ASAN · Berlin

Autonomes • Solidarisches • Antifaschistisches • Netzwerk • Berlin

Basics zur sicheren Kommunikation

- E-Mail Verschlüsselung mit PGP (Windows)
- Datei Verschlüsselung mit PGP (Windows)
- PGP Verschlüsselung mit iOS
- PGP Verschlüsselung mit Android

Version 2.1.0 – Stand 31.01.2021

Inhalt

Gpg4win 3.1.14

Gpg4win ist eine sichere Lösung zur E-Mail und Datei Verschlüsselung mit GnuPGP für Windows.

- Du kannst E-Mails damit signieren, die Empfänger:innen haben damit eine Bestätigung, dass die Nachricht auch tatsächlich von Dir stammt.
- Du kannst E-Mails einschließlich Anhänge damit verschlüsseln, damit sie nicht von Dritten, sondern nur von den Empfänger:innen geöffnet und gelesen werden können.
- Darüber hinaus kannst Du Dateien und Verzeichnisse verschlüsseln, die entweder nur von Dir selbst oder von Dir bestimmten Empfänger:innen entschlüsselt werden können. Dein Passwort zum Entschlüsseln bleibt dabei geheim, dass musst und darfst Du niemensch mitteilen.

Damit das ganze überhaupt funktioniert, musst Du als erstes Dein eigenes Schlüsselpaar erstellen:

Private Key: Das ist Dein privater und geheimer Schlüssel. Mit diesem Schlüssel kannst Du für Dich bestimmte Nachrichten, Dateien und Verzeichnisse öffnen und lesen. Du kannst damit aber auch ausgehende Nachrichten, Verzeichnisse und Dateien verschlüsseln.

Public Key: Das ist Dein öffentlicher Schlüssel, den brauchen Deine Empfänger:innen, damit sie Dich als Absender:in verifizieren und verschlüsselte Nachrichten, Dateien und Verzeichnisse von Dir öffnen und lesen können.

Wichtig!

Damit die Kommunikation und der Datenaustausch funktioniert, brauchst Du also auch die öffentlichen Schlüssel Deiner Kommunikationspartner:innen. Empfänger:innen, die über keinen PGP Schlüssel verfügen, können Deine Nachrichten, Dateien und Verzeichnisse nicht öffnen oder lesen.

Je nach Deinen politischen Aktivitäten solltest Du darauf achten, **wo** Du Deine E-Mailadresse hostest, **wem** Du Deine E-Mailadresse gibst und **wie** Du Deinen Public Key zur Verfügung stellst.

Bei den meisten Standard Email Providern kannst Du davon ausgehen, dass der VS und bald auch die Cops freien Zugang zu den Daten der Nutzer:innen haben. Ein Grund mehr, auch Deine private Kommunikation grundsätzlich zu verschlüsseln und solche E-Mailadressen auch nicht für die politische Arbeit zu verwenden.

Schlüsselpaare können für mehrere E-Mailadressen erzeugt und verwaltet werden, z. B. für Deine private E-Mailadresse, für eine öffentliche E-Mailadresse, für eine E-Mailadresse, die Du nur innerhalb Deiner festen Gruppe oder Bezugsgruppe verwendest. Beim Versand Deiner Nachrichten wählst Du Dein E-Mailkonto mit dem dazugehörigen Schlüssel aus und legst auch die Empfänger:innen fest.

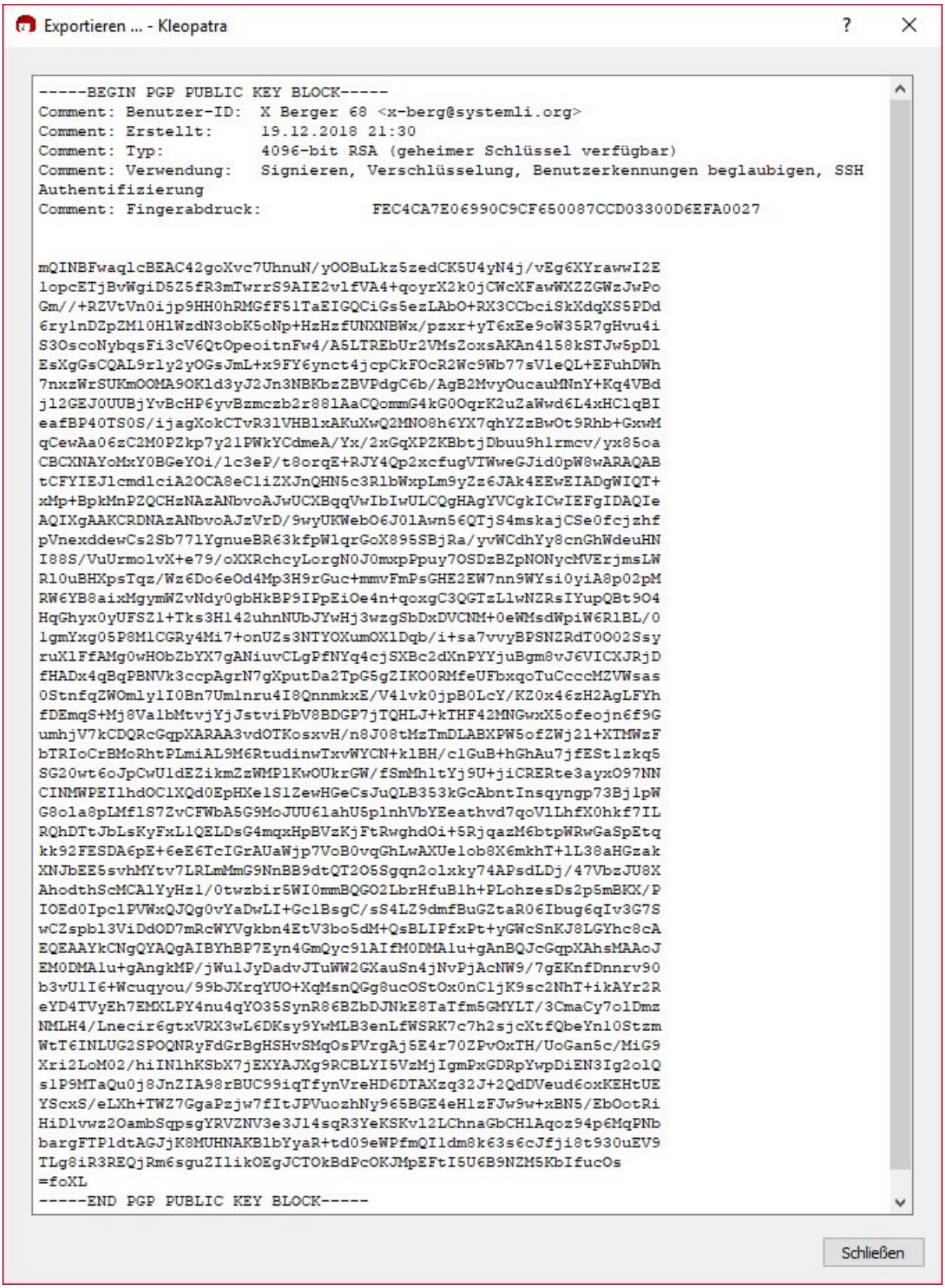
Achtung! Sicherheitshinweis!

Aktive Inhalte im Email Client müssen deaktiviert werden. Dazu zählt die Ausführung von html-Code und das Nachladen externer Inhalte, die oftmals aus Design-Aspekten erlaubt sind. Also nutze zu Deiner eigenen Sicherheit nur Mails im Textformat und verzichte auf „bunte Nachrichten“.

Um die Sicherheit weiter zu erhöhen, kannst Du Deine Nachricht auch in ein Dokument schreiben, das Dokument für die Empfänger:innen verschlüsseln und als Dateianhang versenden.

Es gibt mehrere Möglichkeiten, Deinen Empfänger:innen Deinen persönlichen Schlüssel zur Verfügung zu stellen:

1. Veröffentlichung Deines Public Keys auf einem PGP Server. Jede:r kann über den Verzeichnisdienst nach Namen oder E-Mailadresse suchen und Deinen Schlüssel importieren.
2. Als Zertifikatsdatei (hängen viele E-Mailprogramme optional automatisch mit an) oder Text in einer Standard E-Mail an die Empfänger:innen senden. Das sieht dann etwa so aus (für öffentliche E-Mailadressen kannst Du das auch in Blog/Web publizieren:



3. Du triffst Dich mit den Aktivist:innen Deiner Gruppe/Bezugsgruppe persönlich und tauschst den Public Key direkt auf einem verschlüsselten USB Stick aus.

Systemvoraussetzungen:

Gpg4win läuft ab Windows Versionen 7 oder neuer (bis Windows 10), in 32- und 64bit verfügbar.

Download: https://www.gpg4win.de

Windows XP wird nicht offiziell unterstützt, es können auch nur Teile von Gpg4win verwendet werden.

Eine vollständige Dokumentation von gpg4win in deutscher Sprache findest Du hier:
https://files.gpg4win.org/doc/gpg4win-compendium-de.pdf

Installiert werden folgende Komponenten:

GnuPG
Das Kernstück, das eigentliche Verschlüsselungsprogramm.

Kleopatra Crypto Manager
Ein Zertifikatsmanager für OpenPGP und X.509 (S/MIME); stellt einheitliche Benutzerführung für alle Krypto-Dialoge bereit.

GpgEX
Eine Programmerweiterung für den Microsoft Explorer (Dateiverschlüsselung).

GPA (Optional – Installation empfohlen)
Ein alternativer Zertifikatsmanager für OpenPGP und X.509.

GpgOL
Eine Programmerweiterung für Microsoft Outlook 2003/2007/2010/2013/2016 (E-Mail-Verschlüsselung). Ab Outlook 2010 wird von GpgOL auch Exchange Server unterstützt.

Das **Outlook**-Plugin GpgOL ist kompatibel mit Microsoft Outlook 2010, 2013 und 2016 (sowohl 32 als auch 64bit) und unterstützt E-Mail Transport per SMTP/IMAP und MS Exchange Server (ab Version 2010). Outlook 2003 und 2007 werden nicht mehr vollständig unterstützt.

Für **Mozilla Thunderbird** und **SeaMonkey** kann die Erweiterung Enigmail installiert werden.

Unter MacOS X kann die GPG Suite verwendet werden: https://gpgtools.org

Unter GNU/Linux basierenden System kann meist direkt GnuPG über den Paketmanager installiert werden.

Installation:

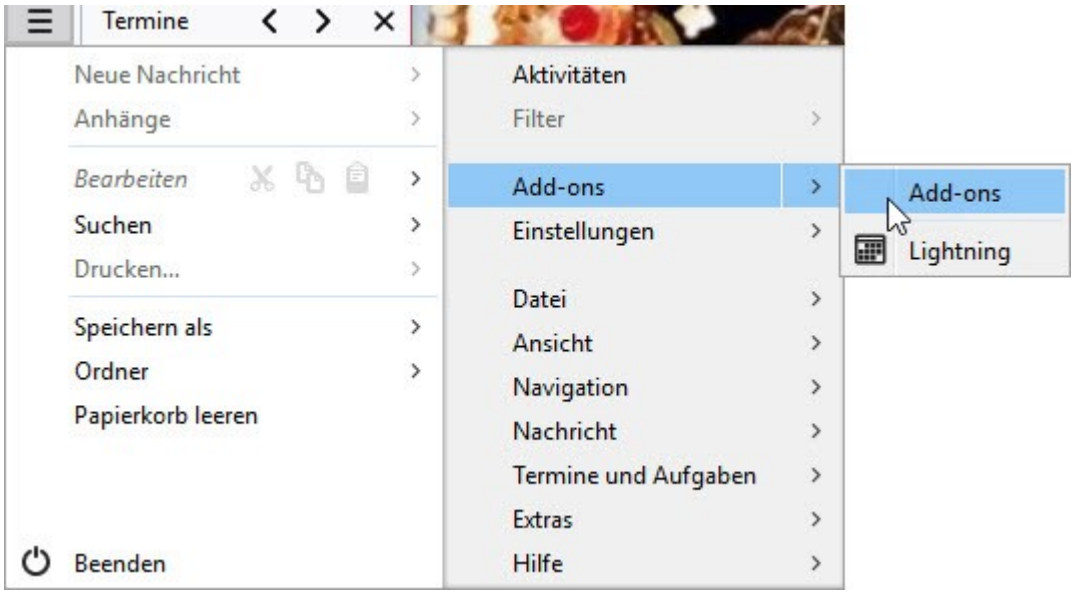
Auf eine Beschreibung der Standard Installation von Gpg4win verzichte ich an dieser Stelle, der Vorgang ist selbsterklärend. Darauf achten, dass das Modul **GPA** mit installiert wird und die Installation abschließen.

Auf den folgenden Seiten wird die Verwendung mit den wichtigsten Funktionen über Cleopatra Crypto Manager und das **GpgOL** Modul für Outlook, sowie von GnuPGP und die Erweiterung **Enigmail** für Thunderbird/Seamonkey beschrieben.

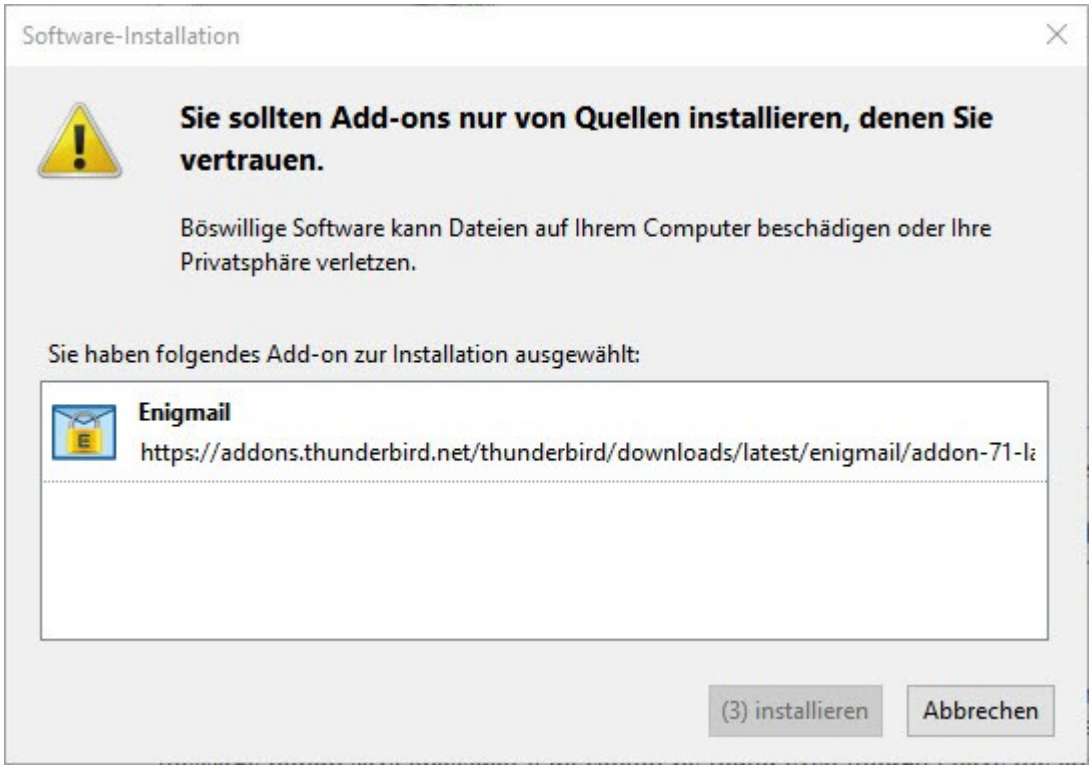
Voraussetzung für die Verwendung von Enigmail ist, dass Du gpg4win installiert hast.

Das Add on Enigmail für Thunderbird bis Version 68

Enigmail installieren



Wenn Du Dein Thunderbird gestartet hast, wählst Du Die Add ons aus.

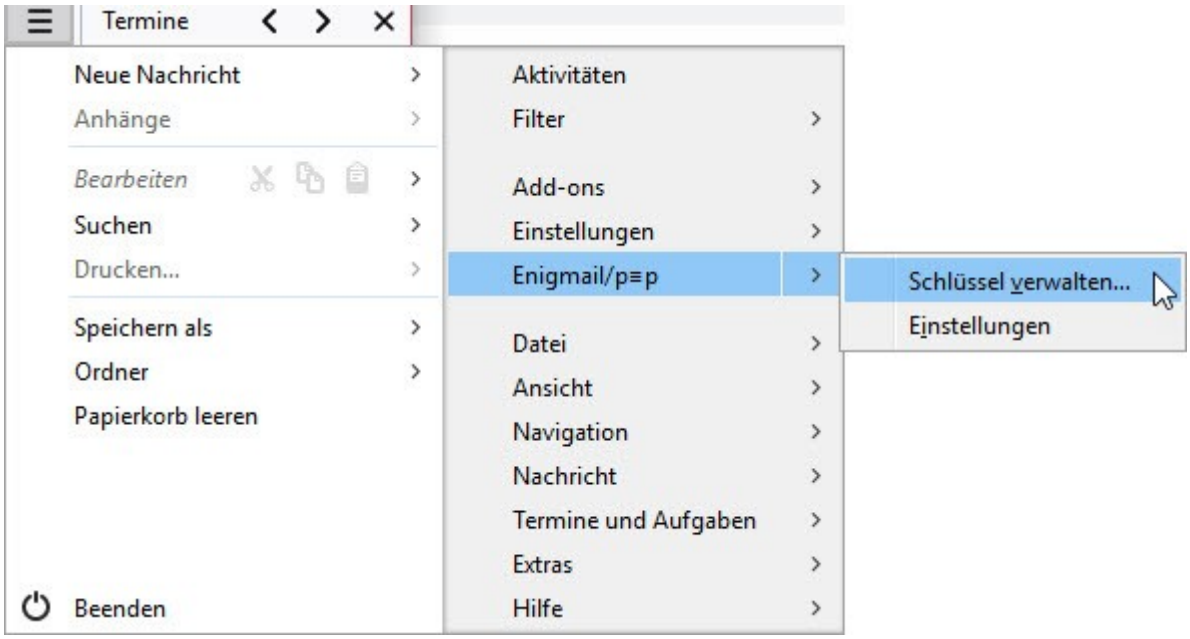


Installiere das Add on Enigmail.

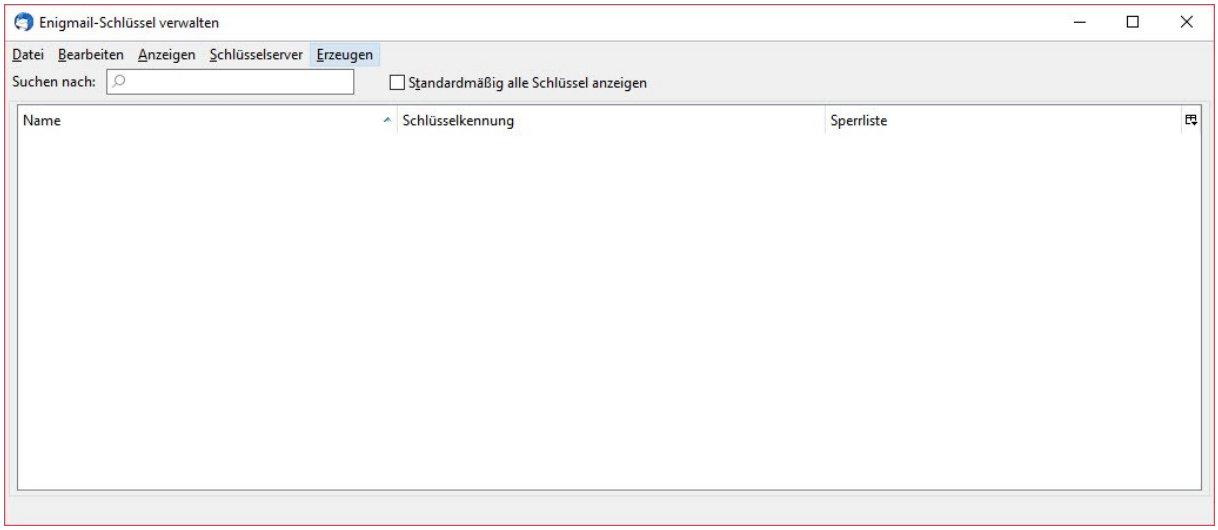
Nach der Installation beendest Du Thunderbird und startest es anschließend wieder neu.

Eine ausführliche Beschreibung in Englischer Sprache findest Du hier:
https://www.enigmail.net/index.php/en/user-manual

Das erste Schlüsselpaar installieren



Du findest nun einen Menüpunkt „Enigmail“ und kannst darüber Deine Schlüssel und Einstellungen verwalten. Rufe als erstes Deine Schlüsselverwaltung auf.



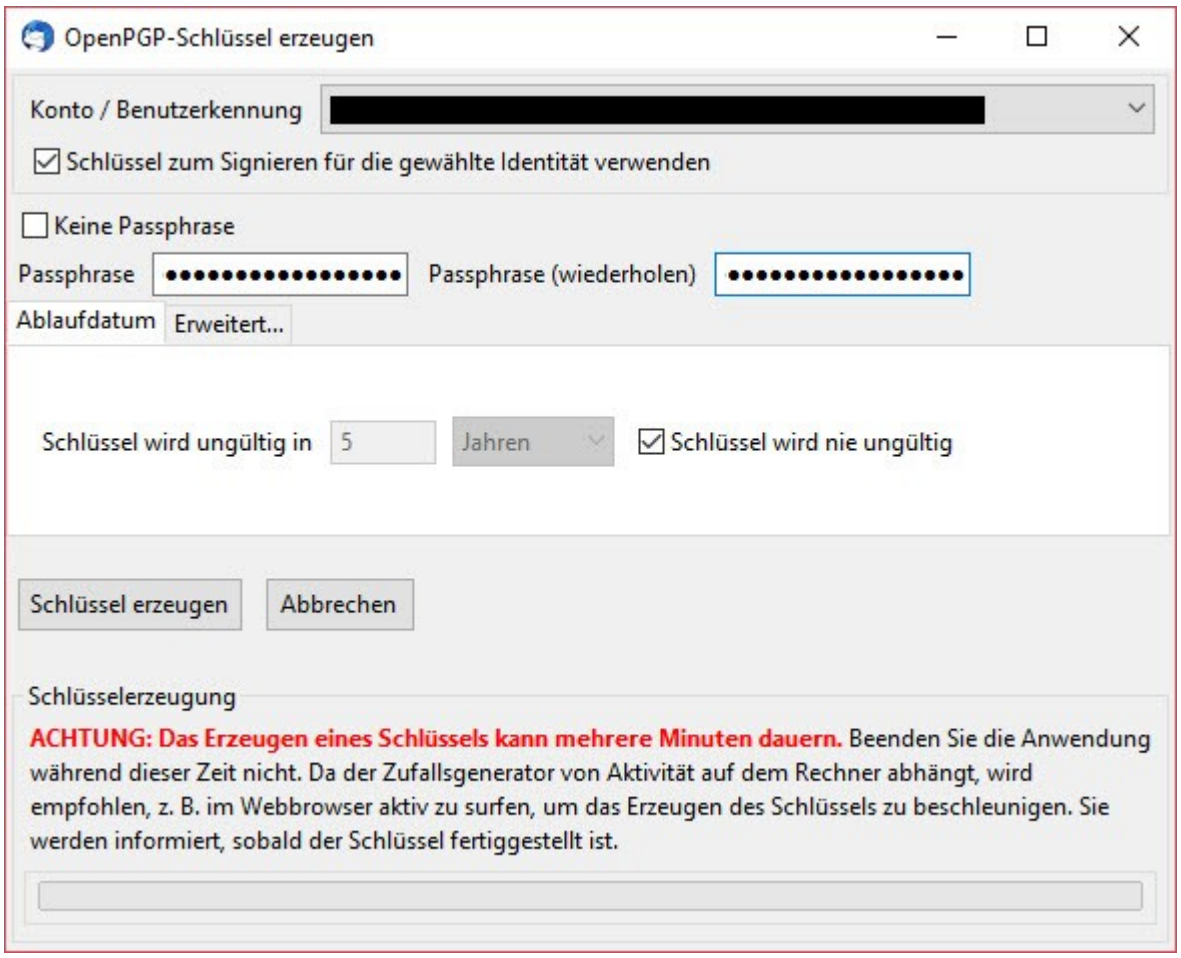
In diesem Fenster werden Dir alle Schlüssel angezeigt, Du kannst sie verwalten oder neue Schlüsselpaare erzeugen.

Als erstes benötigst Du ein eigenes Schlüsselpaar für Deine Mailadresse, einen privaten zum Öffnen von empfangenen Nachrichten/Dateien und einen öffentlichen Schlüssel, damit Deine Kontakte Deine Nachrichten/Dateien öffnen und lesen können.

Empfehlung:

Für Deine politische Arbeit solltest Du niemals Deine private oder eine Deiner „Wegwerf-Email Adressen“ verwenden.

Nutze für Deine politischen Aktivitäten einen sicheren Email Anbieter wie zum Beispiel **riseup.net** oder **systemli.org** und richte dafür umgehend einen PGP Schlüssel ein. Unterstütze die Menschen mit denen Du Kontakt hast, ebenfalls eine sichere Email und PGP für den Austausch von Email Nachrichten einzurichten.



Wenn Du „Erzeugen“ ausgewählt hast, kannst Du hier das E-Mailkonto auswählen, Dein Passwort dafür festlegen und ggf. die Dauer der Gültigkeit Deines Schlüsselpaares festlegen.

Klicke anschließend auf „Schlüssel erzeugen“.

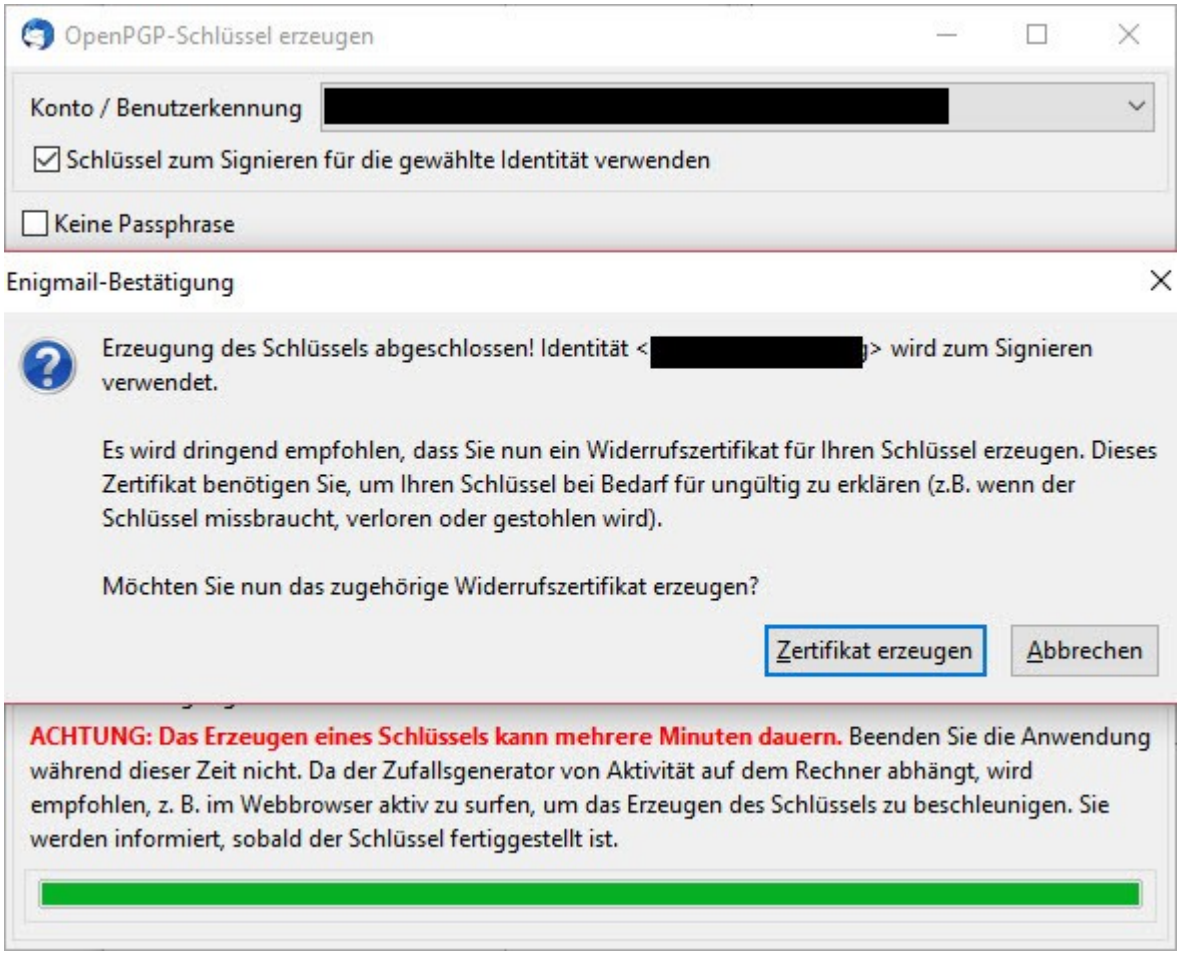
Hinweis:

Enigmail übernimmt auch über Cleopatra und GPA erstellte/importierte private und öffentliche Schlüssel und umgekehrt.

Wer Thunderbird und Enigmail nutzt, muss Cleopatra und GPA nicht zwangsläufig nutzen.

Das Add on hat eine integrierte Schlüsselverwaltung mit Zugriff auf den internen Zertifikatsspeicher Deines Rechners. Das Outlook Add on hat das nicht integriert, da muss GPA oder Cleopatra zur Verwaltung verwendet werden.

Unter „Auf Server suchen…“ kannst Du nach dem Nick oder direkt nach der E-Mailadresse Deiner Kontakte suchen.



Nach Abschluss wird Dir der Vorgang bestätigt.

Wichtig!

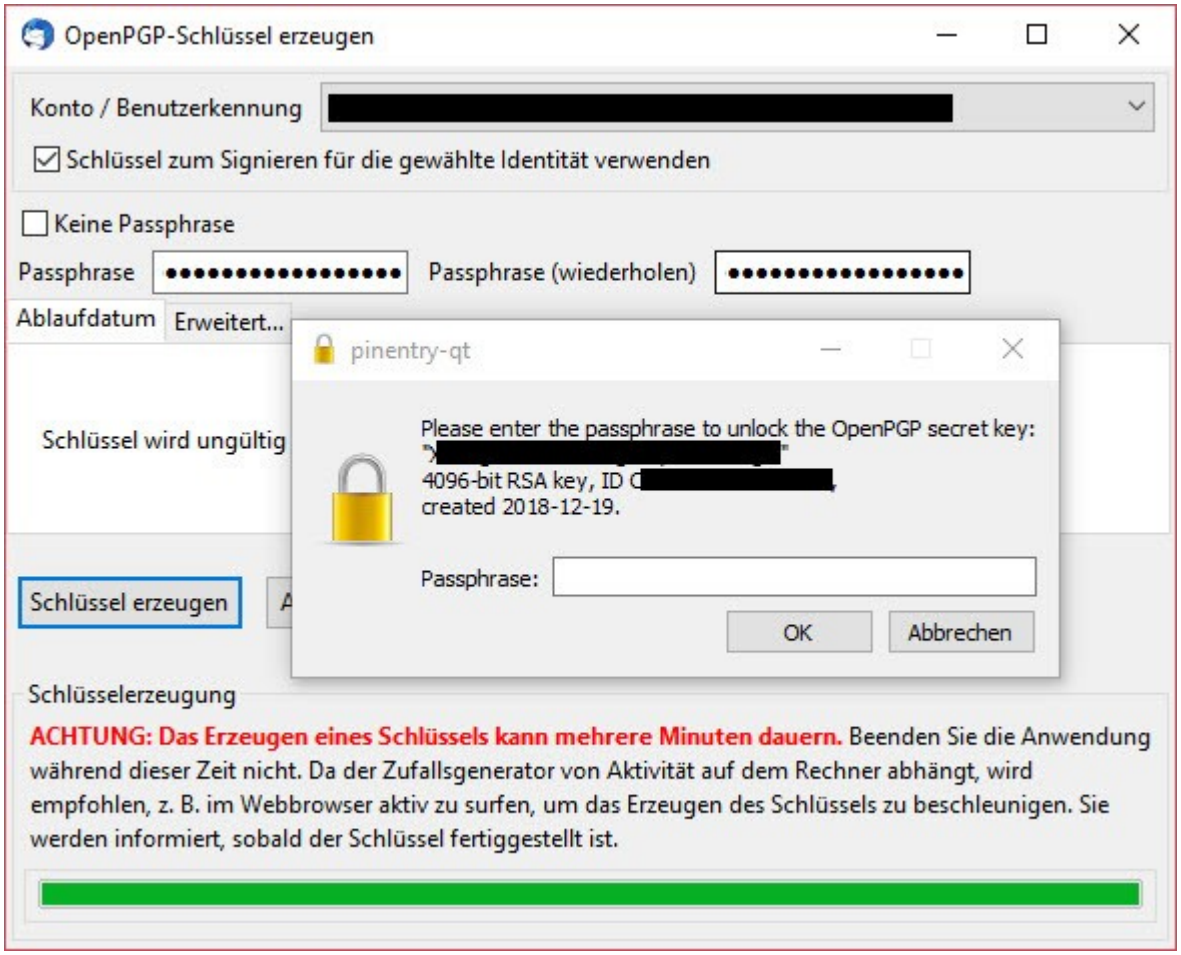
Hier hast Du nun die Möglichkeit ein Widerrufszertifikat zu erzeugen, für den Fall, dass Dein Schlüssel kompromittiert wird.

Dein privater Schlüssel bestätigt nicht nur die Echtheit des Absenders, sondern ist zusammen mit dem Passwort dann auch in der Lage, an Dich gesendete Nachrichten/Dateien zu öffnen und zu lesen.

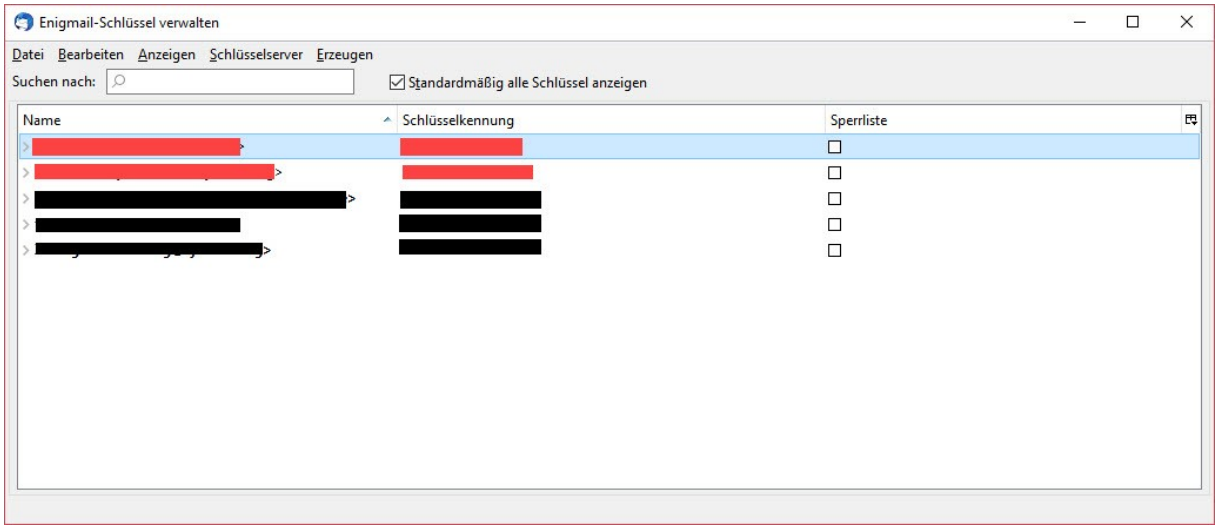
Sichere daher Deinen privaten Schlüssel und das Widerrufszertifikat auf einem mit VeraCrypt verschlüsselten USB Stick und bewahre ihn sicher auf. Am besten außerhalb Deiner Wohnung.

Wenn die Bullen Deinen Rechner beschlagnahmen, Du ihn eventuell nicht vollständig verschlüsselt hast (Systemlaufwerk), dann kannst Du mit Deinem Widerrufszertifikat Deinen Schlüssel für ungültig erklären. Bei den Menschen die mit Dir darüber kommunizieren, wird der Schlüssel als ungültig identifiziert.

Du solltest in solchen Fällen oder wenn Du Dich nach einer Beschlagnahme nicht mehr sicher fühlst, ein neues Schlüsselpaar erzeugen und den Menschen mit denen Du Kontakt hast den neuen Schlüssel mitteilen.



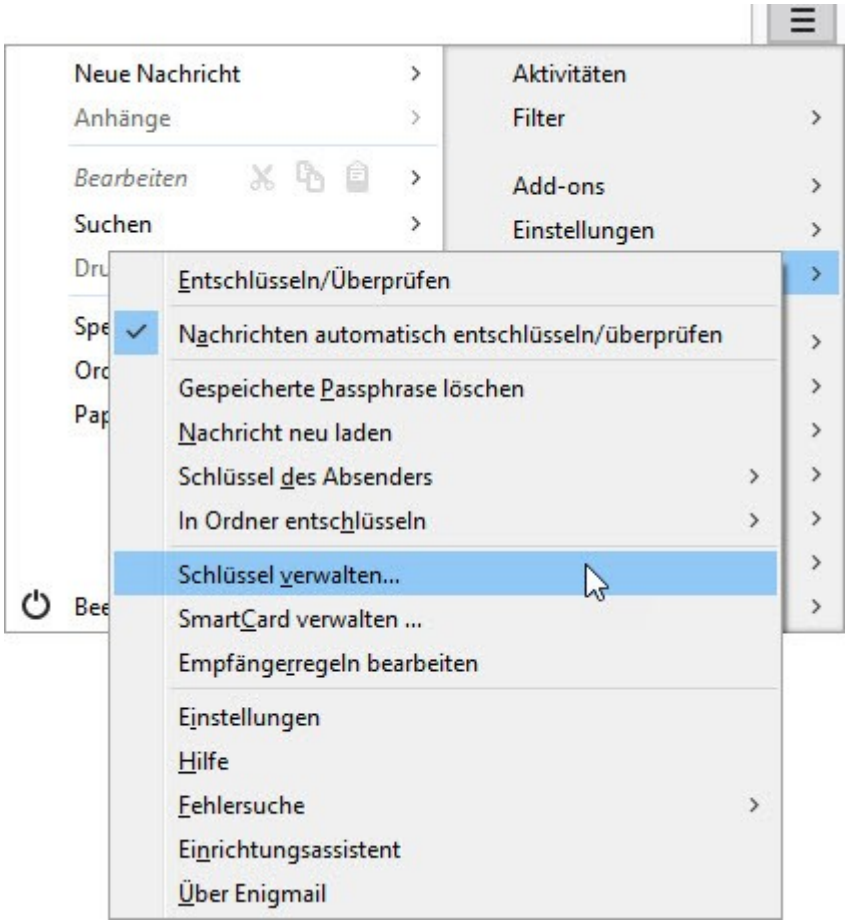
Wenn Du auf „Zertifikat erzeugen“ geklickt hast, musst Du den Vorgang mit Deinem Passwort bestätigen, sonst kann das Widerrufszertifikat nicht erstellt werden.



Fertig, in der Schlüsselverwaltung siehst Du dann Deine(n) privaten Schlüssel (Fettschrift, hier rot gekennzeichnet) und alle öffentlichen Schlüssel (normale Schrift schwarz gekennzeichnet) von den Menschen, mit denen Du Kontakt hast.

Das wird im Laufe der Zeit sehr viel mehr Einträge von öffentlichen Schlüsseln (Public Keys) geben. Du kannst nur sicher kommunizieren, wenn Du die öffentlichen Schlüssel von den Menschen, denen Du vertraust, importiert hast und sie auch Deinen öffentlichen Schlüssel importiert haben.

Enigmail Einstellungen



Über die Einstellungen von Enigmail kannst Du noch weitere Einstellungen vornehmen.

Mit dieser Anleitung sollst Du zunächst in der Lage sein Dein(e) eigenes Schlüsselpaar zu erstellen und zu verwalten, sowie die öffentlichen Schlüssel Deiner Empfänger zu importieren.

Darum wird auf jede einzelne Funktion im Detail nicht eingegangen oder nur kurz angesprochen.

Gespeicherte Passphrase löschen – wenn Du eine Nachricht mit Deinem Schlüssel geöffnet hast, bleibt das Passwort eine (einstellbare) Zeit X gespeichert. Damit kannst Du Deinen Schlüssel wieder verriegeln, wenn Du zum Beispiel Deinen Rechner kurz verlässt.

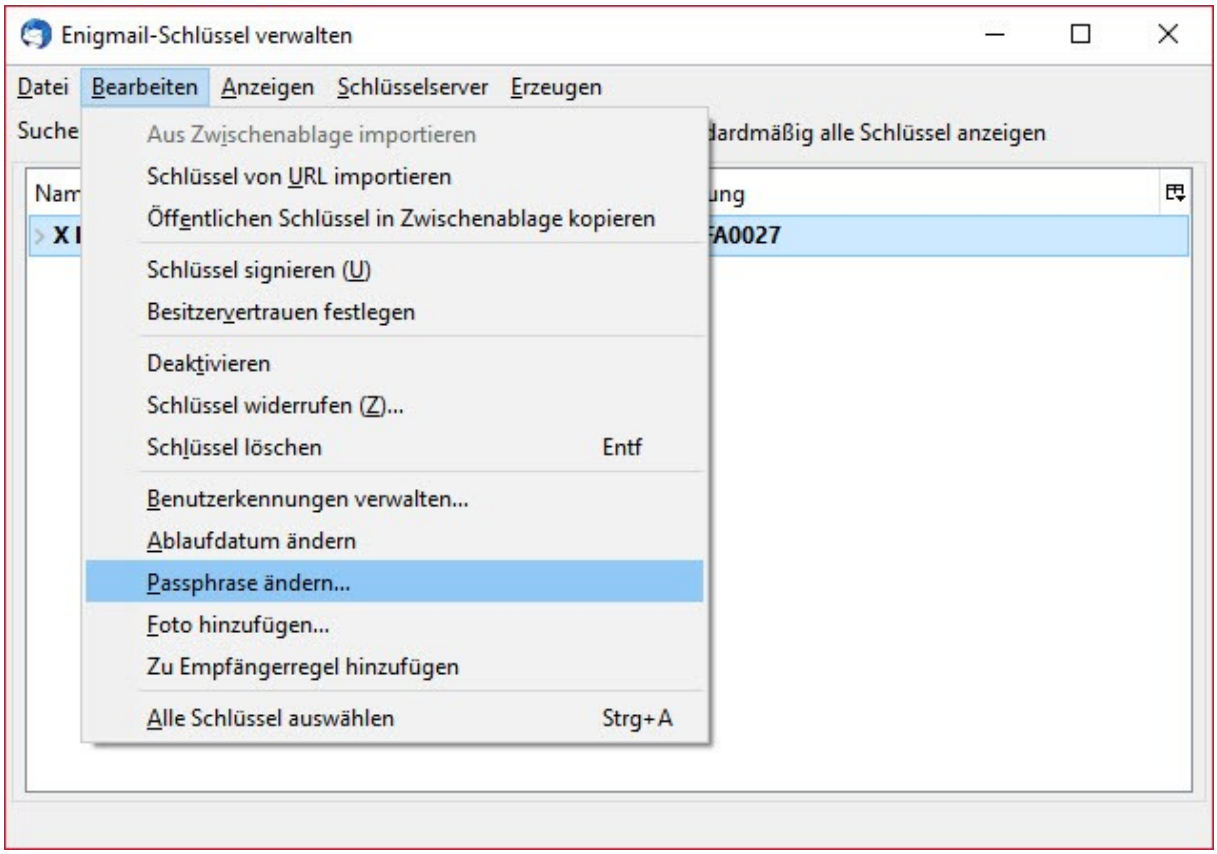
Schlüssel des Absenders – hier kannst Du einige Funktionen für den öffentlichen Schlüssel Deines Kontaktes abrufen, zum Beispiel auch den Schlüssel importieren, sofern er öffentlich publiziert wurde.

Einstellungen – grundsätzliche Funktionen von Enigmail, zum Beispiel wie lange Deine Passphrase gespeichert bleiben soll, bis Du wieder danach gefragt wirst.

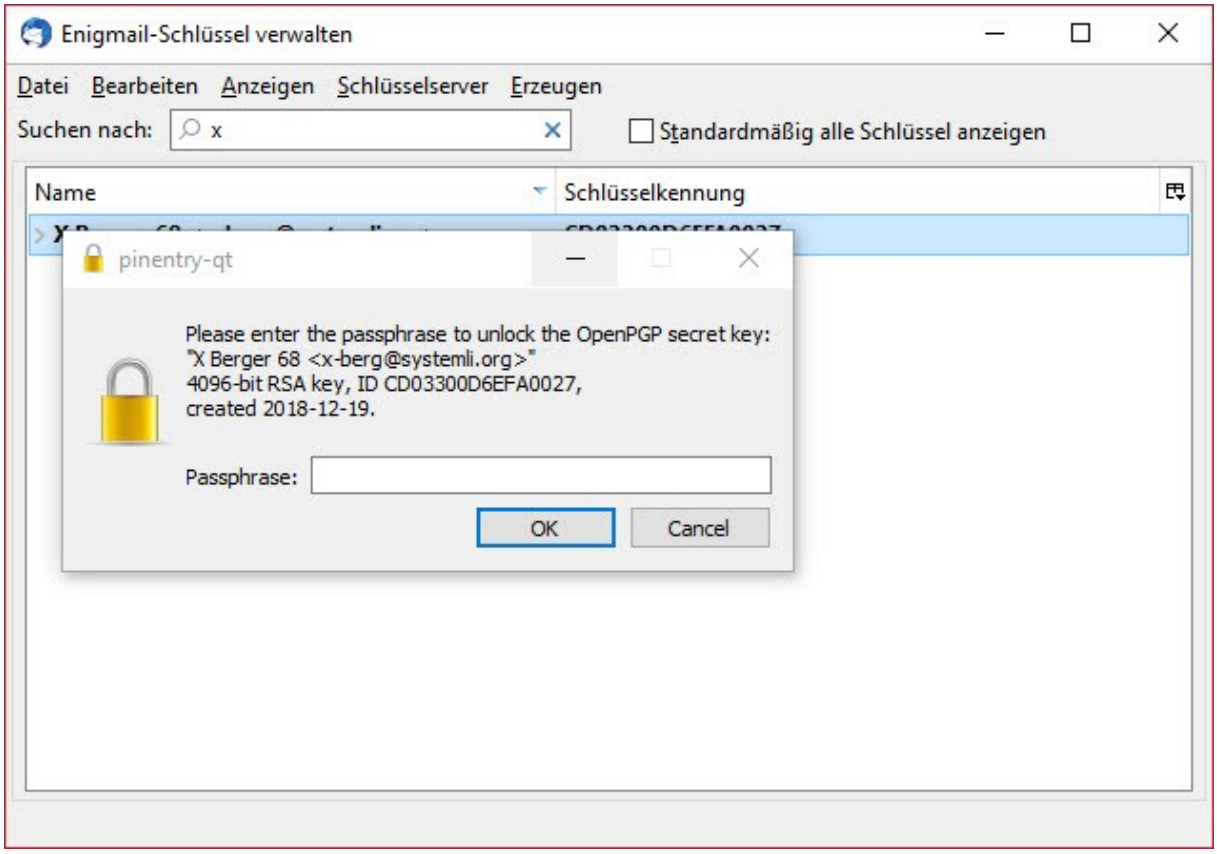
Schlüssel verwalten – die wichtigste Funktion in Enigmail, hier kannst Du Dein(e) Schlüsselpaar(e) und die öffentlichen Schlüssel Deiner Kontakte suchen, importieren, bearbeiten, löschen.

Um eine höchst mögliche Sicherheit zu erreichen, empfiehlt es sich von Zeit zu Zeit in unregelmäßigen Abständen seine Passphrase (Passwort) zu ändern. Dazu rufst Du die Schlüsselverwaltung auf

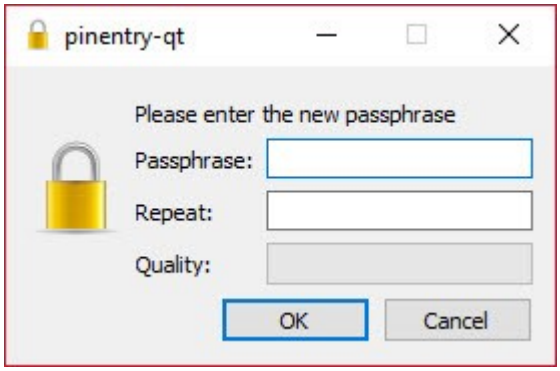
Passwort Deines privaten Schlüssels ändern



In der Schlüsselverwaltung wählst Du „Passphrase ändern…“ aus.



