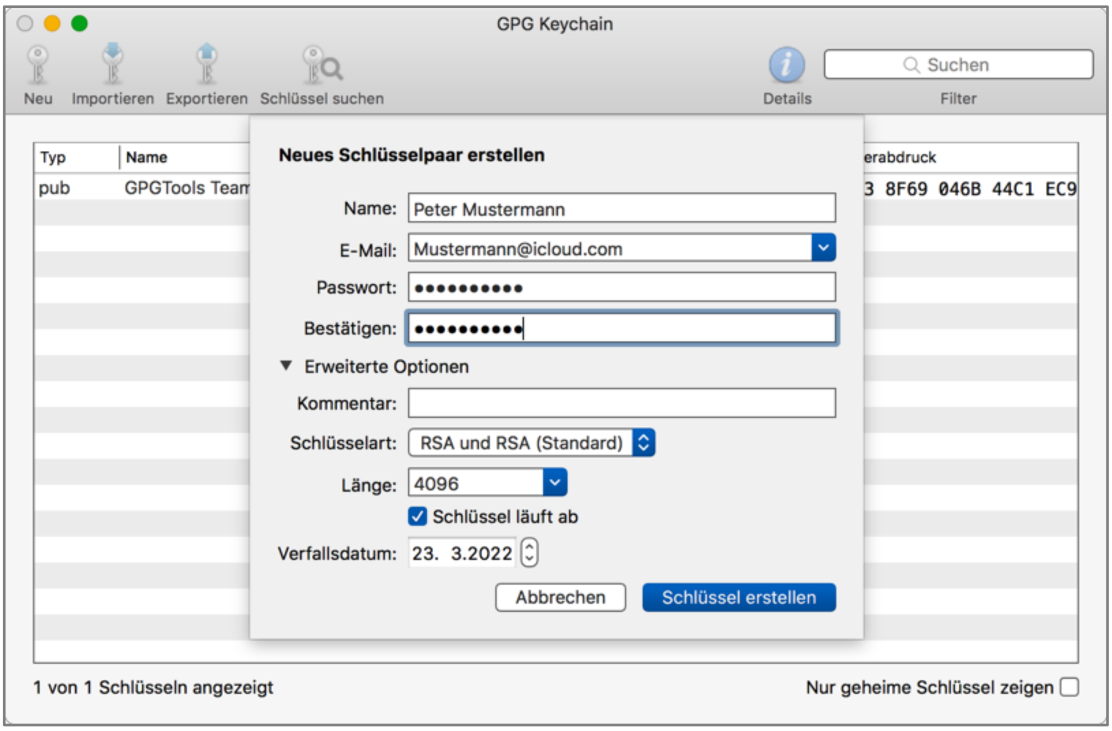

Abb. 5: Ein neues Schlüsselpaar erstellen

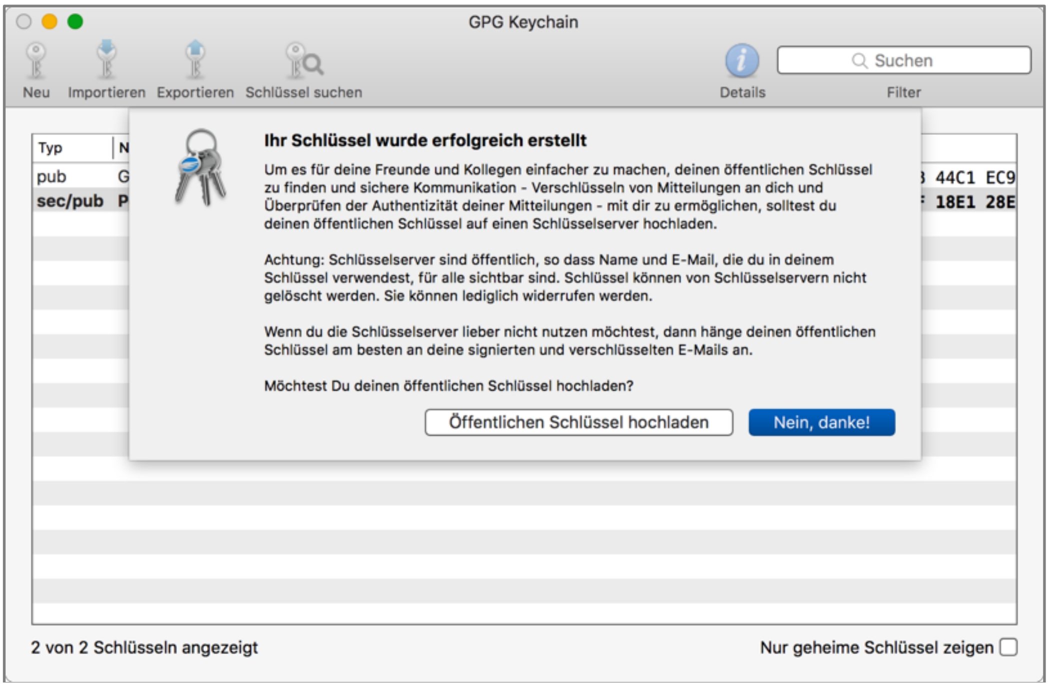

Abb. 6: Ihr Schlüsselpaar wurde erfolgreich erstellt.

GPG Keychain bietet Ihnen an, Ihren öffentlichen Schlüssel auf einen öffentlichen Schlüssel-Server hochzuladen (siehe Kapitel A des vorausgesetzten Arbeitspapiers; 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.

