Giegerich & Partner

gpg4o

Handbuch
Version 6.0

Inhaltsverzeichnis

1 Allgemeines

1.1 Zielgruppe dieses Dokuments

Dieses Dokument beschreibt die Installation, Konfiguration und Verwendung von **gpg4o**® für den Anwender auf einem einzelnen Computer. Administratoren empfehlen wir das **„gpg4o Administrator Handbuch“**, in dem die Installation und Konfiguration von **gpg4o** mit Hilfe von Gruppenrichtlinien beschrieben wird.

1.2 gpg4o – GPG für Outlook

gpg4o ist ein Add-In für Microsoft Outlook® ab Version 2010 und wird sowohl von der 32-, als auch von der 64-Bit Version unterstützt.

gpg4o garantiert eine sichere elektronische Kommunikation. Diese wird durch Ver- und Entschlüsselung, sowie digitale Signaturen erreicht.

Für den einfachen und unkomplizierten Umgang mit öffentlichen Schlüsseln sorgt die integrierte Schlüsselverwaltung und die Möglichkeit den eigenen öffentlichen Schlüssel einer E-Mail anzuhängen und der Import-Hinweis von **gpg4o** bei angehängten öffentlichen Schlüssel.

Die Gültigkeit fremder Schlüssel kann mittels der **„Web of Trust-Funktion“** überprüft werden. Dafür werden Informationen bekannter Schlüsselinhaber herangezogen.

1.3 GnuPG und OpenPGP

Für die Verwendung von **gpg4o** wird **GnuPG** benötigt, das während der erstmaligen Einrichtung vom Anwender installiert werden kann. **GnuPG** ist ein freies Kryptographiesystem. Es wird benutzt zum Ver-und Entschlüsseln von Daten sowie zum Erzeugen und Prüfen digitaler Signaturen. **GnuPG** implementiert den **OpenPGP**-Standard.

Informationen zu **GnuPG**, sowie den Quellcode, finden Sie auf:

https://www.gnupg.org/

Die General Public License (GPL) ist zu finden auf:

http://www.gnu.org/licenses/gpl.html

1.4 Schlüssel, Schlüsselpaar und Schlüsselaustausch

Der von **gpg4o** verwendete **OpenPGP**-Standard arbeitet nach dem Prinzip der asymmetrischen Verschlüsselung. Dabei kommen sogenannte **„öffentliche“** und **„private“** Schlüssel zum Einsatz, die zusammen das sogenannte **„Schlüsselpaar“** bilden. Für Einsteiger ist es immer ein wenig verwirrend was es mit diesen auf sich hat und wie diese miteinander zusammen hängen.

Grundsätzlich ist es so, dass Sie immer den **„öffentlichen“** Schlüssel Ihres Kommunikationspartners benötigen, **bevor** Sie Ihm eine verschlüsselte Nachricht schreiben können. Diesen Schlüssel müssen Sie zumindest einmal importieren. Genauso benötigt Ihr Kommunikationspartner Ihren **„öffentlichen“** Schlüssel, um Ihnen verschlüsselte E-Mails schrei-

ben zu können.

Ihren **„öffentlichen“** Schlüssel können Sie bei Verfassen einer E-Mail bequem anhängen und so Ihren Kommunikationspartnern mitteilen. Zusätzlich gibt es sogenannte Schlüsselserver (oder auch Keyserver genannt) im Internet, auf die Sie Ihren **„öffentlichen“** Schlüssel hochladen können. Mehr dazu finden Sie in Kapitel 8.8.

Die Entschlüsselung der Daten findet hingegen mit dem **„privaten“** Schlüssel statt, nachdem Sie die Passphrase eingegeben haben. Durch Eingabe der Passphrase bestätigen Sie, dass Sie dazu berechtigt sind Zugriff auf die entschlüsselten Daten zu erhalten.

Achtung: Geben Sie Ihren privaten Schlüssel und/oder die dazugehörige Passphrase **niemals** an andere Personen heraus! Diese können sonst Ihre E-Mails lesen und auch in Ihrem Namen signieren.