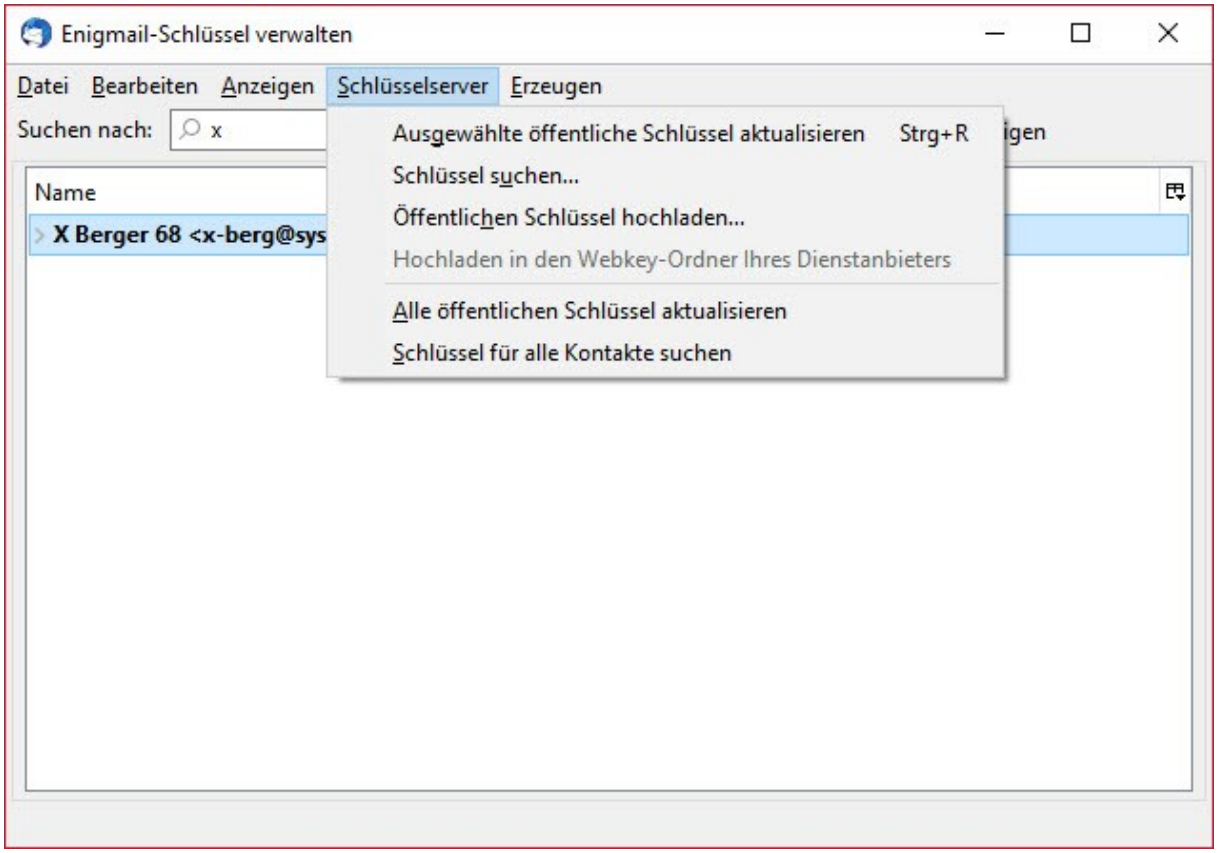
Für alle Aktionen, die die Sicherheit Deines privaten Schlüssels betreffen, musst Du nun Deine Passphrase eingeben. Erst dann kannst Du Dein Passwort neu vergeben.



Da Du Dein altes Passwort bereits bestätigt hast, kannst Du nun ein neues Passwort vergeben. Zur Überprüfung und Sicherheit gegen Tippfehler muss Du Dein neues Passwort doppelt eingeben.

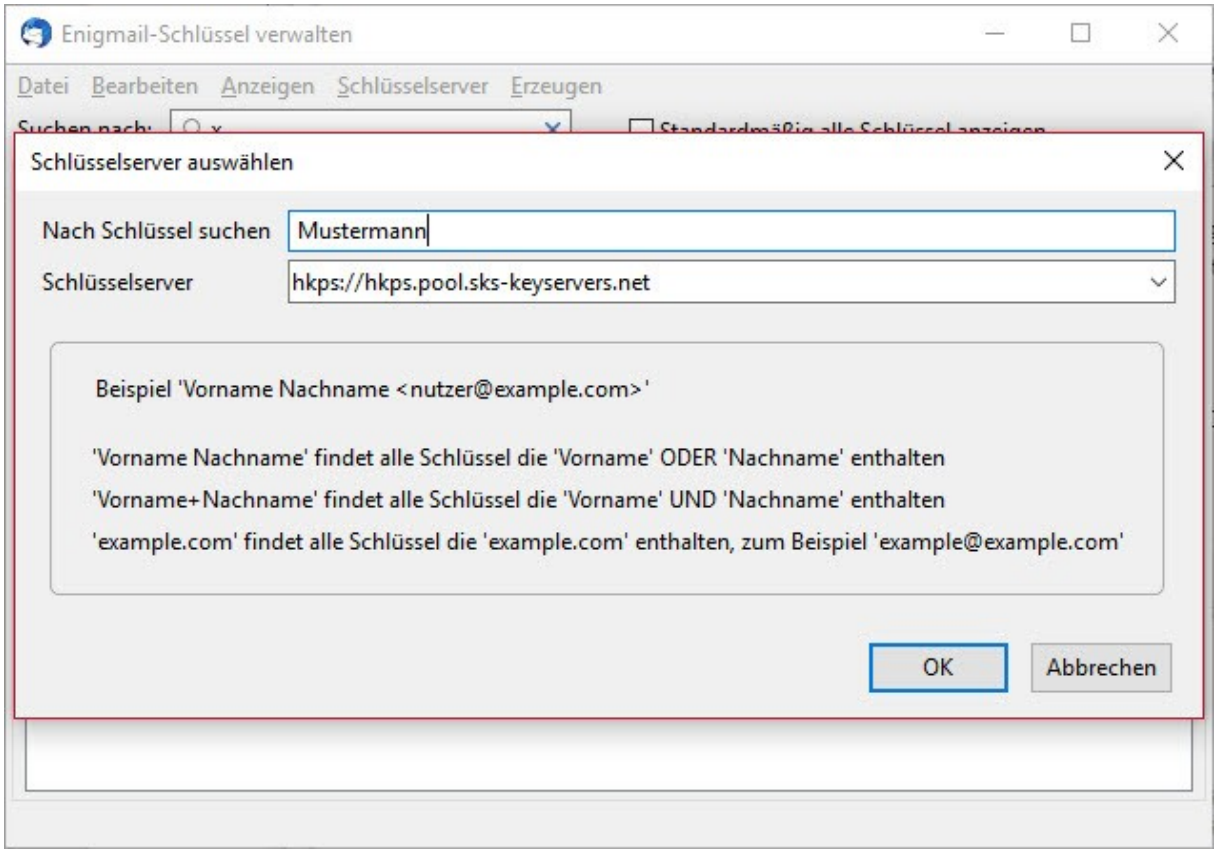
Klicke dann auf OK – Deine Passphrase wurde erfolgreich geändert.

Öffentliche Schlüssel suchen und importieren

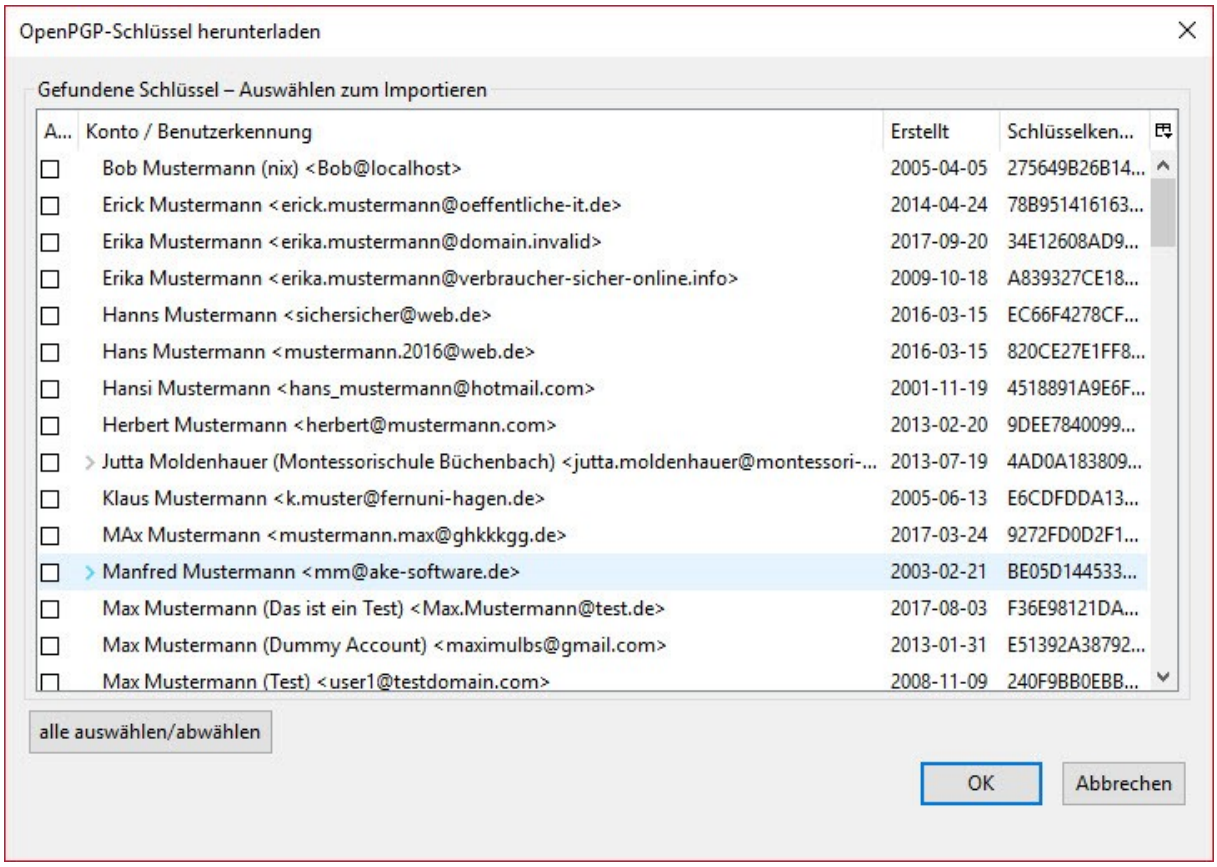


Unter Schlüsselserver hast Du verschiedene Funktionen zur Bearbeitung Deiner Schlüssel.

Du kannst Schlüssel auf einem öffentlichen Schlüsselserver suchen, Deinen eigenen öffentlichen Schlüssel hochladen, usw.



Wenn Du einen Schlüssel Deines Kontaktes suchst, kannst Du das nach verschiedenen Kriterien definieren (siehe Hinweis). Nach Klick auf „OK“ wird der öffentliche Schlüsselserver durchsucht.



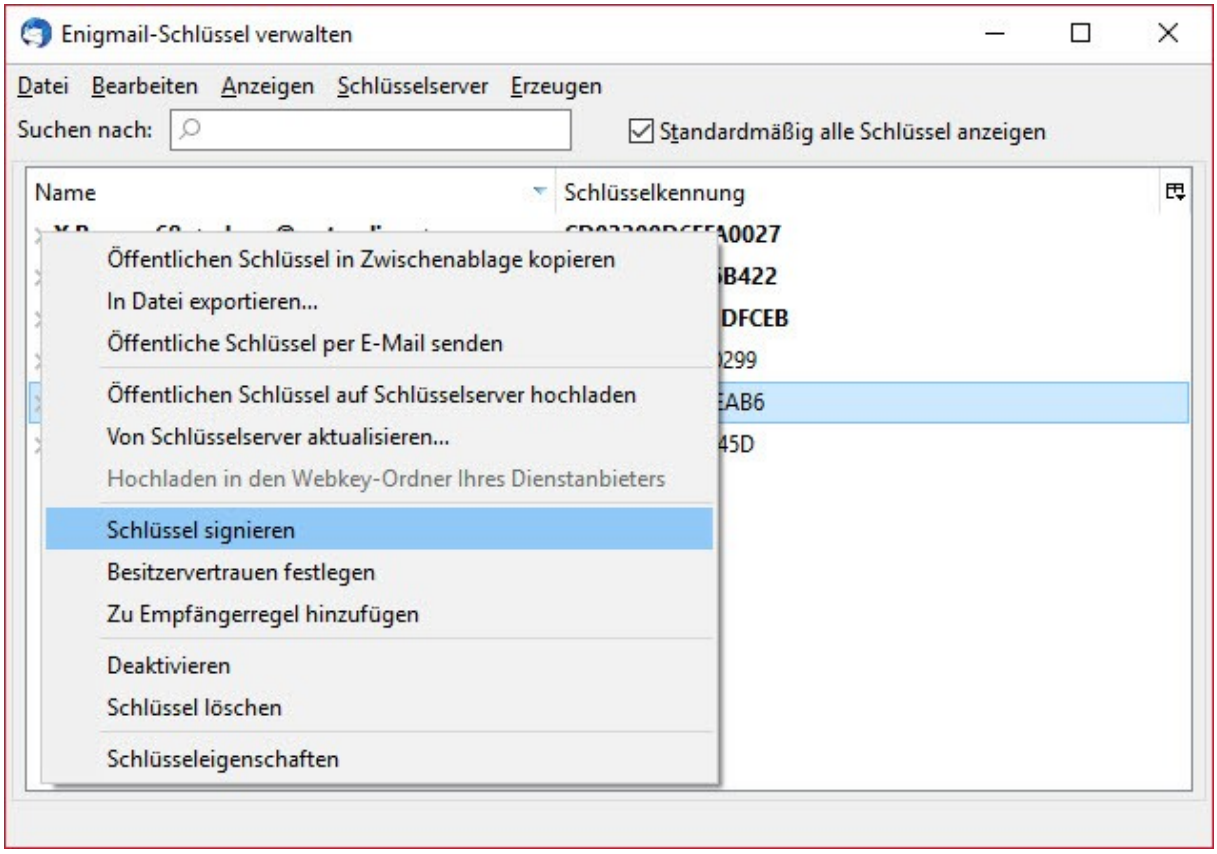
Hier findest Du alle Ergebnisse zu Deinem Suchbegriff und kannst den oder die richtigen Schlüssel nach Auswahl und Klick auf „OK“ importieren.

Schlüssel signieren

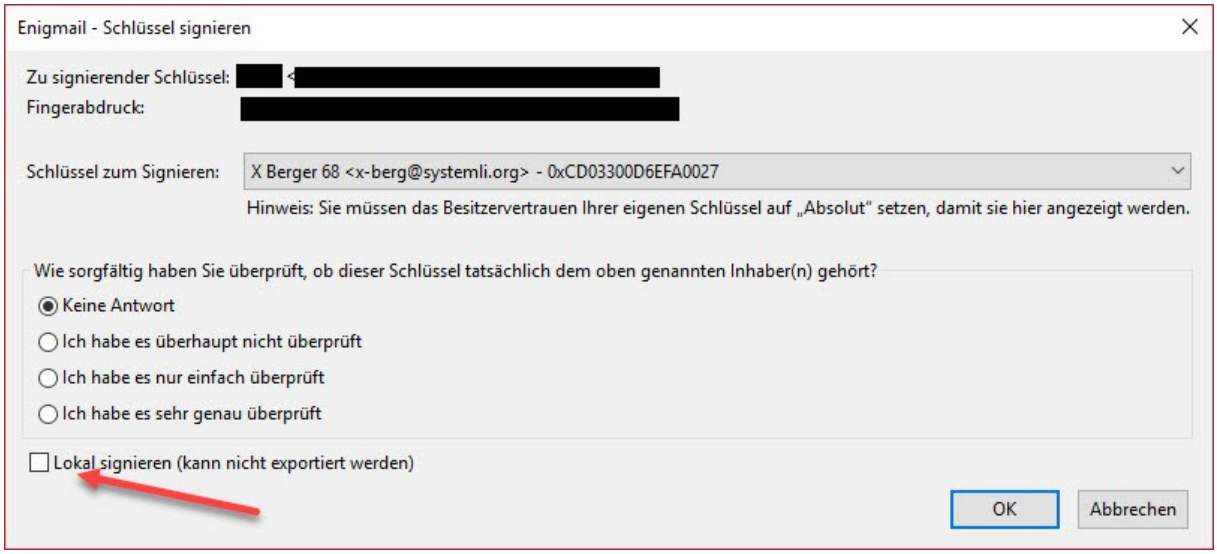
Einen öffentlichen Schlüssel zu erhalten oder von einem Schlüsselserver zu importieren sagt rein gar nichts aus, umgekehrt ist auch nicht sichergestellt, dass der von Dir versendete öffentliche Schlüssel auch tatsächlich von Dir verschickt wurde.

Enigmail bietet Dir die Möglichkeit, öffentliche Schlüssel zu beglaubigen, zum Beispiel wenn Du Dich persönlich oder durch einen Anruf vom richtigen Fingerabdruck überzeugst.

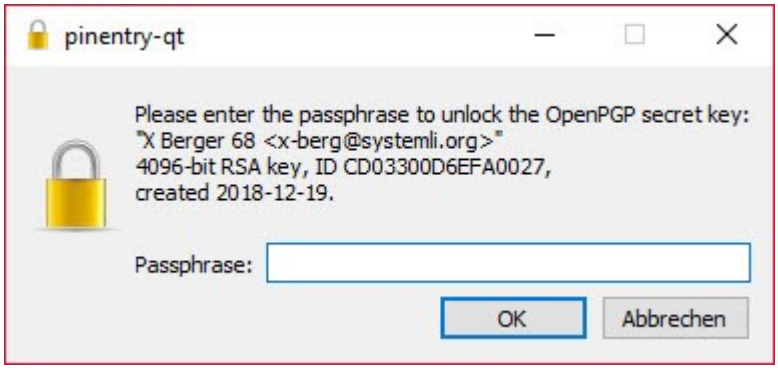
Dazu klickst Du mit der rechten Maustaste auf einen Schlüssel, den Du signieren möchtest.



Hier legst Du fest, ob Du den öffentlichen Schlüssel geprüft hast.

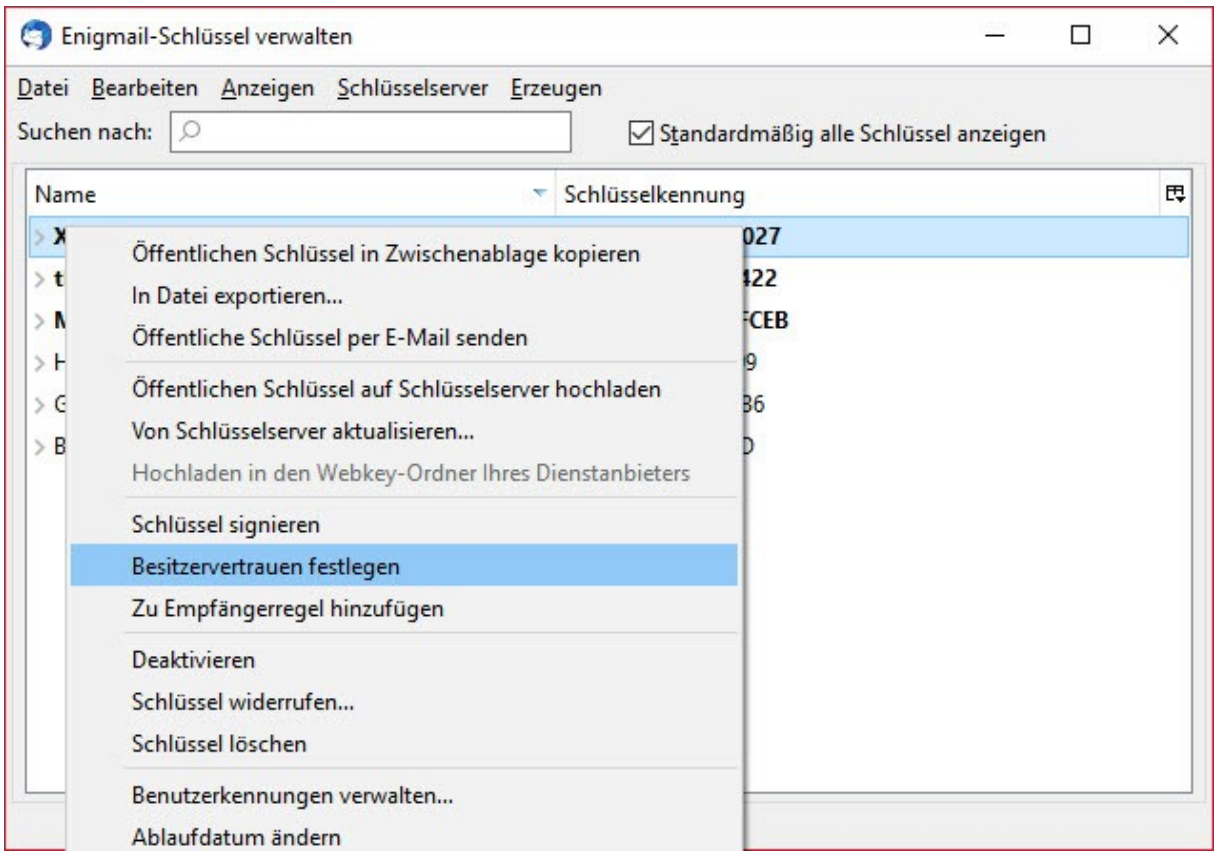


Wenn Du das nicht öffentlich zeigen willst, setze hier (siehe Pfeil) einen Haken (dringend empfohlen).



Der Vorgang wird erst durchgeführt, wenn Du die Aktion mit Deinem privaten Schlüssel verifiziert hast.

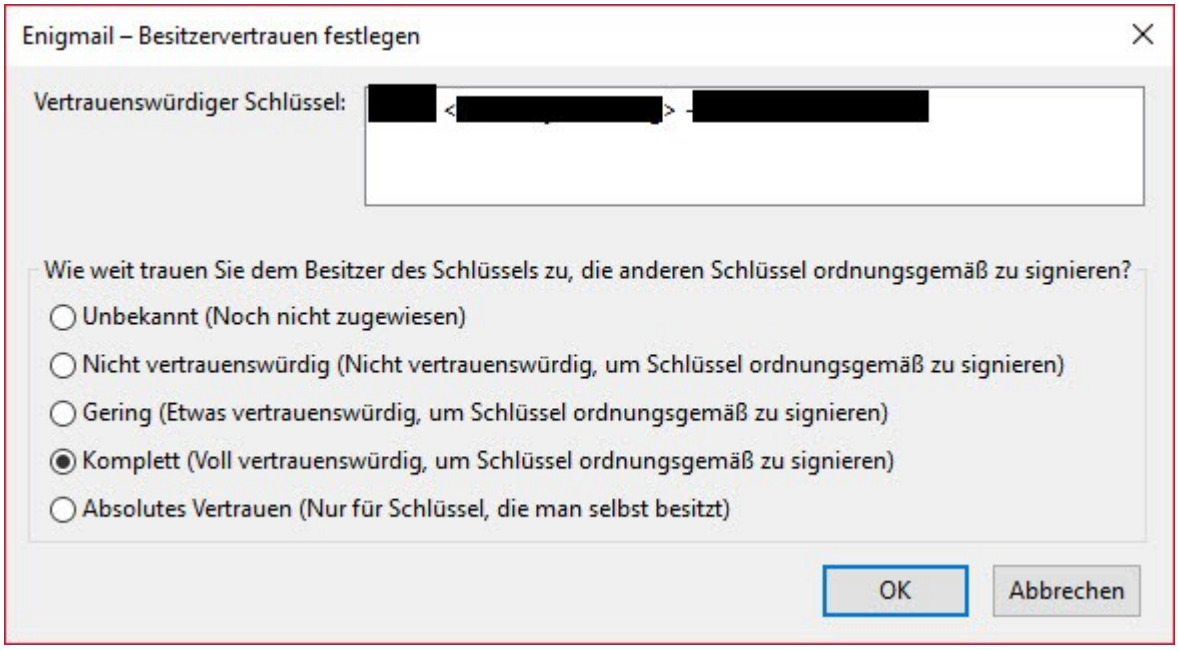
Wichtiger Hinweis!



Enigmail bietet auch die Funktion „Besitzervertrauen festlegen“.

Damit ist **nicht** gemeint, dass Du Dich davon überzeugt hast, dass der Schlüssel tatsächlich der/dem Absender:in gehört oder nicht.

Diese Funktion wird ausschließlich über Schlüssel signieren gewährleistet.



Hier legst Du fest, wie weit Du der/dem Besitzer:in vertraust, andere öffentliche Schlüssel zu signieren.

Beispiel:

Du hast mit User:in „A“ und „B“ einen Schlüssel ausgetauscht, weißt aber, dass „A“ so ziemlich jeden anderen öffentlichen Schlüssel signiert, auch wenn er die Identität nicht geprüft hat.

Hier solltest Du das Besitzervertrauen als „Nicht vertrauenswürdig“ festlegen.

Von „B“ weißt Du, dass er sehr genau die Identität der anderen Schlüssel überprüft und sie auch gewissenhaft signiert.

Hier kannst Du das Besitzervertrauen mit „Komplett“ festlegen.

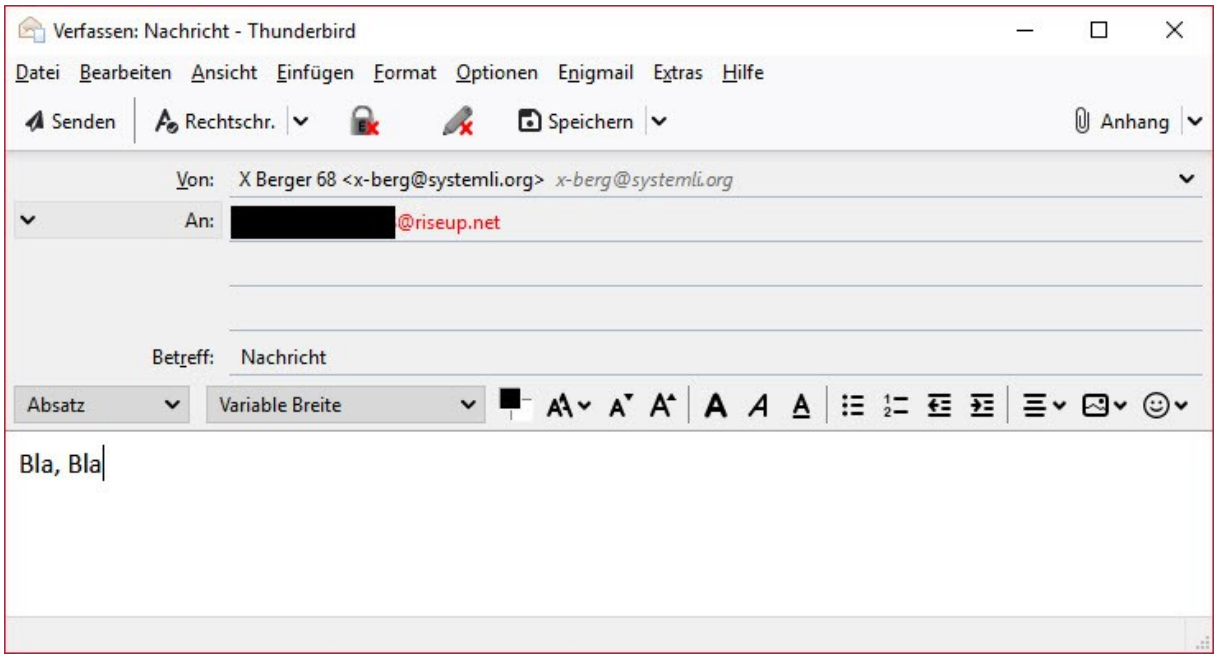
Die Festlegung sagt nichts über die User:in selbst aus, Du kannst beide Schlüssel trotzdem als „sehr genau überprüft“ signieren.

Lediglich von User:in „A“ signierte Schlüssel werden beim Import nicht als vertrauenswürdig eingestuft und müssen von Dir selbst entsprechend geprüft und signiert werden.

Diese Funktion ist nicht notwendig, wenn Du Deine importierten öffentlichen Schlüssel nur lokal signierst.

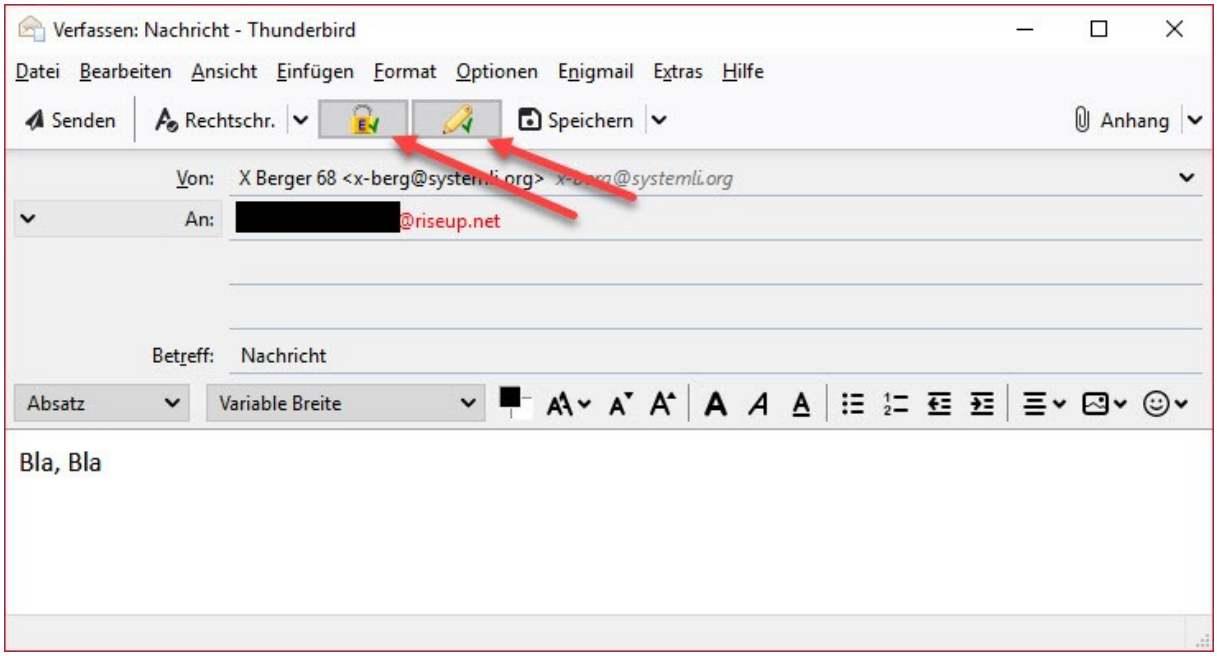
Eine ausführliche Dokumentation zu Enigmail in Englischer Sprache findest Du hier:
https://www.enigmail.net/index.php/en/user-manual

E-Mails mit Thunderbird versenden

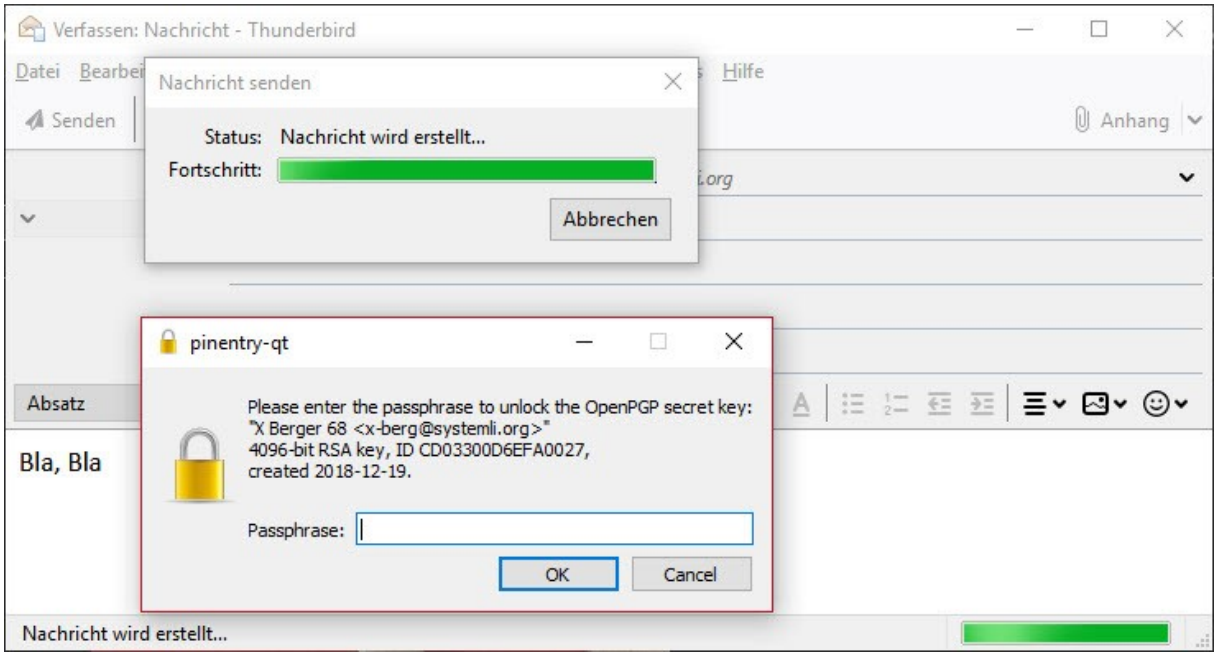


Wenn Du eine neue Nachricht schreiben willst und das Schloss- wie auch Stiftsymbol nicht grau hinterlegt und mit einem roten X versehen sind, dann wird Deine Nachricht nicht automatisch signiert und verschlüsselt.

In dem Fall kannst Du beide Symbole auch manuell auswählen, um Verschlüsselung und signieren zu aktivieren.

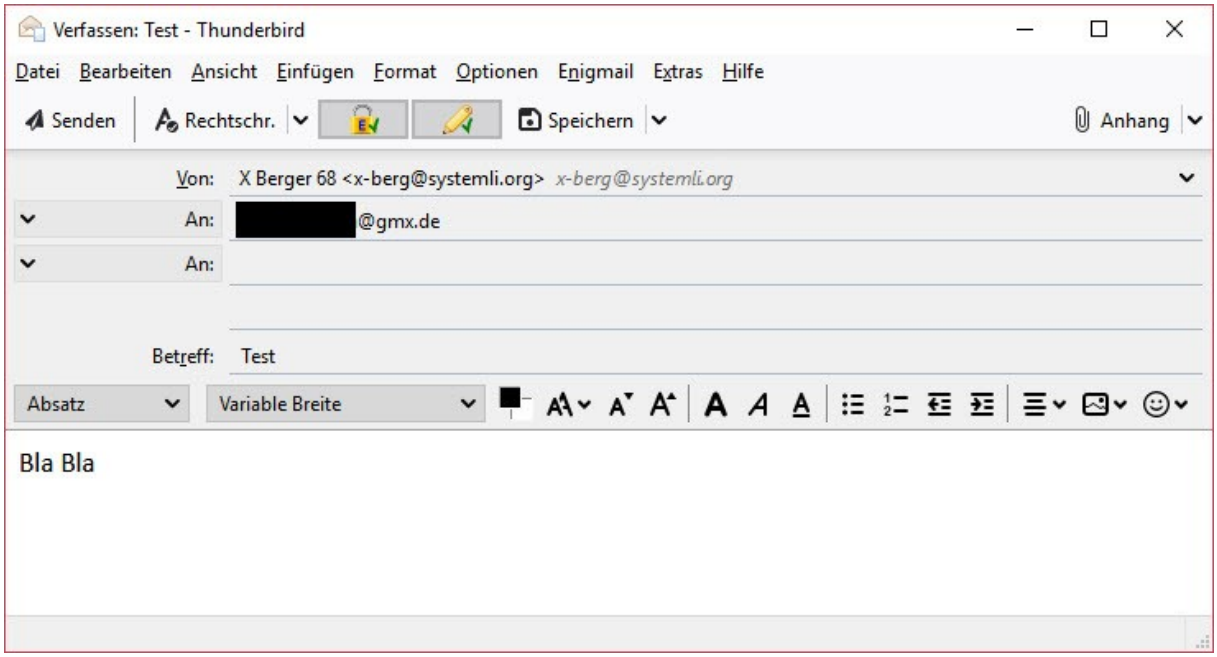


Sind das Schloss- wie auch Stiftsymbol grau hinterlegt und grün angehakt sind, dann wird Deine Nachricht Signiert und verschlüsselt.

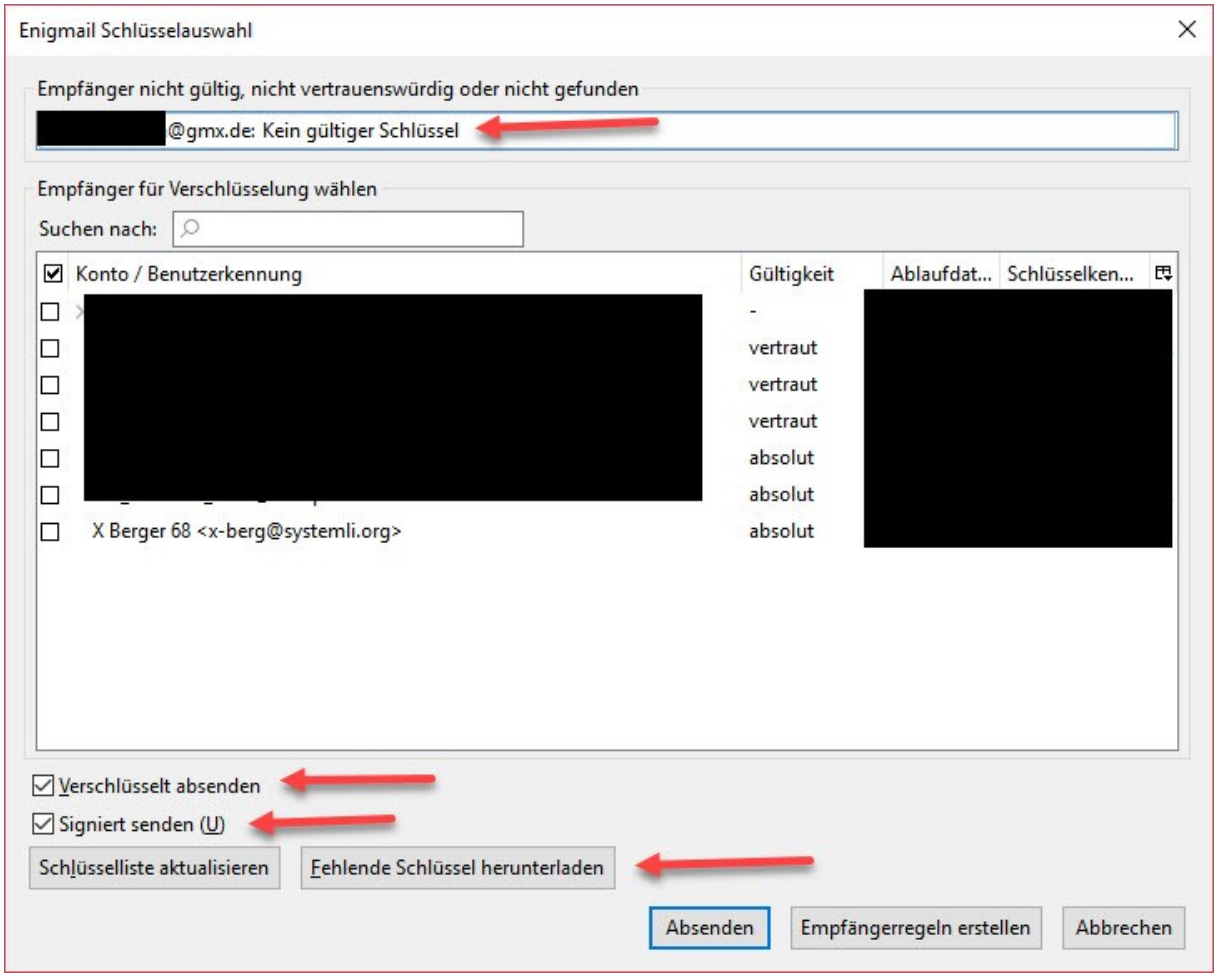


Vorausgesetzt, Du kannst den Vorgang mit dem Passwort Deines privaten Schlüssels verifizieren, erst dann wird diese Nachricht verschlüsselt und signiert versendet. In Deinem Verzeichnis „Gesendet“ wird diese Nachricht ebenfalls signiert und verschlüsselt abgelegt.

Klickst Du später Deine gesendete Nachricht an, muss sie auch wieder mit Deinem privaten Schlüssel geöffnet werden.



Schauen wir uns noch an was passiert, wenn Du für die Empfänger:innen keinen öffentlichen PGP Schlüssel importiert hast, Deine Nachricht ist auf verschlüsseln/signieren eingestellt.



Beim Versuch zu senden öffnet sich die „Enigmail Schlüsselauswahl“ und zeigt Dir ganz oben auch den Grund dafür an.

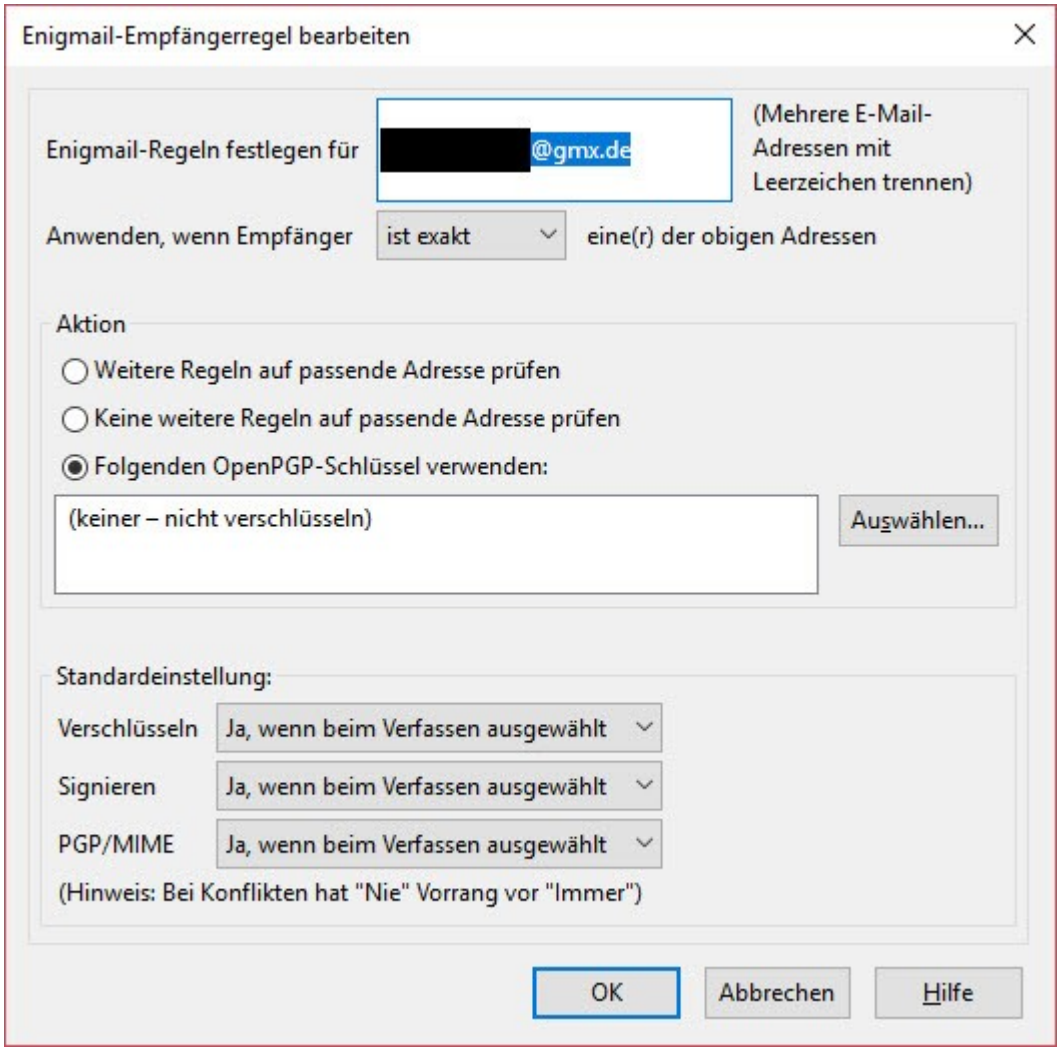
Enigmail bietet hier weit mehr Möglichkeiten und Funktionen als Outlook mit GpGOL an, um das Problem zu lösen:

- Du kannst die Option „Verschlüsselt absenden“ entfernen
- Du kannst die Option „Signiert senden“ entfernen
- Du kannst Deine Schlüsselliste aktualisieren oder fehlende Schlüssel herunterladen, also direkt von Enigmail aus auf einen Schlüsselserver zugreifen

Wenn Du Deine Auswahl getroffen hast, klickst Du auf „Absenden“.

Es gibt immer wieder Empfänger:innen, die keine PGP Verschlüsselung verwenden, auch nicht verwenden können oder dürfen.

Dank der Enigmail Empfängerregeln kannst Du die Prozedur der „Enigmail Schlüsselauswahl“ deutlich reduzieren. Das schauen wir uns auch noch kurz an.



Wenn Du also weißt, dass diese @gmx.de Adresse niemals PGP verwenden wird, dann kannst Du hier festlegen, wie Enigmail beim Senden der Nachricht weiter vorgehen soll.

Legst Du keinen OpenPGP Schlüssel fest, wird die Nachricht nicht verschlüsselt.

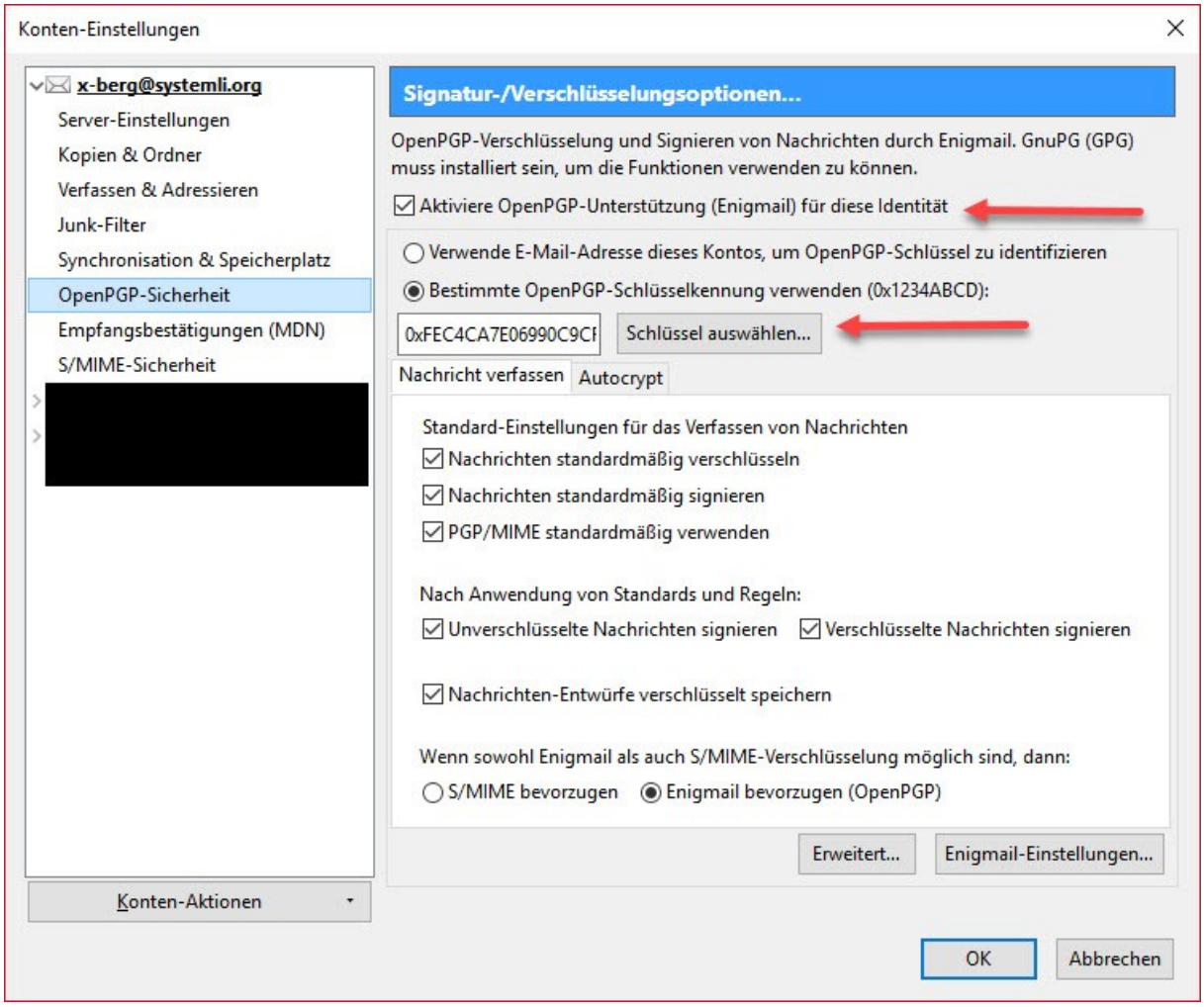
Auch kannst Du die Standardeinstellungen für die Empfänger:innen überschreiben die Du festgelegt hast und die nach Deinen Bedingungen erkannt werden.