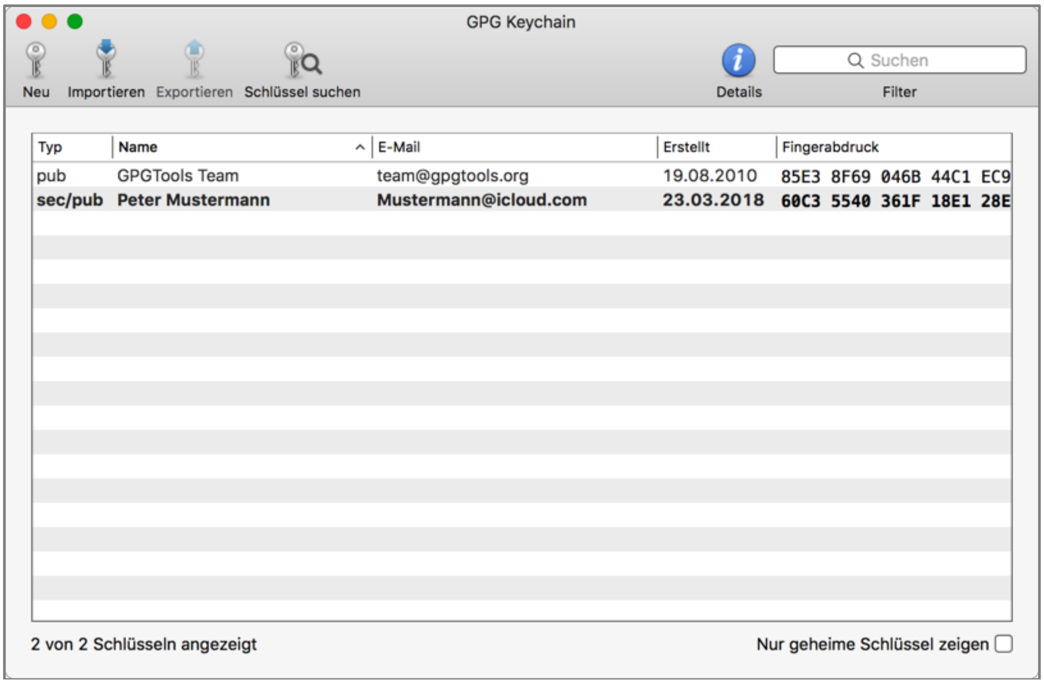

Abb. 7: Ihre Schlüssel in GPG Keychain

Abbildung 7 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).

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 Sie mithilfe von Apple Mail und dem bereits installierten Plugin der GPG Suite eine E-Mail 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 macOS das Programm „GPG Keychain“, 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 seiner GPG Keychain ein eigenes Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, und den öffentlichen von Anna Froehlich. 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.