Wenn Sie eine E-Mail signieren, „Unterschreiben“ Sie die E-Mail und schützen Sie somit vor unerkannten Veränderungen auf dem Weg zu Ihrem Empfänger. Um eine E-Mail zu signieren, müssen Sie als Bestätigung Ihre Passphrase eingeben.

Der Empfänger einer signierten E-Mail kann die Signatur Ihrer E-Mail überprüfen - und somit Veränderungen an der E-Mail entdecken - wenn er ihren **„öffentlichen“** Schlüssel importiert hat.

Zusammengefasst ist zu sagen, dass Sie Ihren **„öffentlichen“** Schlüssel mit gutem Gewissen an alle auf der Welt verteilen können. Im Gegensatz zu Ihrem **„privaten“** Schlüssel, welcher unter allen Umständen sicher verwahrt bleiben sollte.

2 Systemvoraussetzungen

gpg4o wurde für Microsoft Outlook 2010 (und später) unter Microsoft Windows® entwickelt. Details zu den von Giegerich & Partner zertifizierten Plattformen entnehmen Sie bitte der folgenden Tabelle:

Betriebssystem	Outlook 2010	Outlook 2013	Outlook 2016	Outlook 2019
Windows 7	✓	✓	✗ [1]	✗ [1]
Windows 7 (SP1)	✓	✓	✓	✗ [1]
Windows 8	✓	✓	✓	✗ [1]
Windows 8.1	✓	✓	✓	✗ [1]
Windows 10	✓	✓	✓	✓
Mac OS	✗	✗	✗	✗

[1] Betriebssystem wird von Microsoft Outlook nicht unterstützt.

gpg4o funktioniert sowohl mit 32 Bit als auch 64 Bit Outlook und Windows Versionen.

gpg4o verwendet **GnuPG**, eine frei erhältlichen Implementation des OpenPGP-Standards. Genauere Informationen zu den kompatiblen GnuPG-Versionen entnehmen Sie der folgenden Tabelle.

GnuPG Version	gpg4o
v1.4.22 (oder höher)	✓
v2.2.9 (oder höher)	✓

Bei der Ersteinrichtung wird eine von **gpg4o** unterstützte Version automatisch installiert.

3 Funktionsumfang

3.1 Funktionsumfang der Versionen im Vergleich

Funktion	Testversion	Free Version	Vollversion
E-Mails ver-, entschlüsseln, signieren	✓	✓	✓
Zeitgleich verwendbare E-Mail Konten	1	1	beliebig
Nutzung privat/kommerziell	✓ / ✓	✓ / ✗	✓ / ✓
HTML E-Mails	✓	✓	✓
„Nur-Text“ E-Mails	✓	✓	✓
Anzeige von PGP/MIME E-Mails	✓	✓	✓
Individuelle Senderegeln	✓	✗	✓
E-Mails entschlüsselt speichern	✓	✗	✓
Automatischer Up- und Download von Schlüsseln	✓	✗	✓
Prüfung auf GnuPG Updates	✓	✗	✓
Automatische Sicherung von Schlüssel	✓	✗	✓
Zeitraum Support via E-Mail [1]	45 Tage [2]	keinen [3]	1 Jahr [4]
Zeitraum Update	45 Tage [2]	unbegrenzt	1 Jahr [4]
Zeitraum Verwendbarkeit	45 Tage [2]	unbegrenzt	unbegrenzt
Unterstützte Mailserver			
Microsoft Exchange	✓	✗	✓
POP3	✓	✓	✓
IMAP	✓	✓	✓
Outlook.com	✓	✓	✓
Hotmail.com	✓	✓	✓
Weiteres			
Kompatibel mit DATEV-Installationen	✓	✗	✓

[1] Um den Support zu kontaktieren benutzen Sie folgende E-Mail support.gpg4o@giepa.de. Es wird kein telefonischer Support angeboten.