Klickst Du dann auf „Senden“ wird Deine Nachricht entsprechend Deiner Enigmail-Empfängerregel ohne Abfragen versendet

Eigentlich alles ganz einfach, wenn da nicht noch ein Tick Komfort und vor allem ein Tick Sicherheit in der Handhabung beim Versenden von Nachrichten schöner wäre:

1. Du willst eigentlich immer signiert und verschlüsselt senden, sofern es geht (die Empfänger:innen bereits einen PGP Schlüssel haben) und nicht extra die Optionen aktivieren müssen.
2. Du möchtest aus Gründen der Sicherheit einen Hinweis erhalten, wenn Deine Nachricht nicht verschlüsselt gesendet werden kann.
3. Du möchtest auch automatisch Deinen öffentlichen Key mit an eine Nachricht hängen.
4. Wie verwaltest Du mehrere E-Mailkonten mit den dazugehörigen privaten Schlüsseln?

Das hört sich auf den ersten Blick wieder kompliziert, ist es aber nicht. Klicke mit der rechten Maustaste auf Dein E-Mailkontonamen und wähle im Kontextmenü „Einstellungen“ aus.



Es öffnet sich das Fenster „Konten-Einstellungen“, wähle hier die Option „OpenPGP-Sicherheit“ aus.

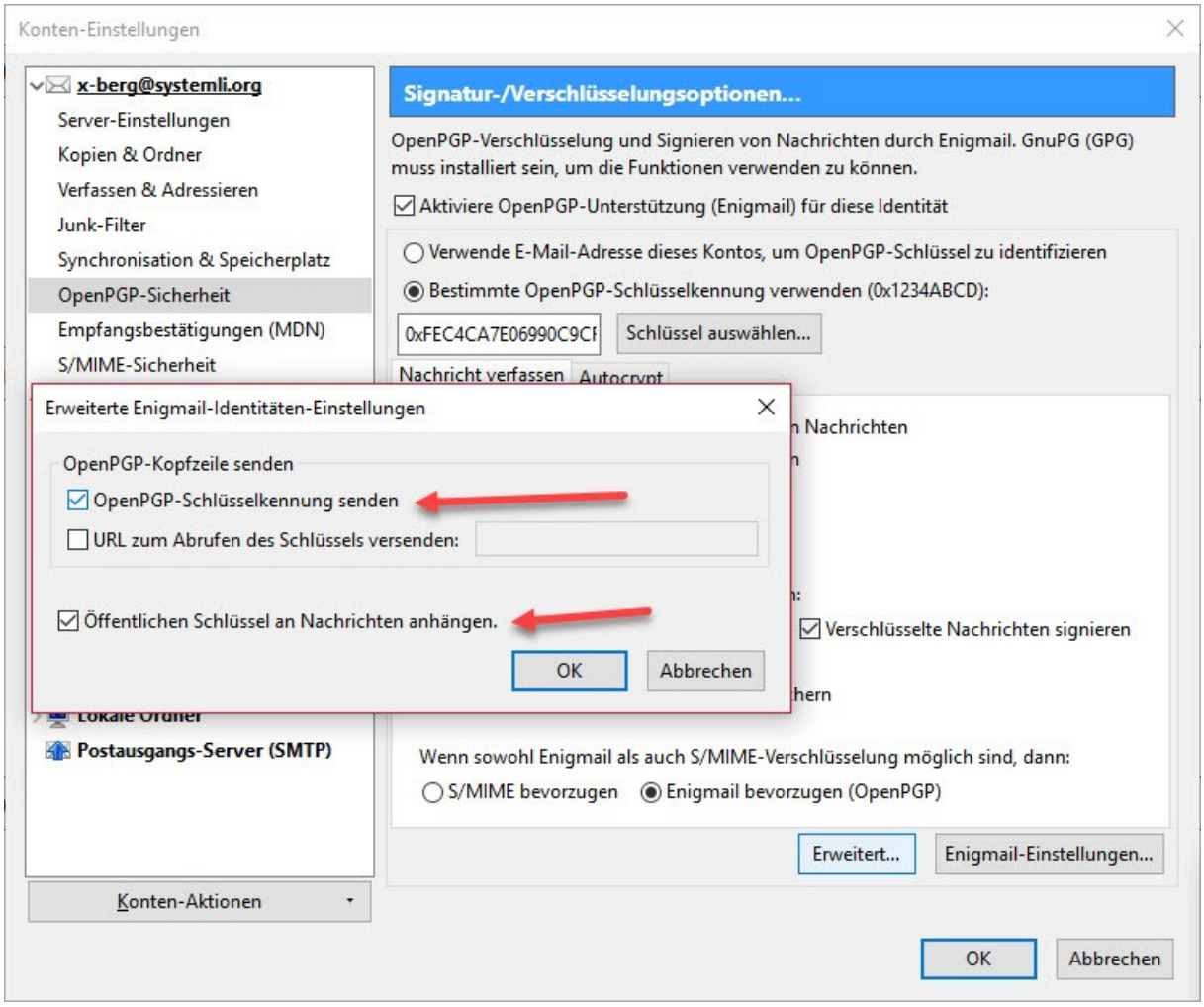
Zuerst aktivierst Du die OpenPGP-Unterstützung für Dein E-Mailkonto.

Im nächsten Schritt wählst Du Deinen privaten Schlüssel für die E-Mailadresse aus, die Du gerade bearbeitest.

Der Abschnitt „Nachricht verfassen“ enthält dann die gewünschten Standardeinstellungen für das Verfassen von Nachrichten.

Am Ende sollte die Option „Enigmail bevorzugen (OpenPGP) ausgewählt sein.

Ein Teil haben wir damit schon für ein Konto geschafft, klicke nun auf „Erweitert…“



Es öffnet sich ein Fenster, in dem Du spezielle Enigmail Einstellungen für Deinen Schlüssel vornehmen kannst.

Open PGP-Schlüsselkennung senden – damit haben die Empfänger:innen die Möglichkeit, die angezeigte Schlüsselkennung mit Deiner Website oder auf dem Key Server zu vergleichen.

URL zum Abrufen des Schlüssels versenden – hier kannst Du einen Link zu einer Seite auf Deiner Homepage eintragen, die Deinen öffentlichen Schlüssel enthält.

Beispiel: www.meine-domain.org/publickey.html

Im Format:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Schlüsseldaten

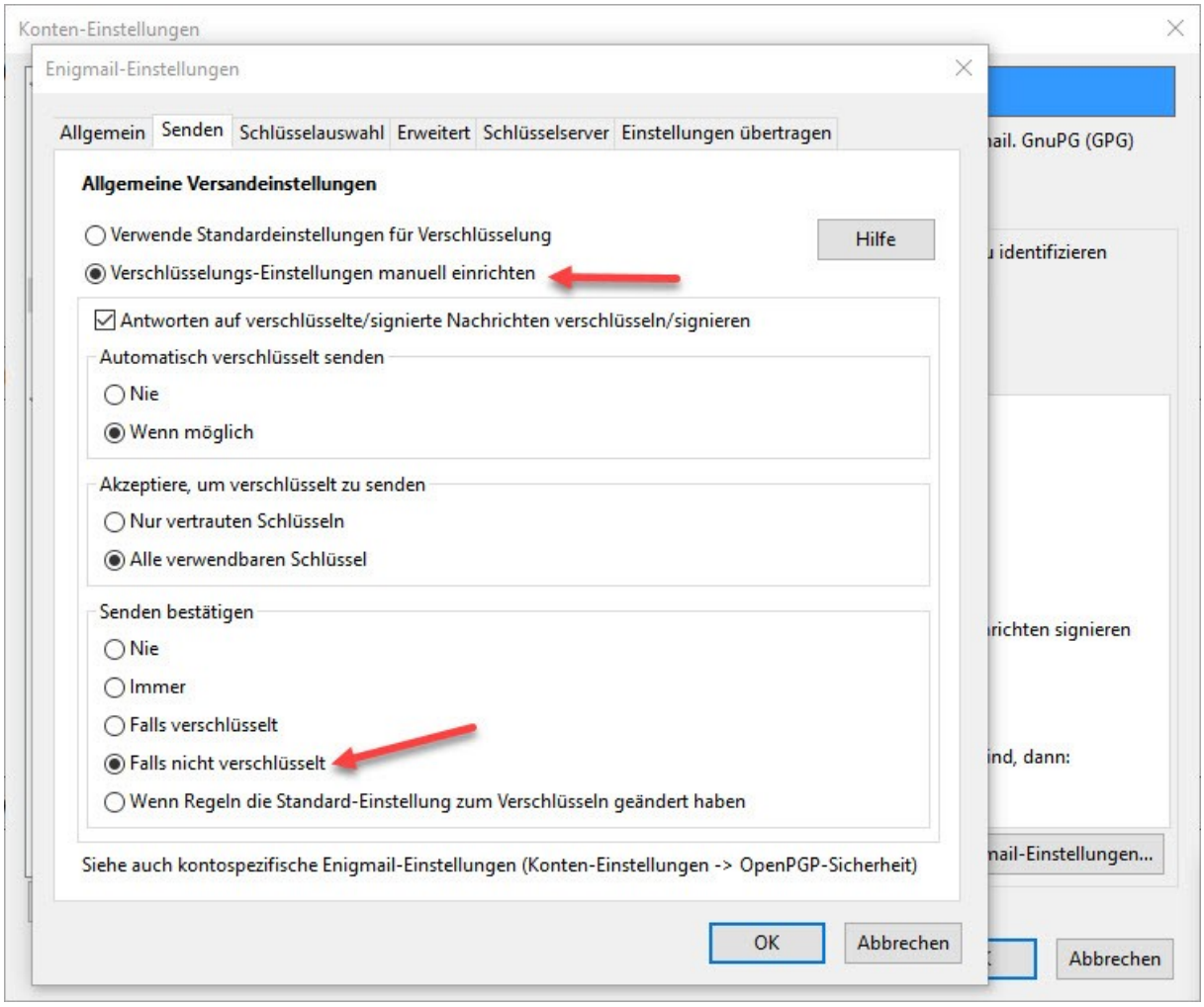
-----END PGP PUBLIC KEY BLOCK-----

Öffentlichen Schlüssel an Nachrichten anhängen – damit sendest Du jedes Mal eine Kopie Deines öffentlichen Schlüssels an die Empfänger:innen mit.

Das ganze dann mit „OK“ speichern.

Jetzt fehlt uns nicht mehr viel und alle notwendigen Einstellungen sind erledigt.

Klicke dazu auf „Enigmail-Einstellungen…“



Im Fenster „Enigmail-Einstellungen…“ klickst Du zuerst auf „Verschlüsselungs-Einstellungen manuell einrichten“.

Unter „Senden bestätigen“ kannst Du nun die Option „Falls nicht verschlüsselt“ senden. Damit musst Du bei jeder Nachricht extra zustimmen, wenn eine Nachricht nicht verschlüsselt gesendet werden kann.

Antworten auf verschlüsselte/signierte Nachrichten verschlüsseln/signieren sollte unbedingt gesetzt sein.

Automatisch verschlüsselt senden „Wenn möglich“ sollte gesetzt sein. Immer ist nicht möglich, wenn Du von Empfänger:innen noch keinen public key importiert hast.

Mit „Akzeptiere, um verschlüsselt zu senden“ kannst Du Deine Sicherheitsstufe noch ein Stück hoch setzen.

„Nur vertrauten Schlüsseln“ bedeutet, dass Du immer jeden öffentlichen Schlüssel den Du importierst auch gründlich geprüft und als „vertrauenswürdig“ eingestuft hast. Sonst kannst Du nicht verschlüsselt an die Empfänger:innen senden.

„Alle verwendbaren Schlüsseln“ bedeutet, dass Du allen Empfänger:innen verschlüsselte Nachrichten senden kannst, sobald Du den public key importiert hast.

Verfügst Du über mehrere E-Mailkonten mit PGP Schlüsselpaaren, wechselst Du einfach zu „OpenPGP-Sicherheit“ des nächsten E-Mailkontos und nimmst dort ebenfalls die gewünschten Einstellungen vor.

PGP Verschlüsselung mit Thunderbird ab Version 78.2.1

Das Addon Enigmal wurde ab der Version 78.0 als nicht mehr kompatibel deaktiviert, eine integrierte OpenPGP-Verschlüsselung stand in der ersten Version 78.0 och nicht zur Verfügung, ab Version 78.2.1 wurde OpenPGP-Verschlüsselung wieder integriert.

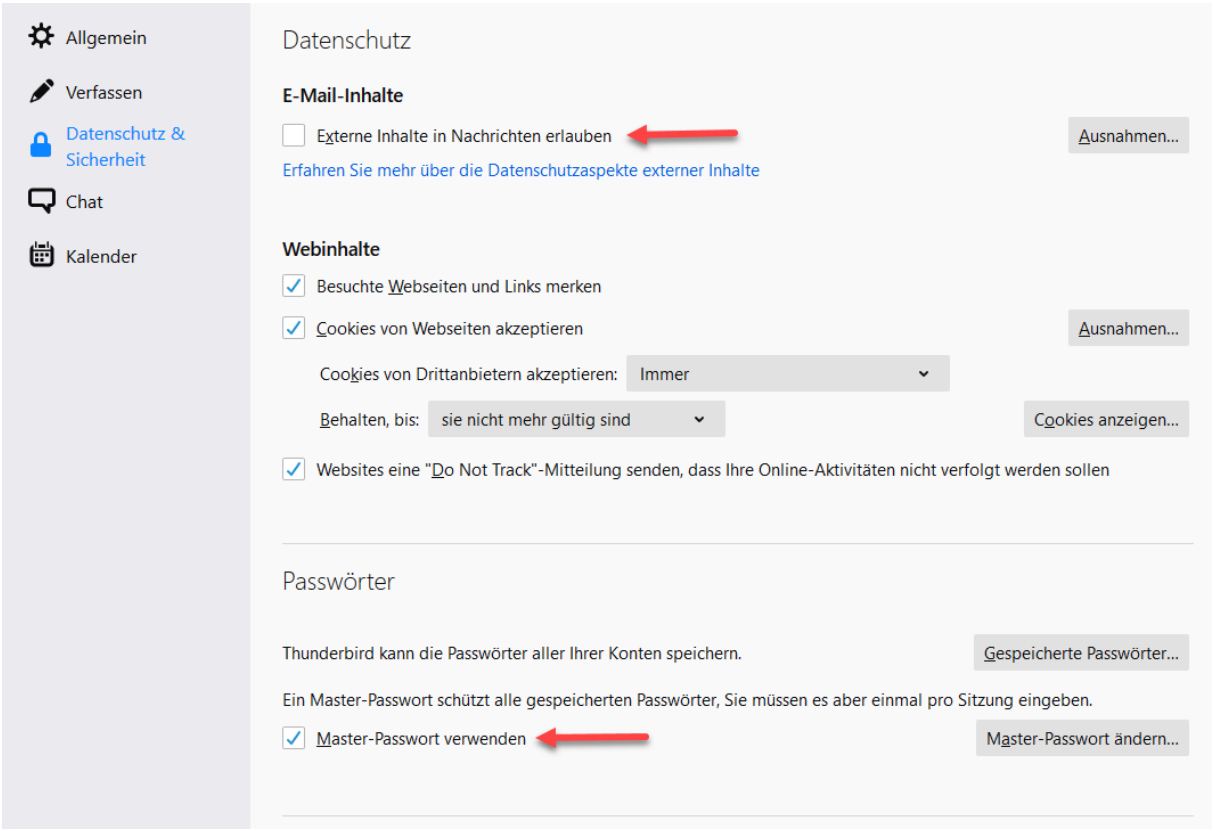
Allerdings gibt es aktuell noch einige erhebliche Änderungen/Einschränkungen laut der Thunderbird Hilfe, so wird zum Beispiel auf die Verwendung von GnuPGP verzichtet.
https://support.mozilla.org/de/kb/openpgp-in-thunderbird-leitfaden-und-faqs

Momentan importiert Thunderbird Deine privaten Schlüssel, entschlüsselt sie nach Eingabe Deines Keypasswords und schützt sie wieder mit einem neuen, automatisch und zufällig erzeugten Passwort. Dieses automatische Passwort wird für alle privaten OpenPGP-Schlüssel benutzt, die in Thunderbird verwaltet werden.

Daher solltest Du die Thunderbird-Funktion zur Erzeugung und Nutzung eines Master-Passwords verwenden. **Ohne Master-Passwort sind Deine Open-PGP-Schlüssel in Deinem Thunderbird-Profilverzeichnis nicht geschützt!**

Jemensch der Zugriff auf Dein Thunderbird hat, kann verschlüsselte Nachrichten ohne Keypassword sofort lesen und auch verschlüsselt versenden!

Bevor Du überhaupt Deine PGP Schlüssel hinterlegst, solltest Du ein Masterpassword einrichten, es wird nur einmal pro Sitzung abgefragt.

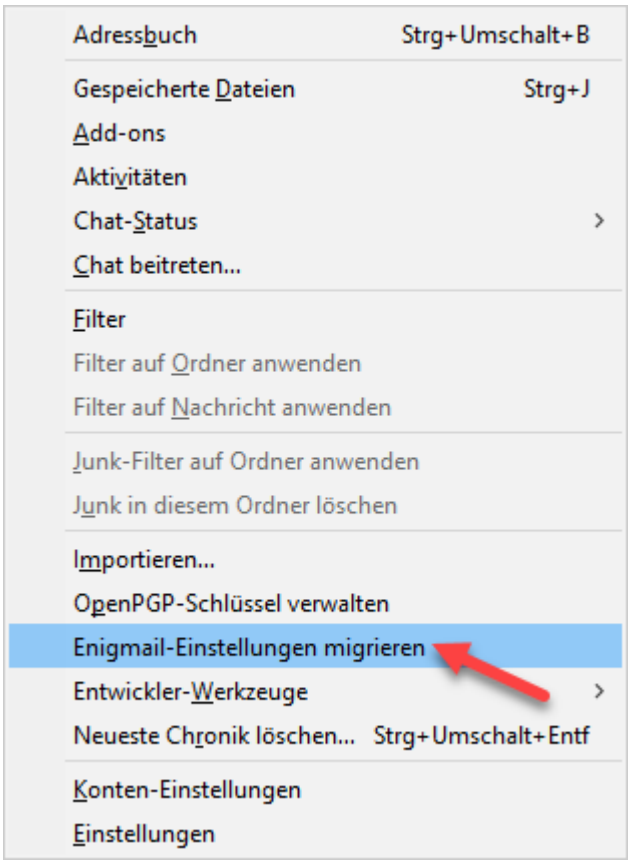


Um die Sicherheit zu erhöhen, schalte auch externe Inhalte in Deinen Nachrichten ab!

Nur über diesen Weg ist es bisher gelungen PGP Verschlüsselung zu knacken.

Deine PGP Schlüssen migrieren

Wenn Du von Thunderbird 68.X auf Thunderbird 78.2.1 oder höher (aktuell Version 78.4.3) umsteigen willst, kannst Du die Enigmail Einstellungen direkt in Thunderbird integrieren oder aber auch manuell wieder einrichten.

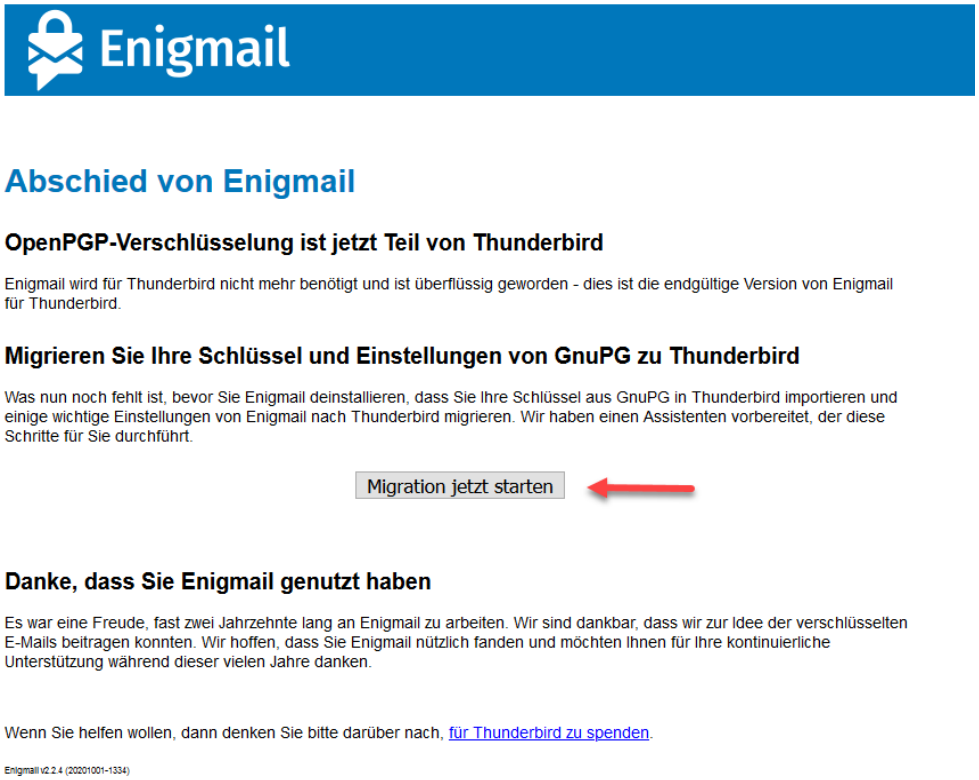


Unter dem Menü „*Extras*“ kommst Du in den Bereich Deiner Schlüsselverwaltung, sowie zu Enigmail 2.2.x Migrationsversion.

Diese Migrationsversion hat nur noch den Zweck, Deine Enigmail Einstellungen, sowie auch Deine persönlichen PGP Schlüssel zu importieren. Alle andere Funktionen aus Enigmail stehen Dir nicht mehr zur Verfügung.

Sowohl Benutzeroberfläche wie Funktionen unterscheiden sich deutlich. Auch der Umstand, dass Thunderbird eine eigene Schlüsselverwaltung verwendet, lässt einen automatischen Import der öffentlichen Schlüssel (Public Keys) nicht zu.

Diese müssen manuell aus GnuPG exportiert und in Thunderbird wieder importiert und bestätigt werden, damit ein verschlüsselter Versand möglich ist.



Nach der Auswahl „Enigmail Einstellungen migrieren“ öffnet sich der Migrations-assistent.

Unter *„Private Schlüssel auswählen“* kannst Du bestimmen, welche der gefundenen privaten Schlüssel (Private Keys) in Thunderbird importiert werden sollen, falls Du nicht alle übernehmen möchtest.

Willst Du alle privaten Schlüssel importieren, kannst Du einfach auf *„Migration Starten“* klicken. Damit werden alle in GnuPG gefundenen privaten Schlüssel importiert.

Wichtig!

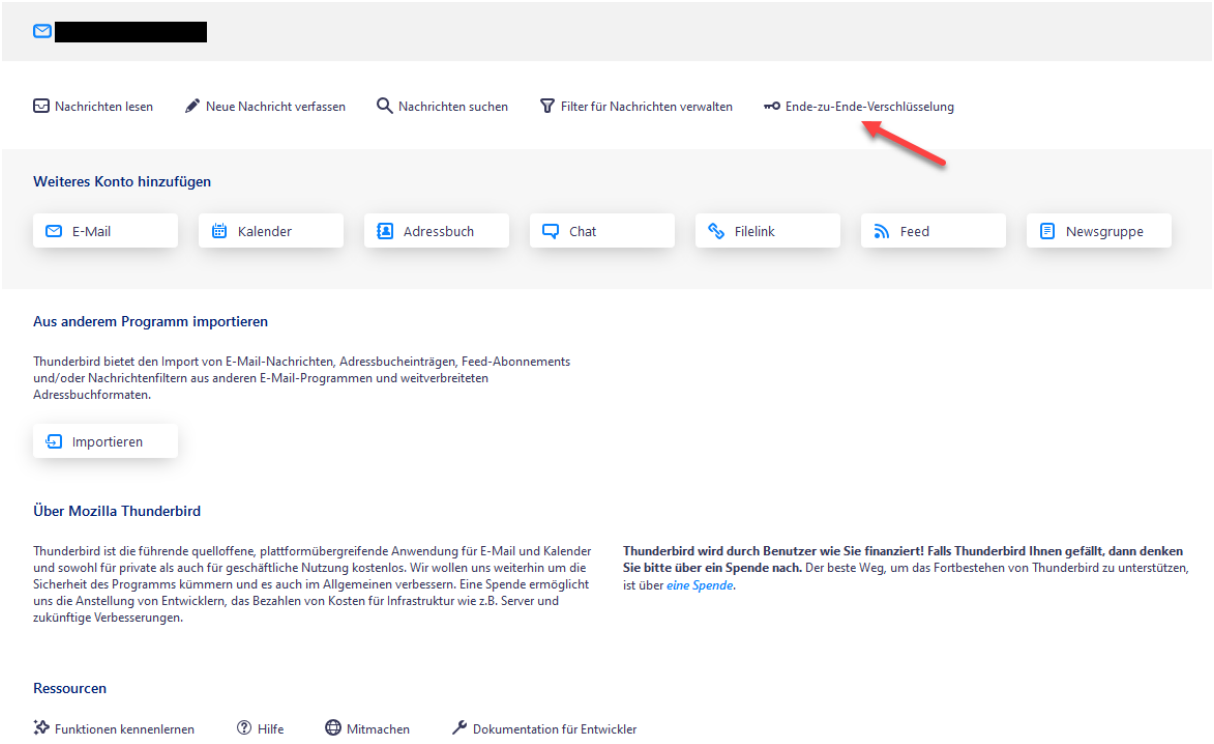
Damit der Import reibungslos verläuft, achte genau darauf welcher Schlüssel gerade importiert werden soll und gebe dafür die richtige Passphrase (Passwort) ein.

Nach Abschluss des Imports bekommst Du einen Hinweis, welche Schlüssel importiert wurden und welche nicht importiert werden konnten.

Bei einer einfachen Konfiguration bist Du dann auch schon fertig, Deine privaten Keys sind damit in Thunderbird hinterlegt und Du kannst sie zum lesen und versenden verschlüsselter Nachrichten verwenden.

PGP Schlüssel manuell hinterlegen

Schlägt der Import fehl oder arbeitest Du mit sogenannten Alias Adressen, kannst Du auch auf anderem Weg Deine privaten Schlüssel für Dein Emailkonto und Alias Adressen hinterlegen und zuordnen.



Klicke dazu links im Menü auf die fett hinterlegte Bezeichnung Deines eingerichteten Emailkontos und klicke rechts in der Übersicht auf „Ende-zu-Ende-Verschlüsselung.

In dem darauffolgenden Fenster kannst Du auch überprüfen, ob Deine importierten privaten Keys auch richtig zugeordnet wurden, ebenso kannst Du die Schlüsseleigenschaften einsehen und ggf. bearbeiten, z. B. Ablaufdatum, Schlüssel importieren, exportieren, neu erzeugen etc.

Im unteren Bereich kannst Du festlegen, ob Deine Nachrichten standardmäßig verschlüsselt werden sollen oder nicht. Um die Sicherheit zu erhöhen, empfehlen wir die Einstellung „*Verschlüsselung standardmäßig verlangen*“.

Damit erhältst Du bei einem fehlenden oder nicht verifizierten Schlüssel einen Warnhinweis, ob Du abbrechen oder unverschlüsselt senden möchtest. Unverschlüsselte Nachrichten zu senden bleibt immer möglich.

Eigene digitale Unterschrift standardmäßig hinzufügen zu aktivieren macht ebenfalls Sinn. Damit kann der Empfänger prüfen, ob die Nachricht tatsächlich von Dir stammt und nicht geändert wurde.

Die hier getroffenen Einstellungen gelten erstmal für das Emailkonto, um Aliasadressen getrennt zu verwalten und separate Schlüssel zu hinterlegen (empfohlen!), sind weitere Einstellungen notwendig.

Ende-zu-Ende-Verschlüsselung

Um Nachrichten zu verschlüsseln oder digital zu unterschreiben, muss eine der Verschlüsselungstechnologien OpenPGP oder S/MIME eingerichtet werden.

Wählen Sie Ihren persönlichen Schlüssel für die Verwendung von OpenPGP oder Ihr persönliches Zertifikat für S/MIME. Für einen persönlichen Schlüssel oder ein persönliches Zertifikat verfügen Sie über den entsprechenden geheimen Schlüssel.
Weitere Informationen

OpenPGP

Thunderbird verfügt über 2 persönliche OpenPGP-Schlüssel für
[redacted]
✓ Derzeit ist die Verwendung der Schlüssel-ID [redacted] festgelegt. Weitere Informationen

Schlüssel hinzufügen...

- ○ **Keiner**
  OpenPGP für diese Identität nicht verwenden
- ○ [redacted]
  Der Schlüssel läuft nicht ab.
- ◉ [redacted]
  Der Schlüssel läuft nicht ab.

Mit der OpenPGP-Schlüsselverwaltung können Sie die Schlüssel Ihrer Kontakte und andere oben nicht aufgeführte Schlüssel anzeigen und verwalten.

OpenPGP-Schlüssel verwalten

S/MIME

Persönliches Zertifikat für digitale Unterschrift:

Auswählen... Leeren

Persönliches Zertifikat für Verschlüsselung:

Auswählen... Leeren

S/MIME-Zertifikate verwalten S/MIME-Kryptographie-Module verwalten

Senden von Nachrichten - Standardeinstellungen

Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E-Mail-Anbieter leicht zugänglich und kann auch Bestandteil einer Massenüberwachung werden.

- ○ Verschlüsselung standardmäßig nicht aktivieren
- ◉ Verschlüsselung standardmäßig verlangen

Falls Sie Verschlüsselung verwenden, benötigen Sie zum Senden einer Nachricht für jeden Empfänger dessen öffentlichen Schlüssel oder das Zertifikat.

Eine digitale Unterschrift ermöglicht den Empfängern zu überprüfen, dass die Nachricht von Ihnen gesendet sowie der Inhalt nicht geändert wurde.

- ☑ Eigene digitale Unterschrift standardmäßig hinzufügen

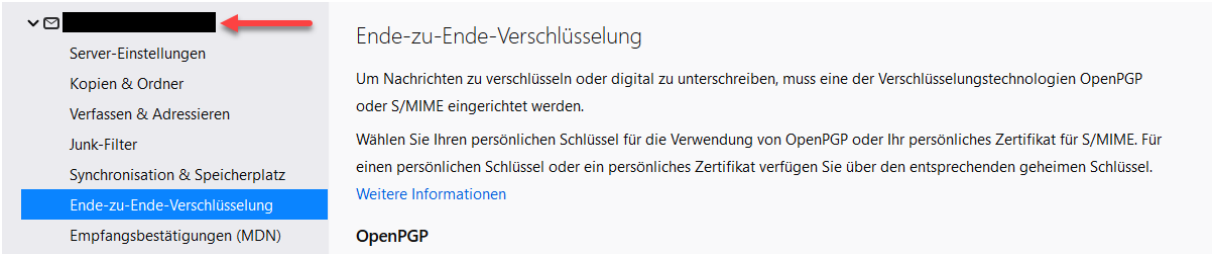
Bevorzugte Verschlüsselungs-Technologie:

- ◉ Automatische Auswahl anhand verfügbarer Schlüssel und Zertifikate
- ○ OpenPGP bevorzugen
- ○ S/MIME bevorzugen

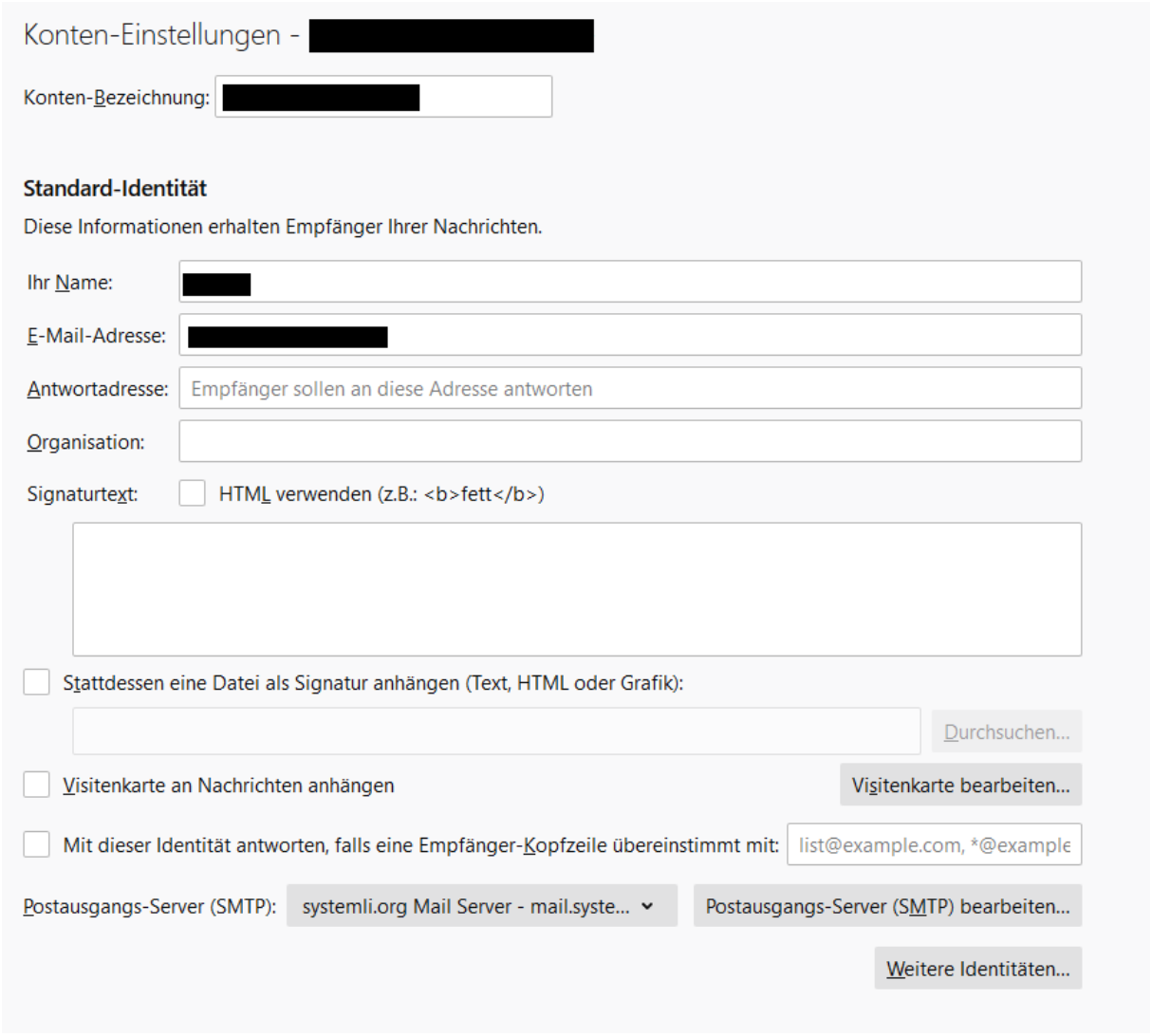
Verwalten von Aliasadressen

Benötigt man mehrere Emailadressen, z. B. persönlich, Freunde, Kontakte, kann man entweder mehrere Emailkonten einrichten, was einen größeren Aufwand/Verwaltung und ggf. mehr Kosten verursacht, oder man nutzt die Möglichkeit virtueller Emailadressen. Du hast dann ein Emailkonto, was man über die Emailadresse des Kontos oder die Aliasadressen anschreiben kann.

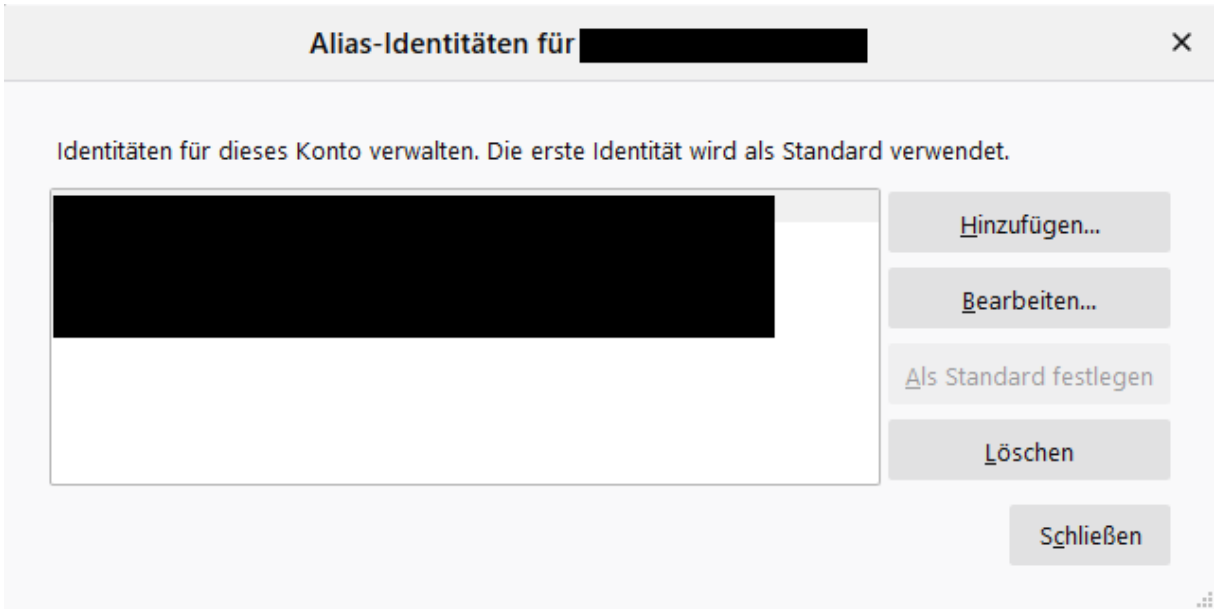
Mit der Aliasadresse kann man auch antworten oder schreiben, was spricht also dagegen, auch für diese Adressen verschlüsselte Kommunikation über eigene private Schlüssel einzurichten?



Um zur Verwaltung der Aliasadresse zu gelangen, klicke ganz oben links im Menü auf die Kontobezeichnung.

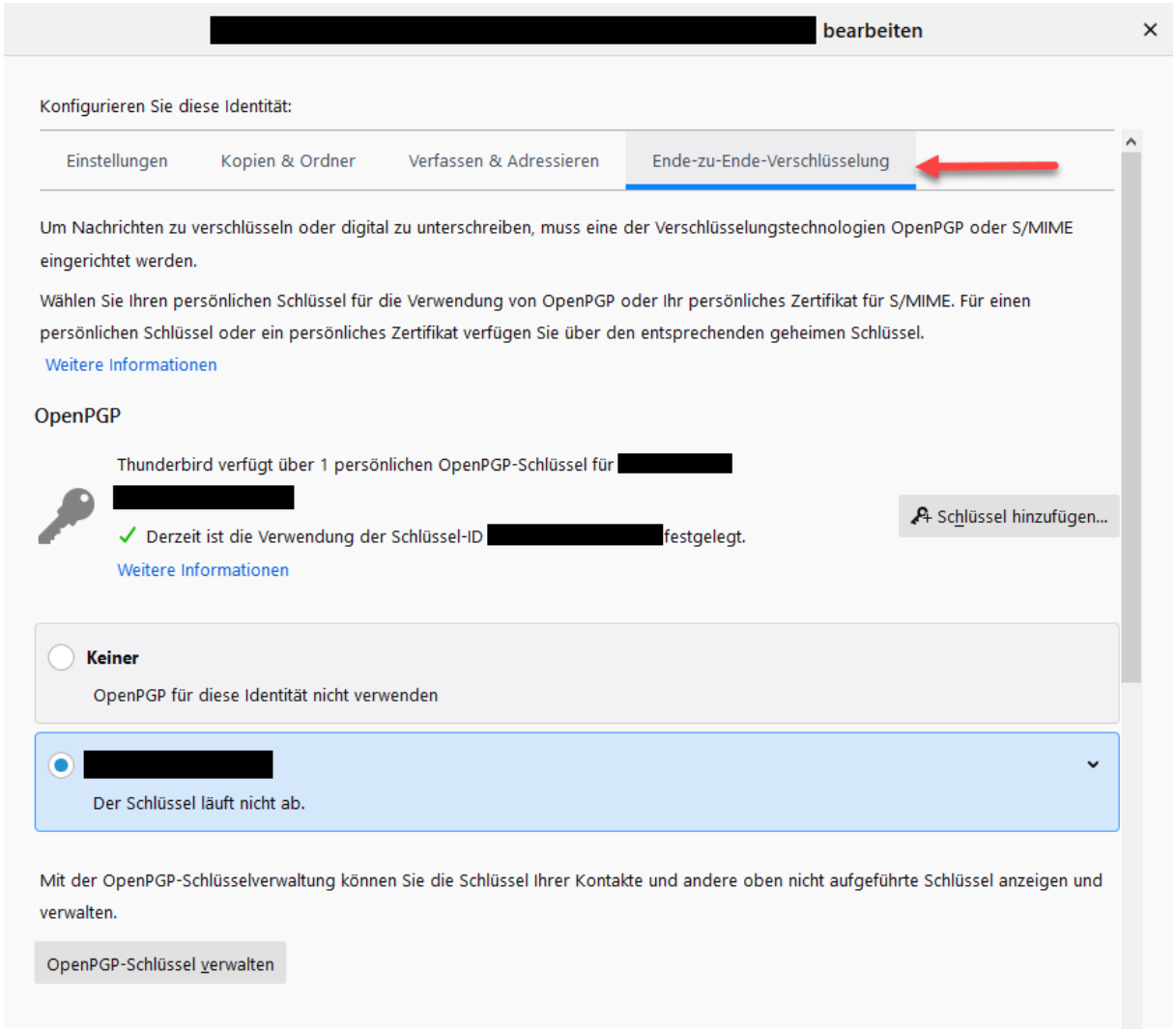


Klicke jetzt ganz unten rechts auf *„Weitere Identitäten…“*



In diesem Fenster werden Dir alle Alias Identitäten angezeigt.

Klickst Du auf eine bestimmte Alias Adresse, kannst Du diese löschen, als Standard festlegen oder Bearbeiten.



Wenn Du auf „*Bearbeiten*“ geklickt hast, wechsel in den Tab „*Ende-zu-Ende-Verschlüsselung*“. Hier kannst Du einen privaten Shlüssel hinterlegen und die gleichen Einstellungen wie im Konto einstellen.

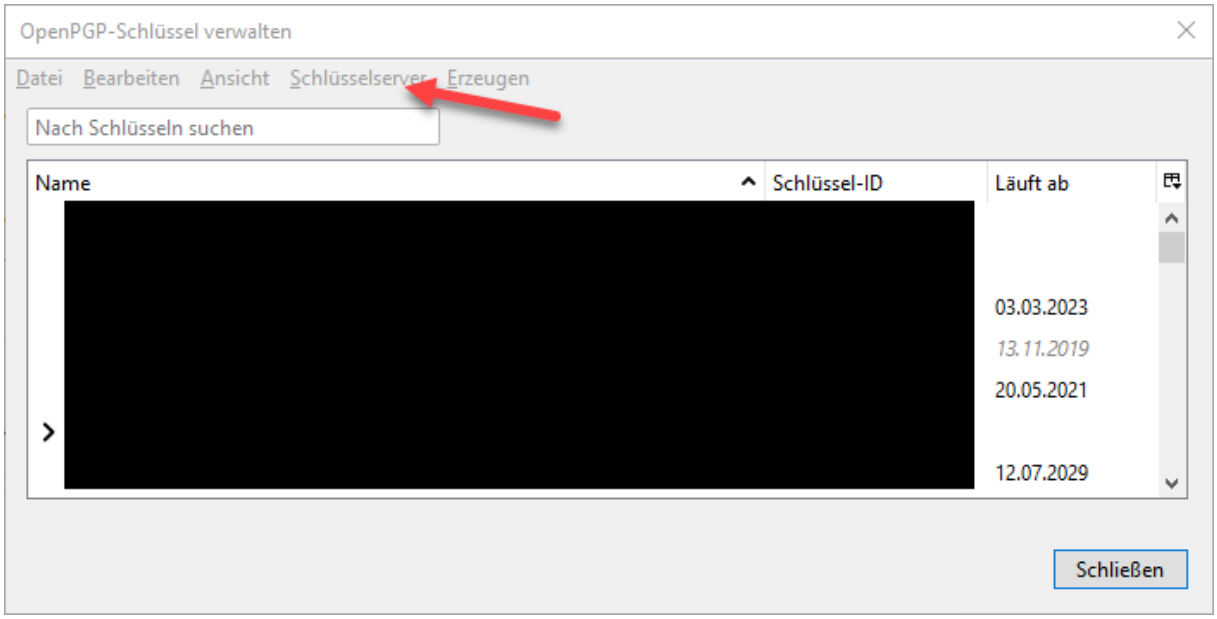
OpenPGP-Schlüssel verwalten

Die Schlüsselverwaltung brauchst Du, um öffentliche Schlüssel zu importieren, die Funktionen unterscheiden sich nicht wesentlich von Enigmail. Daher gehen wir nicht noch mal auf jede einzelne Funktion ein.

Wenn Du Deine Konten eingerichtet hast wirst Du feststellen, dass bis auf Deine eigenen Schlüssel die Verwaltung komplett leer ist. Thunderbird synchronisiert **nicht** mit GnuPG!

Enigmail hatte auch auf Schlüsselservern gesucht, die Schlüssel nicht verifiziert hatten. Derzeit bietet Thunderbird diese Möglichkeit nicht an, da in jüngerer Vergangenheit immer wieder Probleme mit solchen Schlüsselservern auftraten.

Wenn Du so einen Schlüsseln benötigst, kannst Du ihn über GnuPG laden, exportieren und in Thunderbird importieren.



Man kann versuchen, die Funktion „Schlüsselserver“ zu verwenden, die Wahrscheinlichkeit einen Schlüssel zu finden sind jedoch (noch?) relativ gering.

Je nach gewünschter Sicherheitsstufe ist es auch ratsam, öffentliche Schlüssel nicht zu veröffentlichen und nur gezielt und sicher an die Menschen weiterzugeben, mit denen man kommunizieren möchte.

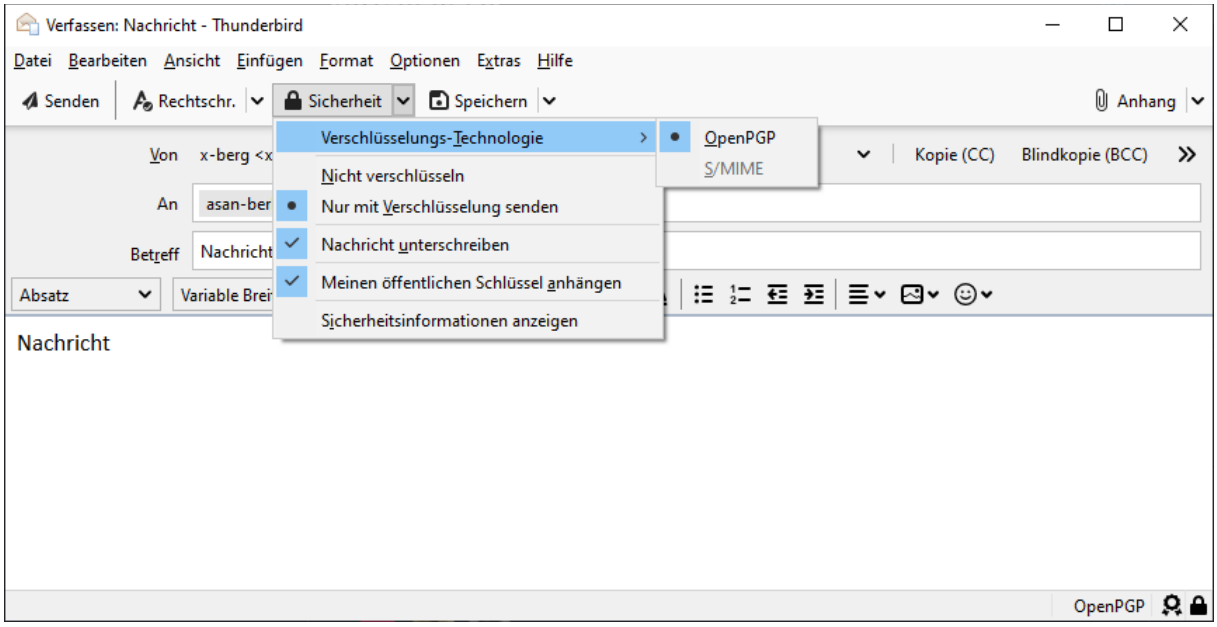
Du startest eine Suche nach veröffentlichten Schlüsseln mithilfe des WKD-Protokolls und suchst nach Schlüsseln auf dem öffentlichen Schlüsselserver keys.openpgp.org. Bisher haben wir noch keinen öffentlichen Schlüssel, der auf den GnuPG Servern veröffentlicht wurde, über diesen Weg gefunden.