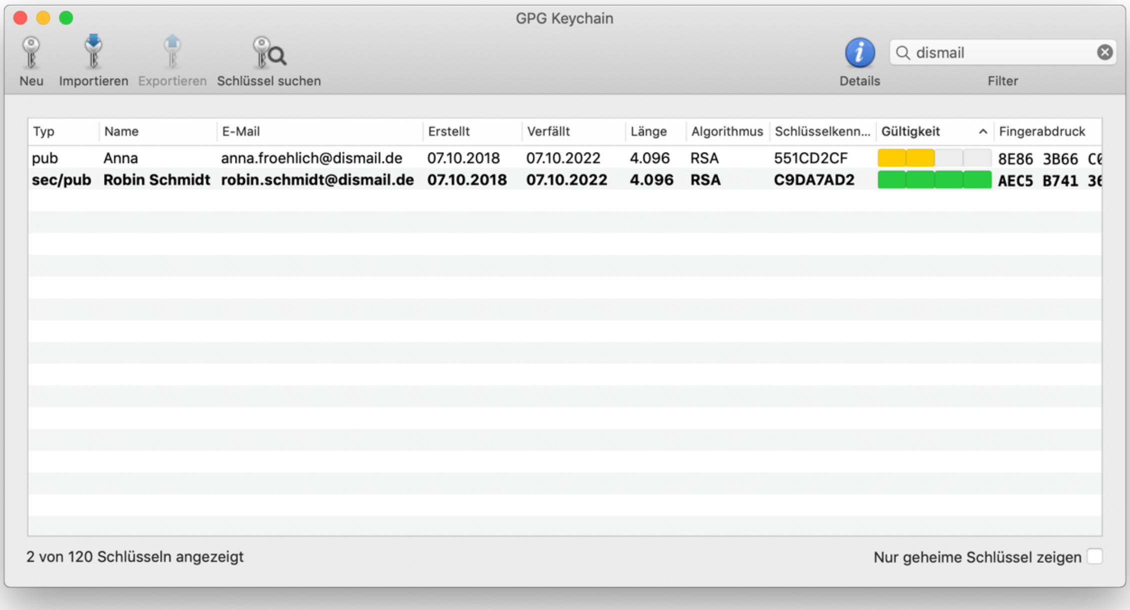

Abb. 8: GPG Keychain – Vorhandene kryptographische Schlüsselpaare

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

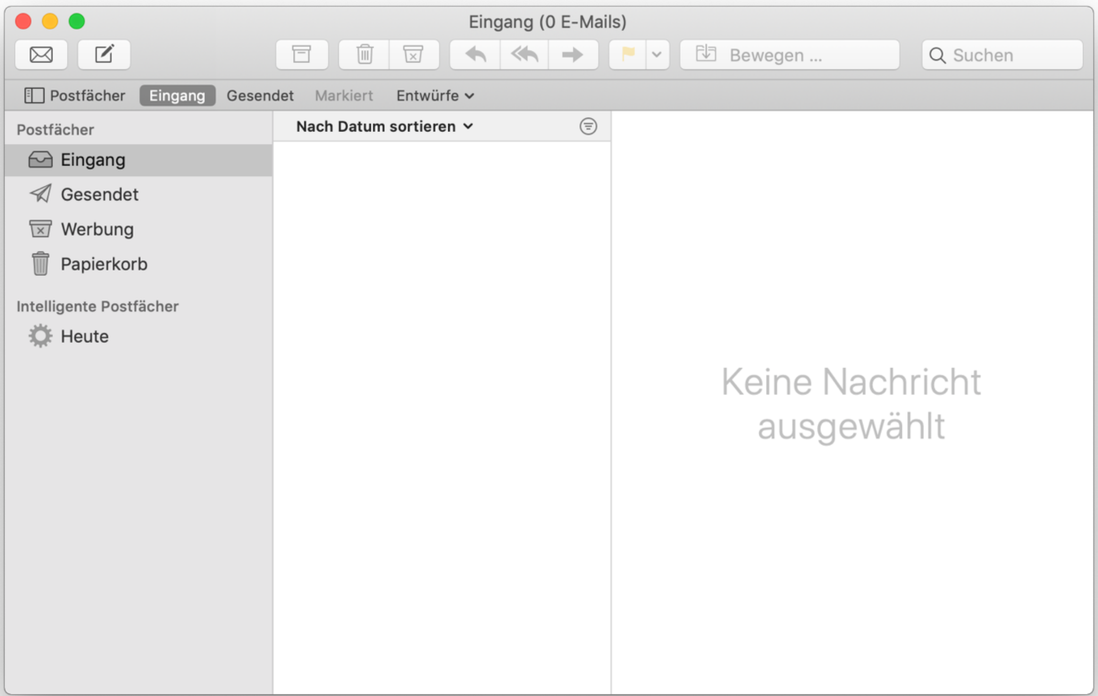

Abb. 9: Apple Mail – Startbildschirm

Werfen Sie zuerst einen Blick in die obere rechte Ecke des E-Mail-Verfassen-Fensters. Wenn Sie dort einen Button mit der Bezeichnung „OpenPGP“ sehen, wurde das GPG Mail Plugin erfolgreich installiert (siehe Abbildung 10).

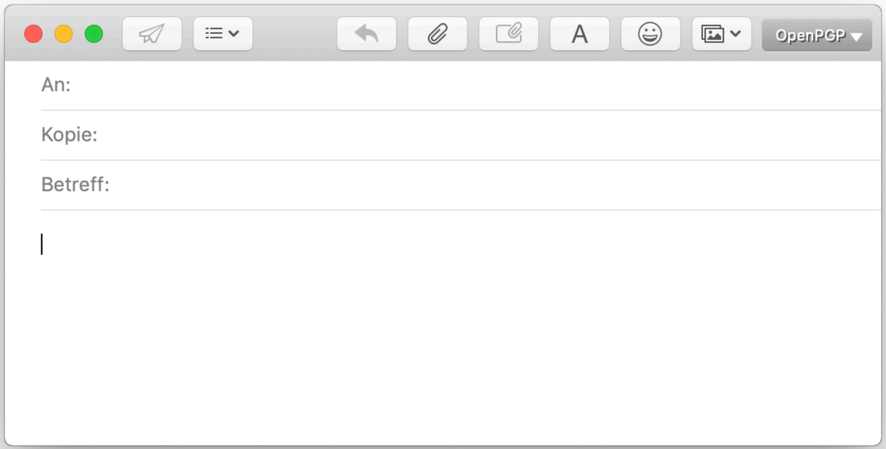

Abb. 10: Apple Mail – Neue E-Mail verfassen

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 Froehlich ein (siehe Abbildung 11). Das GPG Mail Plugin in Apple Mail erkennt automatisch, dass für diese E-Mail (Anna.Froehlich@dismail.de) ein öffentlicher Schlüssel in der GPG Keychain hinterlegt wurde. GPG Mail verwendet diesen, um die zu sendende E-Mail an Anna zu verschlüsseln. GPG Mail verwendet zusätzlich Ihren privaten Schlüssel, um die zu versendende Nachricht zu signieren. Bedenken Sie: GPG Mail kann Ihre E-Mails nur Signieren, wenn Sie über einen privaten Schlüssel passend zu Ihrer E-Mail-Adresse verfügen. Ob GPG Mail Ihre zu versendende E-Mail automatisch verschlüsseln und signieren kann, können Sie anhand des grünen „OpenPGP“-Buttons und der zwei blauen Buttons in der Zeile „Betreff:“ erkennen. Leuchten das Schloss und der gezackte Kreis blau auf, verschlüsselt Apple Mail Ihre zu sendende E-Mail. Wenn Sie auf diese Buttons klicken, so dass sie in der Farbe grau erscheinen, 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.