[2] Verlängerung des Testzeitraumes ist auf Anfrage möglich

[3] Support kann von Nutzern der kostenfreien Version nur in Ausnahmefällen genutzt werden. Nähere Informationen finden Sie im Kapitel 13.4.

[4] Abhängig von der Dauer der Produktwartung (1 Jahr nach Kauf, danach erweiterbar durch den Kauf einer Verlängerung der Produktwartung: +1 Jahr, +3 Jahre oder +5 Jahre)

3.2 PGP/Inline und PGP/MIME

gpg4o kann reine Textnachrichten und HTML E-Mails als PGP/Inline versenden und empfangen. Zusätzlich können PGP/MIME E-Mails empfangen und entschlüsselt werden. Es ist auch möglich die von PGP/MIME signierten E-Mails („Abgetrennte Signatur“) zu verifizieren.

3.3 Was passiert nach Ablauf des Testzeitraumes mit der Testversion

Sie können nur noch E-Mails entschlüsseln, die im Testzeitraum empfangen wurden. Nach Ablauf des Testzeitraumes können E-Mails nicht mehr verschlüsselt/signiert verschickt werden. Die Verlängerung des Testzeitraumes ist auf Anfrage möglich.

3.4 Was passiert nach Ablauf der Produktwartung/Support mit der Vollversion

Wenn die Produktwartung/Support abgelaufen ist, kann **gpg4o** weiterhin genutzt werden. Das heißt, Sie können weiterhin E-Mails verschlüsselt/signiert versenden und verschlüsselte/signierte E-Mails lesen.

Sie haben jedoch keinen Anspruch mehr, neue Updates zu installieren, oder den Support via E-Mail zu kontaktieren.

3.5 Nutzungszeitraum von gpg4o *Free*

Die kostenfreie **gpg4o** Version ist durch keinen Zeitraum beschränkt und kann ständig auf die neusten Versionen aktualisiert werden. **gpg4o** ***Free*** ist in ihrer Funktionalität eingeschränkt. Des Weiteren kann der Support nur in Ausnahmefällen genutzt werden.

4 Installation von gpg4o

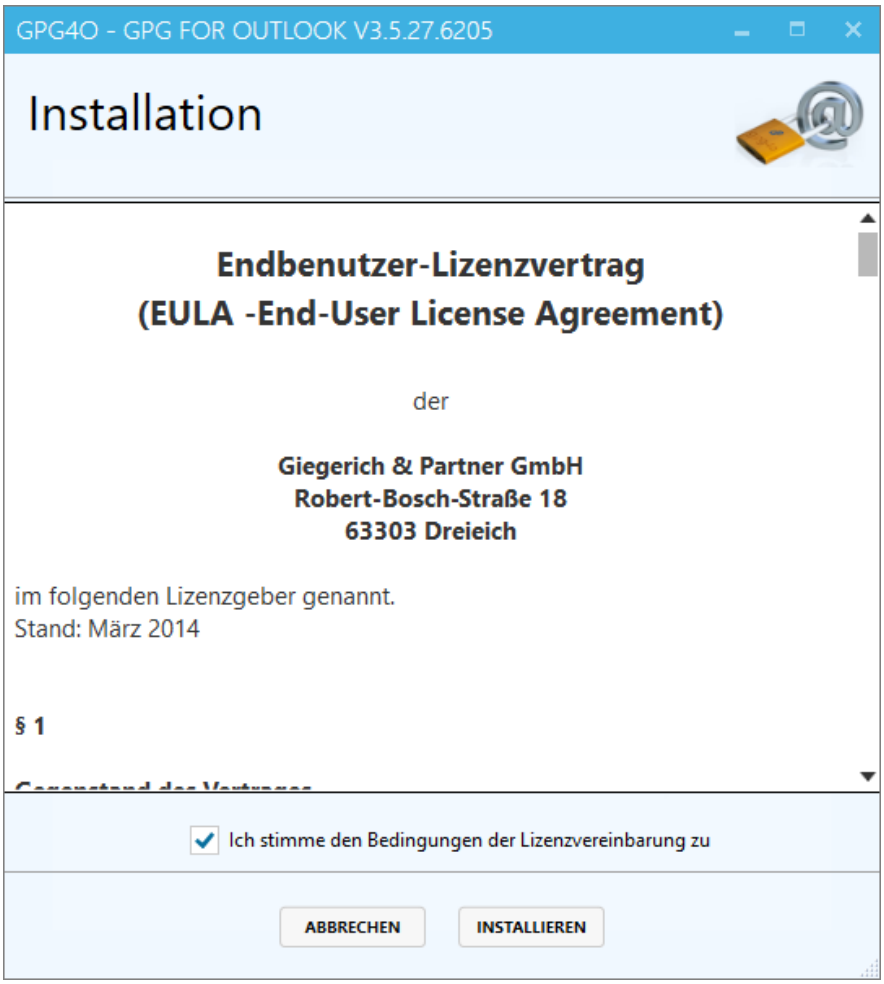
Hinweis: Die aktuelle Version von **gpg4o** finden Sie unter:
https://www.giepa.de/produkte/gpg4o/downloads/