Bleibt also beim Umstieg erst einmal Handarbeit, die vorhandenen GnuPG Schlüssel müssen exportiert und in OpenPGP-Schlüsselverwaltung von Thunderbird importiert werden.

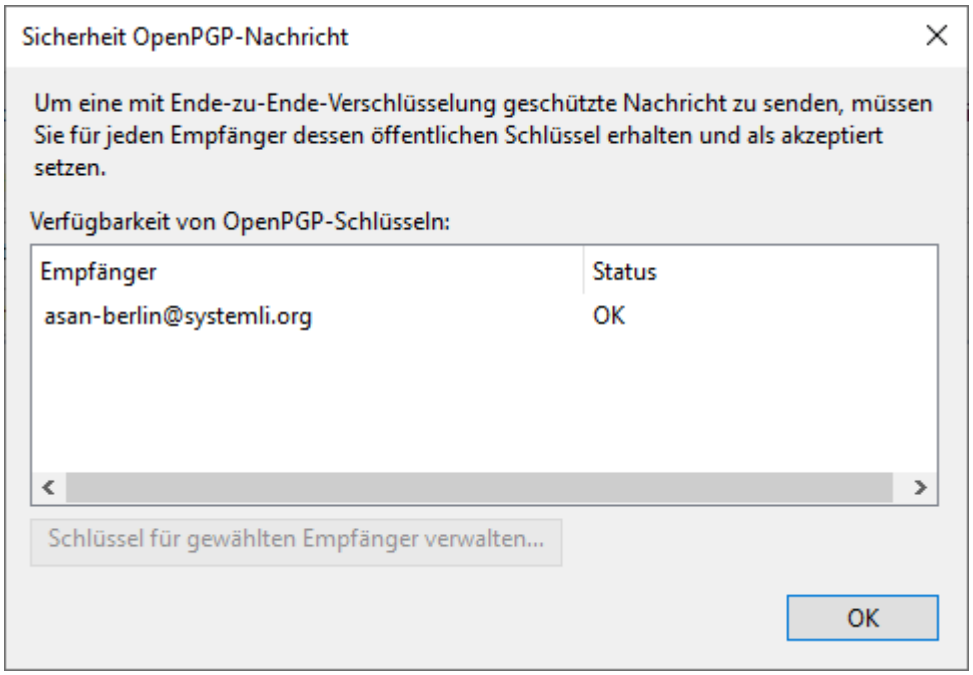
Es besteht die Möglichkeit, alle öffentlichen Schlüssel in einer Datei zu exportieren und in Thunderbird wieder komplett zu importieren. Je nach Menge der öffentlichen Schlüssel kann das zu Problemen führen, momentan dürfen die zu importierenden Schlüsseldateien nicht größer als **5 MB** sein!

Wenn Du also sehr viele Kontakte mit öffentlichen PGP Schlüsseln gespeichert hast, wirst Du die Schritte eventuell mehrmals durchführen müssen, bis Du alle Schlüssel importiert hast.

Verschlüsselte Nachrichten versenden



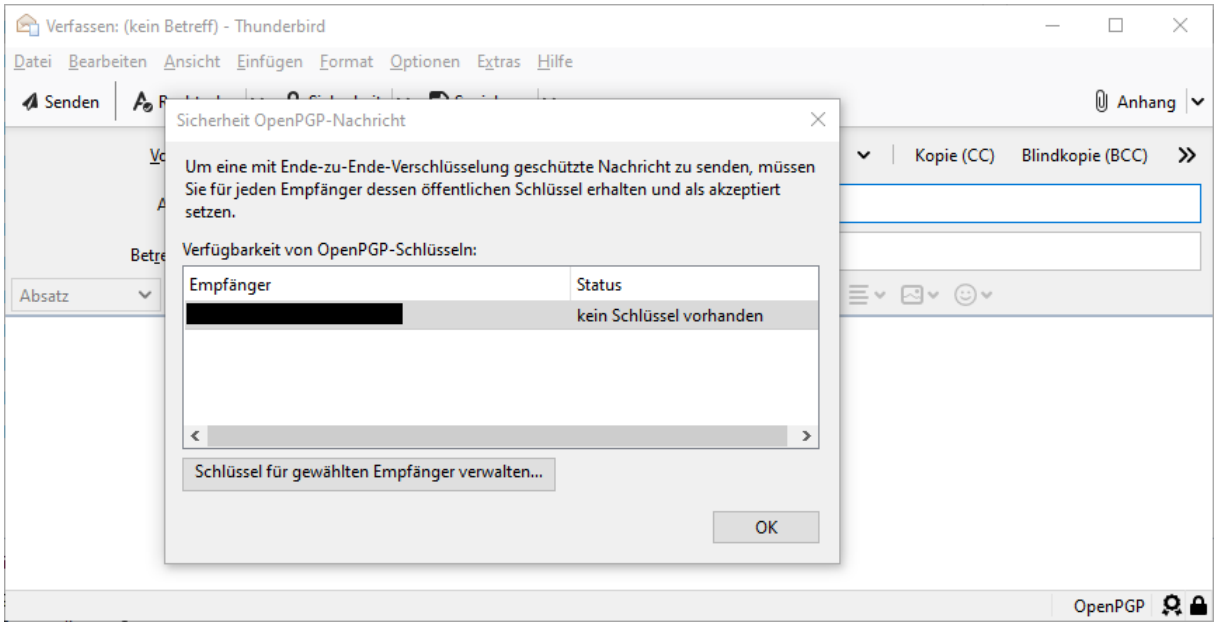
Beim Verfassen von Nachrichten findest Du je nach Voreinstellung alle notwendigen Einstellungen/Informationen unter dem Punkt „**Sicherheit**“. Hier kannst Du getroffene Voreinstellungen für Dein Emailkonto für diese eine Nachricht ändern.



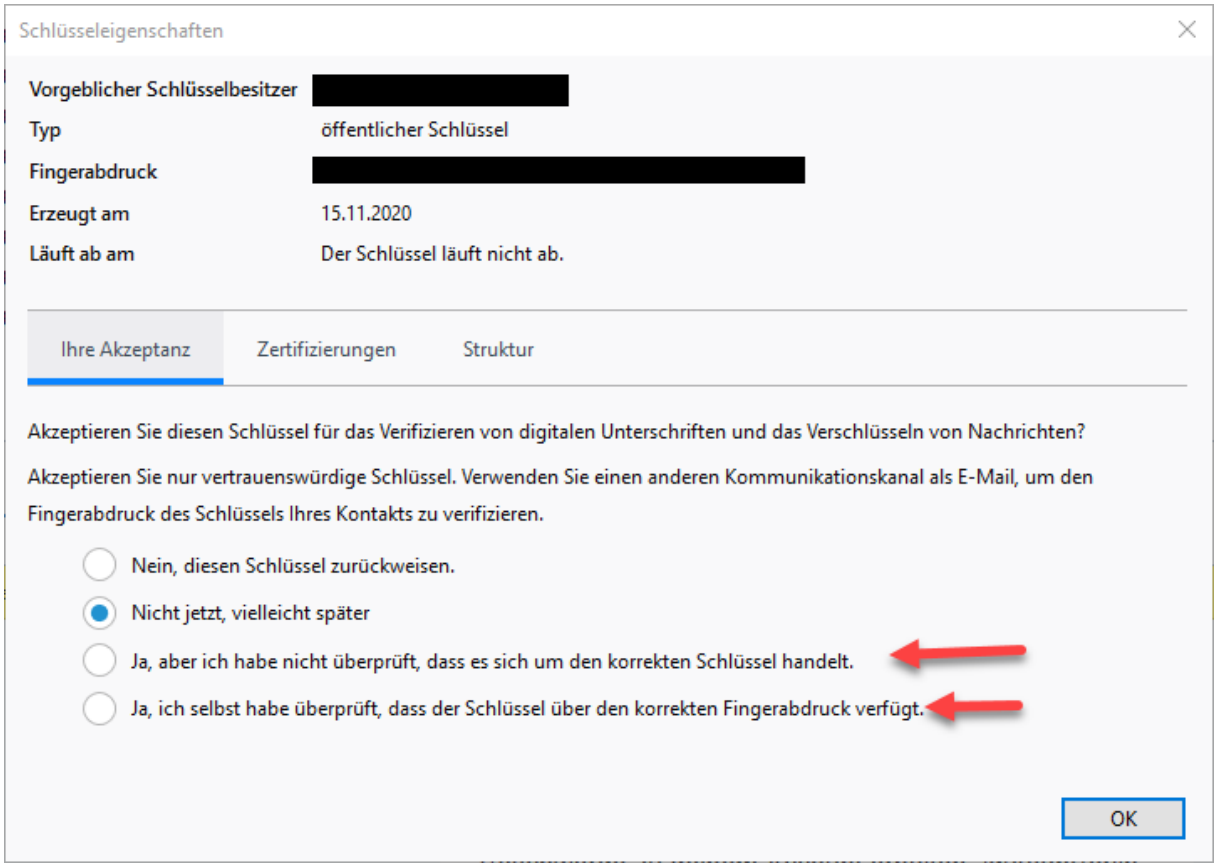
Unter „*Sicherheitsinformationen anzeigen*“ kannst Du prüfen, ob Du a) für den Empfänger einen öffentlichen Schlüssel importiert hast und b) den Schlüssel auch verifiziert hast.

In diesem Beispiel wurde ein Schlüssel erfolgreich importiert und auch verifiziert, d. h. Du vertraust dem öffentlichen Schlüssel.

Deine Nachricht kann also verschlüsselt versendet werden.



Die Anzeige *„kein Schlüssel vorhanden“* kann irreführend sein. Es kann bedeuten, dass tatsächlich kein Schlüssel importiert wurde, es kann aber auch bedeuten, dass der Schlüssel nicht verifiziert wurde. In dem Fall kann keine verschlüsselte Nachricht gesendet werden.



Über die Schlüsselverwaltung kannst Du das prüfen. Findest Du einen Schlüssel, rufe die Schlüsseleigenschaften auf.

Hier kannst Du den importierten Schlüssel verifizieren, entweder ohne den Fingerabdruck zu überprüfen (geringere Sicherheit) oder mit Überprüfung des Fingerabdrucks (hohe Sicherheit).

Anschließend ist das Senden verschlüsselter Nachrichten möglich.

PGP Verschlüsselung mit iOS

Der generelle Vorteil von Smartphones und/oder Tablets ist der, dass man auch von unterwegs mal eben schnell auf Nachrichten reagieren kann, ohne gleich einen Laptop mitschleppen und das System erst hochfahren zu müssen.

Leider setzt sich auch hier die Linie fort, dass PGP den Monopolisten (Microsoft, Apple & Co) eher hinderlich scheint und in den wenigsten „Standard“ Mail Apps integriert ist. iOS tut sich da (ähnlich Tor) etwas schwer, deshalb möchten wir Euch zwei unabhängige Lösungen vorstellen, die leider beide nicht kostenlos sind:

iPGMail: https://ipgmail.com

Das Tool kostet aktuell 2,29 Euro und erlaubt das Beantworten von Nachrichten über die IOS Mail App. Die Handhabung ist allerdings nicht unkompliziert, da zum einen zwischen zwei Apps hantiert werden muss und zum anderen keine Verbindung zu Keyservern besteht. iPGMail ist sozusagen ein Programm, mit dem Du erhaltene Nachrichten bei vorhandenen Schlüsseln entschlüsseln und Antworten oder Nachrichten verschlüsseln, aber nicht senden kannst.

Canary Mail: https://canarymail.io

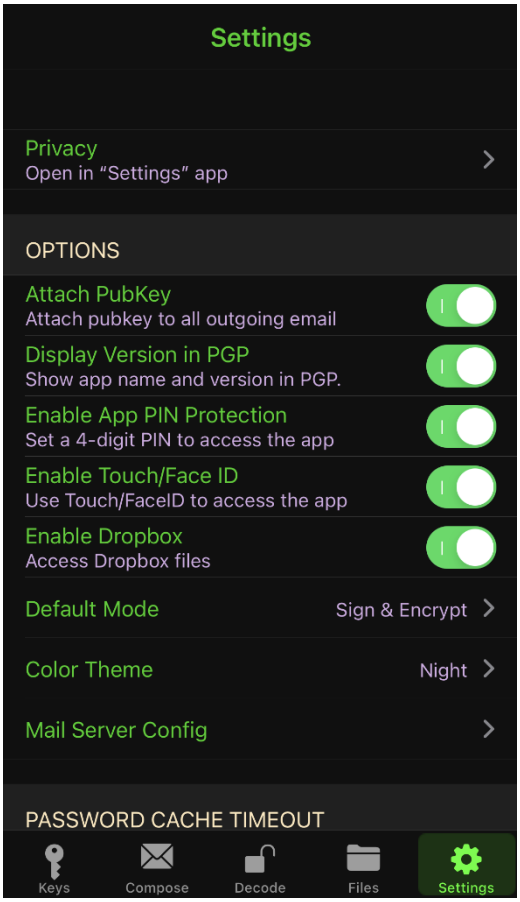
Ein vollwertiger und zugegeben sehr komfortabler Email Client mit vollständig integrierter PGP Funktion. Ideal für alle, die viele PGP Nachrichten empfangen/senden und ohne Komplikationen damit arbeiten wollen. Allerdings hat das Programm auch einen sehr stolzen Preis von 21,99 Euro.

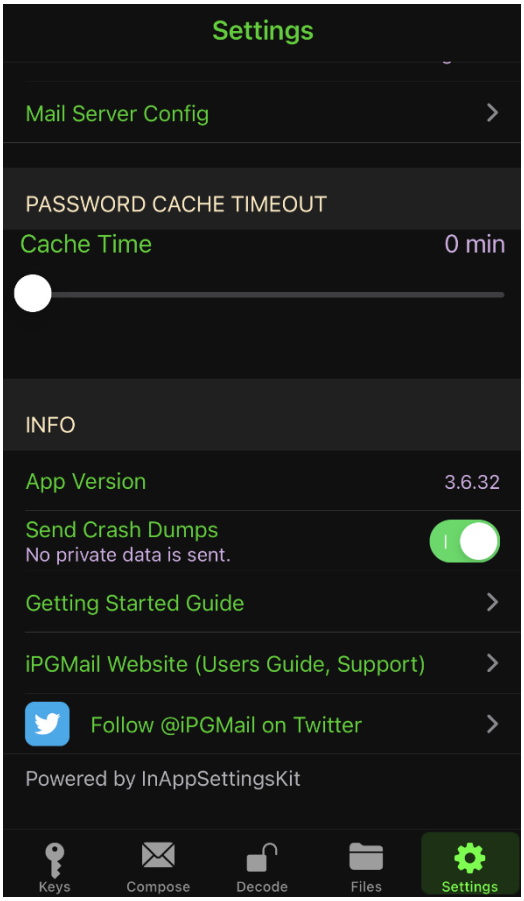
Daher ist abzuwägen, ob man seine Emailkonten auch unterwegs abfragen und bearbeiten möchte bzw. muss, oder auch später Zuhause am PC erledigen kann.

Möglich ist es auf jeden Fall, je nach OS mehr oder weniger einfach bzw. günstig.

Wir wollen auf den folgenden Seiten keine komplette Beschreibung aller App Funktionen machen, sondern lediglich die markanten auf PGP Verschlüsselung bezogenen Schritte beschreiben.

IPGMail - Setup





Wenn Du die App aus dem App Store geladen hast, solltest Du zuerst die Einstellungen bearbeiten, um die App für ihre Nutzung einzurichten und gegen unbefugte Benutzung zu sichern:

Privacy – geht in die iOS Einstellungen für die Zugriffe der App. Siri immer ausschalten.

Attach PubKeys – hängt Deinen öffentlichen Schlüssel an jede ausgehende Nachricht.

Enable App Pin Protection – sollte immer aktiviert sein, um die App vor Zugriff zu schützen.

Enable Touch/Face ID – Geschmackssache ob man damit die App entsperren möchte.

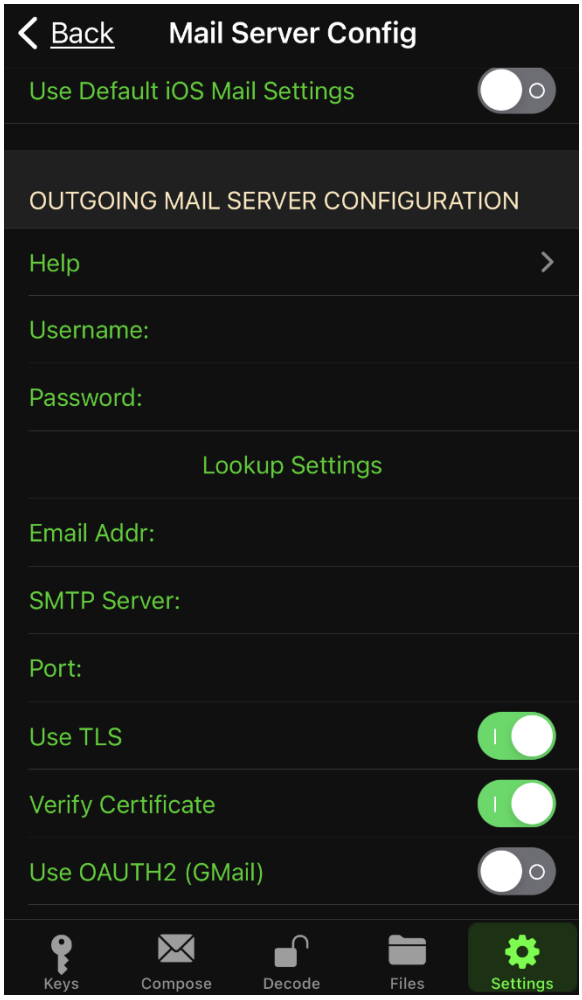
Enable DropBox – eine Möglichkeit außer iTunes, um Schlüssel zu importieren.

Mail Server Config – hier kannst Du festlegen, wie Antworten/Nachrichten gesendet werden.

Cache Time – Hier stellst Du ein, wie lange das Passwort Deines privaten Keys im Speicher bleibt.

Die App vor unbefugter Nutzung durch Dritte zu schützen macht auf jeden Fall Sinn!

Unter Umständen könnten sonst entschlüsselte Inhalte von Dritten eingesehen werden. Daher ist es auch je nach Sicherheitsbedürfnis auch nicht sinnvoll den Cache zu nutzen oder auf zu lange Zeit einzustellen.



Grundsätzlich kann iPGMail keine Emails abrufen, es gibt in der App auch keinen Posteingang oder IMAP Verzeichnisse. Du musst empfangene Nachrichten aus einem Emailprogramm an iPGMail übergeben und kannst lediglich auf diese Nachrichten direkt aus der App antworten.

Use Default iOS Mail Settings

Diese Einstellung erlaubt Dir, Nachrichten über die Apple iOS Mail App zu versenden. Dabei kannst Du mehrere Emailkonten und deren Schlüssel nutzen. Die Emailkonten müssen dazu in der Apple IOS Mail App eingerichtet sein.

Outgoing Mail Server Configuration

Verwendest Du nur eine Emailadresse, kannst Du ausgehende Nachrichten direkt über Deinen Mailserver z. B. @systemli.org oder @riseup.net senden.

Hier kannst Du Deine Zugangsdaten für Dein Emailkonto eingeben. iPGMail ist damit mit jedem Mailserver kompatibel und von keinen bestimmten Anbieter abhängig.

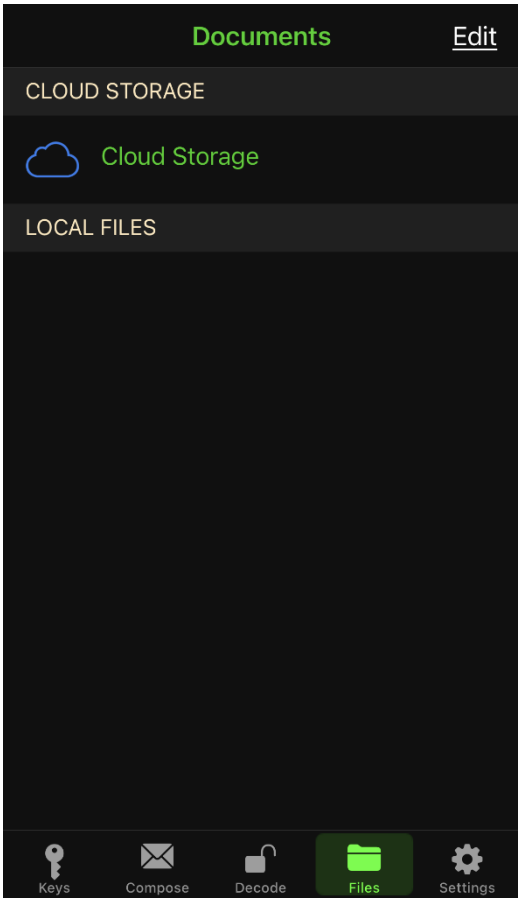
Die dritte Möglichkeit wäre, den über Compose bereits verschlüsselten Inhalt einer Nachricht über die Zwischenablage in den Body (Nachrichtenfeld) einer beliebigen Mail App zu kopieren und zu versenden.

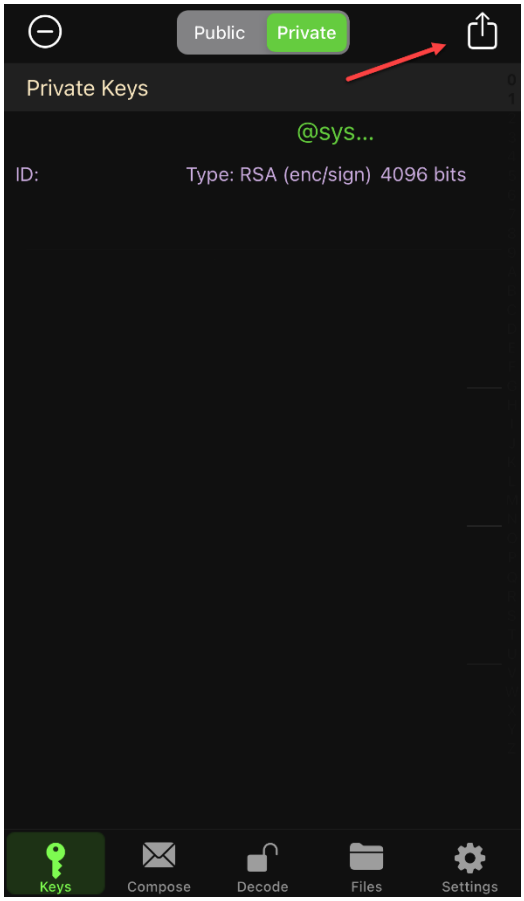
Wir sehen also, dass iPGMail keine klassische Email App ist, sondern lediglich eine Brücke zwischen PGP Verschlüsselung und einer beliebigen Email App bildet.

Es gibt also keinen Komfort in Richtung Benutzerfreundlichkeit, was sich auch in der Schlüsselverwaltung und in der Entschlüsselung bemerkbar macht.

Dennoch ist es ein weiterer Baustein zu Deiner eigenen Sicherheit, auf den Du bei sensiblen Inhalten (eigentlich grundsätzlich) nicht verzichten solltest. Am Ende ist es eine Frage der Gewöhnung, mag sein ein wenig umständlich, aber nichts was man sich nicht im Laufe der Zeit schnell aneignen könnte.

IPGMail – Schlüssel verwalten





Die Schlüsselverwaltung kann auf verschiedene Arten erfolgen, es besteht leider keine direkte Verbindung zu öffentlichen Keyservern. Alle Schlüssel die Du verwendest (private/öffentliche), müssen in iPGMail importiert werden.

Das kann je nach Vertrauen über Cloudspeicher (**Cloud Storage**) gelöst werden, Next Cloud von Systemli wird dabei auch unterstützt.

Die zweite Möglichkeit besteht über **iTunes**, wenn Du Dein iPhone oder iPad synchronisierst. Unter **Dateifreigabe → iPGMail → Dateien hinzufügen…** kannst Du die Schlüssel hinzufügen und mit Deinem iOS Gerät synchronisieren. Die importierten Dateien findest Du unter **Local Files**.

Sofern der Schlüssel eines Absenders in einer Email angehängt ist, kannst Du den Anhang u. U. an iPGMail übergeben. Die App erkennt automatisch, dass es sich um einen Schlüssel handelt und fügt ihn der Keyverwaltung hinzu. Das geht übrigens auch, wenn man den kompletten Code des Schlüssels (z. B. von einer Website) in die Zwischenablage kopiert und in die iPGMail wechselt.

Lösche nach dem Import alle Dateien aus der Cloud oder Local Files, um Zugriff durch Dritte so gut wie möglich zu reduzieren.

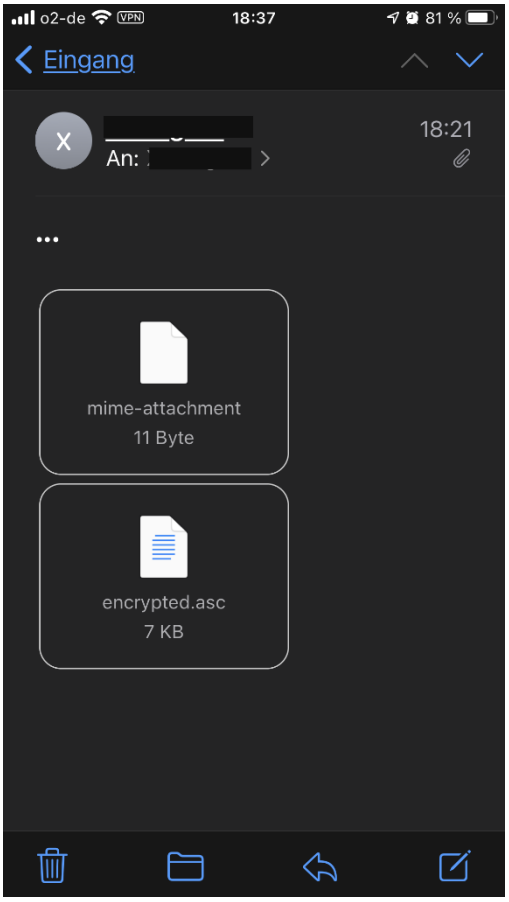
Deine importierten Keys findest Du unterteilt in Public (öffentlich) und Private (geheime Schlüssel).

Unter dem Tab Private kannst Du zur Not über das Symbol ganz oben rechts Create Private Key auch ein neues Schlüsselpaar erzeugen. Nicht empfohlen, ein sicherer Schlüssel mit einem Key Size von 4096 kann bis zu 5 Minuten dauern.

Weiter möglich ist ein BackUp zu speichern, was Du dann unter Files findest.

Darum immer die App mit wenigstens PIN schützen!

IPGMail – entschlüsseln/verschlüsseln



Hast Du jetzt öffentliche und private Schlüssel importiert, ist Deine App einsatzbereit und kannst an das Entschlüsseln ran gehen.

Wenn Du in Standard Email Apps eine verschlüsselte Nachricht empfängst, ist der verschlüsselte Inhalt entweder als Anhang beigefügt, oder als verschlüsselter Code im Emailbody.

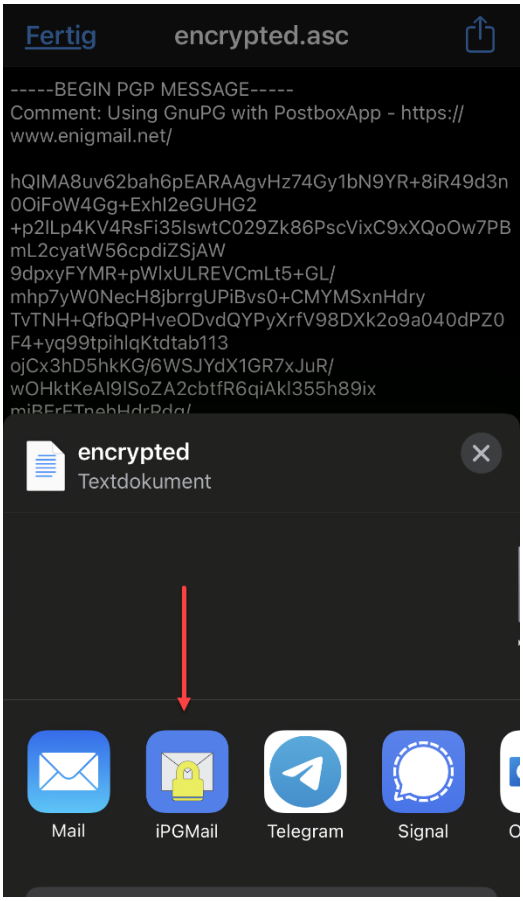
In diesem Beispiel ist die Nachricht im encrypted.asc

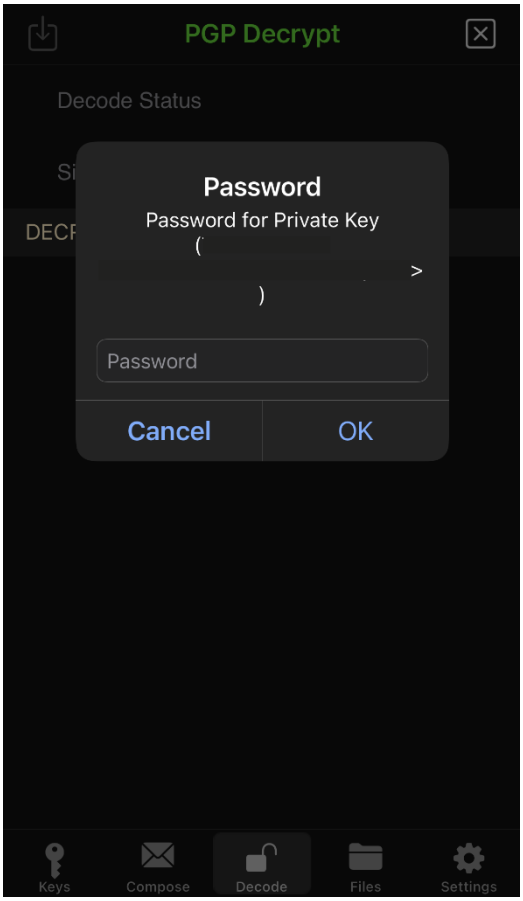
Tippst Du die Datei an, kannst Du den Inhalt sehen, so sieht es auch aus, wenn sich der verschlüsselte Inhalt im Emailbody befindet.

Hier kannst Du über das Symbol ganz oben rechts den Text weiterverarbeiten, wie z. B. an eine andere App übergeben.

Hast Du die verschlüsselte PGP Nachricht im Emailbody erhalten, bietet die iOS Email App diese Möglichkeit zu iPGMail nicht an. Du kannst in dem Fall den gesamten Text kopieren und zu iPGMail wechseln. Die App erkennt den Inhalt der Zwischenablage und fragt Dich nun, ob der Inhalt importiert oder der Zwischenspeicher gelöscht werden soll.

Wählst Du Import aus, wirst Du zur Eingabe des Passwortes Deines geheimen Schlüssels aufgefordert, um den Inhalt zu entschlüsseln.





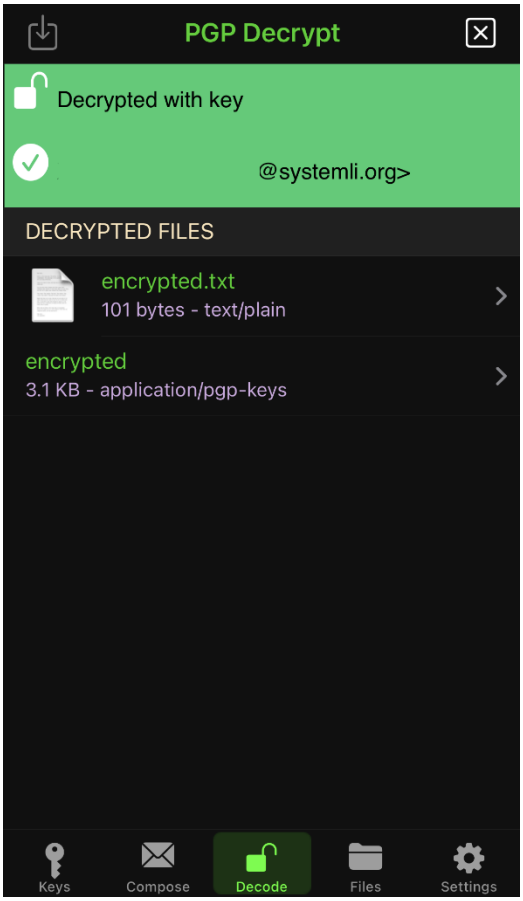
In dem Beispiel einer angehängten verschlüsselten Nachricht kannst Du die Datei wie zuvor beschrieben beliebig weiterverarbeiten.

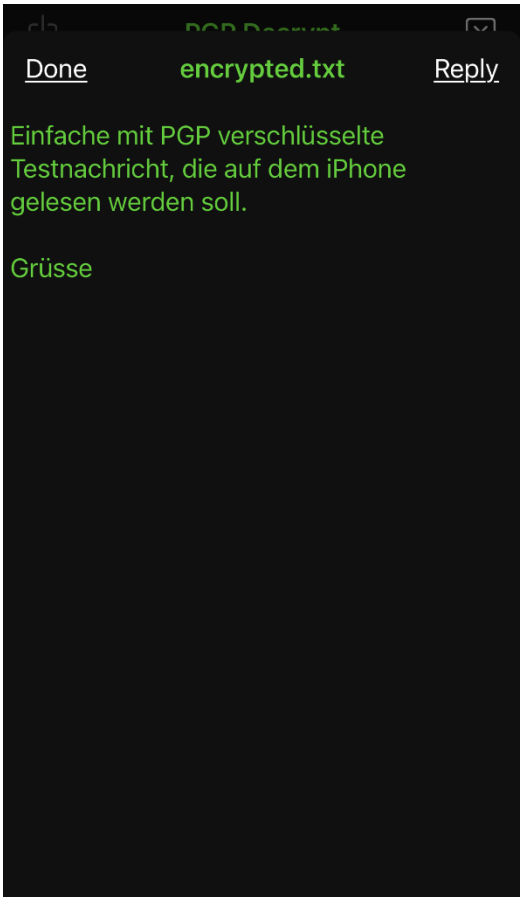
Wähle die iPGMail App aus, um die Datei direkt zur Weiterverarbeitung zu übergeben. Wenn Du alles richtig gemacht hast, musst Du die App zuerst entsperren.

Die übergebene Datei wird von iPGMail sofort als verschlüsselter Inhalt erkannt und das Passwortfenster des als Empfänger identifizierten Schlüssels öffnet sich.

Wäre die Einrichtung der Schlüsselverwaltung fehlerhaft oder unvollständig, käme eine Fehlermeldung.

Gib nun Dein Passwort ein, um den Inhalt zu entschlüsseln.





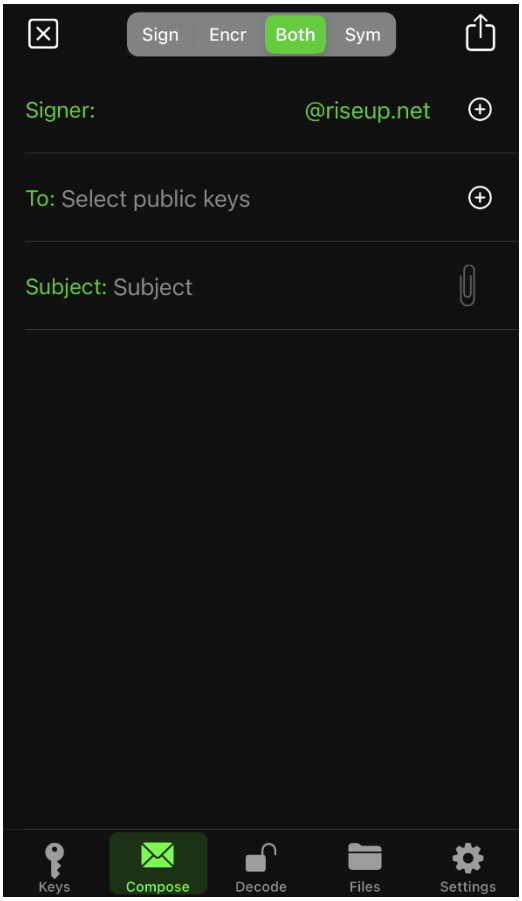
War die Passworteingabe richtig, findest Du die entschlüsselte Datei im Bereich Decode mit den Informationen zu Schlüssel und Emailadresse.

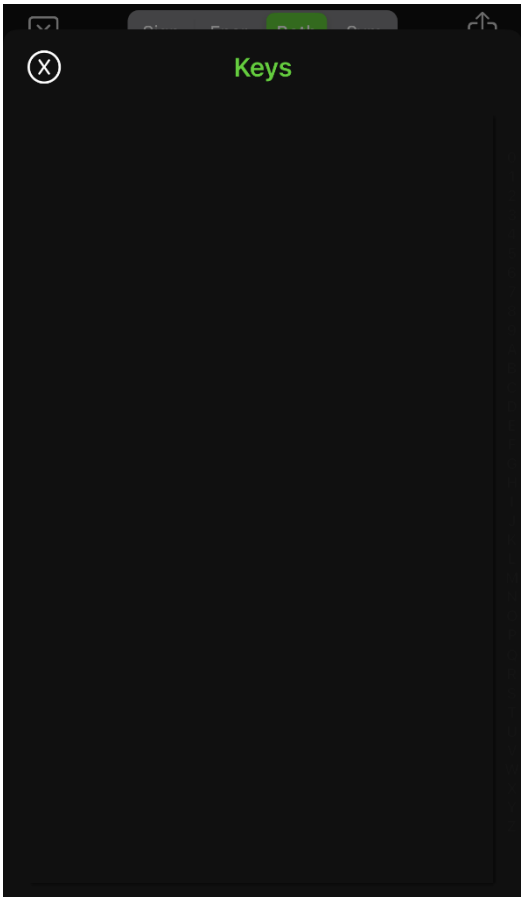
Die eigentliche Nachricht ist in der Datei encrypted.txt die zweite Datei enthält den mitgesendeten öffentlichen Schlüssel.

Hier würde die Einstellung **Cache Time** greifen, der Inhalt bleibt nun die eingestellte Zeit entschlüsselt. Würde eine dritte Person in der Zeit an Dein Smartphone oder Tablet kommen, iPGMail dazu nicht durch PIN gesichert, wäre der Inhalt nicht mehr sicher.

Um die Nachricht zu lesen, tippe auf encrypted.txt

In einem neuen Fenster kannst Du nun den entschlüsselten Inhalt lesen und auch gleich beantworten.





Ab hier beginnt **Compose**, zu antworten bzw. eine verschlüsselte Nachricht zu erzeugen. Ob als **Reply** (Antwort) oder neu unterscheidet sich in der Anwendung nicht.

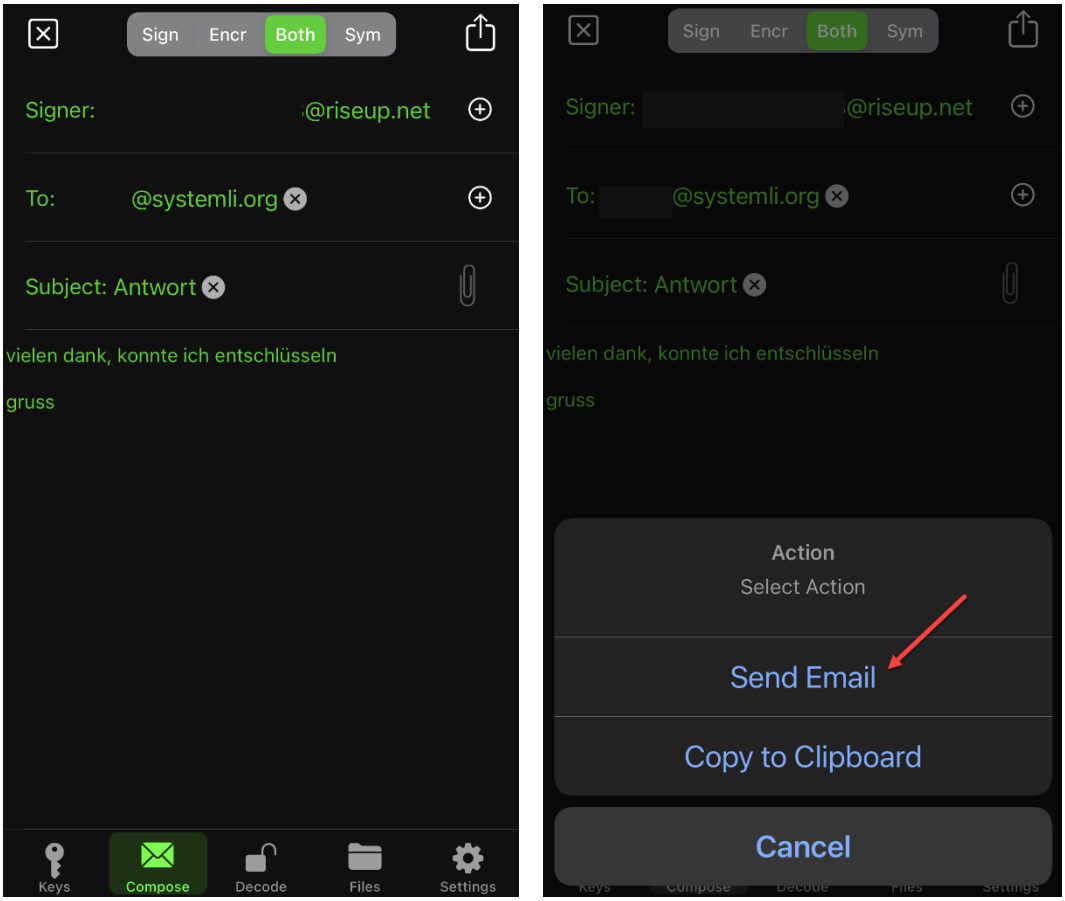
Signer ist der Absender der Nachricht, wird bei einem Reply automatisch gesetzt, hast Du mehrere geheime Schlüssel, kannst Du den Absender auch wählen.

To ist der Empfänger, die Auswahl begrenzt sich hier auf die bisher vorhandenen importierten Schlüssel Deiner Empfänger. Tippst Du auf das **+** Zeichen, öffnet sich Deine Schlüsselverwaltung und Du kannst den Key des Empfängers auswählen. Es werden Dir bei **Signer** nur Deine geheimen und bei **To** nur die öffentlichen Schlüssel zur Auswahl angeboten.

Subject ist die Betreffzeile einer Email

Büroklammer erlaubt Dir Anhänge wie Bilder und Dokumente anzufügen, die ebenfalls verschlüsselt werden.

Textfeld im unteren Bereich enthält Deine Nachricht.



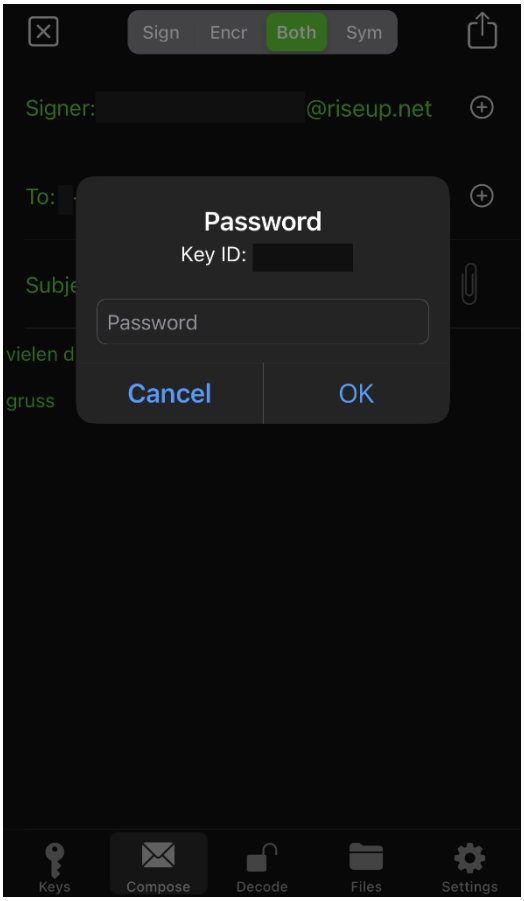
So sollte zum Beispiel eine fertige Antwort / Nachricht aussehen.

Du hast jetzt noch die Möglichkeit, entgegen Deiner Voreinstellung zu verändern, ob Du nur signieren, nur verschlüsseln oder verschlüsseln + signieren möchtest. Beides zusammen macht Sinn.

Über das Symbol ganz oben rechts kommst Du ins Aktionsmenü.

Hast Du einen SMTP Account in iPGMail hinzugefügt oder in der iOS Mail App eingerichtet, kannst Du die Nachricht über **Send Email** nun direkt versenden.

Möchtest Du eine andere App zum versenden Deiner Nachricht nutzen, kannst Du auch **Copy to Clipboard** auswählen, um den Inhalt später in den Emailbody zu kopieren. Den Empfänger und die Subject Zeile musst Du in der anderen Email App erneut eingeben und vom richtigen Absenderkonto senden.



Egal welche der beiden Optionen Du wählst, Du musst nun das Passwort Deines geheimen Schlüssels korrekt eingeben, um den Inhalt einschließlich eventueller Anhänge zu verschlüsseln.

War die Eingabe erfolgreich, hast Du ein Ergebnis ähnlich dem Beispiel der zuvor empfangenen Datei.

Mit klick auf den blauen Pfeil sendest Du die verschlüsselte Nachricht an Deine Empfänger:innen.

Hast Du **Copy to Clipboard** vorher ausgewählt, hast Du den Inhalt bereits in Deiner Zwischenablage und kannst ihn in den Emailbody einer beliebigen Email App einsetzen, adressieren und absenden.

Alles in allem ist iPGMail eine simple, einfache und günstige Lösung, PGP auch in Email Apps zu realisieren, die diese Funktion von sich aus nicht unterstützen.

Hast Du ein paar Mal Nachrichten entschlüsselt, verschlüsselte Nachrichten erzeugt und versendet, sind die wenigen Schritte gar nicht mehr so umständlich oder kompliziert.

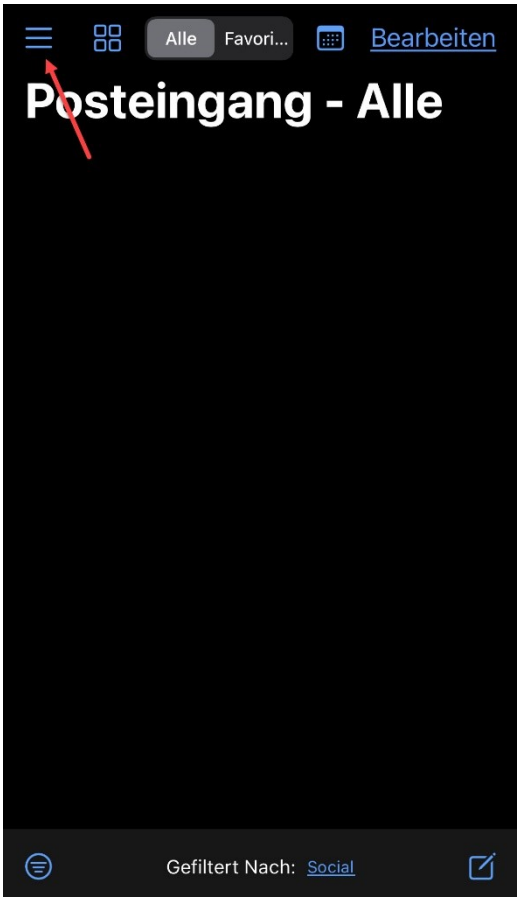
Was vielleicht etwas nervt ist die unkomfortable Schlüsselverwaltung. Für Absender:innen, die ihre Schlüssel auf öffentlichen Keyservern hinterlegen, könnte man den Import verkürzen und die öffentlichen Schlüssel direkt beziehen.

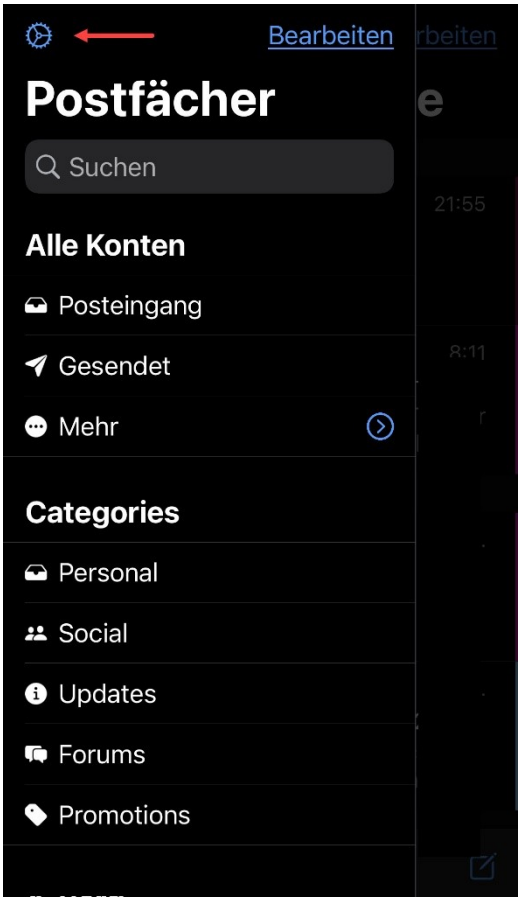
Ist das nicht der Fall, muss man auch in jedem beliebigen anderen Emailprogramm mit PGP Unterstützung (Thunderbird ab Version 78 ebenso) die öffentlichen Schlüssel manuell importieren.