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

GPG Mail wird nun auf Ihren privaten Schlüssel in der GPG Keychain zugreifen, um die empfangene verschlüsselte E-Mail zu entschlüsseln. 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 (siehe Abbildung 12). Geben Sie daher im Feld „Passphrase:" das Passwort ein, das Sie zum Erstellen den Schlüsselpaars verwendet haben. Bestätigen Sie anschließend mit „OK". Sollten Sie diese Passphrasen-Abfrage nicht sehen, kann das daran liegen, dass Sie diese erst vor kurzem eingegeben haben.

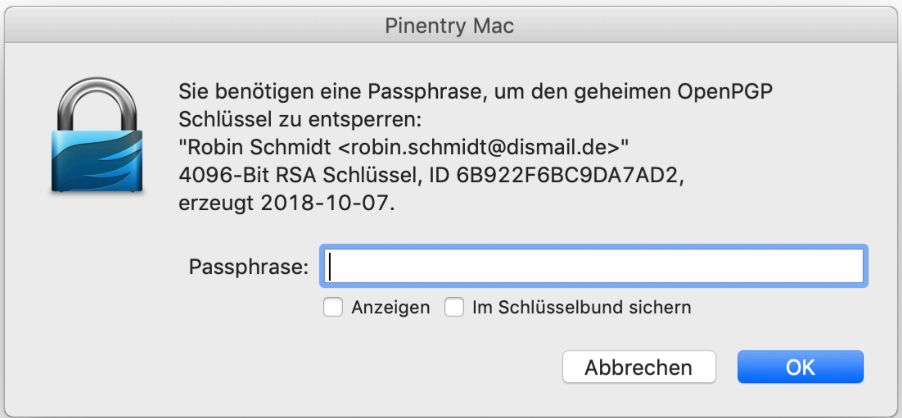

Abb. 12: GPG Services – Entsperren Ihres privaten Schlüssels

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

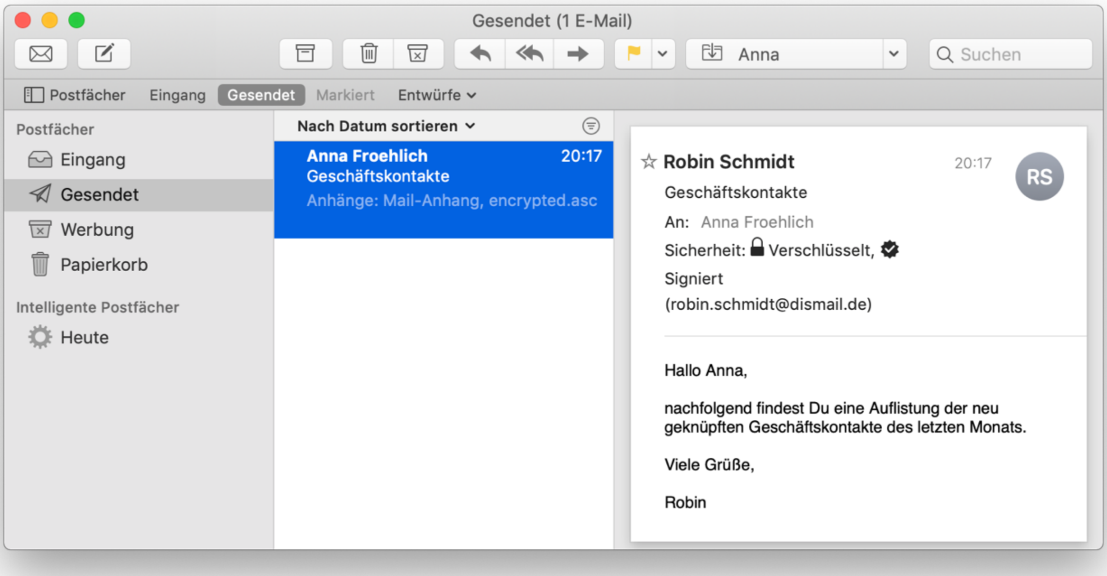

Abb. 13: Apple Mail – Verschlüsselte und signierte E-Mail versendet

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 Apple Mail und klicken Sie auf die erhaltene verschlüsselte E-Mail. In unserem Fall erhält Robin von Anna eine verschlüsselte Antwort-E-Mail (siehe Abbildung 14).