Für die Installation benötigen Sie lokale Administratorrechte. Schließen Sie bitte vor der Installation von **gpg4o** die Anwendung Microsoft Outlook, damit die Installation korrekt ausgeführt werden kann. Führen Sie anschließend die Datei `gpg4o_setup.exe` durch einen Doppelklick aus.

Im Start-Dialog werden Sie nach dem Installationspfad gefragt. Hier ist die Voreinstellung in der Regel die richtige Wahl. Bestätigen Sie den Installationspfad mit `Weiter`.

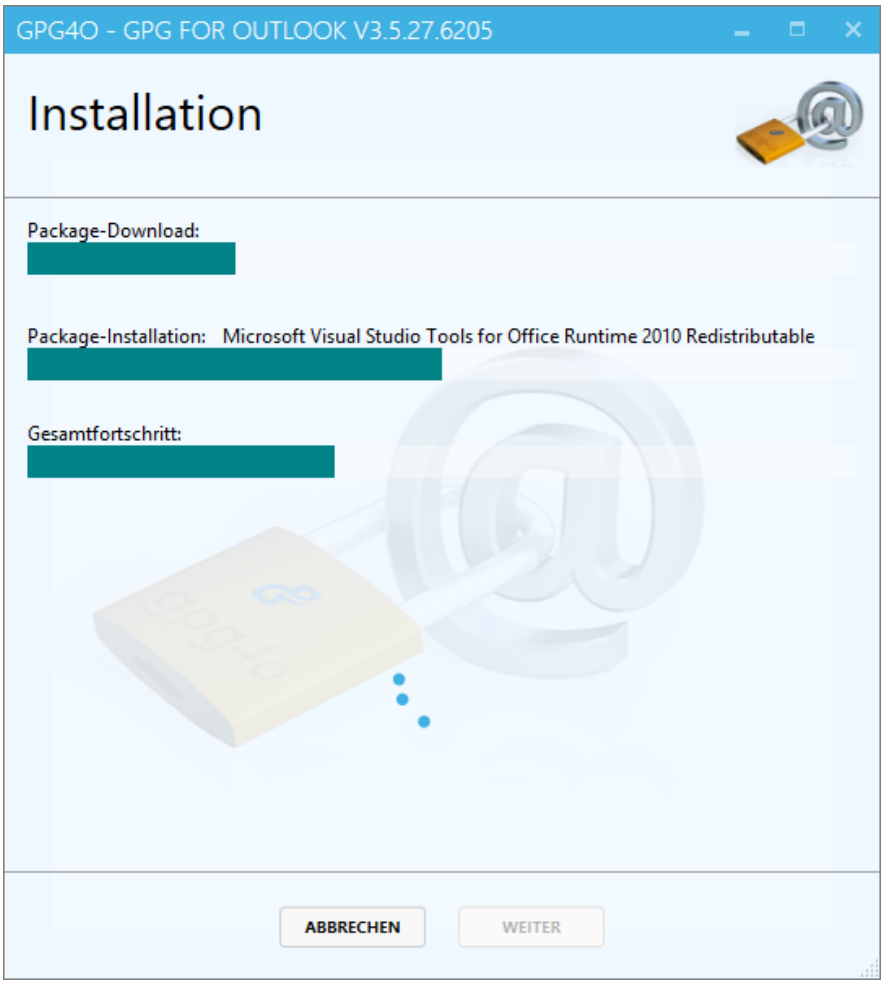
Standardmäßig wird **gpg4o** in diesen Ordner installiert:

```
C:\Program Files (x86)\Giegerich und Partner GmbH\gpg4o - GPG for Outlook\
```