Ist das Sicherheitsbedürfnis hoch, bleibt auch nur der persönliche Schlüsselaustausch und manuelle import.

Unter dem Strich eine kleine, praktische App die ihren Zweck erfüllt und für gelegentlichen Emailverkehr vollkommen ausreichend ist.

Canary – Setup





Wenn Du die App aus dem App Store geladen hast, solltest Du zuerst die Einstellungen bearbeiten, um die App für ihre Nutzung einzurichten und gegen unbefugte Benutzung zu sichern.

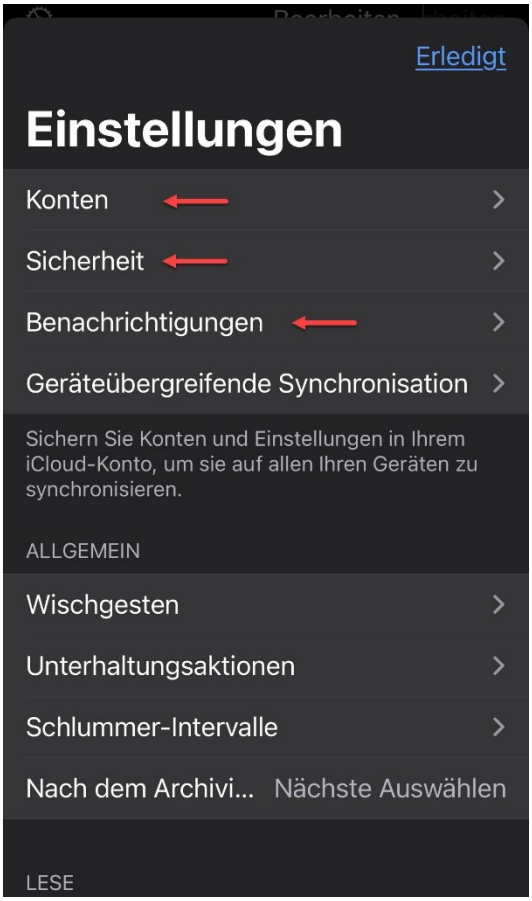
Canary bietet als vollständiger Emailclient eine ganze Menge mehr Einstellungen wie iPGMail, die wir nicht alle vollständig erklären wollen. Viele Einstellungen wie Design, Standard Browser oder nach Unterhaltung organisieren sind rein persönliche Geschmackssache.

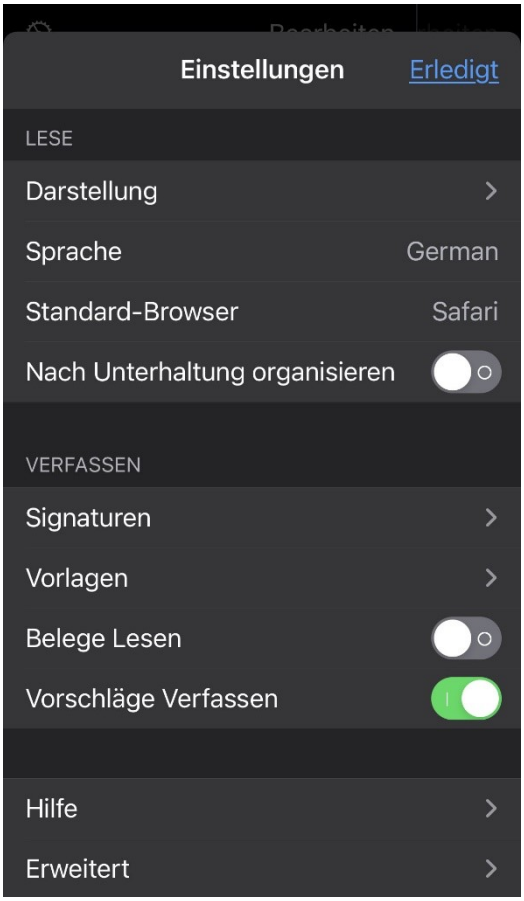
Auf alle anderen wichtigen Themen, die Sicherheit der App und Einfluss auf die PGP Verschlüsselung haben, gehen wir ein. Grundsätzlich solltest Du Dich immer mit den Einstellungen neuer Programme vertraut machen und ggf. dessen Funktionen zu hinterfragen.

Beginnen wir als erstes mit den Einstellungen, klicke dazu oben links auf die drei horizontalen Linien.

Damit öffnest Du das App Menü und später Deine eingerichteten Emailkonten, Mailein- und Ausgänge, IMAP Ordner usw.

Den Zugang zu den Einstellungen findest Du immer ganz oben links bei dem Zahnradsymbol.





Konten: mit **Konto Hinzufügen** richtest Du Deine Emailkonten ein. Neben einer Standardauswahl der gängigen Emailanbieter kannst Du unter **Andere** auch den Emailanbieter Deines Vertrauens wie zum Beispiel systemli.org oder riseup.net einrichten. Canary fragt den Host nach den Einstellungen ab, funktioniert das mal nicht, kannst Du unter **Zeige Erweiterte Einstellungen** die Angaben auch selbst eintragen und mit Einloggen anmelden – fertig.

Sicherheit: hier kann man gleich drei wichtige App Funktionen verwalten, die App vor unbefugtem Zugriff schützen, Externe Inhalte laden abschalten und die Verschlüsselungsmethoden samt Schlüssel verwalten. Dazu später mehr, gehen wir erst das Einstellungsmenü kurz durch.

Benachrichtigungen: hier kannst Du festlegen wie Du benachrichtigt werden möchtest und für welche Emailkonten Du Benachrichtigungen erhalten möchtest.

Push Benachrichtigungen als **Benachrichtigungstyp** nutzen Komponenten eines Servers, während Nachrichten holen direkt auf Deinem Gerät implementiert sind. Wenn Du auf Nummer sicher gehen willst, verzichte auf Push Benachrichtigungen.

Geräteübergreifende Synchronisation: ist ein typisches Apple Feature, wenn Du Canary auf einem iPhone, iPad und einem Mac nutzt, werden die Programmeinstellungen über die iCloud synchronisiert. **Beabsichtigst Du sensible Inhalte zu teilen, schalte die Funktion aus!**

Wischgesten, Unterhaltungsaktionen, Schlummer-Intervalle, Nach dem Archivieren/Löschen, Darstellung, Sprache, Standard Browser, Nach Unterhaltung organisieren, Signaturen, Vorlagen, und Vorschläge Verfassen sind alles „Komforteinstellungen“, die Dir das Arbeiten mit der App erleichtern sollen bzw. es Dir erlauben, sie Deinen persönlichen Bedürfnissen anzupassen.

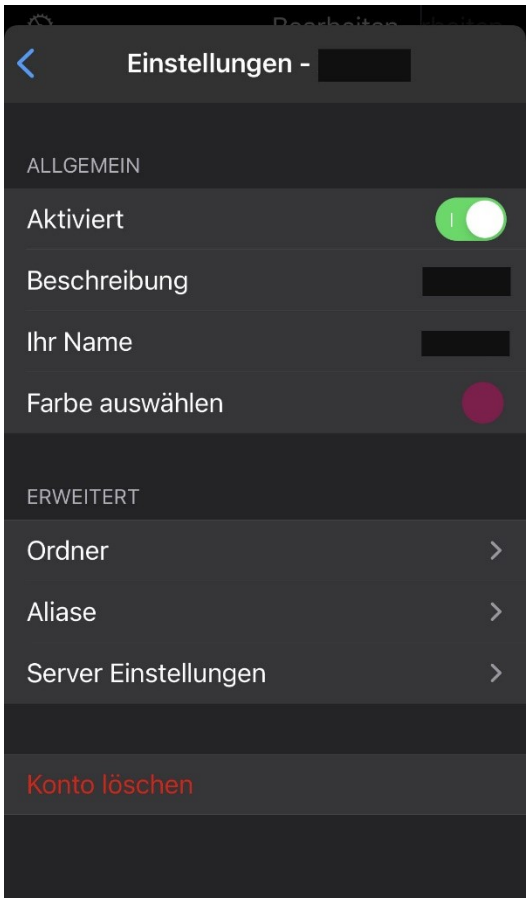
Belege Lesen: ist empfohlen abzuschalten, damit forderst Du eine Lesebestätigung an und aktivierst ein „Lesetracking“. Die Funktion ist bei vielen Emailservern nicht sehr beliebt und wird auch oft geblockt.

Signaturen sind ganz nett, wenn man als Gruppe oder Organisation immer einen bestimmten Nachrichten Abschluss mit zum Beispiel Kontaktdaten, URL zum Blog, etc. unter die Nachricht setzen möchte.

Vorlagen sind ganz nützlich, wenn man viele Standardanfragen hat und den Text nicht jedes mal komplett neu eintippen möchte.

Erweitert: enthält einige Tools und Informationen zur App.

Gehen wir nun auf weitere Einstellungen in speziellen Kategorien ein und beginnen bei **Konten**.



Wenn Du ein Emailkonto unter **Konten** eingerichtet hast findest Du im Anschluss Deine Emailkonten aufgelistet und kannst dort weitere Einstellungen vornehmen. Canary lässt grundsätzlich eine nicht begrenzte Zahl von Emailkonten zu.

Aktiviert: Wenn Du ein Emailkonto mal nicht brauchst, kannst Du es hier deaktivieren anstatt sofort zu löschen. Das reduziert die Anzeige in der App, den Traffic (Datenverbrauch im Mobilfunknetz) und natürlich auch den Stromverbrauch des Geräts.

Beschreibung: dient für Dich zur Beschriftung des Kontos später im App Menü.

Ihr Name: solltest Du (wenn überkaupt) nur mit großerVorsicht verwenden, denn das wird als Absender mit der Antwortemailadresse mitgesendet. Also niemals Klarnamen oder Angaben, die Rückschlüsse auf Deine Person zulassen verwenden!

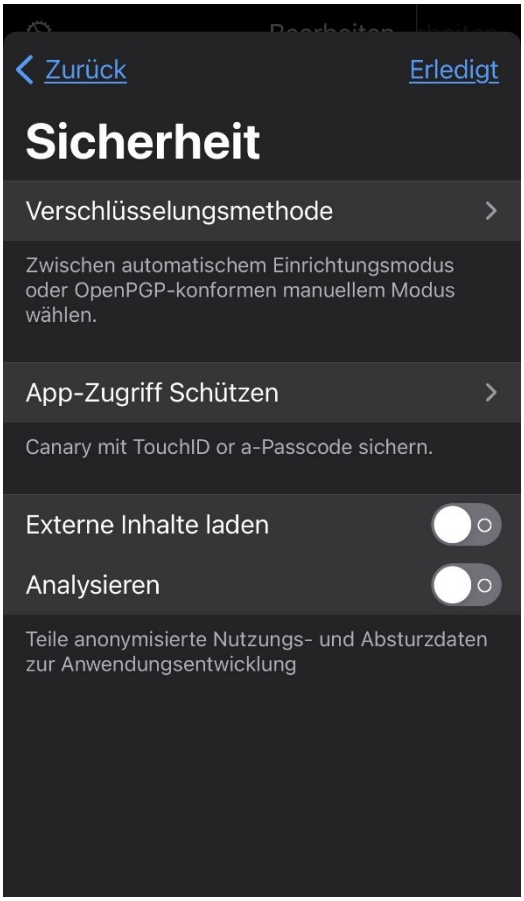
Farbe auswählen: ermöglicht in der Ansicht **Alle Konten** rechts am Rand eine dünne Farbmarkierung der Nachrichten. Damit kannst Du schon optisch erkennen, an welches Deiner Emailkonten die Nachricht gesendet wurde.

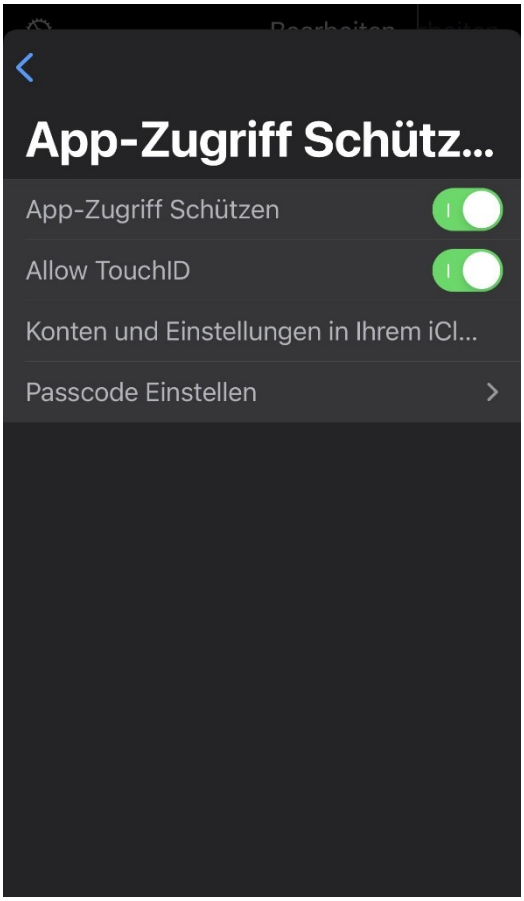
Ordner: hier kannst Du festlegen, ob Du alle oder nur bestimmte Ordner Deines IMAP Emailkontos mit Deinem Smartphone synchronisieren möchtest. Auch hier gilt, es reduziert die Anzeige in der App, den Traffic (Datenverbrauch im Mobilfunknetz) und natürlich auch den Stromverbrauch des Geräts.

Aliase: die App ist sogar in der Lage, Deine Emailaliase zu verwalten, hier gibst Du die Alias Email-adressen ein. Ein Alias ist kein Emailkonto sondern nur eine von X Emailadressen eines Emailkontos. Das heißt Du verwendest in einem Emailkonto mit einem Zugang mehrere Emailadressen, über die Du Nachrichten mit unterschiedlichen Emailadressen senden, empfangen und beantworten kannst. Auch für Alias Emailadressen können PGP Schlüssel verwendet werden.

Servereinstellungen: erlauben Dir Deine Anmeldeinformationen, einschließlich der erweiterten Einstellungen zu dem Emailkonto zu ändern. Das kennst Du bereits vom Einrichten Deines Emailkontos.

Konto löschen: wenn Du es gar nicht mehr brauchst, dann kannst Du es komplett aus der App löschen. Damit werden auch alle Daten unwiderruflich von Deiner App gelöscht.





Auf den Punkt Sicherheit sollte man grundsätzlich immer einen besonderen Blick werfen, zum einen um seine Daten zu schützen, zum anderen um die Geschwätzigkeit von Apps etwas einzudämmen.

Externe Inhalte laden: HTML Mails sind ganz „nett“, sehen stylisch aus, machen was her und sind vielleicht ansprechender als nur Text.

Aber: auf diesem Weg kann Schadcode geladen und die Sicherheit von PGP Verschlüsselung auf Dein Gerät geladen werden!

Wenn Dir sichere Informationen wichtig sind, **schalte das immer aus!**

Analysieren: es behindert die Funktion der App in keiner Weise, wenn Du auf Deine (versprochene) anonyme Unterstützung verzichtest!

App-Zugriff Schützen: hier kannst Du zusätzlich zum Geräteschutz auch die Verwendung Deiner Email App schützen. Generell einschalten macht Sinn.

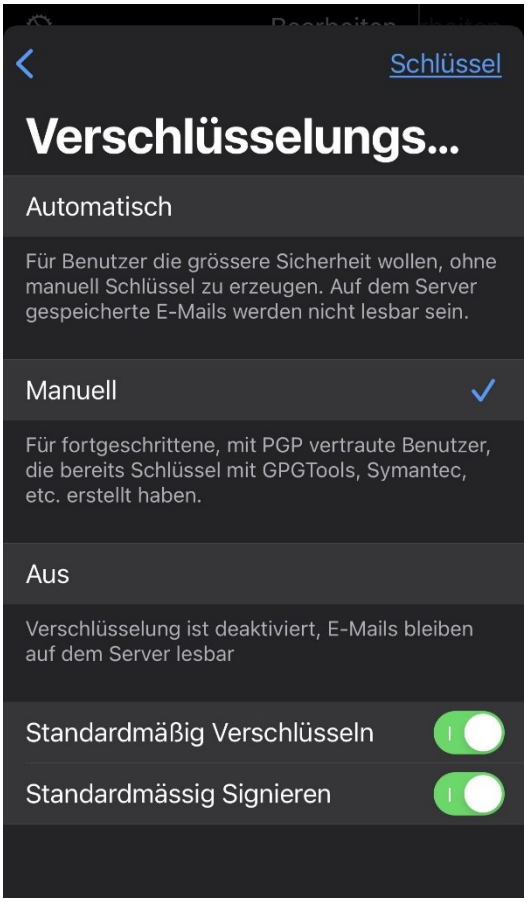
Allow TouchID: zum Schutz werden Deine im Gerät gespeicherten Fingerabdrücke verwendet, sofern Du diese Funktion eingerichtet hast.

Passcode einstellen: willst Du die App nicht über Fingerabdrücke freischalten, kannst Du hier einen Passcode einrichten, den Du bei Verwendung der App eintippst.

Konten und Einstellungen in Ihrem iCloud-Konto sichern, um diese mit allen Geräten zu synchronisieren: hier wird nur der Intervall festgelegt, die Funktion selbst schaltest Du über **Geräteübergreifende Synchronisation** im Hauptmenü der Einstellungen ab.

Canary – Schlüsselverwaltung

In der Einstellung Sicherheit erhalten wir über **Verschlüsselungsmethode** auch Zugang zur Verschlüsselung und PGP Schlüsselverwaltung.



Automatisch: (**nicht empfohlen!**) verwendet zwar Verschlüsselung, verspricht auch, dass Nachrichten nicht lesbar auf dem Server gespeichert werden, ist aber nicht mit PGP Verschlüsselung zu vergleichen.

Manuell: (**empfohlen!**) an dieser Stelle zwingst Du den Emailclient zur Verschlüsselung grundsätzlich PGP zu verwenden. Andere Verschlüsselungsmethoden werden nicht akzeptiert.

Aus: (**nicht empfohlen!**) hiermit schaltest Du generell für alle Emailkonten die Verschlüsselung ab!

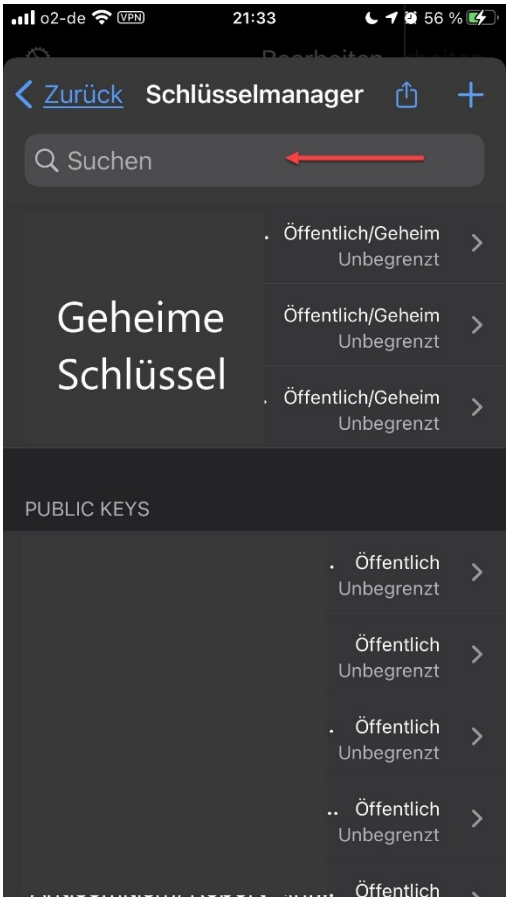
Standardmäßig verschlüsseln: (**empfohlen!**) damit kannst Du verhindern, dass Nachrichten versehentlich ohne Verschlüsselung versendet werden. In jeder Mail kannst Du separat bestimmen, ob Du verschlüsseln willst oder nicht.

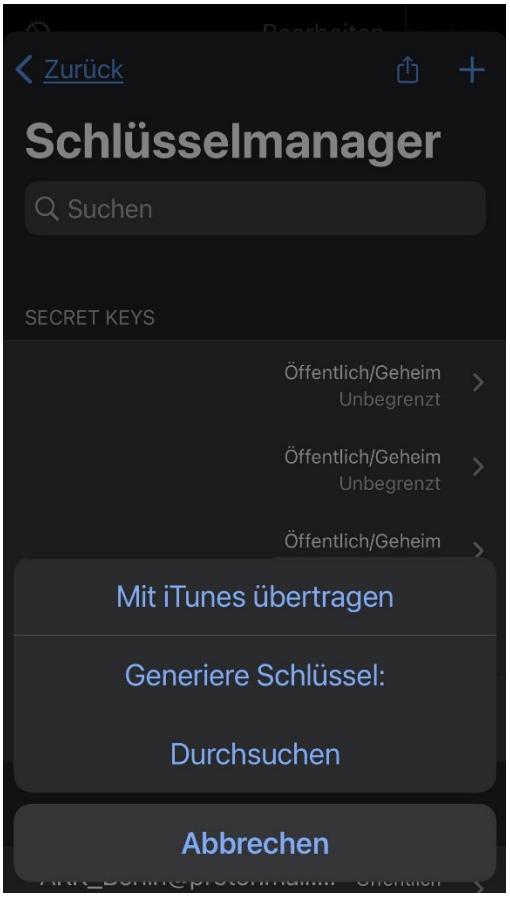
Standardmäßig signieren: (**empfohlen!**) die Signatur legt fest, sofern der Empfänger sie akzeptiert oder ein verifizierter Server bestätigt hat, dass die Nachricht auch von Dir stammt. Unabhängig davon, ob sie verschlüsselt wurde oder nicht.

Tippst Du oben rechts auf **Schlüssel**, gelangst Du in die zentrale Schlüsselverwaltung von Canary Mail.

Das sieht jetzt sehr umständlich und nach vielen Tipp Wegen aus, um an die Schlüsselverwaltung zu kommen. Diesen langen Weg wird man voraussichtlich nur bei der Einrichtung der PGP Verschlüsselung oder beim Hinzufügen vieler Schlüssel wählen.

An späterer Stelle beim Verfassen von Emailnachrichten werden wir feststellen, dass es noch weitere, einfachere Wege zu Deinem Schlüsselspeicher gibt, die Dir diesen langen Tipp Weg ersparen.





Hier bist Du nun in Deiner Schlüsselverwaltung. Im oberen Bereich siehst Du Deine eigenen geheimen Schlüssel, ohne die Du keine Nachrichten versenden kannst.

Wenn Du noch keinen geheimen Schlüssel hast, kannst Du mit Generiere Schlüssel ein Schlüsselpaar (geheim + öffentlich) erzeugen. Der Schlüssel wird nach RSA Länge 4096 bits erstellt.

Achtung! Du wirst beim erstellen gefragt, ob der Schlüssel zum **Keychain** (schlüsselbung) hinzugefügt werden soll. **Das tust Du bitte nicht!**

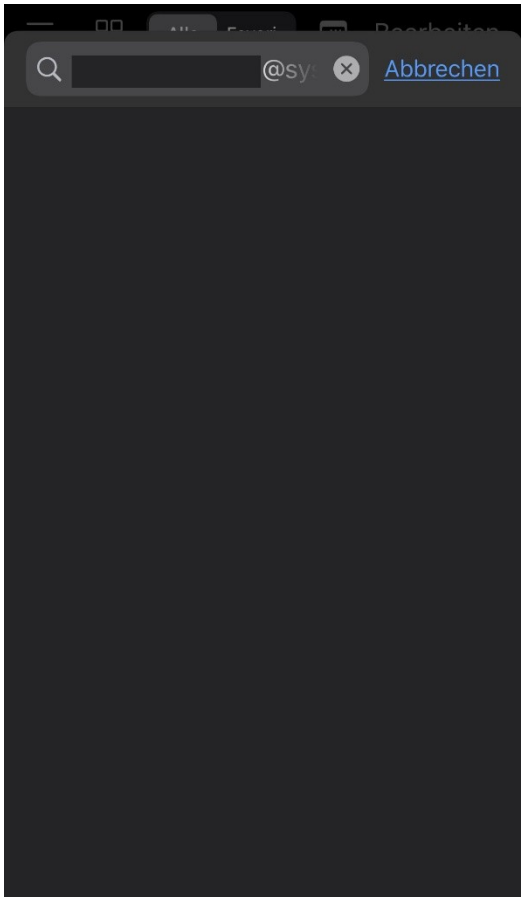
Auch wenn das im Grunde bequem und einfach ist, was nützt ein Schlüssel, egal wie gut und lang er auch ist, wenn er irgendwo herum hängt?

Wenn Du schon Deine Passwörter aufschreiben willst oder musst, dann auf keinen Fall in eine Note oder sonstige ungeschützte App! Verwende dazu wenigstens einen lokalen Keysafe, den Du mit einem Mega guten und langen Passwort schützt, dass Du im Kopf hast.

Darunter siehst Du alle Public Keys (öffentliche Schlüssel) aller Deiner Empfänger:innen, mit denen Du verschlüsselt schreiben möchtest.

Du kannst geheime und öffentliche Schlüssel entweder **mit iTunes** in die App übertragen oder über Durchsuchen von einem anderen Speicherort.

Wenn Du eine Cloud verwenden möchtest, nutze einen Cloudservic dem Du vertrauen kannst, wie zum Beispiel die **Systemli Nextcloud** https://www.systemli.org/service/cloud/



In der Schlüsselverwaltung gibt es noch ein Suchfeld.

Dieses Suchfeld ist nicht dazu gedacht, Deine bereits gespeicherten öffentlichen Schlüssel zu durchsuchen.

Wenn Du hier eine Emailadresse eintippst, werden öffentliche Schlüsselserver durchsucht, ob für diese Adresse bereits ein öffentlicher Schlüssel existiert.

Beispiel:

Tippst Du nur **beispiel@** ein, bekommst Du gleich eine Liste vorhandener PGP Schlüssel angezeigt, die damit beginnen.

Rechts auf dem **>** kannst Du Informationen zur vollständigen Emailadresse und dem Fingerprint aufrufen.

Links mit **+** kannst Du den Schlüssel importieren, ist bereits ein Haken da, ist der Schlüssel bereits vorhanden.

Wichtig!

Bei öffentlichen Schlüsseln ist nur die Nachricht sicher!

Ohne den Fingerprint persönlich zu prüfen, weißt Du nicht wem Du da tatsächlich, wenn auch sicher schreibst!

Bei Gruppen/Organisationen, die ihre Emailadresse und den Schlüssel öffentlich in Blogs oder Websites publizieren, macht die Hinterlegung auf einem Schlüsselserver durchaus Sinn. Du kannst Den Fingerprint des importierten Schlüssels auf der Website oder dem Blog gegenprüfen. Stimmt der Fingerprint, kannst Du Dir sicher sein, dieser Gruppe/Organisation zu schreiben.

Je nach Aktionslevel ist es auch sinnvoll, öffentliche Schlüssel persönlich bei einem Treffen auf einem USB Stick zu teilen. Dann kannst Du Dir tatsächlich sicher sein, dass Emailadresse und Schlüssel auch tatsächlich den Genoss:innen gehören, die Du persönlich kennst und mit denen Du schreibst.

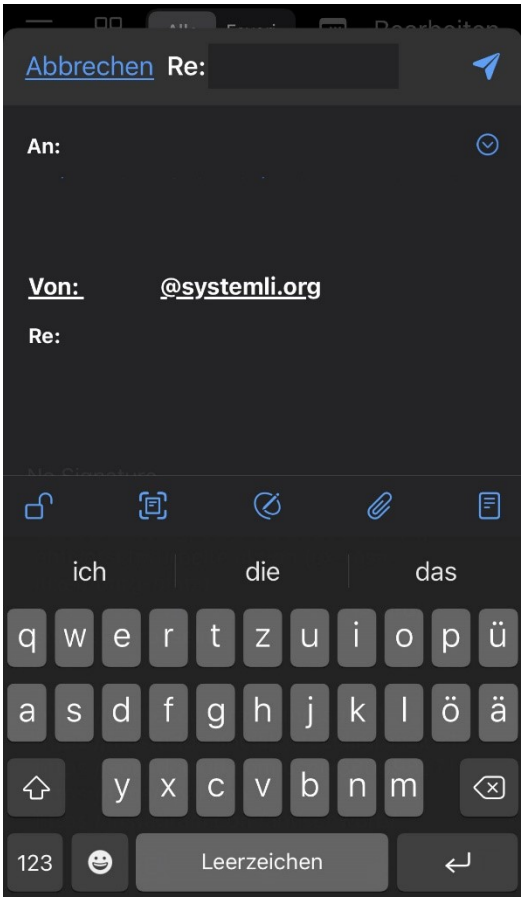
In dem Fall gehe behutsam mit den anvertrauten Emailadressen und öffentlichen Schlüsseln um, es wird triftige Gründe geben, warum Deine Genoss:innen sowohl mit Emailadresse, wie auch Schlüssel nicht einfach überall hausieren gehen.

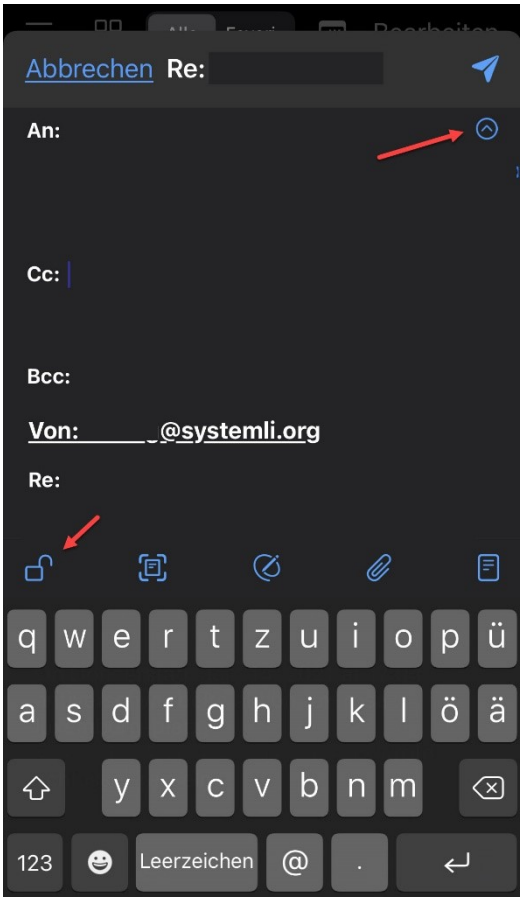
PGP Verschlüsselung ist und bleibt keine Lebensversicherung!

Sicherheit steht und fällt mit ihrem Umgang, von unsicheren Passwörtern angefangen, über den Schutz der Entschlüsselungsprogramme, bis zum Umgang mit den verschlüsselten Inhalten.

Und nicht jede Information muss digital dokumentiert werden, überlege immer, was Du besser direkt aus Deinem Kopf direkt in einen anderen Kopf kommunizierst.

Canary – verschlüsseln





Zunächst erst mal ganz unspektakulär. Du tippst ganz unten rechts auf das Symbol neue Nachricht erstellen und es öffnet sich ein fast leeres Nachrichtenfenster.

An: da kommt die Emailadresse rein an die Du schreibst. Später wird dort ein kleines Band mit Empfänger:innen zu sehen sein, mit denen Du öfter schreibst und die Du durch antippen auswählen kannst.

Mit dem Symbol Pfeil nach unten rechts von **An:** kannst Du im **Cc:** weitere Empfänger für alle Empfänger:innen sichtbar oder **Bcc:** Emailadressen nur für Dich sichtbar hinzufügen. Damit Verschlüsselung funktioniert, brauchst Du von allen Empfänger:innen einen gültigen öffentlichen Schlüssel.

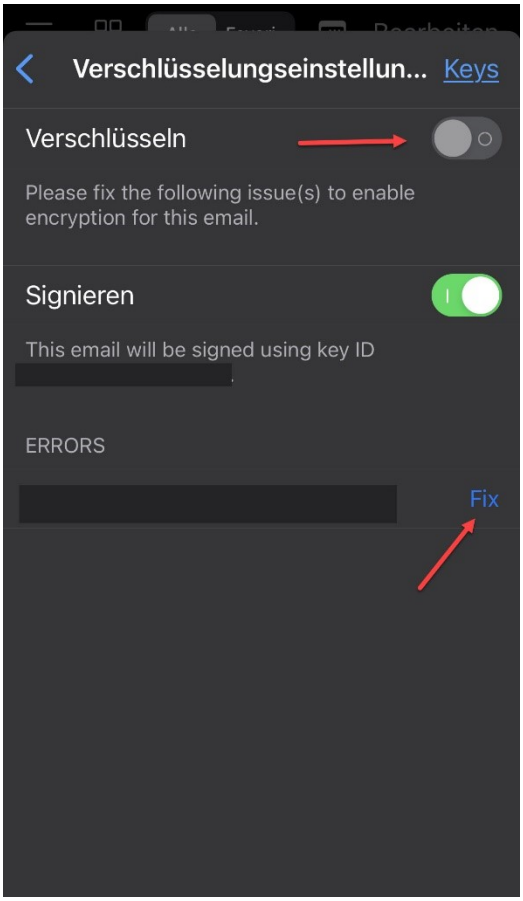
Von: ist in der Regel Deine Emailadresse, hast Du mehrere Emailkonten oder Alias Adressen, kannst Du durch antippen die richtige Absenderadresse auswählen.

Betreff: oder **Re:** sollte irgendwas drin stehen, Nachrichten ohne Betreff werden oft von Mailservern oder Programmen als Spam interpretiert.

Im Schreibfeld kommt dann die eigentliche verschlüsselte Nachricht und ggf. eine Signatur.

Unter dem Schreibfeld hast Du fünf Funktionen von links nach rechts:

Schloss: zeigt Dir den aktuellen Status der Nachricht an, verschlüsseln möglich oder nicht möglich.
Foto: Einfügen eines Fotos von der Kamera.
Stift: hier kann mit Finger oder Stift Freihand geschrieben/gezeichnet werden
Büroklammer: hier kannst Du beliebige Anhänge wie Bilder, Dokumente an die Nachricht anhängen.
Dokument: hier kannst Du eine Vorlage auswählen, sofern Du das eingerichtet hast.



Wenn Du bei **An:** noch keine Emailadresse eingegeben hast oder eine Emailadresse, die Deiner Schlüsselverwaltung nicht bekannt ist, wird ein offenes Schloss angezeigt.

Tippst Du auf das **Schloss**, kommst Du direkt zur Schlüsselverwaltung für Deine Nachricht.

Verschlüsseln: ist deaktiviert und kann auch nicht aktiviert werden, da Du entweder noch keine Emailadresse eingetragen hast oder für die eingetragene Adresse kein Schlüssel bekannt ist.

Signieren: kannst Du grundsätzlich immer, auch wenn Du unverschlüsselt sendest. Darunter wird Dir der Fingerprint Deines eigenen Schlüssels angezeigt, mit dem Du signierst.

Errors: hast Du eine oder mehrere Emailadressen als Empfänger:innen eingetragen, für die Du noch keinen öffentlichen Schlüssel in Deiner Schlüsselverwaltung importiert hast, werden Dir hier die betroffenen Emailadressen aufgelistet.

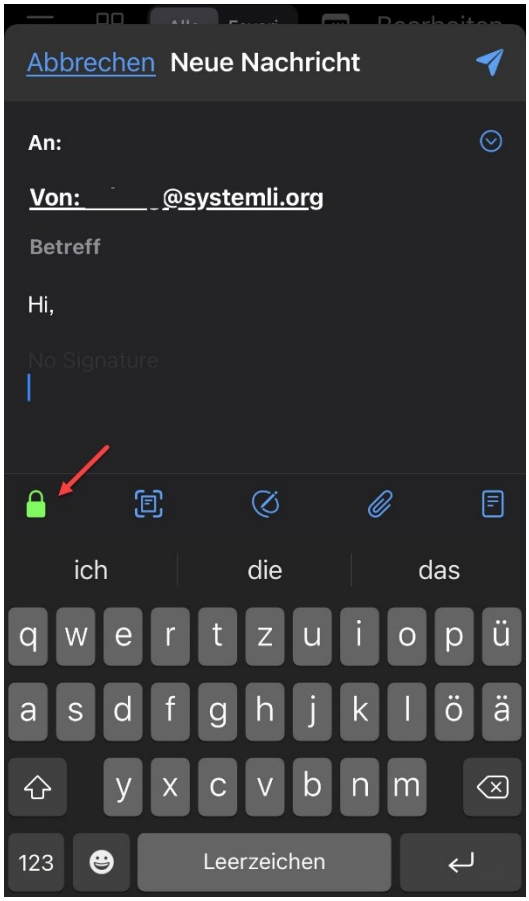
Verschlüsseln lässt sich erst aktivieren, wenn alle **Errors** behoben sind, wenn für alle Empfänger:innen ein gültiger öffenbtlicher PGP chlüssel existiert.

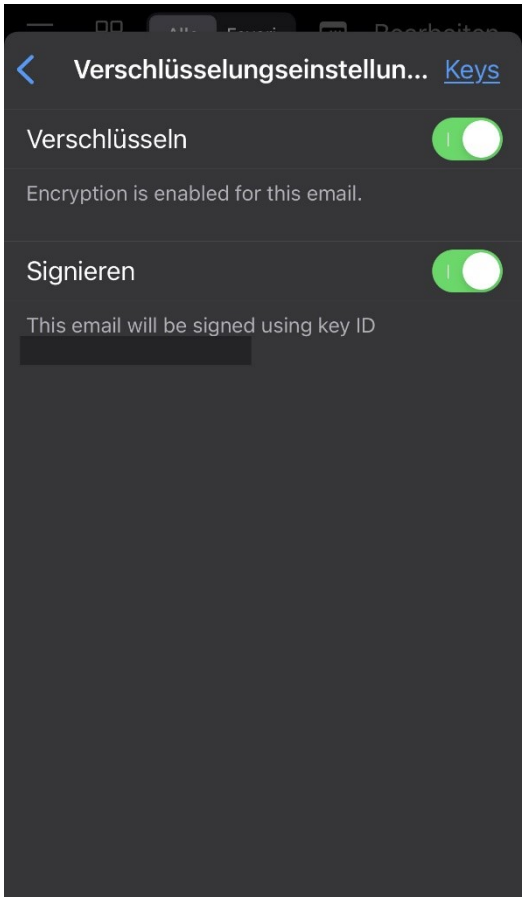
FIX: rechts neben der Emailadresse führt Dich sofort in Deine Schlüsselverwaltung und sucht die eingegebene Emailadresse auf öffentlichen Schlüsselservern.

Wird ein Schlüssel nicht gefunden, kann es mehrere Gründe dafür geben:

- Empfänger:in hat keinen PGP Schlüssel
- Tippfehler bei der Emailadresse der Empfänger:in
- Empfänger:in hat den Schlüssel nicht auf einem Keyserver veröffentlicht

Um die Nachricht zu senden, musst Du Dir den Public Key besorgen, oder bei mehreren Empfänger:innen die Emailadresse heraus löschen.





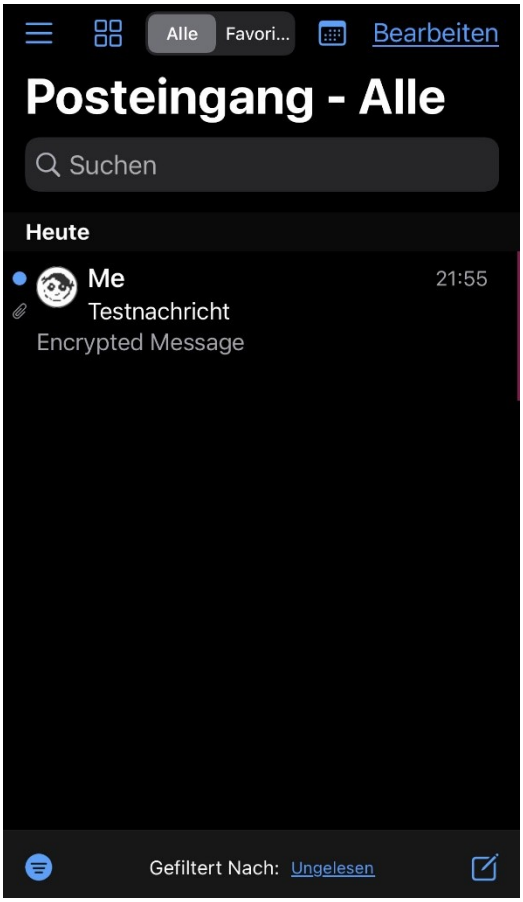
Schreibst Du eine Nachricht an eine Emailadresse für die Du bereits einen Schlüssel hast oder hast Du alle Probleme gefixt (fehlende Schlüssel importiert), wird Dir das Schloss nicht mehr offen, sondern grün angezeigt.

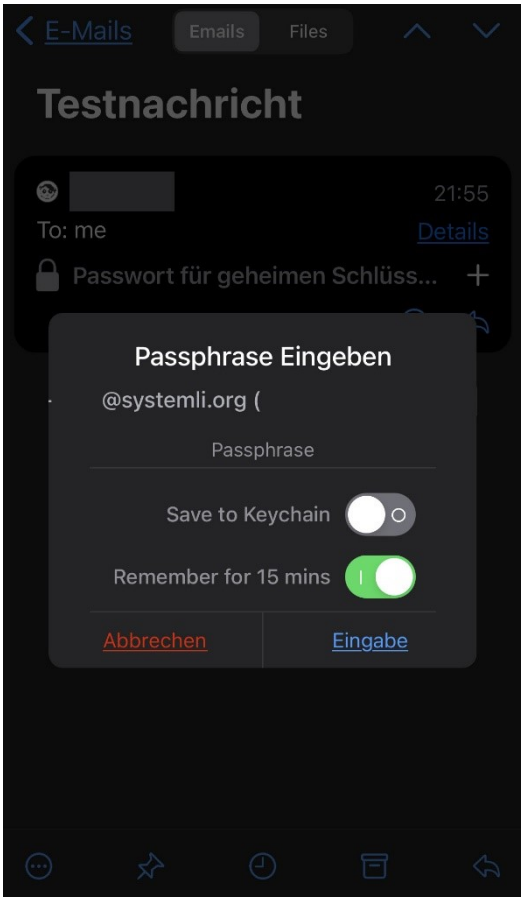
Tippst Du auf das Schloss, siehst Du **Verschlüsseln** ist aktiviert und **Signieren** ist aktiviert.

Der **Error** Eintrag ist ausgeblendet, da es keine Probleme mit dieser Nachricht gibt.

Möchtesst Du nur verschlüsseln aber nicht signieren, bleibt die Schlossanzeige trotzdem grün. Die Verschlüsselung für Deine Nachricht ist gewährleistet und Du kannst sie mit dem Senden Symbol ganz oben rechts verschicken.

Canary – verschlüsseln





Der große Moment ist da, Du bekommst Deine **Encrypted Message** (verschlüsselte Nachricht) in Deinen Posteingang.

Wie Du siehst, ist der **Betreff** der Nachricht **nicht verschlüsselt**, diese Funktion wird von Enigmail unterstützt, aber von vielen anderen Programmen nicht.

„Unsere Aktion heute Nacht am Potsdamer Platz“ wäre also kein schlauer **Betreff**.

Wenn Du auf die Nachricht tippst, öffnet sich die Nachricht und wird vom Passphrase Fenster überlagert.

Wenn Du auf **Abbrechen** tippst siehst Du nur Empfänger:in, Absender:in und Betreff der Nachricht, alles andere bleibt ausgeblendet. Tippst Du auf das **+** neben **Passwort für geheimen Schlüssel**, kommt wieder das Passphrase Fenster.

Hier wird Dir die Emailadresse und Fingerprint Deines geheimen Schlüssels angezeigt, wenn Du mehrere Konten und Schlüssel eingerichtet hast, wird das automatisch durch die Empfänger:innen Emailadresse identifiziert.

In die Zeile Passphrase gibst Du das Passwort Deines geheimen Schlüssels ein.

Damit Du die Nachricht auch lesen kannst, musst Du eine der beiden Optionen wählen:

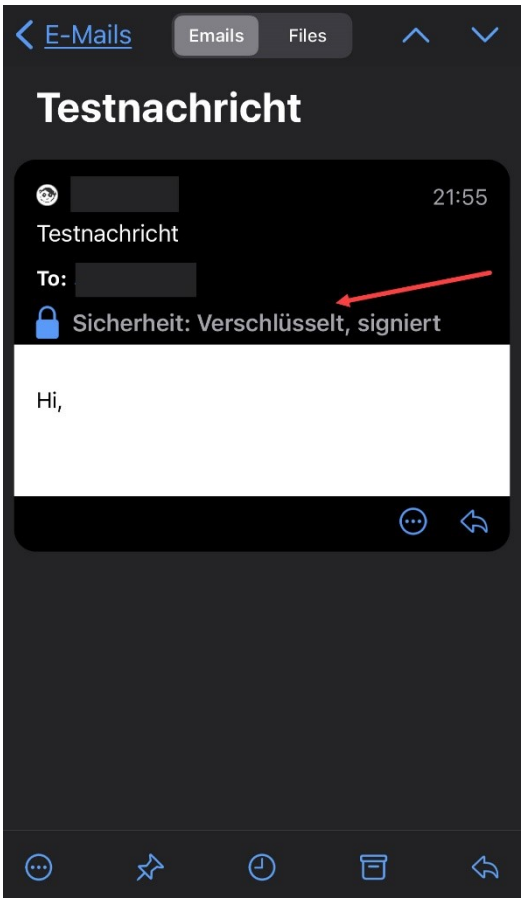
Save to Keychain: Du hinterlegst den Schlüssel fest in einem Schlüsselbund (**nicht empfohlen!**)

Remember for 15 Mins: Dein Passwort bleibt für 15 Minuten im Speicher der App. Du kannst die Nachricht dann lesen und beantworten, ohne das Passwort erneut einzugeben.

Lässt Du Deine App im Hintergrund,zum Beispiel um einen Artikel im Browser zu lesen und kehrst zur Appo zurück, kannst Du 15 Minuten lang ohne weitere Passworteingabe diese und auch andere Nachrichten lesen, die Du mit Deinem geheimen Schlüssel geöffnet hast.

Beendest Du die App, wird Dein Passwort sofort aus dem App Speicher gelöscht und Du musst das Passwort Deines geheimen Schlüssels erneut eingeben.

Tippe nach Passworteingabe auf **Eingabe**.



Die empfangene Nachricht ist nun vollständig entschlüsselt und der Inhalt für Dich sichtbar.

In der Zeile **Sicherheit** bekommst Du zwei wichtige Informationen:

Verschlüsselt: der Inhalt dieser jetzt entschlüsselten Nachricht hat Dich verschlüsselt erreicht.

Signiert: die Signatur der jetzt entschlüsselten Nachricht wurde als gültig identifiziert.

Dort könnte auch nicht signiert oder im ungünstigsten Fall Signatur ungültig stehen.

Ist das Passwort Deines geheimen Schlüssels aus Deinem Speicher wieder verfallen, bleibt die Nachricht verschlüsselt gespeichert und es wieder die Eingabe des Passworts notwendig.

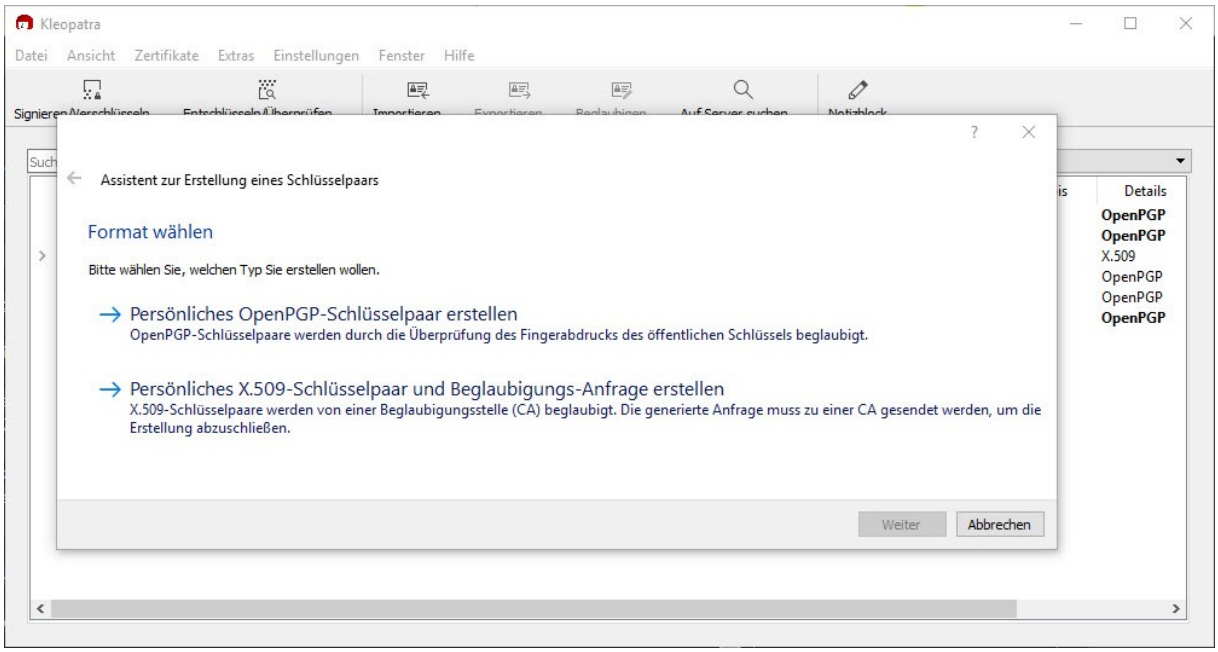
Solange Du also Inhalte oder Anhänge nicht in ein ungeschütztes Medium bewegst (Ausdrucken/Papier, Text in ein Notepad kopieren, Anhänge auf unverschlüsselten Datenträger speichern, usw.), solange bleiben Deine Nachrichten vor dem Zugriff Dritter geschützt.