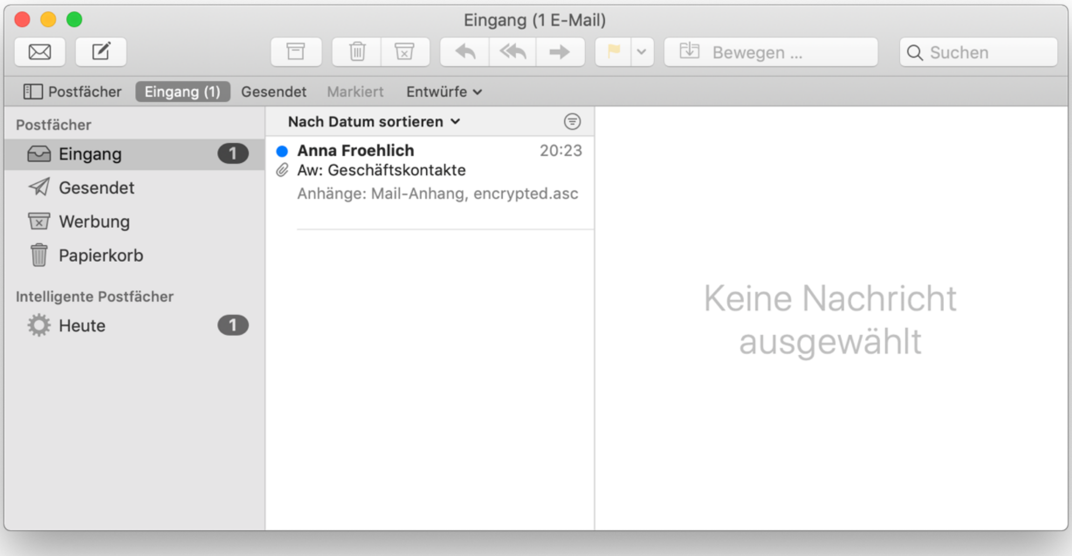

Abb. 14: Apple Mail – Posteingang mit verschlüsselter E-Mail

GPG Mail wird nun auf Ihren privaten Schlüssel in der GPG Keychain zugreifen, um die empfangene verschlüsselte E-Mail zu entschlüsseln. 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 Schlüselpaars verwendet haben (siehe Abbildung 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.

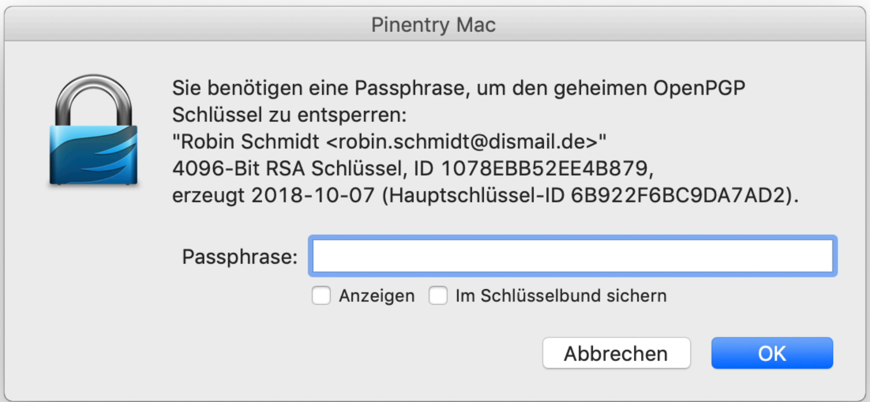

Abb. 15: GPG Services – Entsperren Ihres privaten Schlüssels

GPG Mail 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).

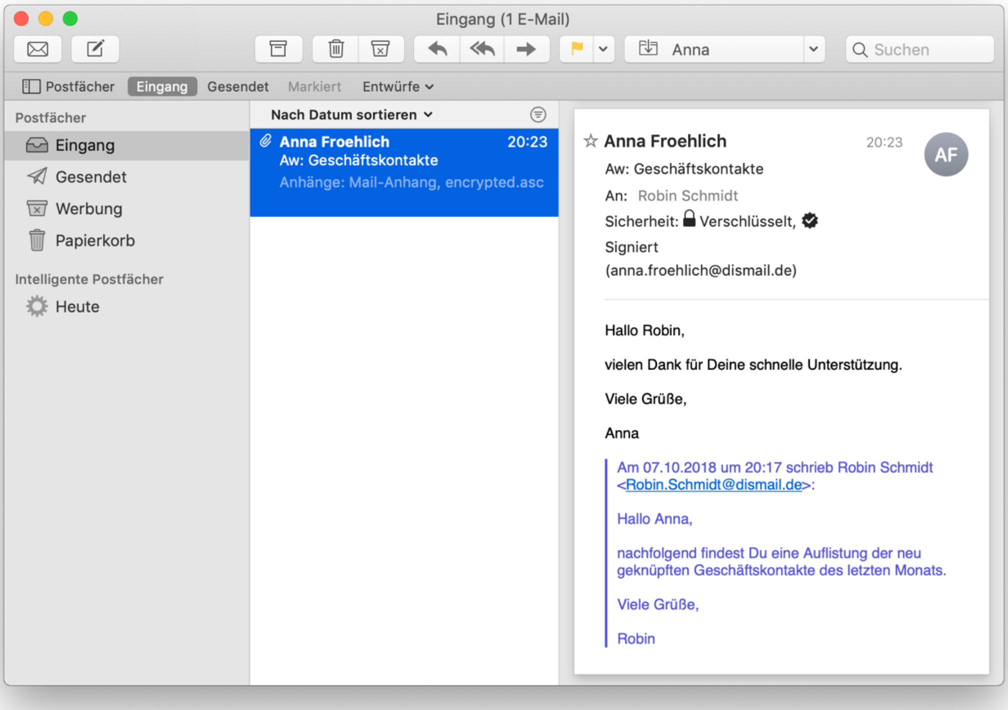

Abb. 16: Apple Mail – Posteingang mit entschlüsselter E-Mail

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 die 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 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 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: `2798E813`

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: `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 17).