Wenn Sie sich entschlossen haben, den Endbenutzer-Lizenzvertrag zu akzeptieren (Voraussetzung für die Installation), klicken Sie zuerst auf

`Ich stimme den Bedingungen der Lizenzvereinbarung zu` und danach auf `INSTALLIEREN`.



Nachdem eventuell fehlende Systemkomponenten heruntergeladen und installiert wurden, wird **gpg4o** installiert.

Die Installation von **gpg4o** ist erfolgreich abgeschlossen, starten Sie nun Microsoft Outlook, um mit der Einrichtung von **gpg4o** zu beginnen.

5 Erstmalige Einrichtung

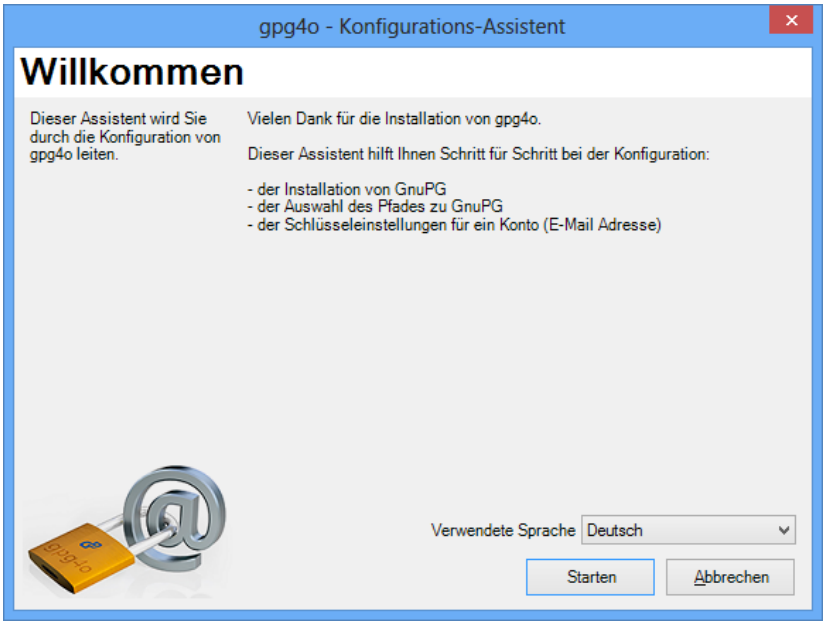
Sobald Sie Microsoft Outlook nach der Installation von **gpg4o** starten, erscheint der Konfigurations-Assistent, der Ihnen bei der Ersteinrichtung behilflich sein wird.