Dabei zu beachten ist auch, dass Dateien löschen nicht bedeutet, dass digitale Inhalte nicht mehr da sind. Es gibt zahlreiche Tools, die gelöschte Daten wieder rekonstruieren können.

Emailverschlüsselung mit PGP ist neben sicherem Verantwortungsvollem Umgang und Verhalten auch nur ein weiterer Baustein eines Sicherheitskonzepts in der Nutzung digitaler Technik, Netzwerken und Geräten.

Schlüsselverwaltung mit Cleopatra

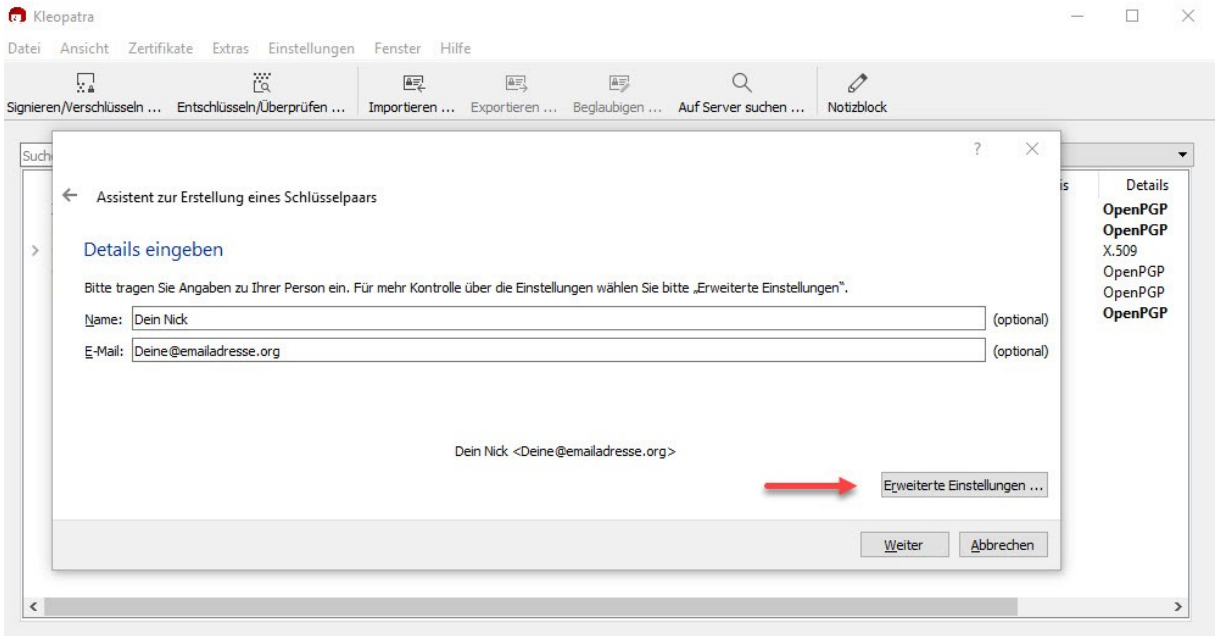
Deinen erstes Schlüsselpaar erstellen



Wenn Du zum Beispiel Outlook 2016 benutzt, musst Du mit der Schlüsselverwaltung von Cleopatra arbeiten und über den Assistenten ein persönliches Schlüsselpaar erstellen. Das Outlook Plugin ist nur in der Lage zu signieren und zu ver- und entschlüsseln.

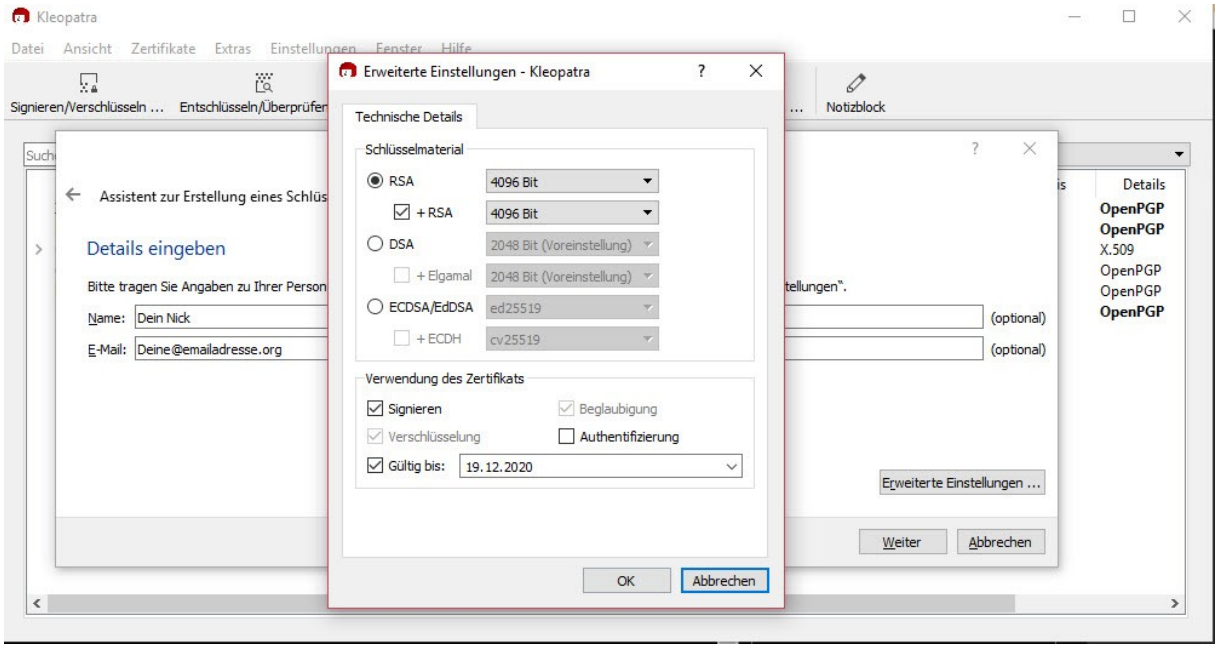
Wähle „Persönliches OpenPGP-Schlüsselpaar erstellen aus.

Startet der Assistent bei der erstmaligen Verwendung nicht automatisch, gehe zu „Datei“ → „Neues Schlüsselpaar…“

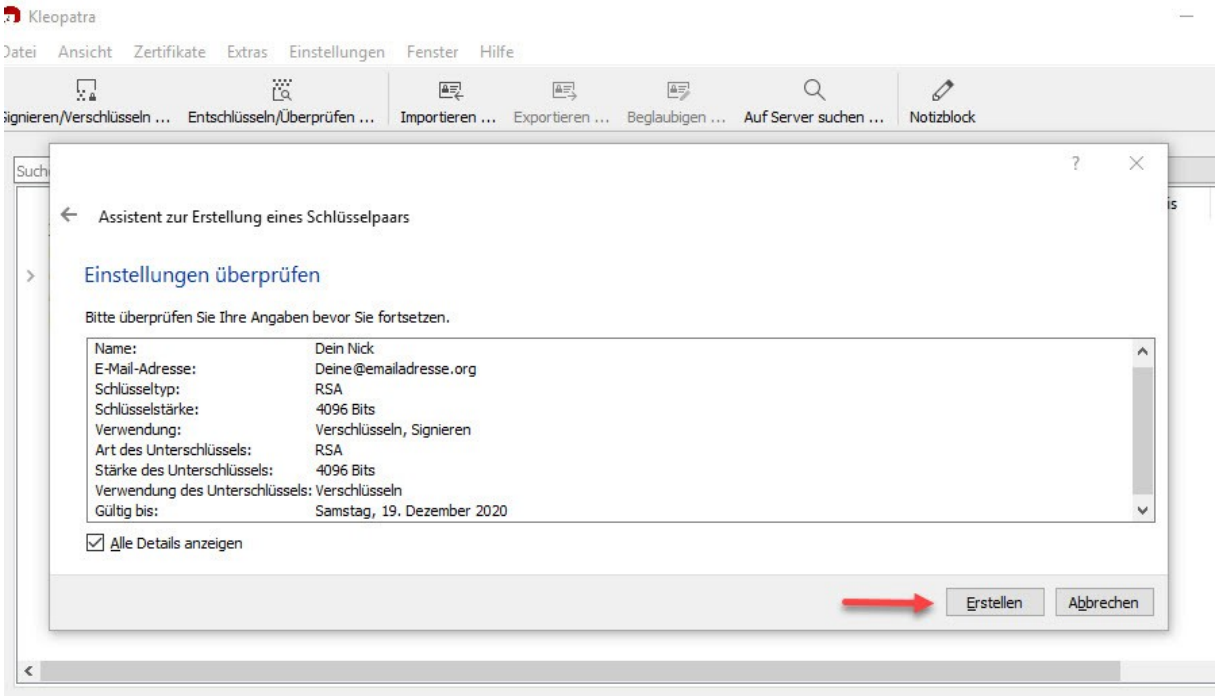


Hier kannst Du nun einen Nick eingeben und Deine E-Mailadresse. Unter den erweiterten Einstellungen kannst Du Gültigkeit und Schlüsselstärke einstellen.

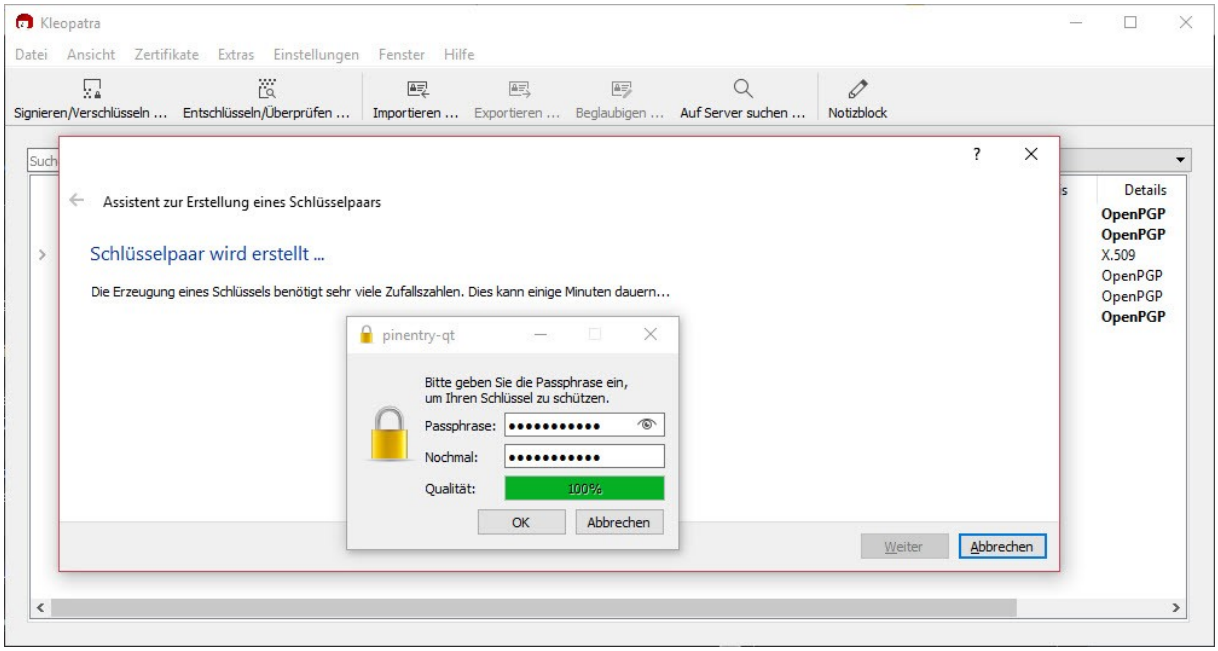
Klicke nach eventuell notwendigen Einstellungen auf „Weiter“.



Hier siehst Du die erweiterten Einstellungen für Dein Schlüsselpaar.

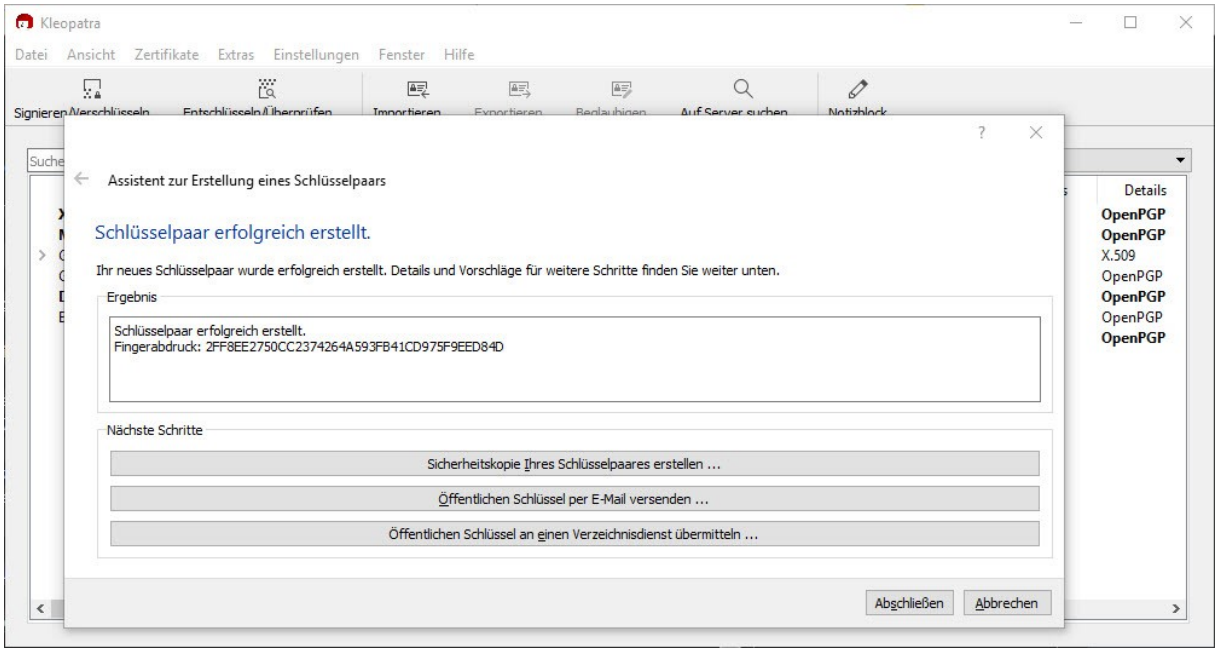


Nach dem Klick auf „Weiter“ kannst Du nochmal Deine Einstellungen überprüfen und Dir alle Parameter dazu ansehen. Wenn alles ok ist, klicke auf „Erstellen“.



An dieser Stelle musst Du Dir ein Sicheres Passwort für Deine Schlüssel vergeben und zur Bestätigung doppelt eingeben. Die Qualität Deines Passwortes wird Dir angezeigt.

Auch wenn 123456 für Dich einfach ist, macht nicht wirklich Sinn, wähle ein Passwort, dass Du noch nicht verwendest und präge es Dir gut ein. Klicke abschließend auf „OK“.



Fertig! Dein Schlüsselpaar wurde erfolgreich erstellt.

Sichere Dein Schlüsselpaar auf einem mit VeraCrypt verschlüsselten USB Stick und bewahre ihn sicher auf. Am besten außerhalb Deiner Wohnung.

Du kannst über den Assistenten Deinen Privaten Schlüssel an alle Deine Kontakte versenden.

Und Du kannst Deinen privaten Schlüssel an einen Verzeichnisdienst übermitteln, damit Dich jeder finden und den Schlüssel importieren kann. Spätestens an dieser Stelle wirst Du gefragt, ob Du ein Widerrufszertifikat erstellen willst.

Wenn die Bullen Deinen Rechner beschlagnahmen, Du ihn eventuell nicht vollständig verschlüsselt hast, dann kannst Du mit Deinem Widerrufszertifikat Deinen Schlüssel über einen anderen Rechner

für ungültig erklären. Bei den Menschen die mit Dir darüber kommunizieren, wird der Schlüssel als ungültig identifiziert.

Du solltest in solchen Fällen oder wenn Du Dich nach einer Beschlagnahme nicht mehr sicher fühlst, ein neues Schlüsselpaar erzeugen und den Menschen mit denen Du Kontakt hast den neuen Schlüssel mitteilen.

Sichere daher das Widerrufszertifikatebenfalls auf dem mit VeraCrypt verschlüsselten USB Stick und bewahre ihn sicher auf. Am besten außerhalb Deiner Wohnung.

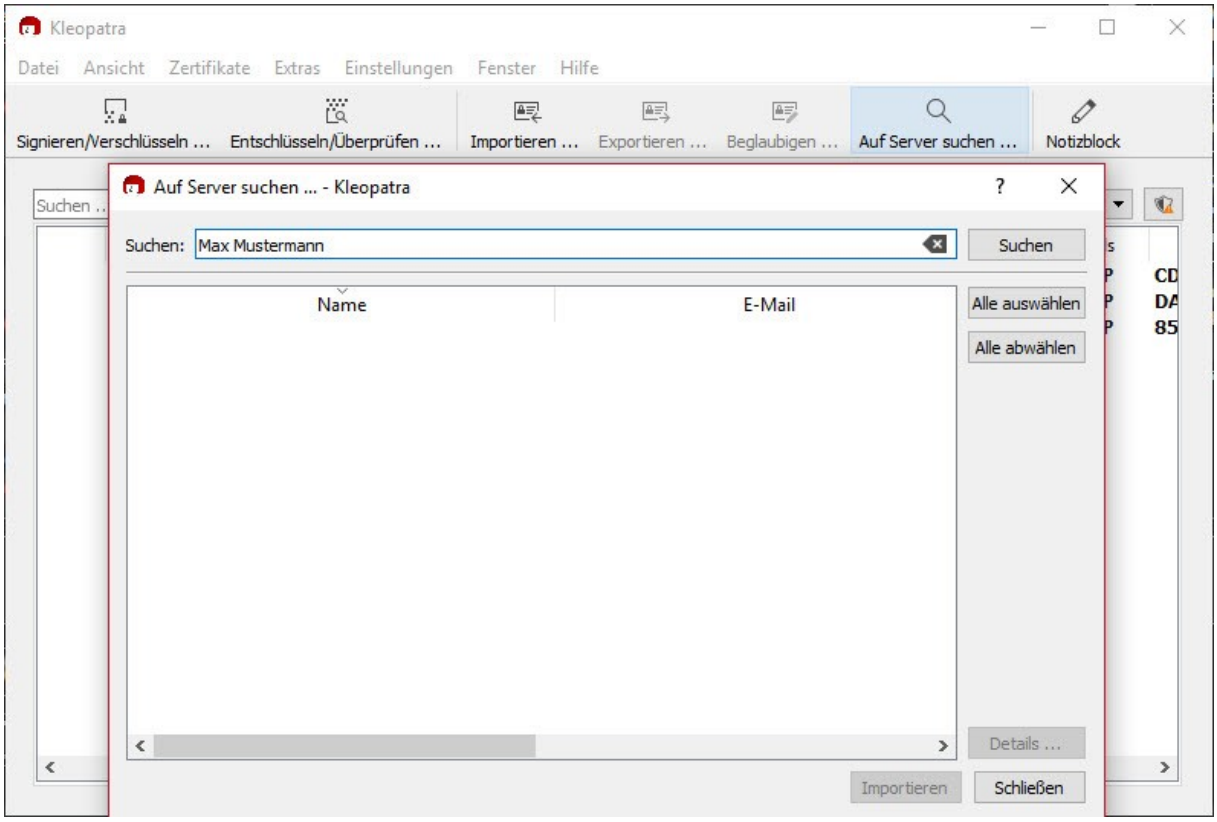
Allgemeine Hinweise

Du hast also Deinen erstes Schlüsselpaar erstellt und könntest nun loslegen.

Wenn Du auch Deinen privaten Nachrichtenverkehr verschlüsseln möchtest, dann kannst Du jetzt noch weitere Schlüsselpaare erstellen und in Deinem Zertifikatsspeicher verwalten.

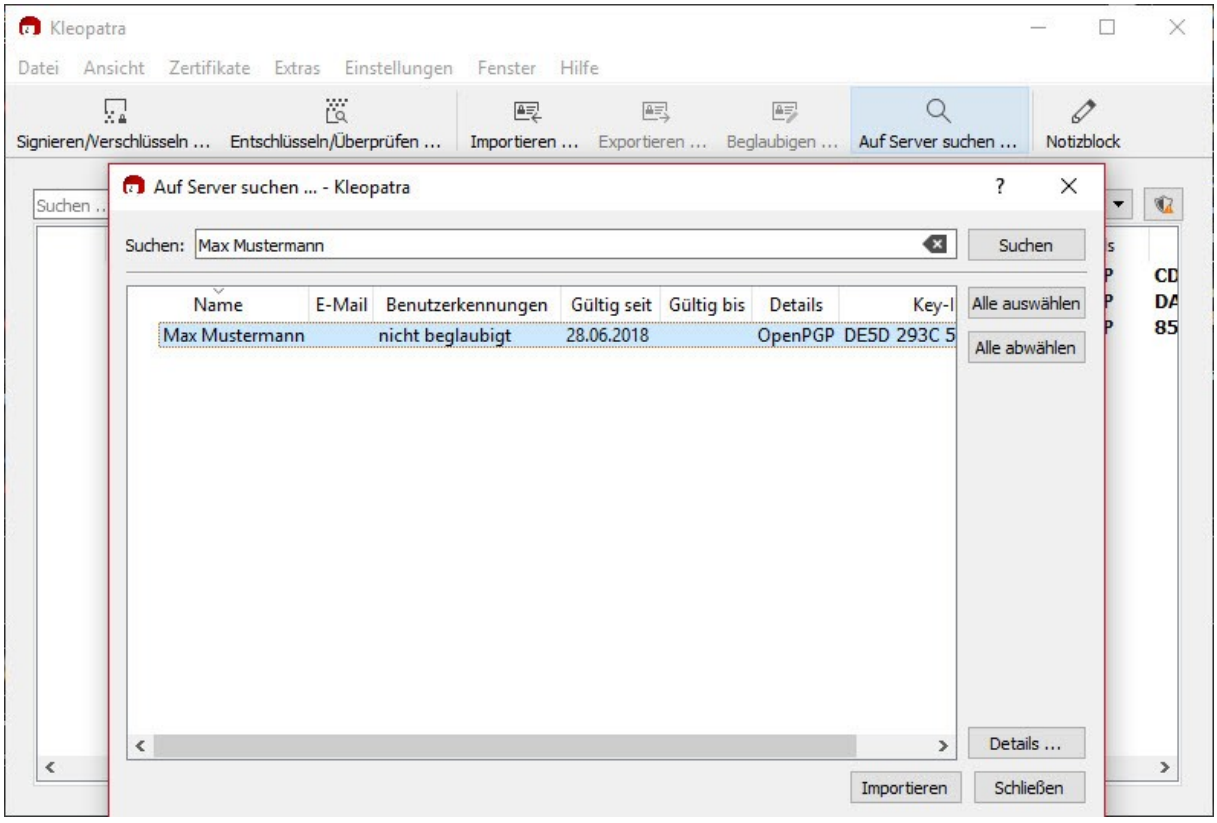
Damit Du aber verschlüsselt kommunizieren kannst, benötigst Du von den Menschen denen Du verschlüsselt schreiben willst den öffentlichen Schlüssel und sie benötigen auch Deinen öffentlichen Schlüssel.

Öffentliche Schlüssel suchen und importieren



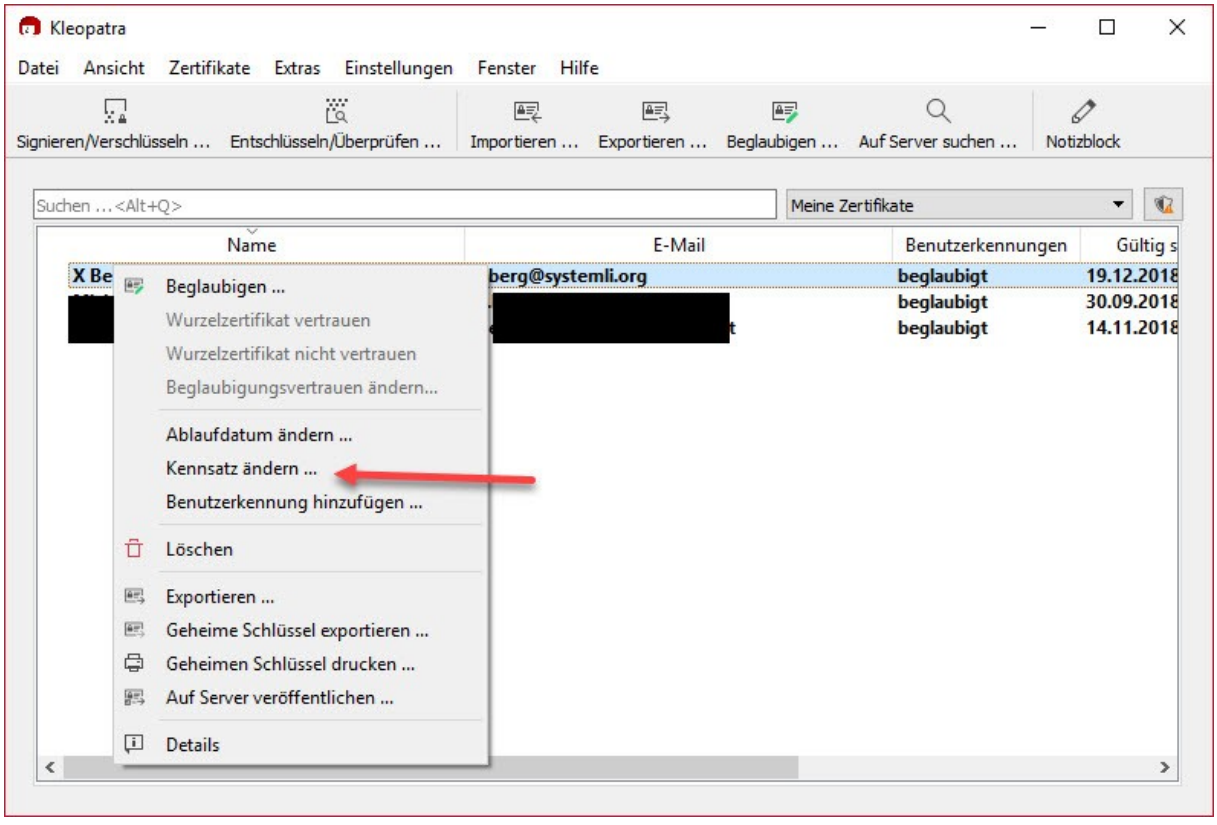
Dazu klickst Du einfach auf „Auf Server suchen…“

In dem darauffolgenden Fenster gibst Du entweder den gesuchten Namen oder die Mailadresse ein und bestätigst mit „Suchen“.

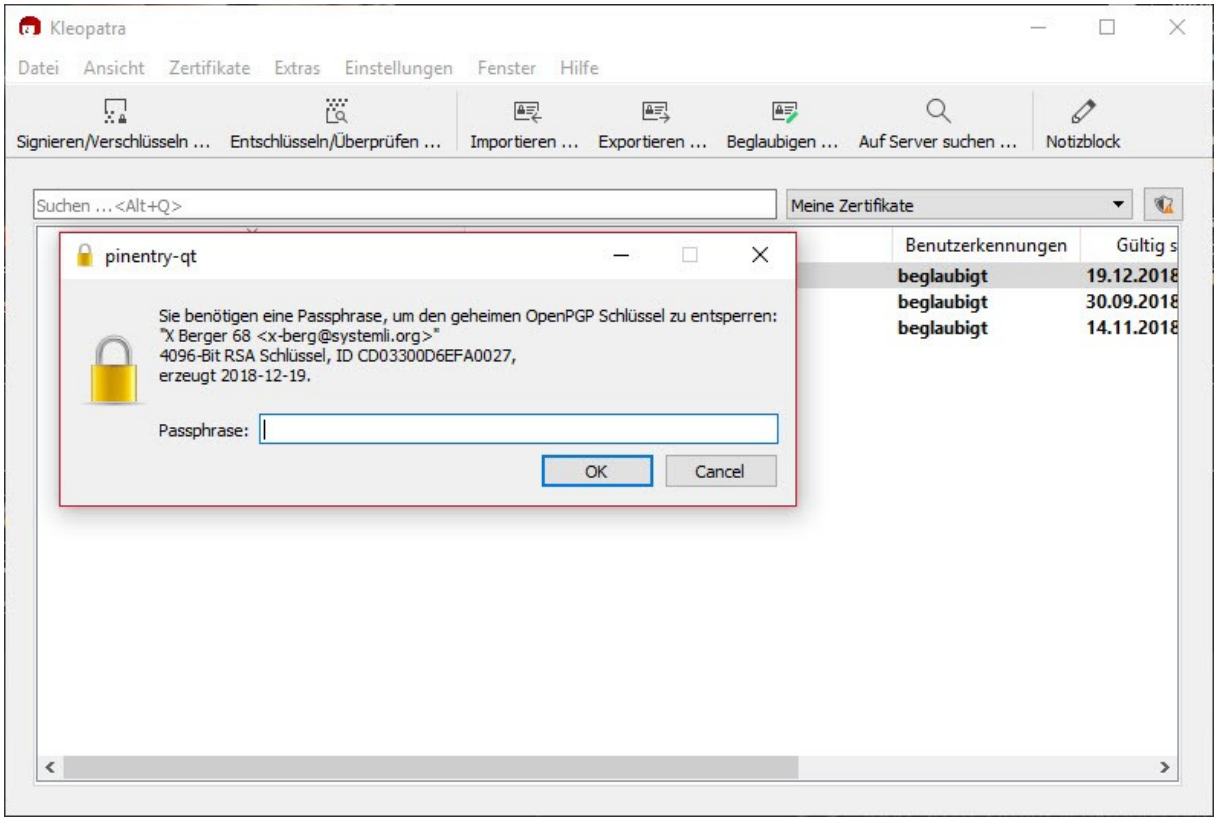


Nach kurzer Zeit hast Du das Suchergebnis und kannst den gewünschten Schlüssel über „Importieren“ auswählen.

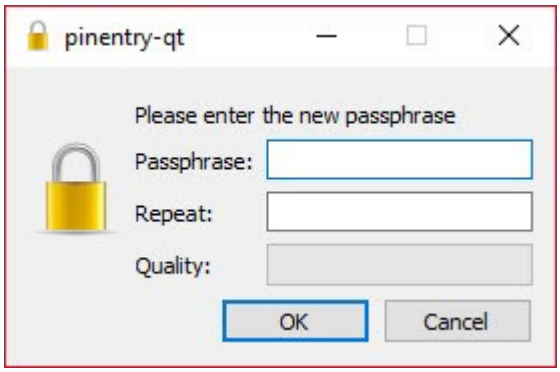
Passwort Deines privaten Schlüssels ändern



Bei Cleopatra ist der Begriff für Passwort ändern, Passphrase ändern oder Kennwort ändern „**Kennsatz ändern…“.** Wähle dazu vorher den zu ändernden privaten Schlüssel aus.



Auch bei Cleopatra kannst Du Deinen privaten Schlüssel nur bearbeiten, wenn Du Dich mit Deinem Passwort verifizierst.



Da Du Dein altes Passwort bereits bestätigt hast, kannst Du nun ein neues Passwort vergeben. Zur Überprüfung und Sicherheit gegen Tippfehler muss Du Dein neues Passwort doppelt eingeben.

Klicke dann auf OK – Deine Passphrase wurde erfolgreich geändert.

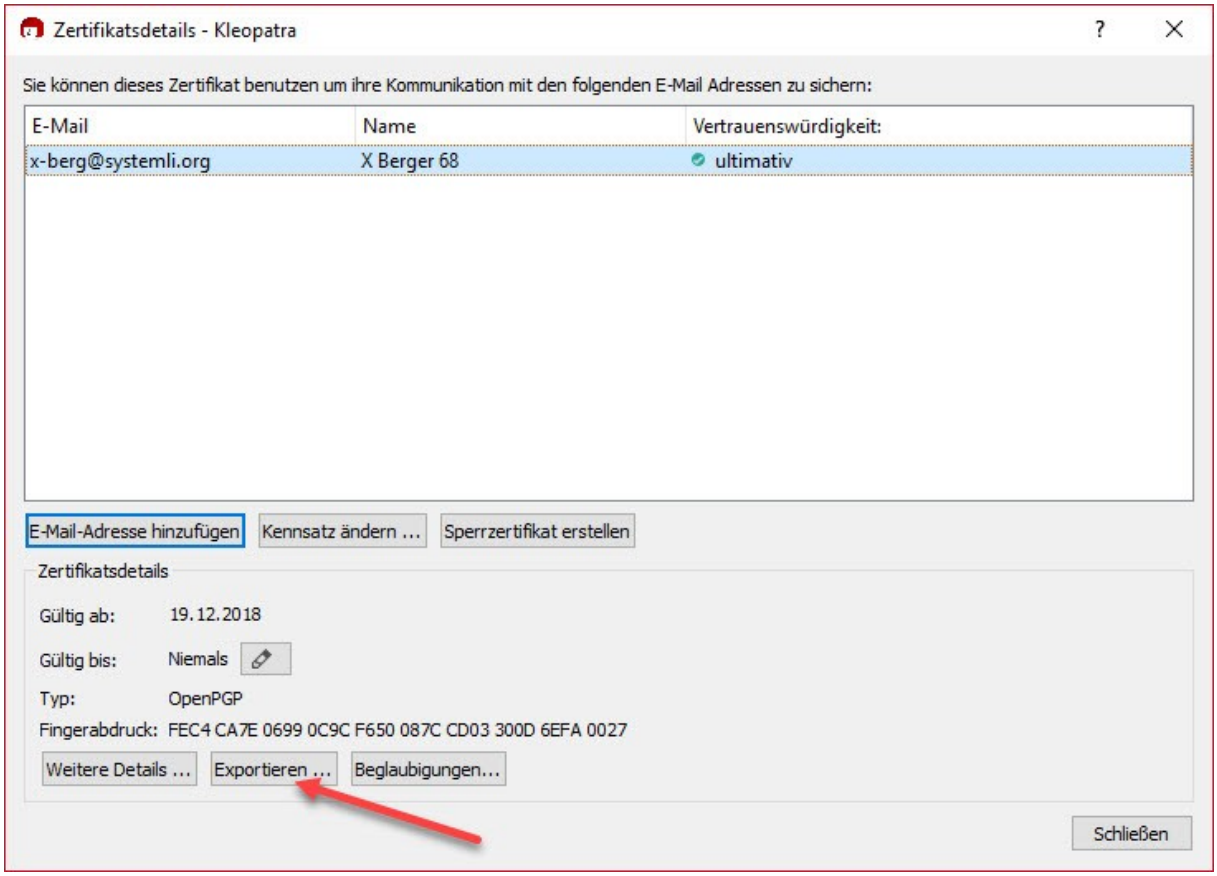
Deinen öffentlichen Schlüssel teilen

Zu Anfang wurden drei Möglichkeiten aufgezeigt, Deinen öffentlichen Schlüssel zu verteilen.

Die Veröffentlichung auf einem Schlüsselserver hast Du eventuell schon beim Erstellen Deines Schlüsselpaares gemacht, Du kannst das aber auch nachträglich noch tun. Allerdings solltest Du dann auch ein Sperrzertifikat erstellt haben, um Deinen öffentlichen Schlüssel wiederrufen zu können.

Damit kann jeder nach Deinem Nick oder Deiner E-Mailadresse suchen und Deinen öffentlichen Schlüssel importieren.

Wie weit Du einem öffentlichen Schlüssel vertrauen kannst, hängt vom Fingerabdruck des Schlüssels ab. Jeder Schlüssel ist einmalig und hat seinen eigenen Fingerabdruck.



Wenn Du auf einen Schlüssel doppelklickst, öffnet sich ein Fenster mit den Zertifikatsdetails, hier kannst Du zum Beispiel für jeden Schlüssel den Fingerabdruck einsehen und prüfen.

„**Exportieren…**“ ist nicht die Funktion zum Export eines öffentlichen Schlüssels!

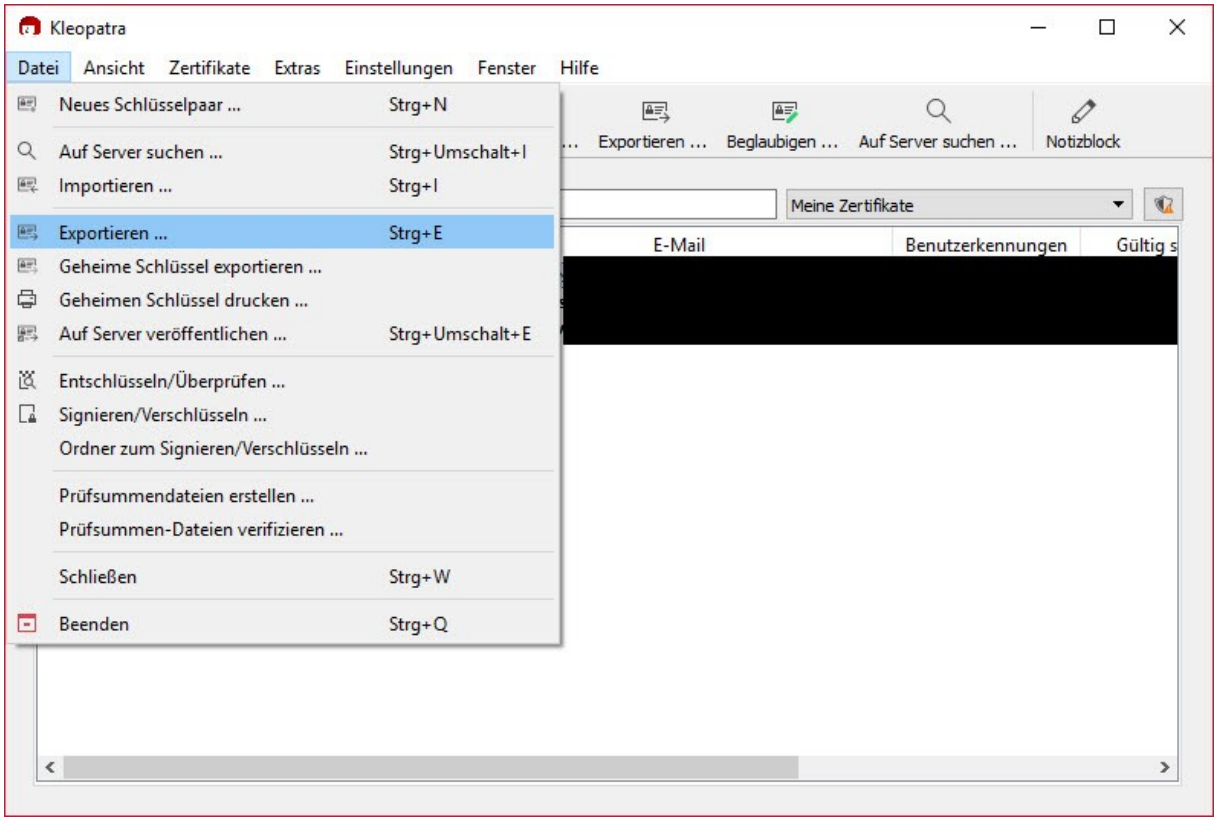
Hier kannst Du Dir den Schlüssel im Klartext anzeigen lassen (siehe 2. Möglichkeit) und ihn

a) Auf einer Homepage oder Blog veröffentlichen, damit jeder Deinen Schlüssel von dort importieren und Deinen Fingerabdruck prüfen kann.
b) In einer E-Mail versenden, viele Programme erkennen den Schlüssel im E-Mail Body (nur Text E-Mail) und können ihn auch importieren.
c) In eine Textdatei kopieren und anschließend die Extension (Dateikennung) auf .pgp ändern, um ihn zum Beispiel als Anhang zu versenden oder um einen Public key von einer Homepage in Deine Schlüsselverwaltung zu importieren

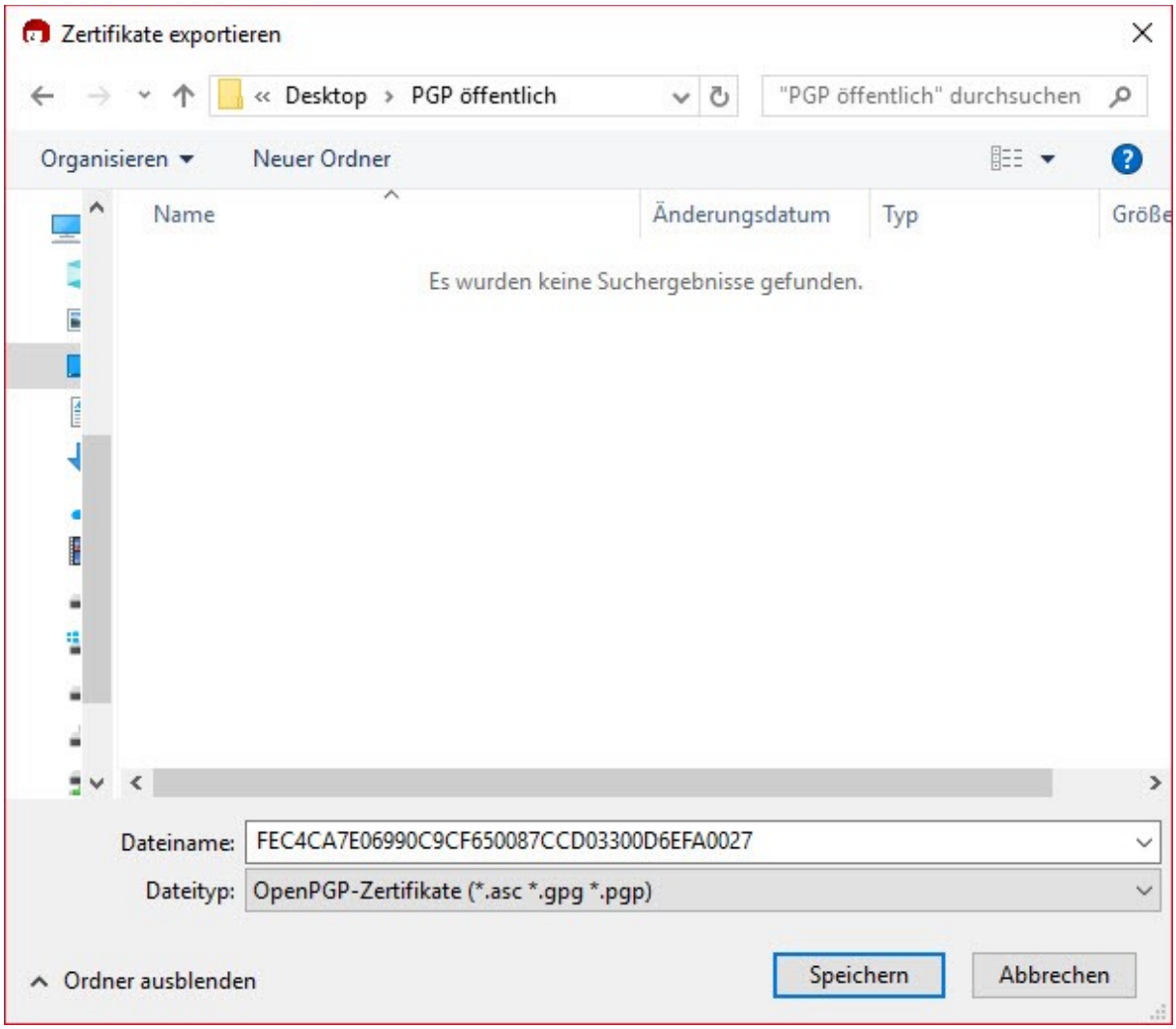
Cleopatra kann folgende Schlüsseldateien erkennen und importieren:

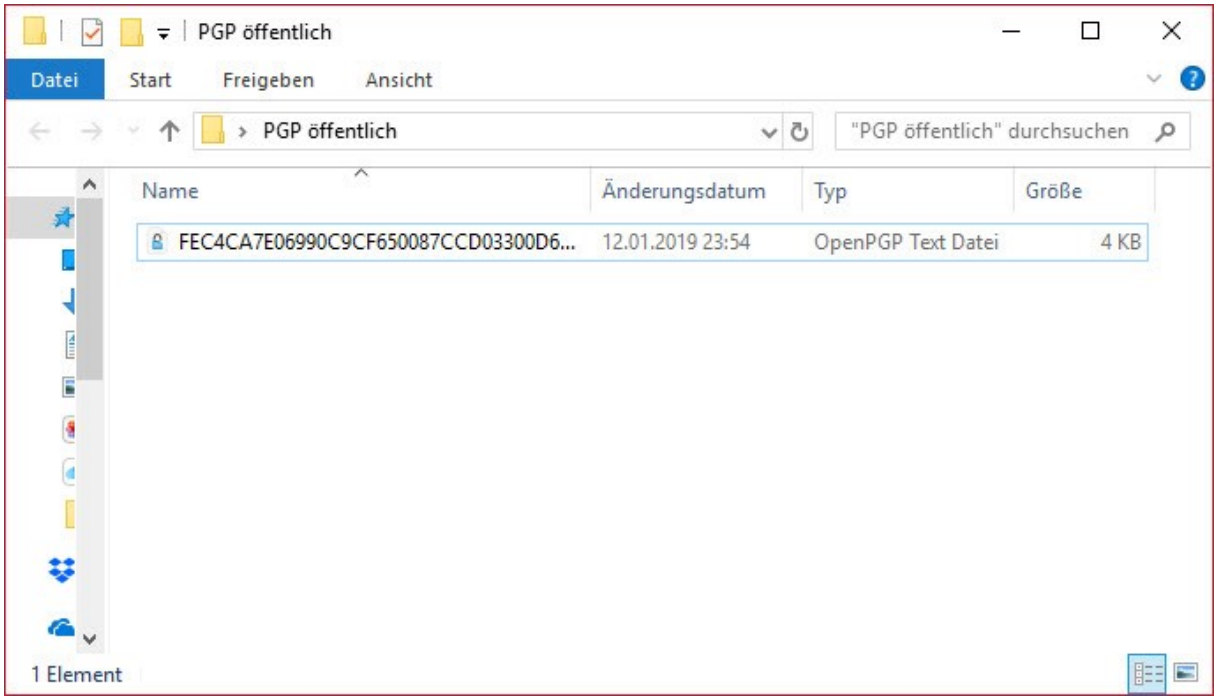
*.asc *.cer *.cert *.crt *.der *.pem *.gpg *.p7c *.p12 *.pfx *.pgp

Wenn Du Deinen oder einen anderen öffentlichen Schlüssel als fertige Schlüsseldatei exportieren willst, wähle dazu aus dem Menü „Datei“ → „Exportieren“ aus.