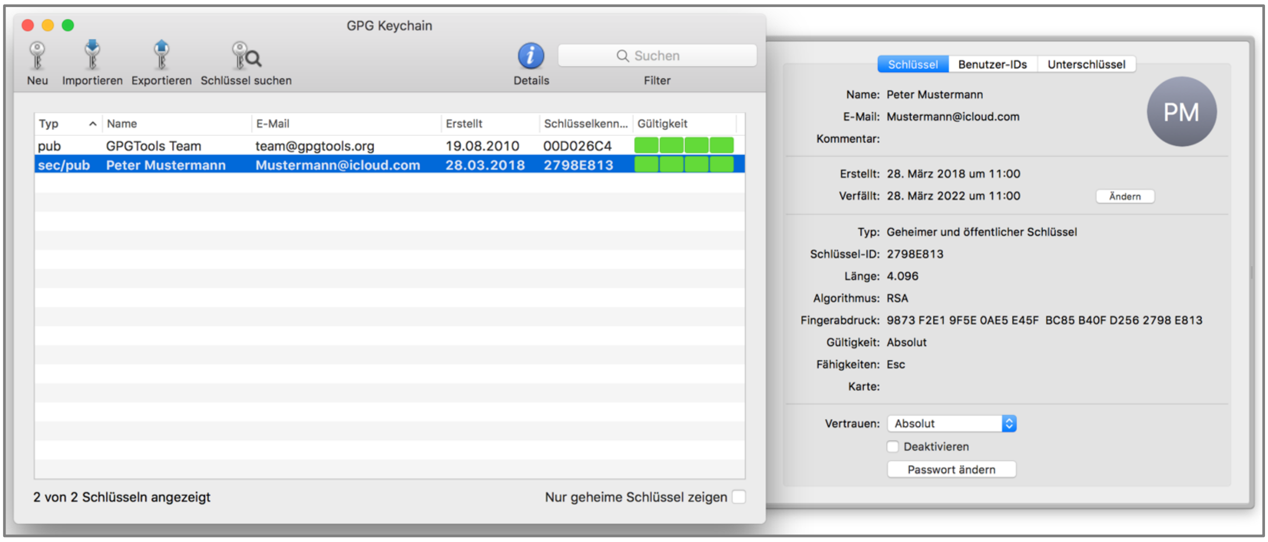

Abb. 17: GPG Keychain – Details eines Schlüsselpaars

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. Eigens 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 oder Freundes 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 18). 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.

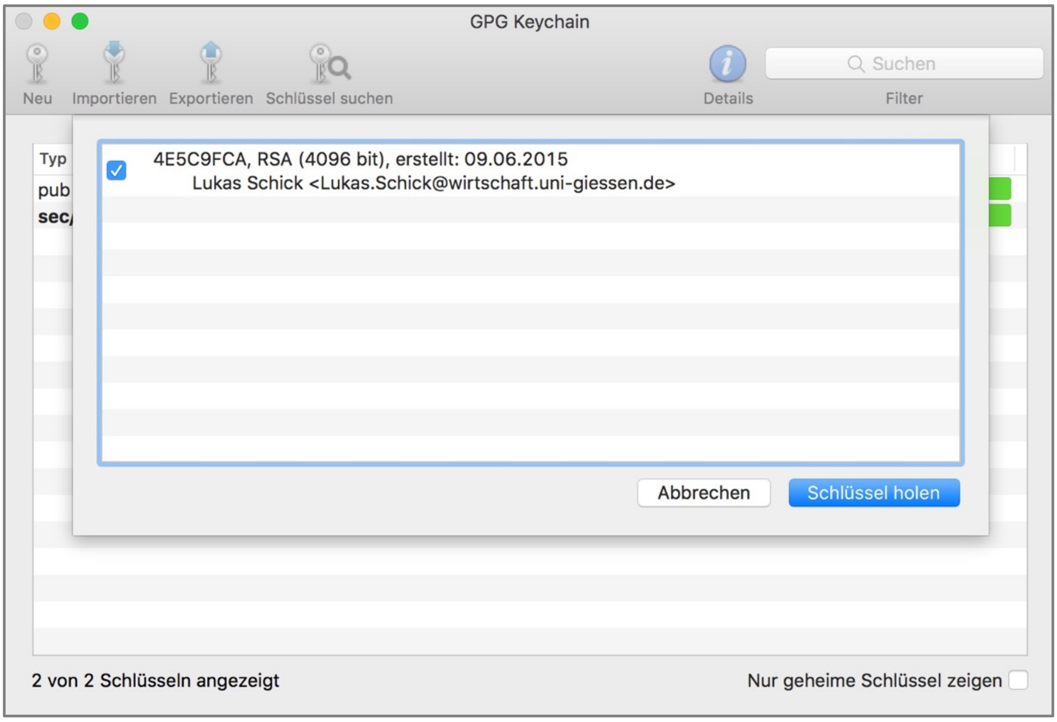

Abb. 18: GPG Keychain – Importieren eines Schlüssels

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 einen kompromittiertes Schlüsselpaar zu widerrufen, gehen Sie wie folgt vor: Öffnen Sie die GPG Keychain und klicken Sie per Rechtsklick auf Ihr zu widerrufendes Schlüsselpaar (siehe Abbildung 19). Klicken Sie anschließend auf „Widerrufen ...". Ein sich öffnendes Fenster zeigt Ihnen zur Sicherheit ein Warnungshinweis. Klicken Sie auf den Button „Schlüssel widerrufen" (siehe Abbildung 20).

Nach einer kurzen Wartezeit hat die GPG Keychain Ihr Schlüsselpaar widerrufen. Ein weiteres sich öffnendes Fenster zeigt Ihnen an, ob das Schlüsselpaar erfolgreich widerrufen wurde (siehe Abbildung 21). GPG Keychain fragt Sie weiterhin, ob es den widerrufenen öffentlichen Schlüssel für Sie in ein öffentliches Schlüsselverzeichnis hochladen soll. Wenn Sie Ihren öffentlichen Schlüssel in einem öffentlichen Schlüsselverzeichnis zur Verfügung gestellt haben, sollten Sie an dieser Stelle „Öffentlichen Schlüssel hochladen" anklicken. Ihre Kommunikationspartner aktualisieren dann deren Schlüssellisten basierend auf neuen Informationen aus öffentlichen Schlüsselverzeichnis und erhalten dadurch automatisch Kenntnis über Ihren Widerruf. Wenn Sie Ihren Schlüssel nur lokal vorhalten, müssen Sie dies nicht zwingend durchführen.

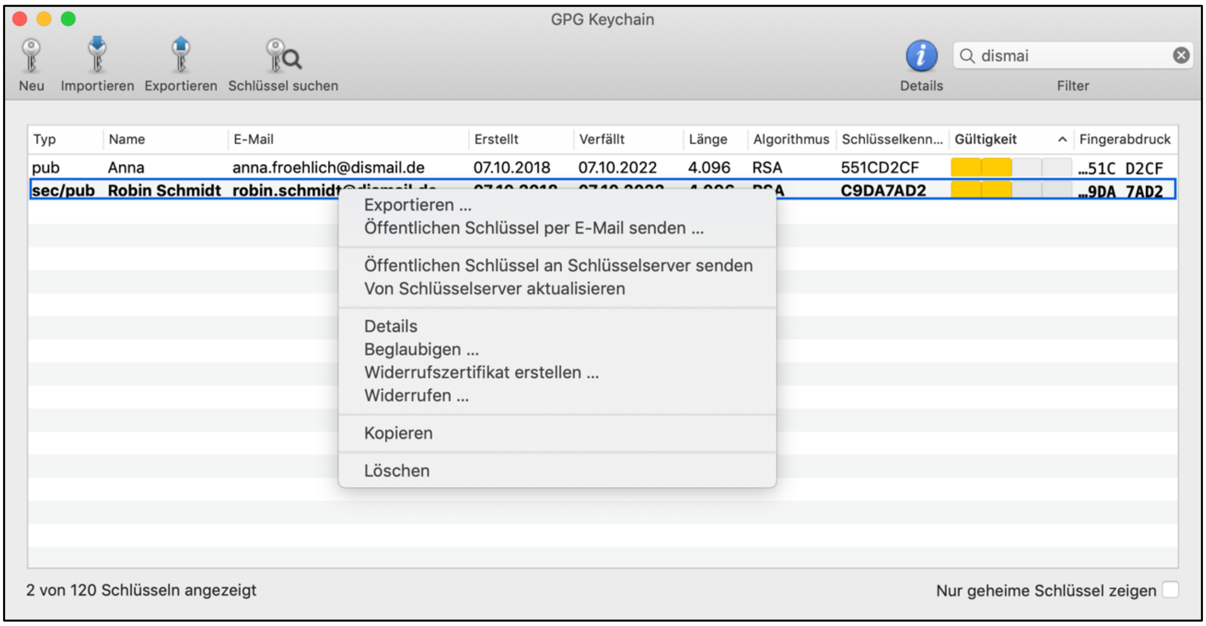

Abb. 19: GPG Keychain – Schlüsselpaar widerrufen

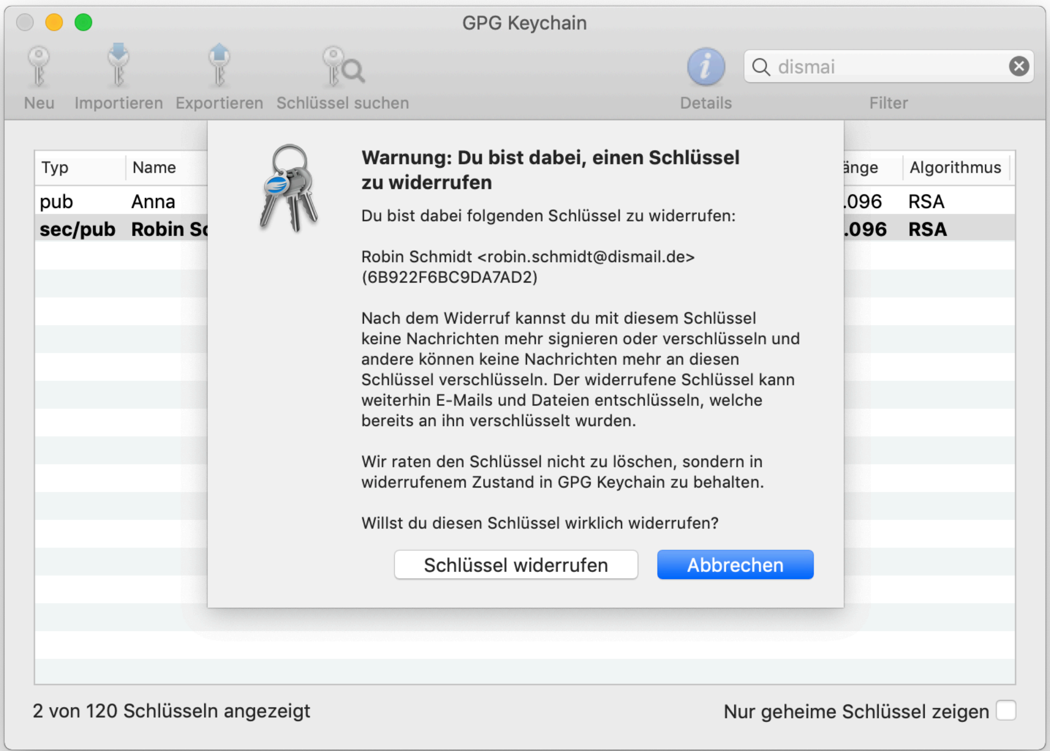

Abb. 20: GPG Keychain – Warnhinweis Schlüsselpaar widerrufen

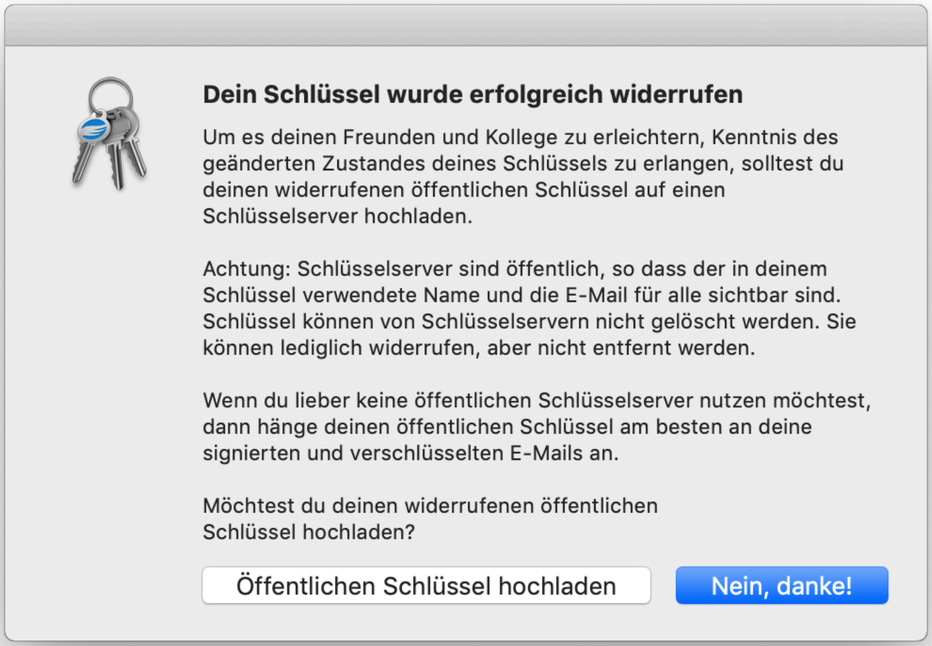

Abb. 21: GPG Keychain – Schlüsselpaar widerrufen

GPG Keychain 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 der GPG Keychain auf Ihrer Festplatte abgelegt werden. Sie müssen dann eigenständig der Aufgabe des Schützens und Sicherns dieses Zertifikats nachkommen. Wenn Sie entweder auf „Nein, danke!