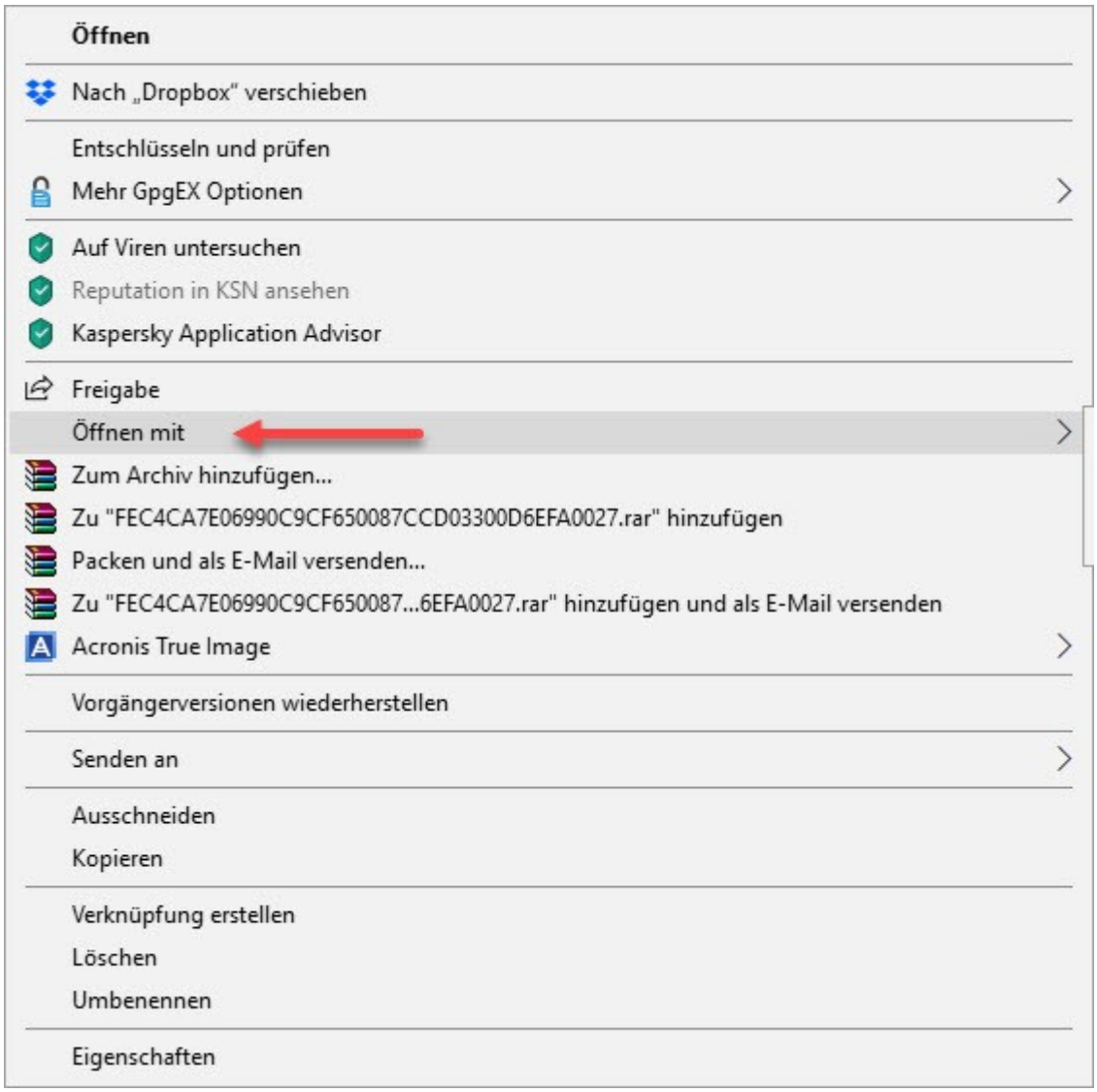


Cleopatra speichert den Schlüssel mit dem Namen Deines Fingerabdrucks.





In dem von Dir gewählten Verzeichnis befindet sich nun der exportierte öffentliche Schlüssel.



Möchtest Du den Inhalt überprüfen, kannst Du Dir mit Rechtsklick und Auswahl von „Öffnen mit“ → „Editor“ Deinen Schlüssel wie unter 2. Anzeigen lassen.

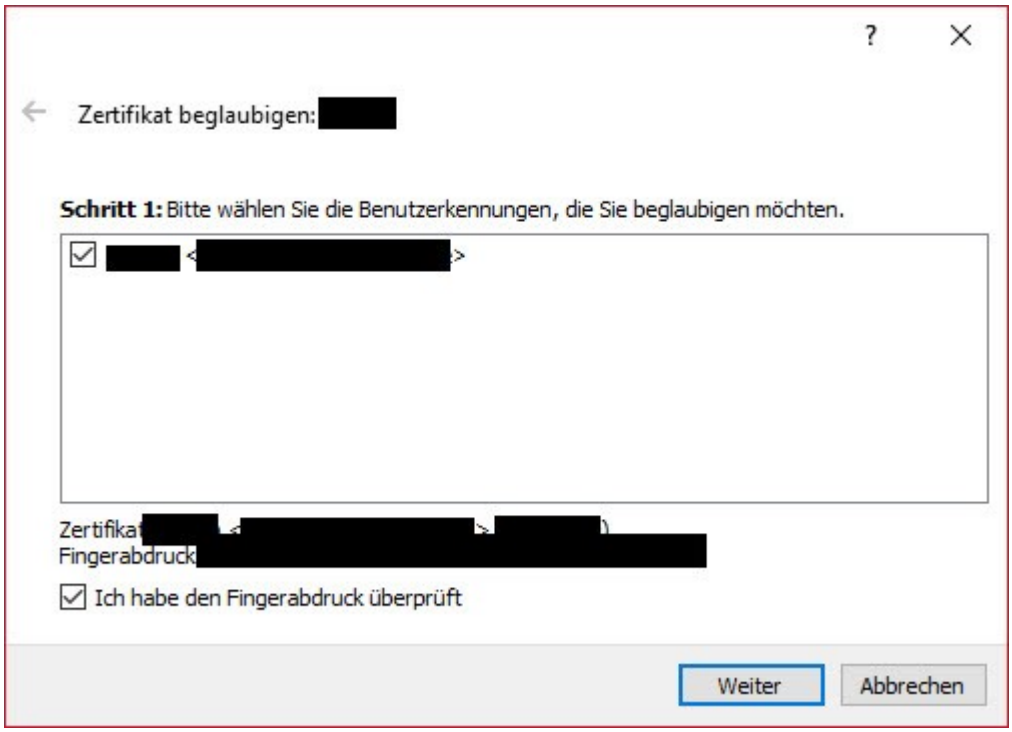
Den Exportierten Schlüssel kannst Du nun entweder persönlich auf einem USB Stick weiter verteilen oder per E-Mail versenden.

Der Fingerabdruck und was es damit auf sich hat

Einen öffentlichen Schlüssel zu erhalten oder von einem Schlüsselserver zu importieren sagt rein gar nichts aus, umgekehrt ist auch nicht sichergestellt, dass der von Dir versendete öffentliche Schlüssel auch tatsächlich von Dir verschickt wurde.

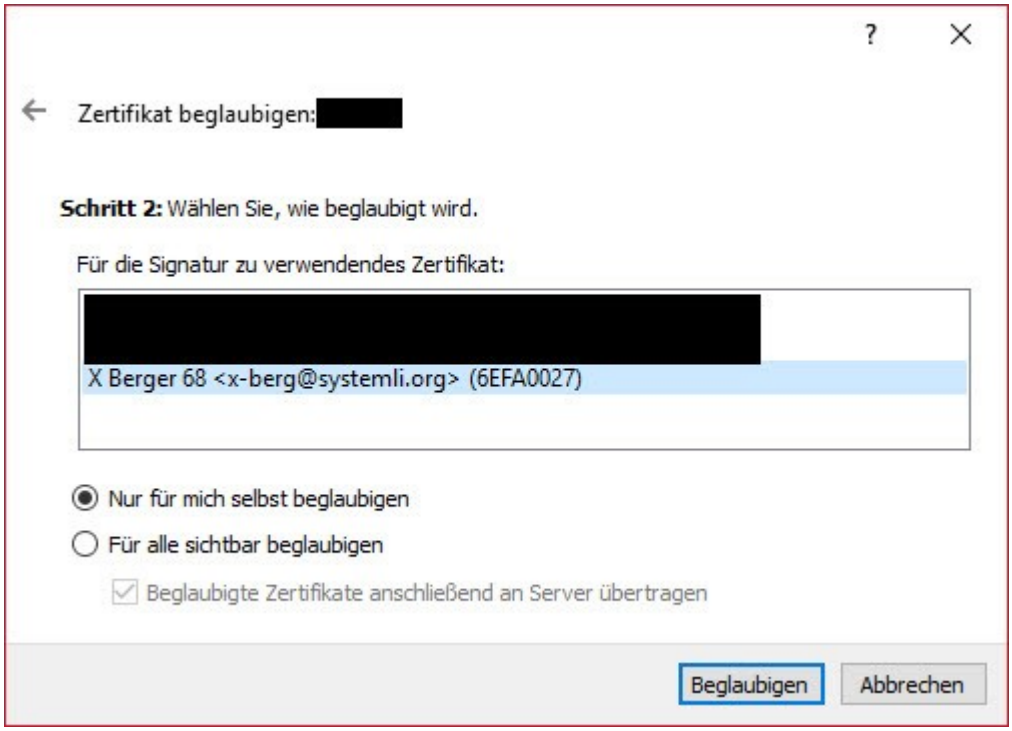
Cleopatra bietet Dir die Möglichkeit, öffentliche Schlüssel zu beglaubigen, zum Beispiel wenn Du Dich persönlich oder durch einen Anruf vom richtigen Fingerabdruck überzeugst.

Dazu klickst Du mit der rechten Maustaste auf einen Schlüssel, den Du beglaubigen möchtest.



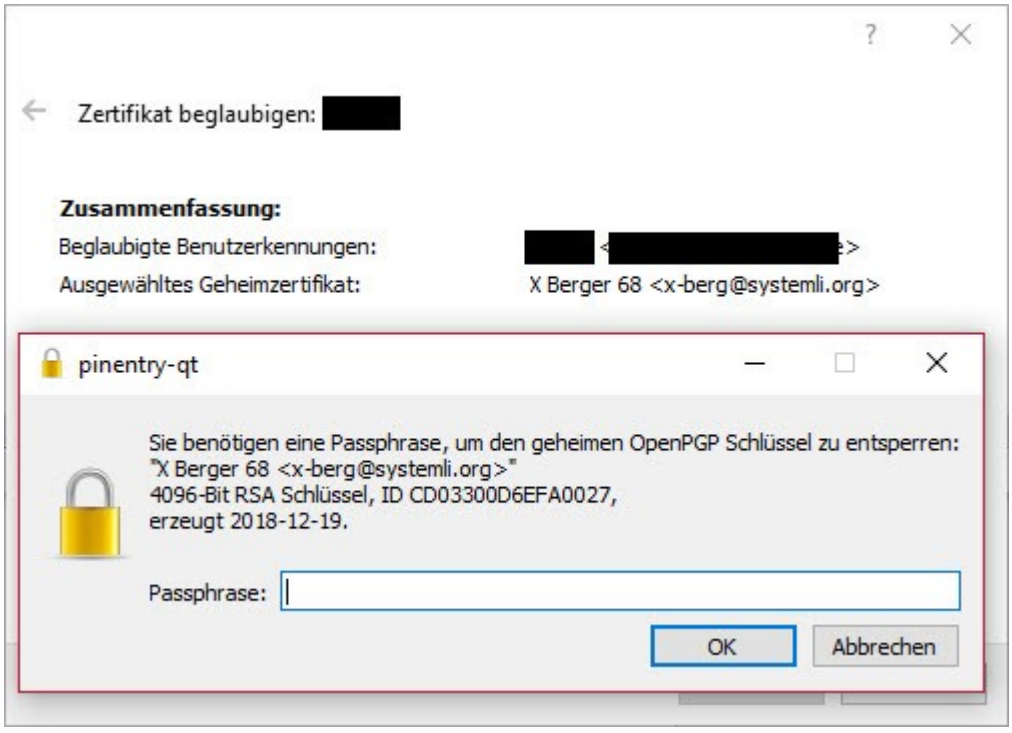
Hier kannst Du den Schlüssel auswählen, die Daten nochmals überprüfen und bestätigen, dass der Schlüssel vertrauenswürdig ist.

Klicke anschließend auf „Weiter“.

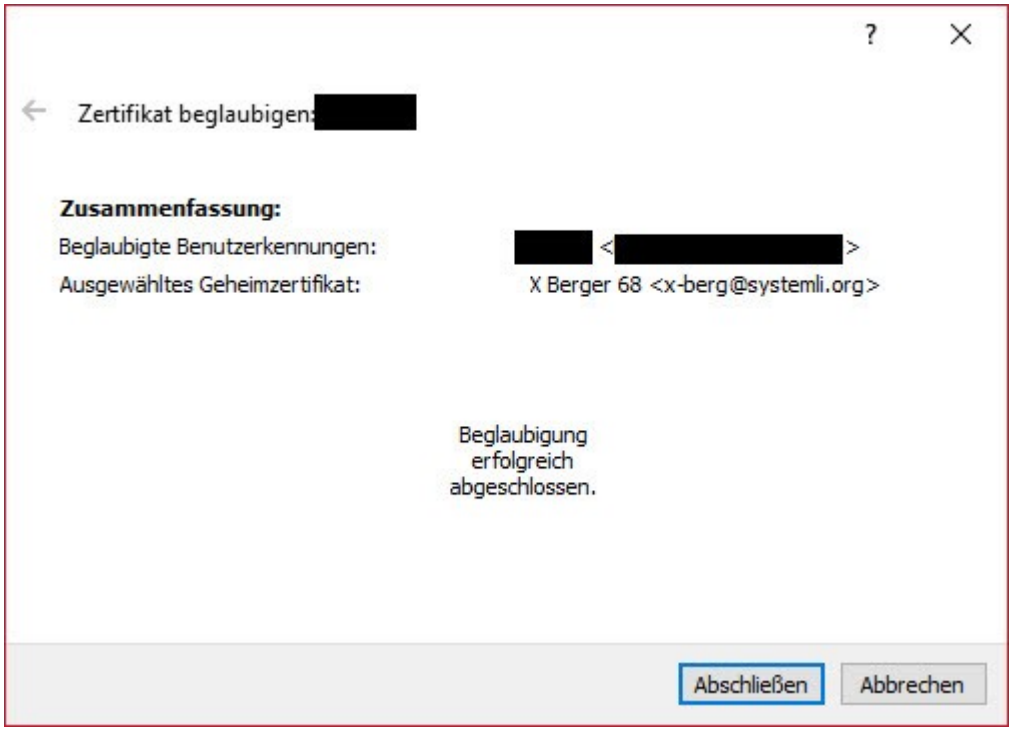


Hier legst Du fest, mit welchem Deiner privaten Schlüssel Du zertifizieren möchtest und ob Du den öffentlichen Schlüssel nur für Dich selbst oder für alle sichtbar beglaubigen möchtest.

Für Deine politische Arbeit solltest Du von einer öffentlichen Beglaubigung ansehen.



Der Vorgang wird erst durchgeführt, wenn Du die Aktion mit Deinem privaten Schlüssel verifiziert hast.



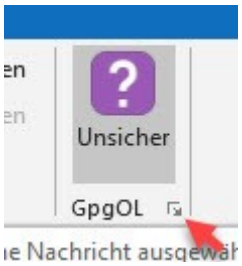
In der Zusammenfassung bekommst Du eine Bestätigung, ob der Vorgang erfolgreich abgeschlossen werden konnte.

Eine ausführliche Beschreibung für „Anfänger“ und Fortgeschrittene findest in Deutscher Sprache findest Du hier: https://files.gpg4win.org/doc/gpg4win-compendium-de.pdf

E-Mails mit Outlook versenden

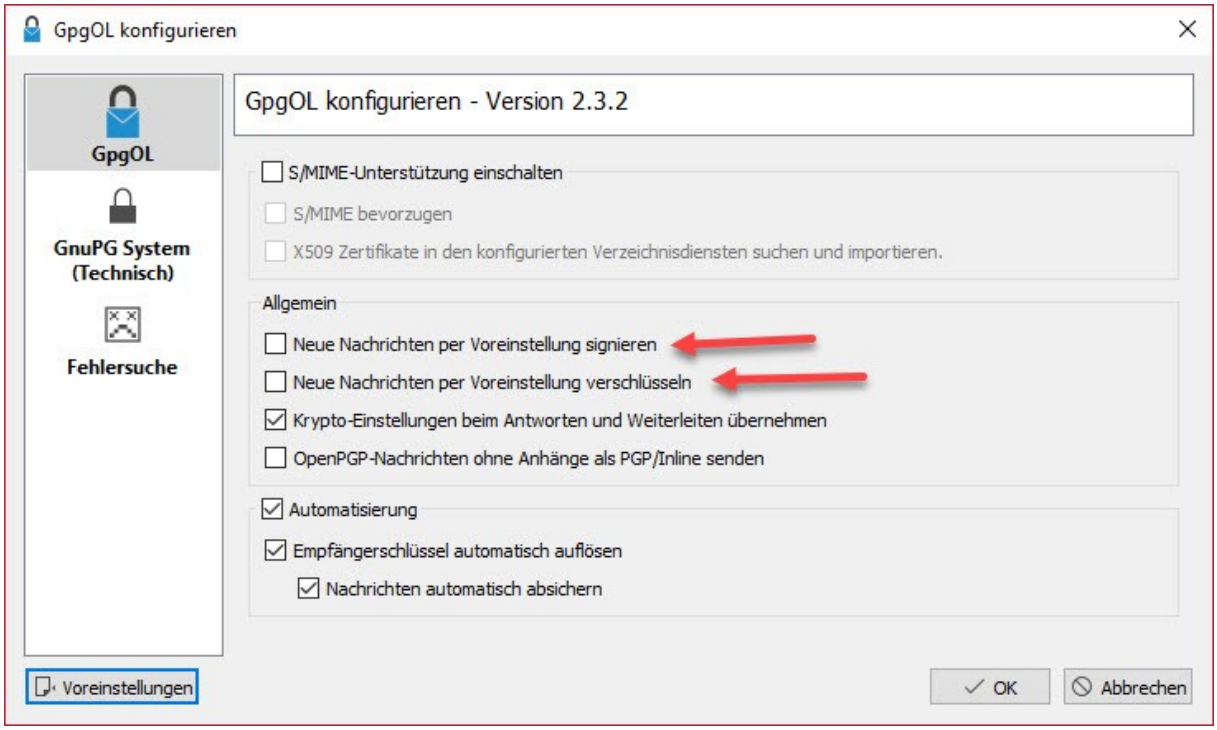
Microsoft Office Produkte sind schön, leisten auch sehr viel, Eingriffe in Sicherheit und Berechtigungen sind allerdings mehr für „Konzernlösungen“ ausgelegt, dort gibt es in der Regel „Systemverwalter:innen“, der sich damit herumschlagen.

Wenn Du also unbedingt Outlook verwenden musst/möchtest, dann stellt gpg4win eine GpGOL zur Verfügung:



Das Symbol findest Du ganz leicht oben in Deinem Menü Band.

Klickst Du in das kleine Kästchen unten rechts, öffnet sich das Fenster zur GpGOL Konfiguration.

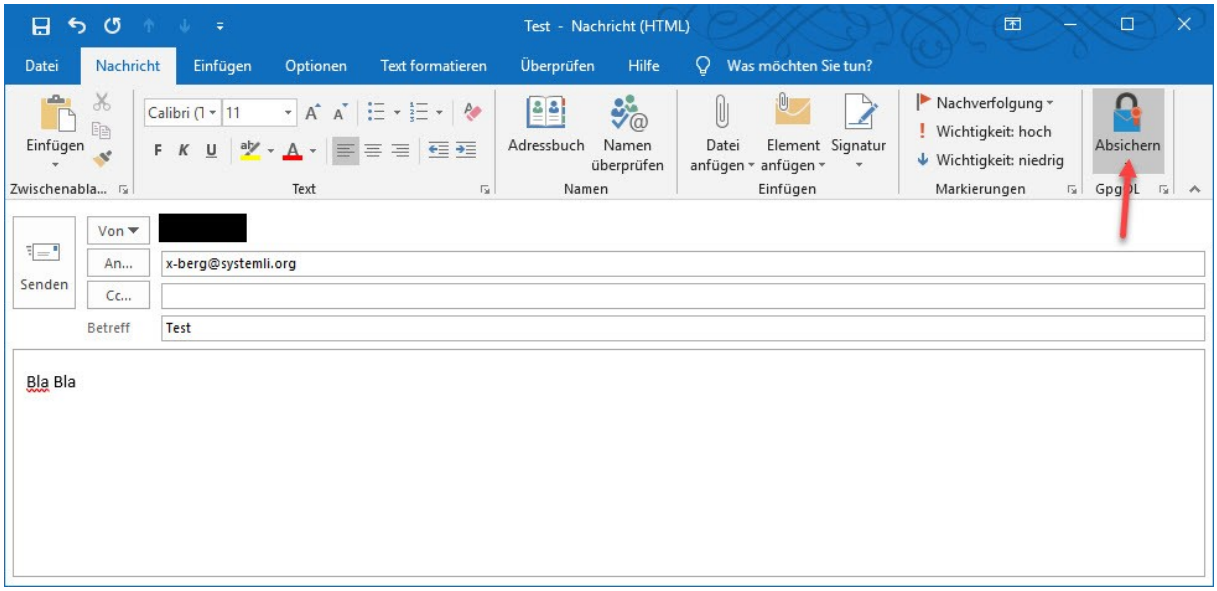


Hier kannst Du nun definieren, ob Du neue Nachrichten immer signieren oder verschlüsseln möchtest. Die Krypto Einstellungen beim Antworten und Weiterleiten zu übernehmen, sowie die Automatisierungseinstellungen machen Sinn.

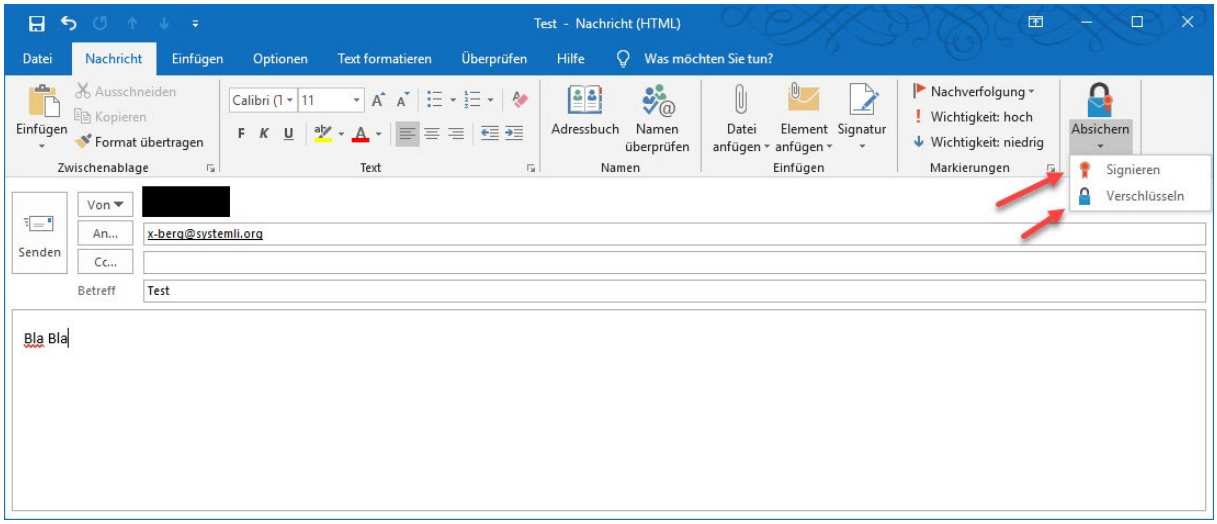
OpenPGP Nachrichten ohne Anhänge als PGP/Inline versenden bedeutet, dass der verschlüsselte Inhalt nicht als Anhang, sondern im E-Mail Body gesendet wird. Diese Option kann das Verhalten beim Entschlüsseln auf der Empfänger:innen Seite negativ beeinflussen. Kommt es zu Komplikationen, solltest Du diese Option nicht anhaken.

GnuPG System (Technisch) – enthält sehr viele Systemspezifische Parameter, die nicht ohne triftigen Grund geändert werden sollten.

Falls was schief geht, mit „Voreinstellungen“ setzt Du alle Eingaben wieder auf den GpGOL Standard zurück, mit dem alles funktionieren sollte.

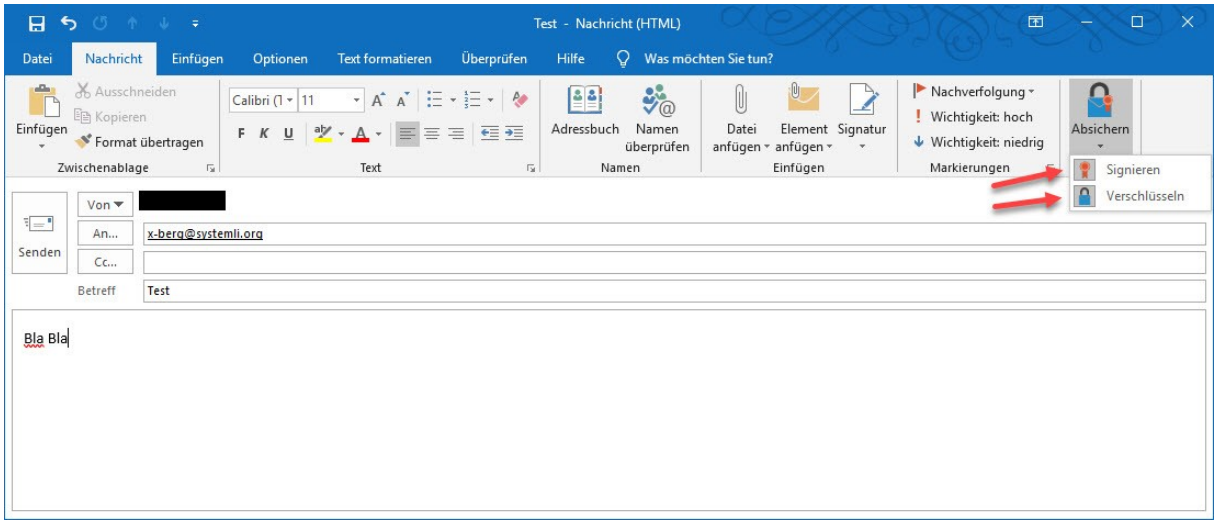


Wenn Du eine neue Nachricht schreibst, siehst Du im Menü Band die GpGOL Option, aber leider nicht die aktuellen Einstellungen, ob verschlüsseln/signieren eingestellt ist.

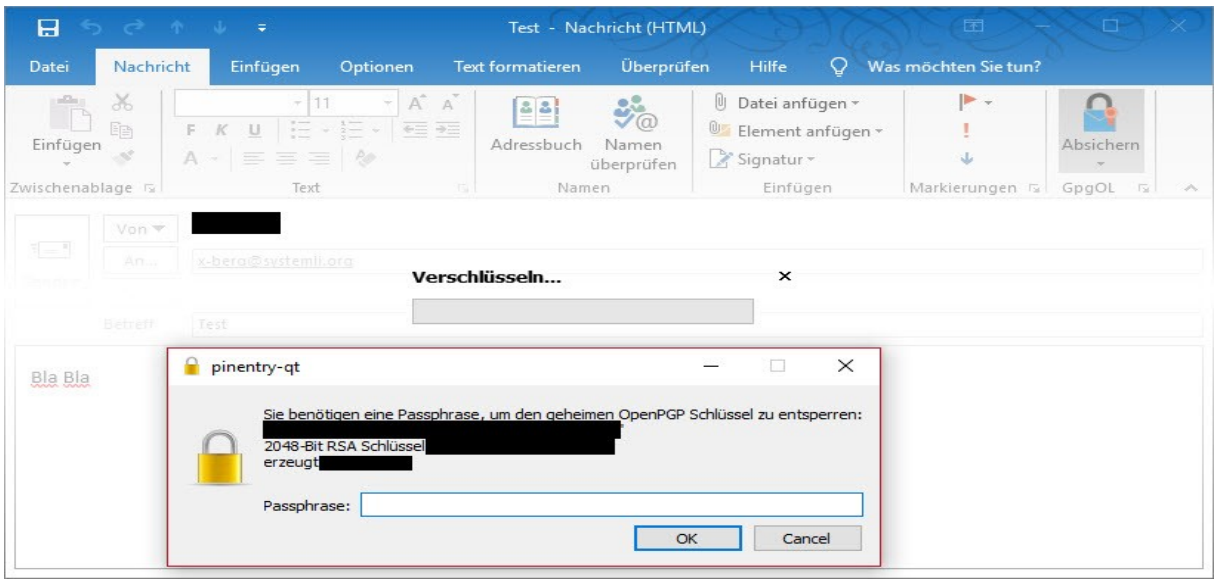


Klickst Du auf das GpGOL Icon, dann kannst Du die aktuelle Einstellung prüfen, ein kleines Menü zeigt Dir an, ob verschlüsseln, signieren oder beides für diese Nachricht aktiviert ist.

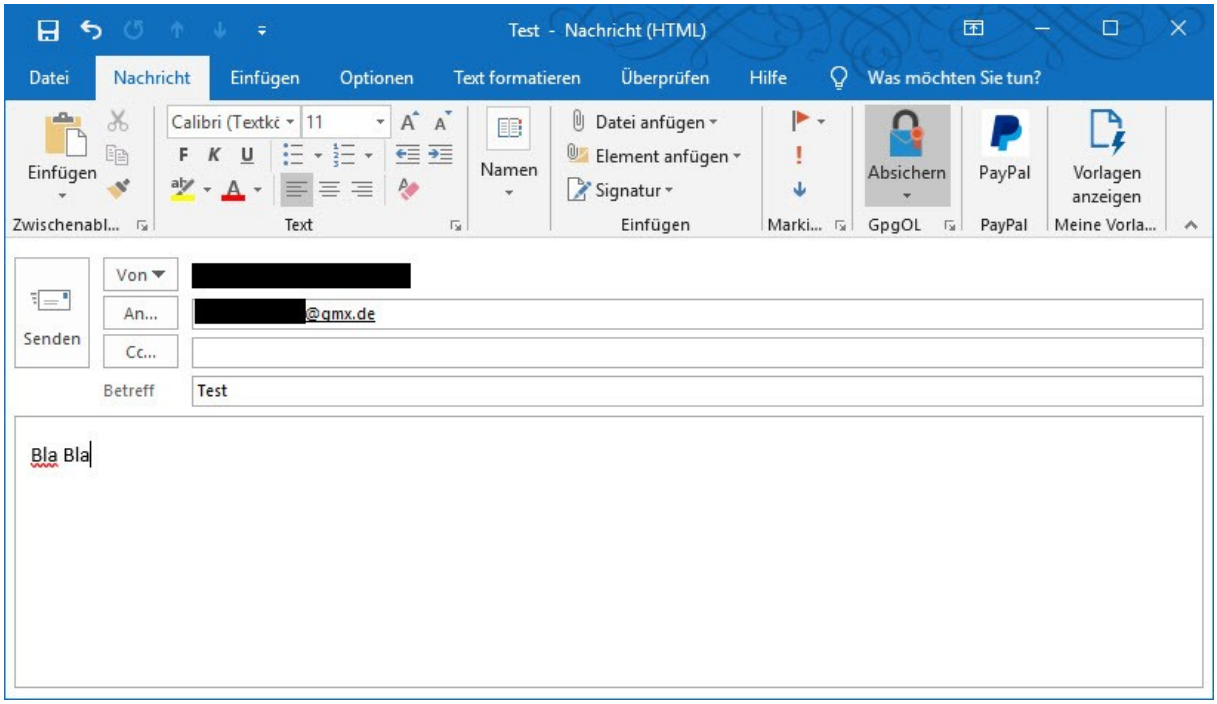
Hier sind beide Optionen nicht aktiviert.



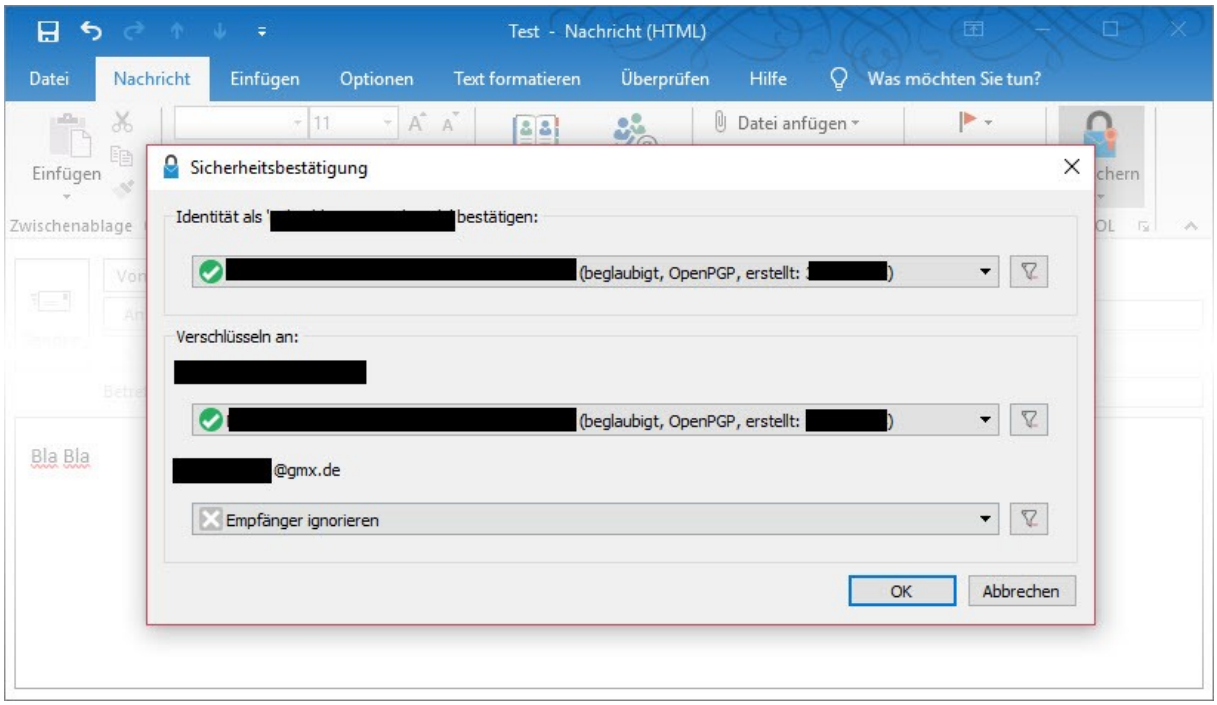
Ist das Icon für Signieren oder Verschlüsseln oder beide grau hinterlegt, dann ist diese Option für diese Nachricht aktiviert.



Zum Absenden der Nachricht ist auch hier das Passwort Deines privaten Schlüssels erforderlich.



Was aber tun, wenn der Empfänger noch keinen PGP Schlüssel besitzt?



Ist für den Empfänger kein öffentlicher Schlüssel importiert oder vorhanden, öffnet sich das Fenster „Sicherheitsbestätigung“. Das Fenster kann auch kommen, wenn Du mehrere E-Mailadressen und PGP Schlüssel in Outlook verwendest.

Ganz oben legst Du für die Signatur Deinen eigenen Schlüssel fest.

Im 2. Abschnitt „Verschlüsseln an:“ legst Du sowohl Deinen eigenen, wie auch die Schlüssel der Empfänger:innen fest.

Ist für die Empfänger:innen kein PGP Schlüssel importiert oder bekannt, wird Outlook diese Nachricht für Dich unter gesendet verschlüsseln, an die Empfänger:innen geht sie jedoch unverschlüsselt im Klartext raus. GpGOL bietet keine Schnittstelle zu Deiner Schlüsselverwaltung, um Schlüssel zu suchen und zu importieren. Dazu musst Du Cleopatra starten.

Dateien und Verzeichnisse mit PGP verschlüsseln

Warum einzelne Dateien oder Verzeichnisse verschlüsseln?

Sieht auf den ersten Blick wie ein unnötiger Mehraufwand aus.

Du hast Deine Laufwerke und Dein Bootlaufwerk mit VeraCrypt verschlüsselt, Deine Daten sind also bei Dir sicher gespeichert und bereits verschlüsselt.

Wenn Du Dateien mit anderen teilst, verlassen diese Informationen Deine sichere Umgebung, auch wenn Sie in einer mit PGP verschlüsselten Nachricht übertragen werden. Du musst Dich also Fragen, wie weit Du der Infrastruktur Deiner Empfänger:innen vertrauen kannst.

Du hast Dir PGP in Deinem E-Mailprogramm eingerichtet, versendest Deine Nachrichten nur noch verschlüsselt, Deine Informationen sind somit geschützt.

Wir wissen heute, dass durch eine falsche Konfiguration der E-Mailsoftware (HTML E-Mails) zwar nicht der PGP Schlüssel geknackt werden kann, jedoch über Schadcode im HTML Zugriff auf den entschlüsselten Inhalt möglich ist. Hier kannst Du die Sicherheit erhöhen, wenn Du auf Informationen im E-Mail Body verzichtest und stattdessen einen mit PGP verschlüsselten Dateianhang verwendest.

Unter Umständen möchtest Du Dateien wie zum Beispiel eine Agenda oder ein Protokoll vom letzten Plenum über einen Messenger wie z. B. Signal verteilen, aber sicherstellen, dass die Informationen nur von sicheren Empfängern geöffnet werden können.

Messenger haben zwar in der Regel inzwischen eine Ende zu Ende Verschlüsselung, Gruppenchats haben das aktuell nicht bei allen Messenger Anbieter:innen. Ebenso hast Du keine exakten Informationen darüber, in welcher Form Daten bei E-Mail- und Messenger Anbieter:innen auf Servern gespeichert werden.

Erinnern wir uns an dieser Stelle daran, wie PGP im Nachrichtenaustausch funktioniert:

Sender:in und Empfänger:in brauchen jeweils ihren eigenen geheimen Schlüssel (private key) und die öffentlichen Schlüssel (public key) ihrer Kontakte. Nur dann ist es möglich, dass eine verschlüsselte E-Mail nur an einen vorher festgelegten Kontakt zugestellt und entschlüsselt werden kann.

Die gleiche Lösung funktioniert in wenigen kurzen Schritten auch mit einzelnen Dateien und/oder Verzeichnissen, vollkommen unabhängig davon, wie Du Deine Dateien/Verzeichnisse teilst.

Du kannst also mit Deinem PGP Schlüssel Dateien und Verzeichnisse signieren und für Dich selbst, wie auch für bestimmte, von Dir ausgewählte Empfänger:innen verschlüsseln.

Deine Empfänger:innen erhalten bei der Entschlüsselung die Information, dass die Dateien/Verzeichnisse sicher von Dir stammen. Nicht von Dir bestimmte Dritte werden nicht in der Lage sein, die verschlüsselten Dateien und Verzeichnisse zu entschlüsseln und darauf zuzugreifen.

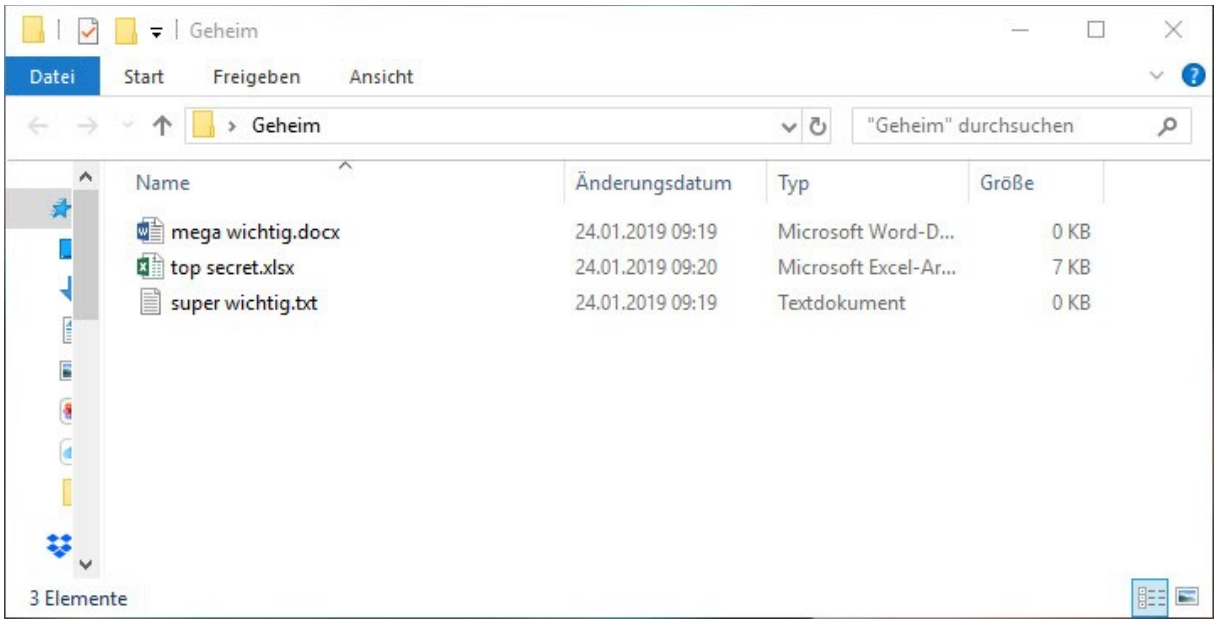
Wenn Du die Informationen auf einem USB Stick teilen willst, könntest Du das sicherlich auch mit einem durch VeraCrypt verschlüsselten USB Stick oder eines Containers lösen.

<u>Nachteil:</u>

Deine Empfänger:innen benötigen die VeraCrypt Software **und** das Passwort zum entschlüsseln des USB Stick oder der des Containers.

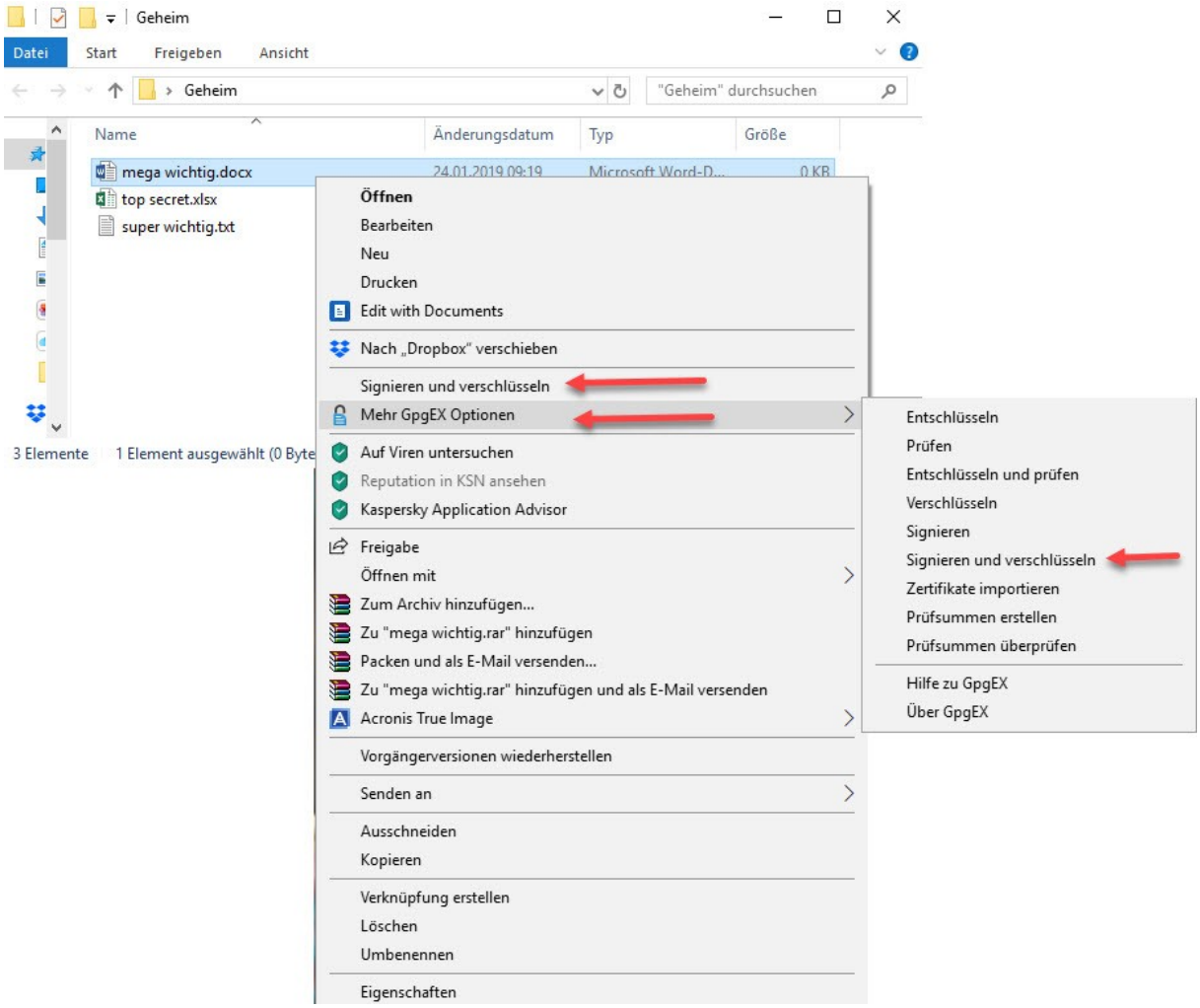
Mit der täglichen, selbstverständlichen Nutzung von PGP ist es nicht mehr nötig, ggf. eine zusätzliche Software zu installieren und ein persönliches Passwort zu teilen.

Einzelne Dateien verschlüsseln



Als Beispiel haben wir ein Verzeichnis „Geheim“ in dem Du Deine Dateien gespeichert hast, die Du entweder als E-Mailanhang oder über Signal oder über einen USB Stick teilen willst.

Die Auswahl der Dateien erfolgt mit „Shift“ oder „STRG“.

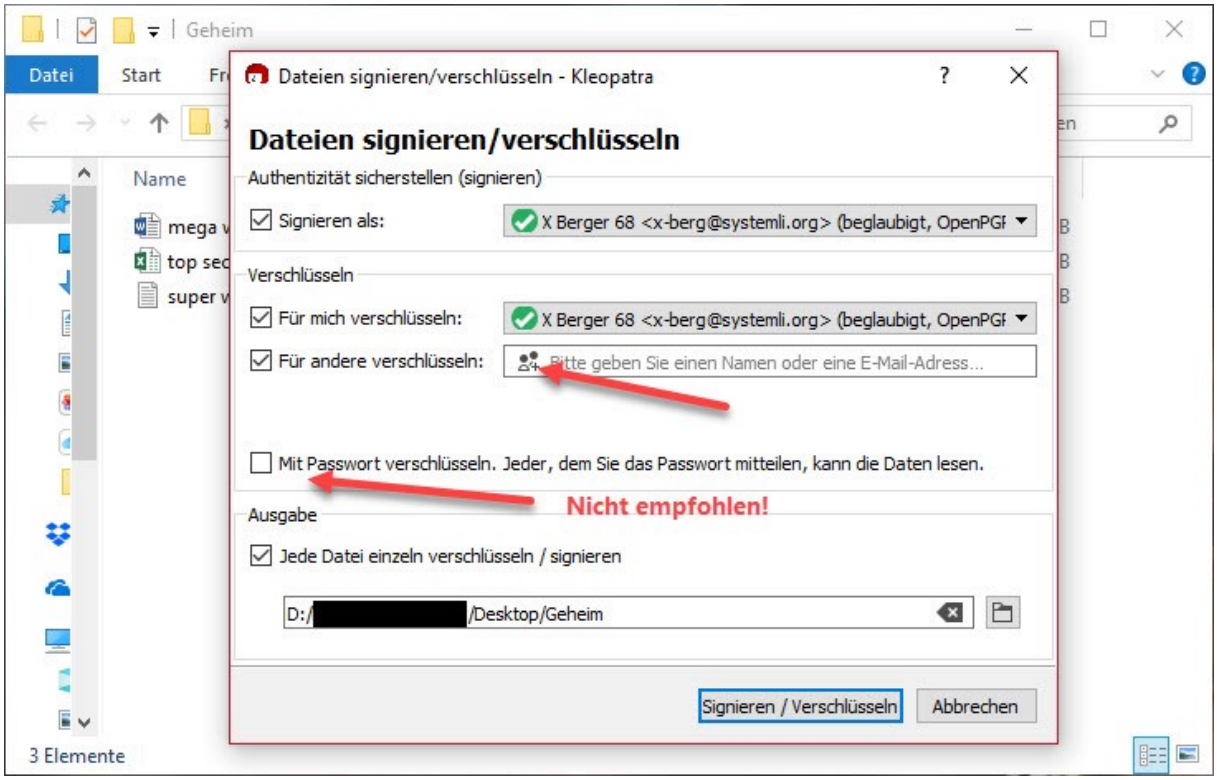


Wenn Du in Deinem Verzeichnis die gewünschten Dateien ausgewählt hast (hier nehmen wir eben mal die Datei „mega wichtig.docx“), kannst Du mit Klick der rechten Maustaste Dein Kontextmenü erreichen.

GpgEX stellt Dir damit auf ganz simple Art und Weise die Option der PGP Verschlüsselung im Dateisystem bereit.

Im Normalfall sollte der obere Befehl „Signieren und verschlüsseln“ für die Standardanwendung ausreichen.

Das Menü „Mehr GpgEX Optionen“ stellt zwar noch unterschiedliche Szenarien bereit, Du wirst aber feststellen, dass sich fast immer das gleiche Fenster öffnet und lediglich in den Checkboxen die entsprechenden Haken fehlen.



Wir möchten also die Datei „mega wichtig.docx“ signieren und verschlüsseln, um sie an bestimmte Menschen zu verteilen. Zuerst wählst Du Deinen Schlüssel aus, mit dem Du die Datei signieren möchtest. Damit stellst Du für Deine Kontakte sicher, dass die Datei auch tatsächlich von Dir stammt.

Im nächsten Schritt wählst Du „Für mich verschlüsseln“ und den Schlüssel dazu aus, damit Du selbst auf die verschlüsselte Datei Zugriff hast.

Wichtig!

Wenn Du etwas verschlüsselst, dabei vergisst den Haken „Für mich verschlüsseln“ zu setzen und die Originaldateien löschst, dann hast Du keinen Zugriff mehr auf den verschlüsselten Inhalt. Hast Du ebenfalls „Für andere verschlüsseln“ nicht angehakt und kein Empfänger:in bestimmt, dann ist die Datei unwiederbringlich verloren!

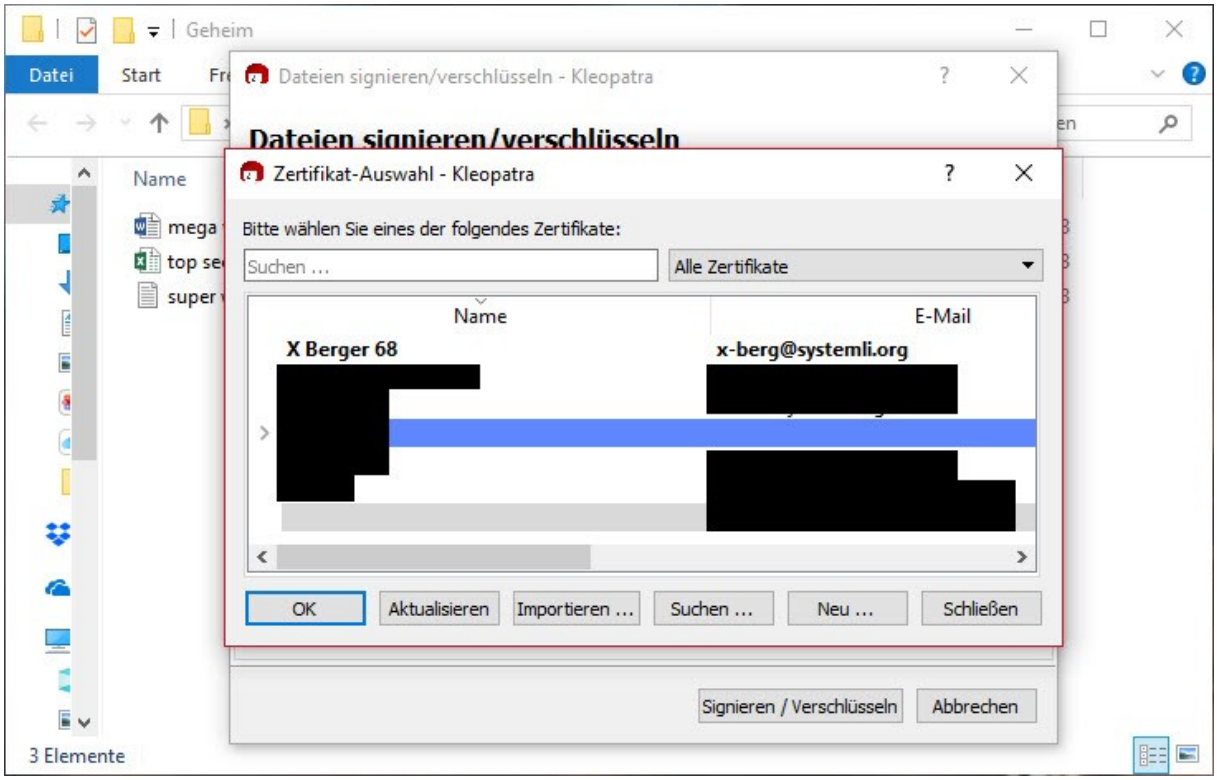
Im dritten Schritt legst Du mit „Für andere Verschlüsseln“ und Klick auf das kleine User:innen Symbol alle Kontakte fest, die auf Deine verschlüsselte Datei zugreifen sollen.

„Mit Passwort verschlüsseln“ ist eine Funktion, die Du **niemals** oder nur mit äußerster Vorsicht nutzen solltest!

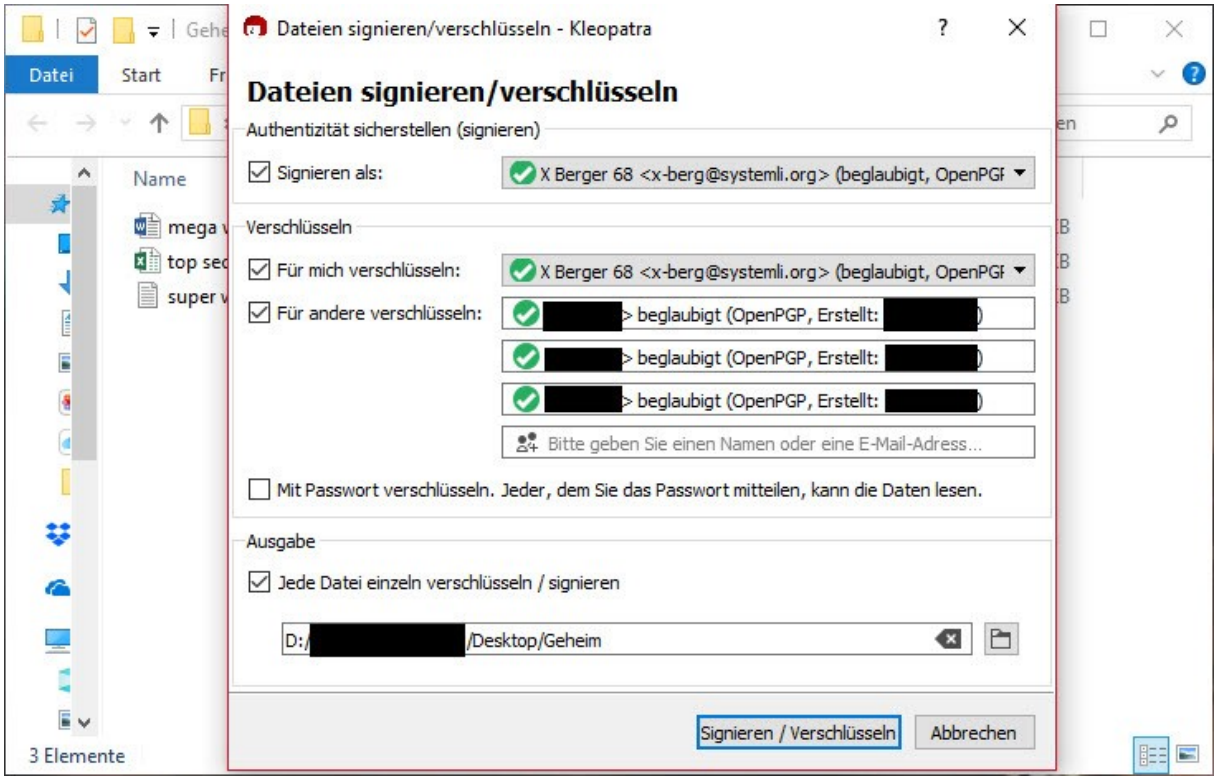
Die Datei wird zwar ebenfalls nach PGP Standard verschlüsselt, allerdings kann jede(r) auf diese Datei zugreifen, sofern er das Passwort dazu kennt. Das bedeutet, Du musst ein persönliches von Dir erstelltest Passwort teilen.

Vielleicht denkst Du jetzt, dass ist doch nicht schlimm, für andere Dinge verwendest Du das Passwort ja nicht, Du änderst sowieso Deine Passwörter regelmäßig unregelmäßig und beim nächsten Mal machst Du wieder ein anderes Passwort.

Das ist löblich. Nur gehen Deine Passwörter niemensch etwas an, nicht umsonst gibt es in Betriebssystemen und Sicherheitssoftware Optionen, die Dein Verhalten bei der Vergabe von Passworten analysieren und auftretende Regelmäßigkeiten bei der Vergabe blockieren können.



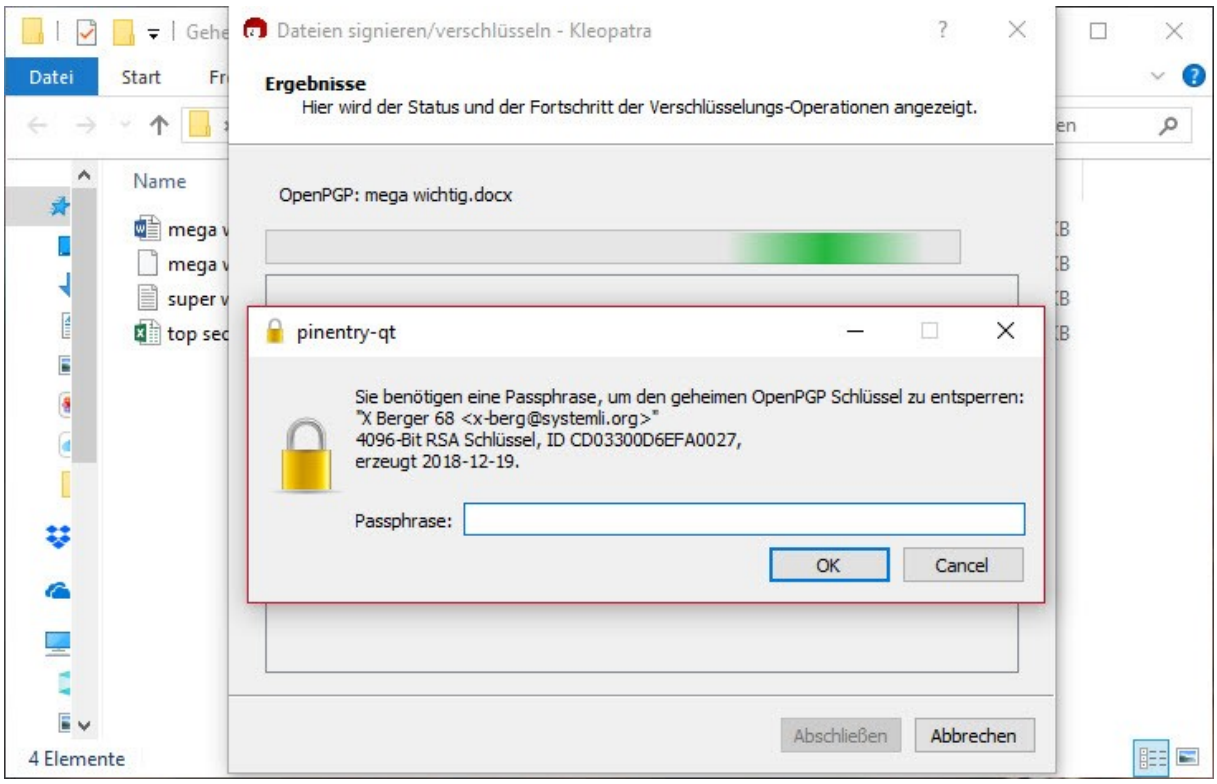
Hier kannst Du mit gedrückter „Shift“ oder „STRG“ Taste auch mehrere Kontakte auswählen, die Deine Datei öffnen können.



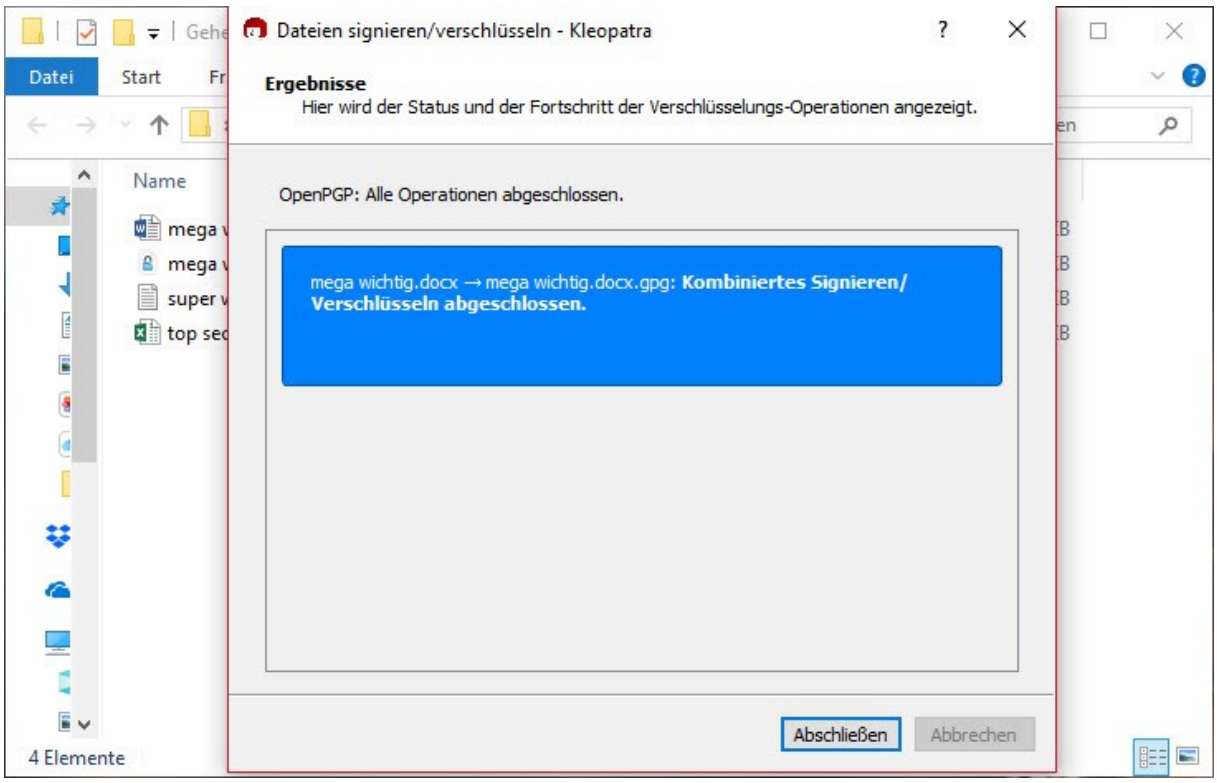
Nach Auswahl der Kontakte hast Du erneut das Fenster „Dateien signieren/verschlüsseln“ vor Dir. Du kannst noch Änderungen daran vornehmen, ist alles korrekt, klicke auf „Signieren / Verschlüsseln“.

Unter „Ausgabe“ kannst Du festlegen, ob jede Datei einzeln verschlüsselt werden soll (wenn Du mehr als eine Datei auswählst) oder ob ein .tar Archiv erzeugt werden soll, in dem sich alle Dateien befinden.

Darüber hinaus kannst Du den Speicherort Deiner verschlüsselten Dateien ändern.



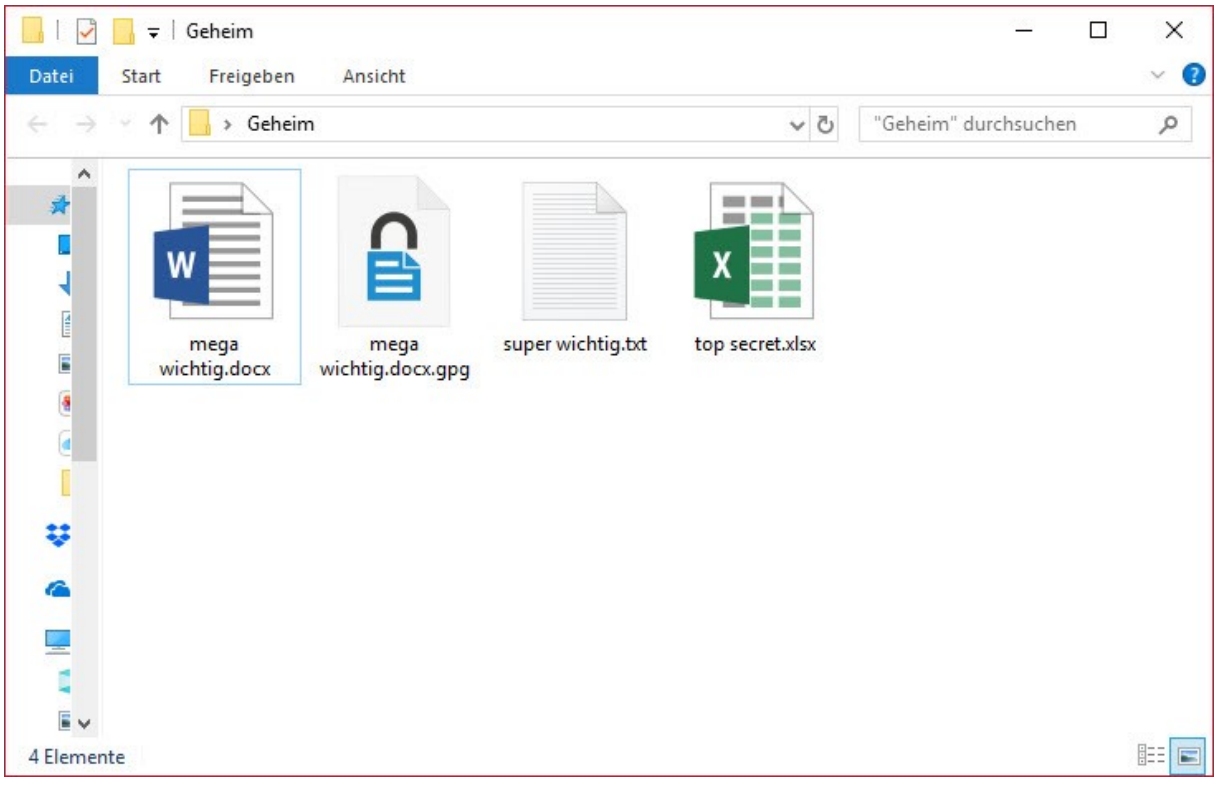
Keine Aktion ohne Legitimation. Damit der Vorgang gestartet wird, musst Du Dich mit Deinem Passwort Deines privaten Schlüssels, den Du dafür verwendest, authentifizieren.



Nach Abschluss der Verschlüsselungsoperationen wird Dir das Ergebnis angezeigt.

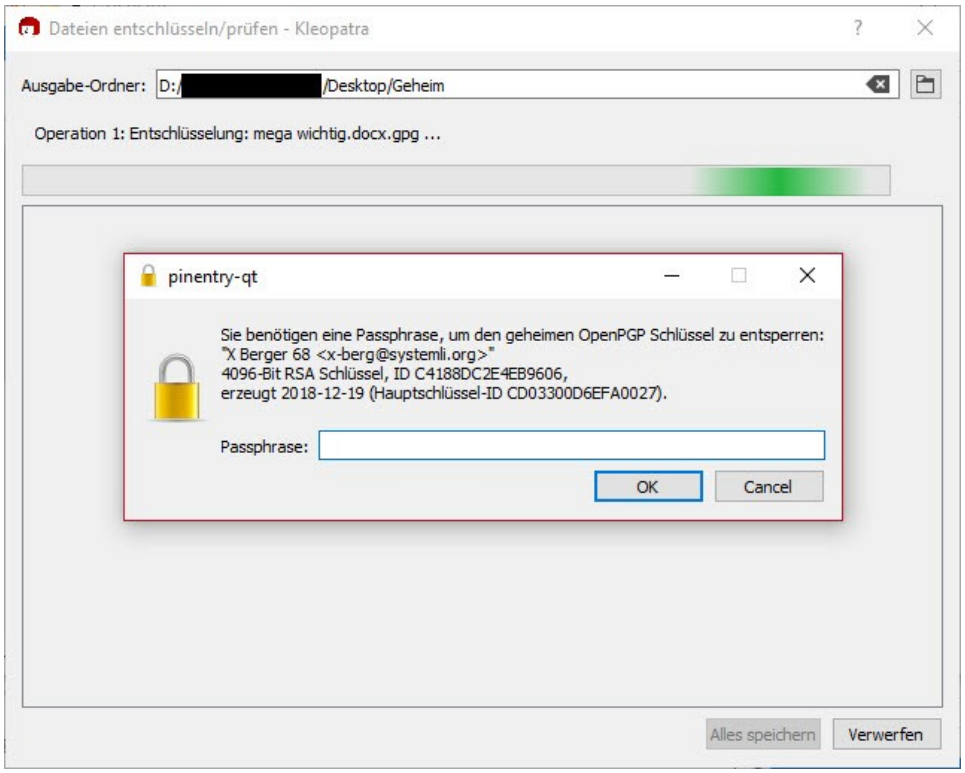
Wurden alle Operationen abgeschlossen, befindet sich Deine Datei in dem vorher festgelegten Verzeichnis.

Dateien entschlüsseln

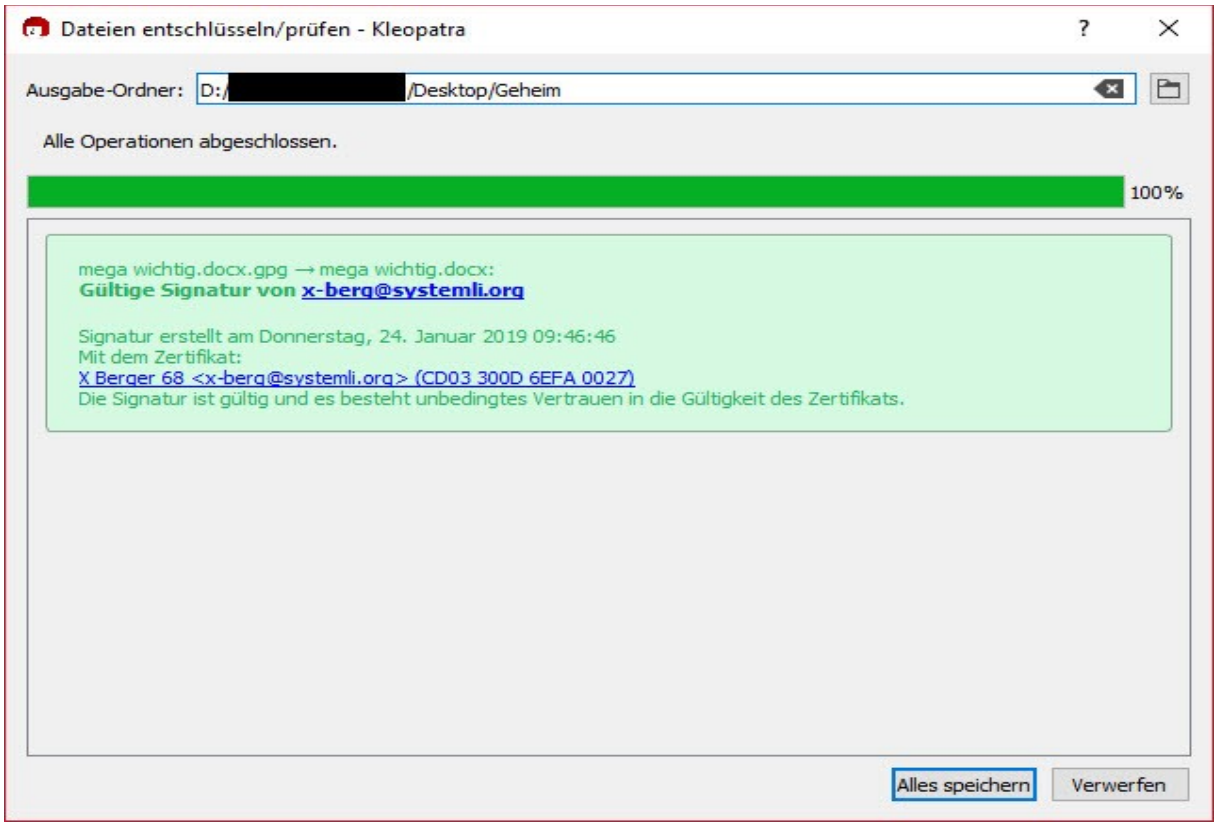


Hier befindet sich Deine Datei „mega wichtig.docx.gpg“, die Du nun verteilen kannst und auch nur von den vorher festgelegten Nutzer:innen geöffnet werden kann.

Dazu reicht es aus, wenn Du die Datei „mega wichtig.docx.gpg“ per Doppelklick öffnest.

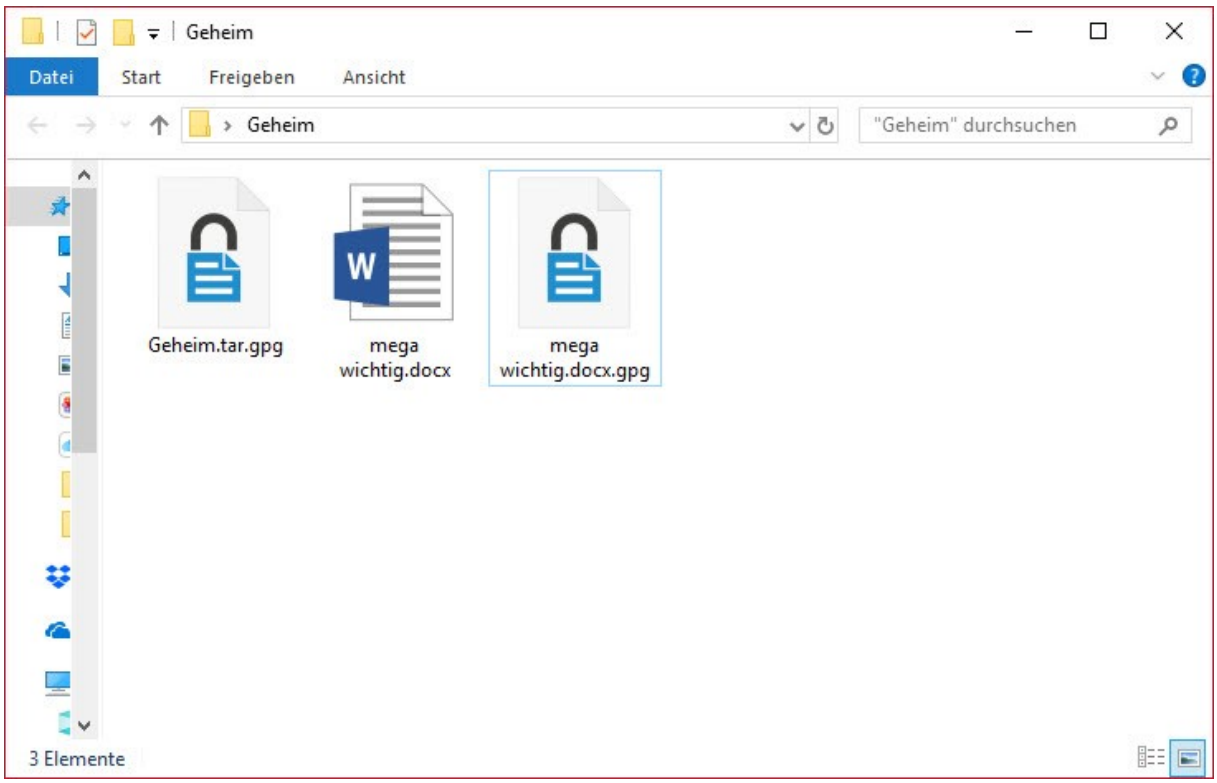


Sofern keine Einschränkungen auf Deinem Rechner konfiguriert sind, öffnet sich das Aktionsfenster von Cleopatra und fordert die Eingabe Deines Passwortes für Deinen privaten Schlüssel.



Hier wird Dir angezeigt, dass die Datei „mega wichtig.docx.gpg“ eine gültige Signatur enthält und die Datei entschlüsselt werden konnte.

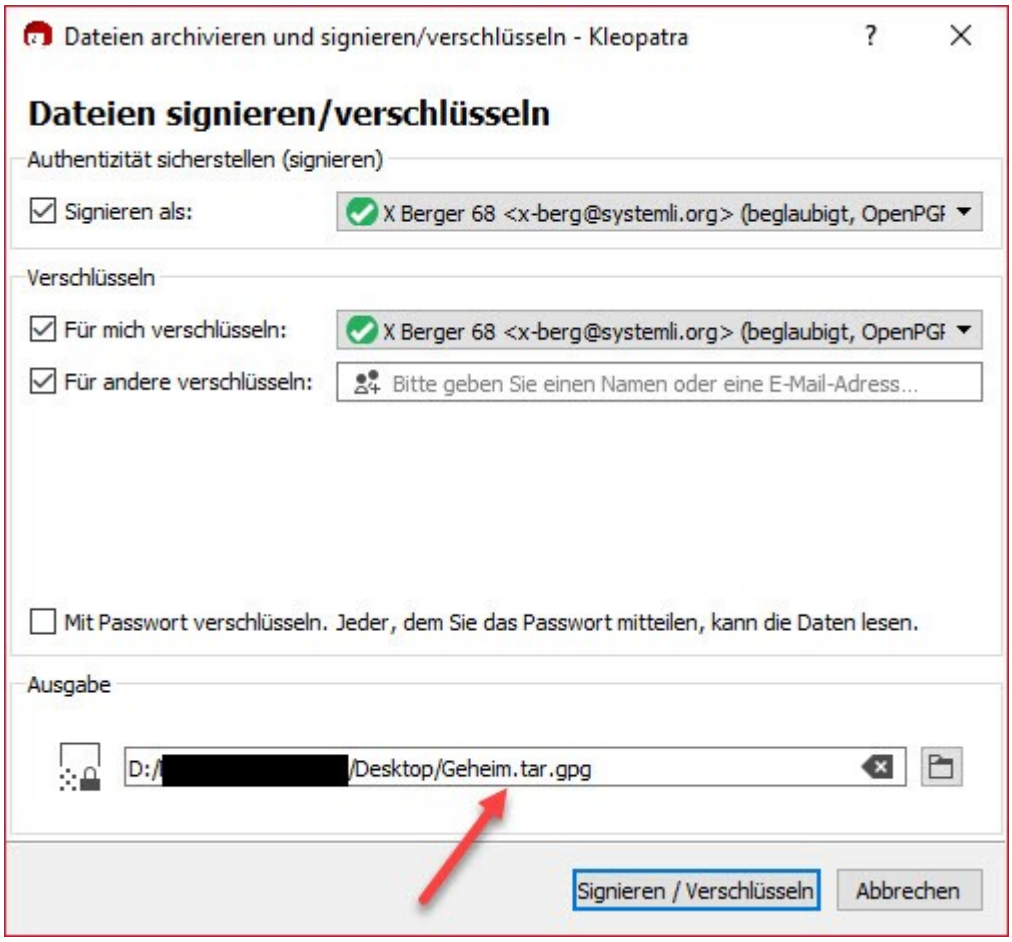
Klicke auf „Alles speichern“ um die entschlüsselte Datei zu speichern oder verwerfen um den Vorgang abzubrechen.



Die Datei „mega wichtig.docx“ kann nun in Deinem Verzeichnis geöffnet werden.

Achte darauf, entschlüsselte Dateien nur in einem sicheren Laufwerk zu speichern!

Verzeichnisse verschlüsseln und entschlüsseln



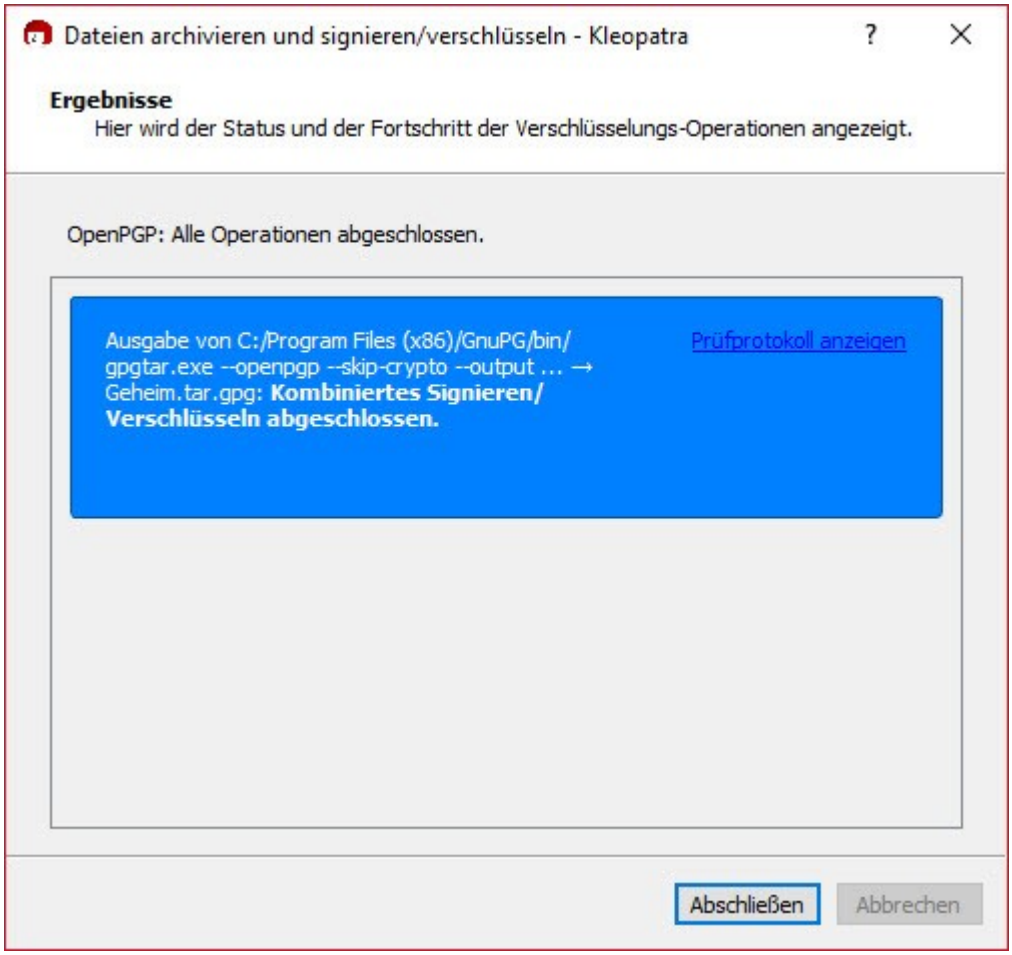
Diese Funktion unterscheidet sich kaum von der Verschlüsselung einzelner Dateien, lediglich der Ansatz ist ein anderer. Statt einzelne Dateien auszuwählen gehst Du mit der Maus zu dem Verzeichnis (hier „Geheim“) und wählst mit Rechtsklick aus dem Kontextmenü „Signieren und verschlüsseln aus.

Hier fehlt lediglich unter „Ausgabe“ die Option „Jede Datei einzeln verschlüsseln / signieren“, alle anderen Optionen sind wie beim verschlüsseln / signieren einzelner Dateien anzuwenden. Daher gehe ich an dieser Stelle nicht extra darauf ein.

Ein weiterer Unterschied ergibt sich aus der Dateibezeichnung, da es sich um ein Verzeichnis mit (vermutlich) mehreren Dateien handelt, wird eine gepackte Datei .tar erzeugt und verschlüsselt:

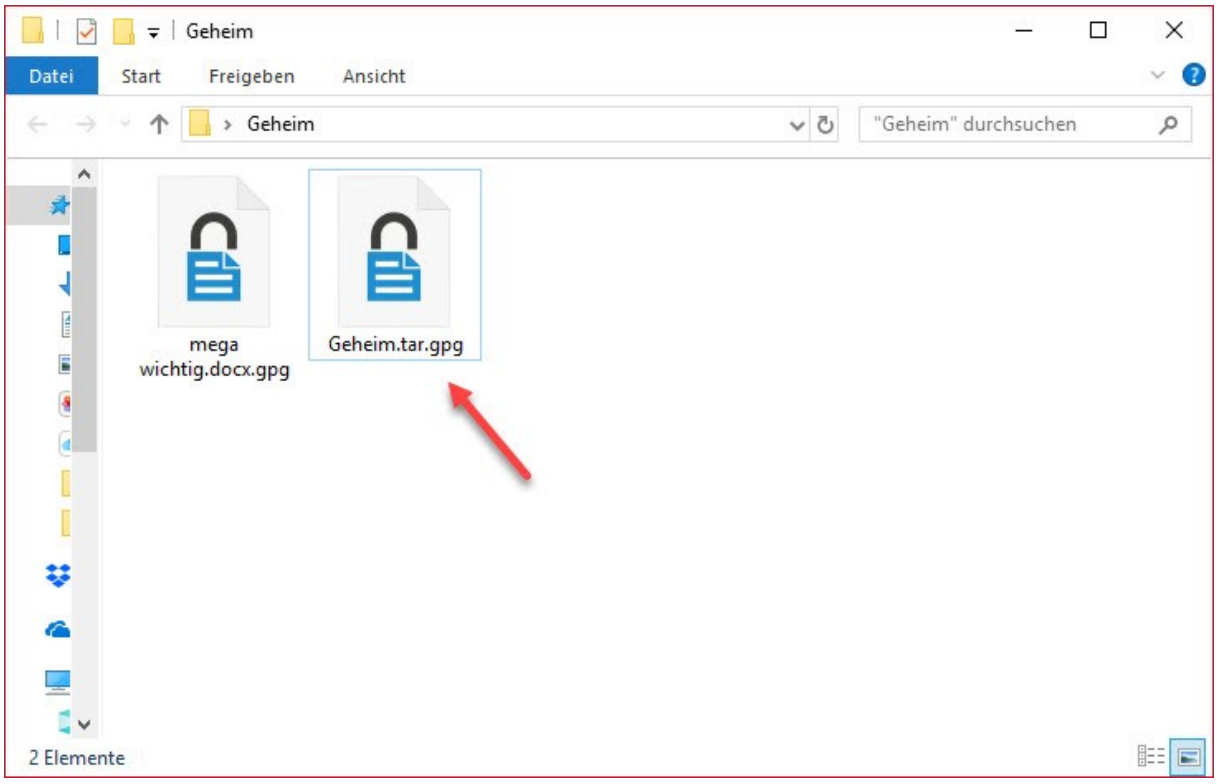
Verzeichnisname.tar.gpg – in diesem Beispiel kommt dabei Geheim.tar.gpg raus.

Wenn Du alles eingestellt und Deine Empfänger:innen eingestellt hast, klickst Du auf „Signieren / Verschlüsseln“.

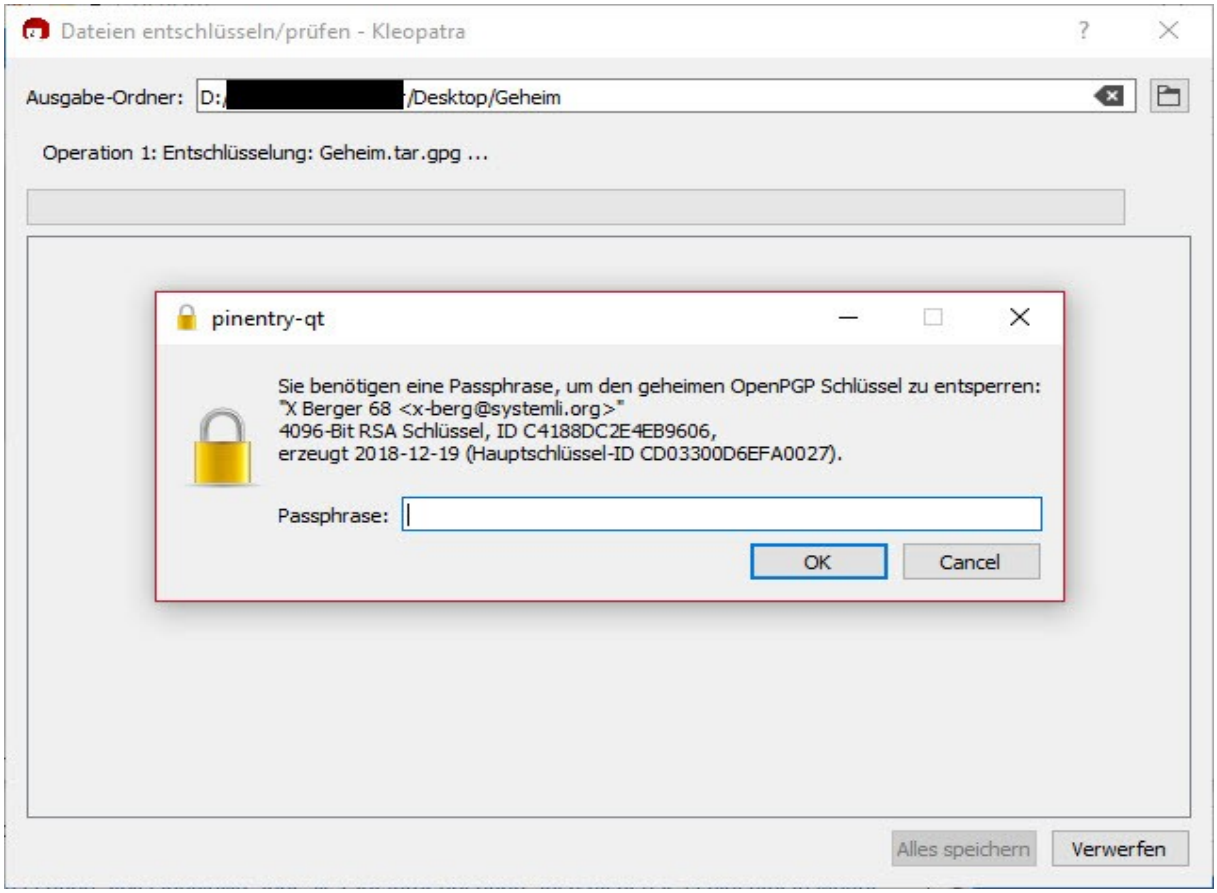


Nach Abschluss der Verschlüsselungsoperationen wird Dir das Ergebnis angezeigt.

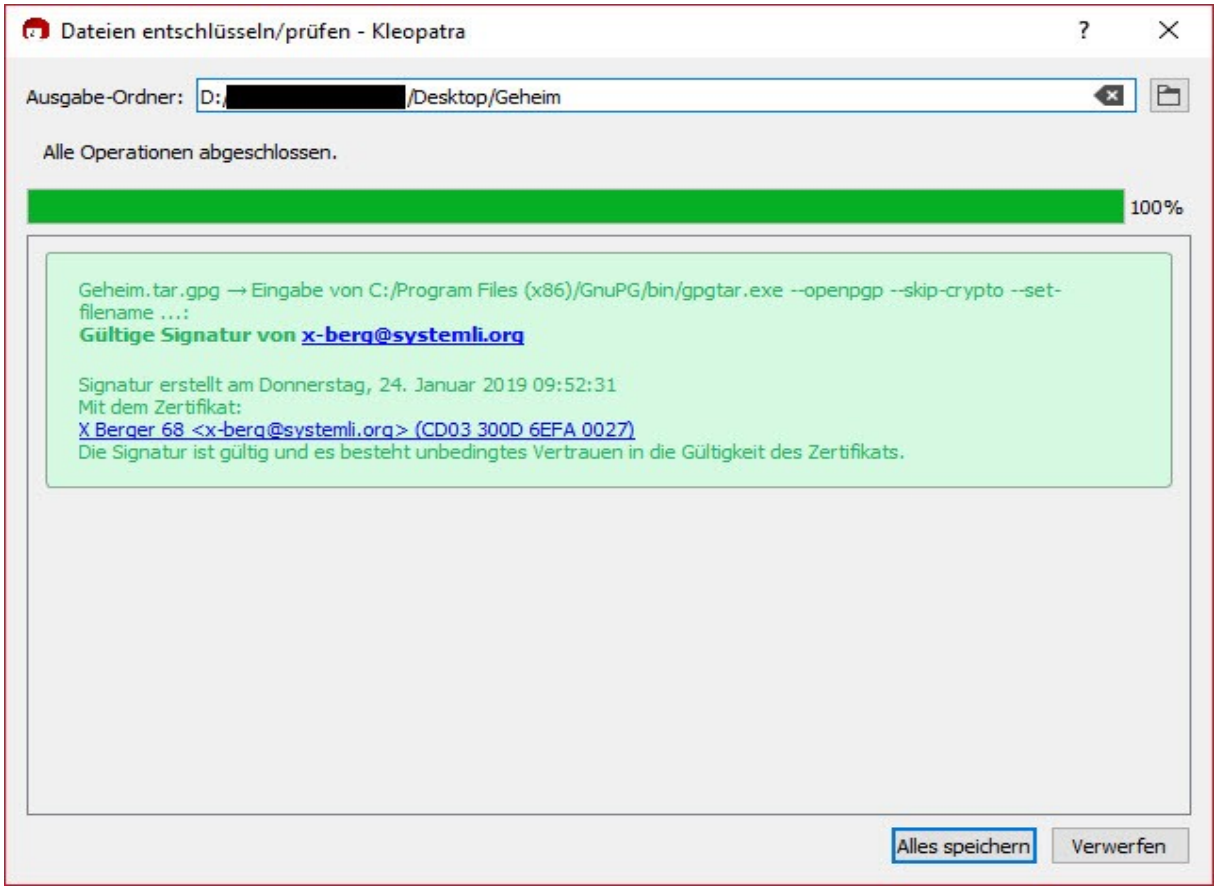
Wurden alle Operationen abgeschlossen, befindet sich Deine Datei in dem vorher festgelegten Verzeichnis.



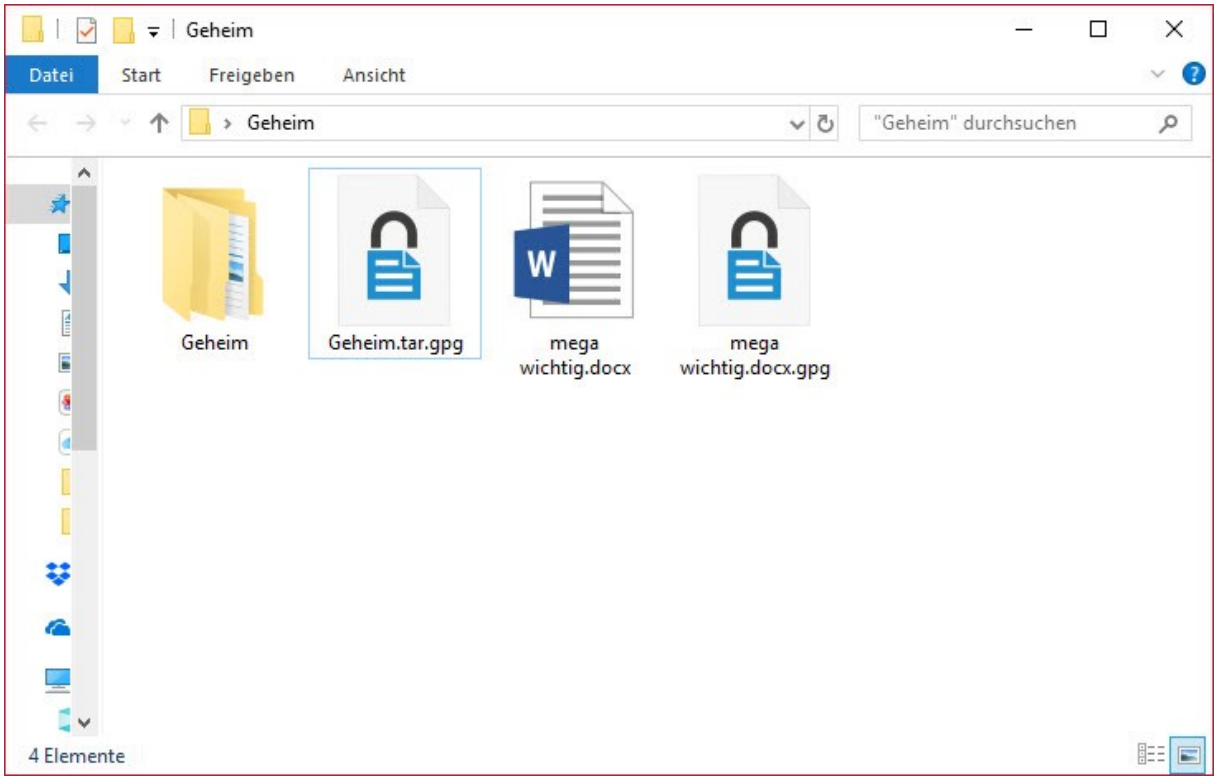
Nun hast Du das gepackte und verschlüsselte Verzeichnis gespeichert.



Das Entschlüsseln ist genauso einfach und vom Ablauf der gleiche Prozess, wie bei einzelnen Dateien.



Klicke auf „Alles speichern“ um die entschlüsselte Datei zu speichern oder verwerfen um den Vorgang abzubrechen.



Das Verzeichnis „Geheim“ kann nun in Deinem Verzeichnis geöffnet und die darin enthaltenen Dateien eingesehen, geöffnet, ggf. bearbeitet werden.

Achte immer darauf, entschlüsselte Dateien nur in einem sicheren Laufwerk zu speichern!

Wenn Du Dein Bootlaufwerk nicht mit VeraCrypt verschlüsselt hast (**DRINGEND EMPFOHLEN!**), dann speichere unverschlüsselte Dateien ausschließlich in einer verschlüsselten Containerdatei oder Festplatte, USB Stick.

Daten sicher löschen, aber wie?

Dateien über das Betriebssystem zu löschen ist **keine** Lösung!

Die Funktion „Löschen“, selbst mit Hinweis „Soll endgültig gelöscht werden?“ ist nichts weiter als ein Ausblenden der Dateien mit einer Markierung, dass der Speicherplatz der gelöschten Dateien verwendet werden kann.

Mit Recoverytools können gelöschte Dateien oftmals vollständig wiederhergestellt werden.

Bitte macht Euch zu diesem Thema schlau, zum Beispiel hier: https://www.netzwelt.de/dateien-sicher-loeschen/index.html

Hier werden auch einige nützliche Tools vorgestellt und erklärt.

Richtig, ggf. noch ein Programm und ein paar Arbeitsschritte mehr – bedenke jedoch, dass Dir der kleine Aufwand enorm viel persönliche Lebenszeit erspart und auch die Deiner Freund:innen.

Je weniger die Cops wissen und von Dir besitzen, umso sicherer ist Dein Leben.