“ oder auf „Öffentlichen Schlüssel hochladen“ geklickt haben, zeigt Ihnen die GPG Keychain den widerrufenen Schlüssel weiterhin in der Liste Ihrer Schlüssel an (siehe Abbildung 22).

Wie Sie in Abbildung 22 sehen, hat Robin Schmidt sein Schlüsselpaar widerrufen. Die GPG Keychain signalisiert dies, indem die Zeile des widerrufenen Schlüssels grau erscheint und die Gültigkeit rot markiert wurde. Robin hat auf diese Weise sein Schlüsselpaar erfolgreich widerrufen.

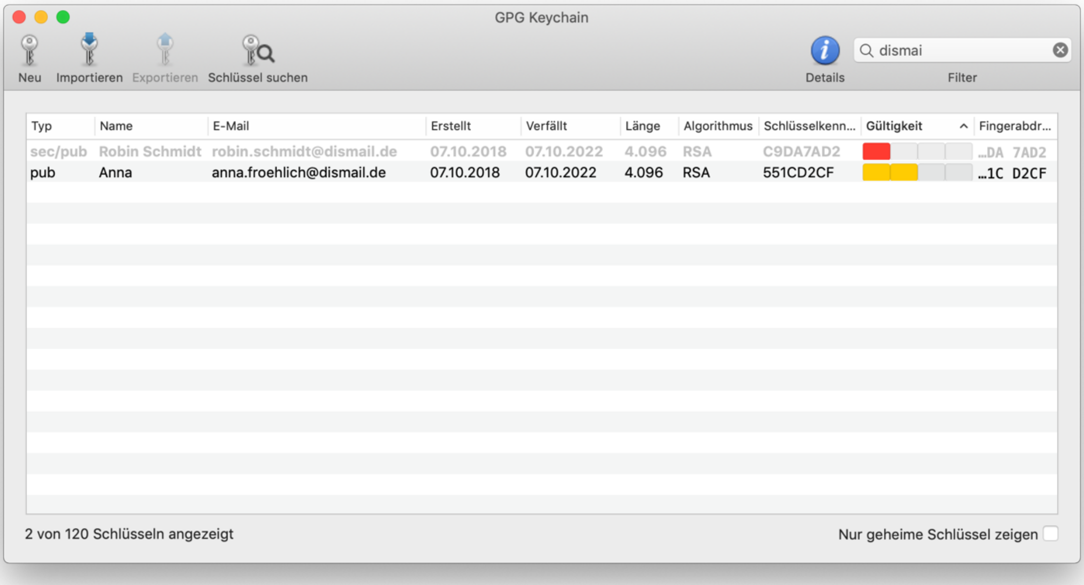

Abb. 22: GPG Keychain – Schlüsselpaar widerrufen

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/.