5.1 Einfache Einrichtung

5.1.1 Start

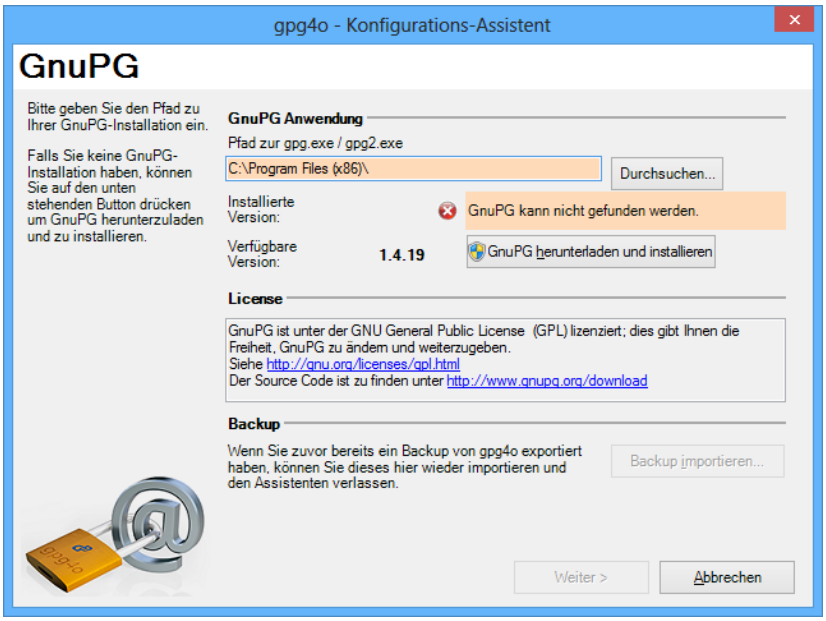
Auf der ersten Seite des Assistenten haben Sie die Möglichkeit, die Anzeigesprache der Anwendung zu ändern. Haben Sie die Sprach-Einstellung vorgenommen, klicken Sie auf Starten, um mit der Konfiguration zu beginnen.

Über die Schaltfläche Abbrechen können Sie den Assistenten beenden, er wird jedoch bei jedem Start von Microsoft Outlook aufgerufen, bis er einmal vollständig durchlaufen wurde und ein Konto zur Verwendung mit **gpg4o** konfiguriert wurde.



5.1.2 GnuPG

Auf dieser Seite wird die Komponente **GnuPG** eingerichtet, welche die Ver- und Entschlüsselung der Daten durchführt.



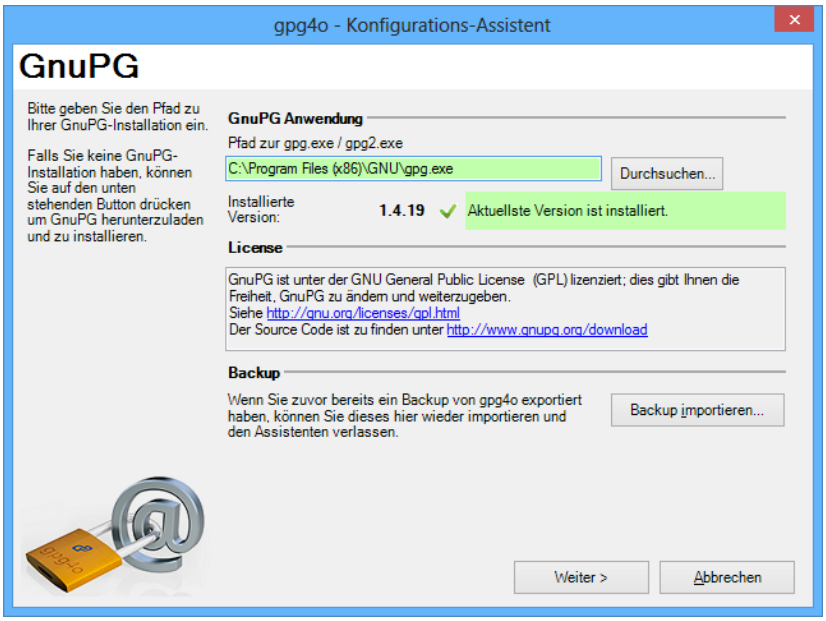
*Ansicht wenn keine gültige **GnuPG**-Installation gefunden wurde.*

Falls **GnuPG** schon auf Ihrem Computer installiert ist, wird der Pfad automatisch eingetragen und grün hinterlegt. Wurde ein installiertes **GnuPG** nicht gefunden, wird die Auswahl rötlich hinterlegt.

Wenn Sie noch kein **GnuPG** installiert haben, starten Sie die Installation über die Schaltfläche GnuPG herunterladen und installieren.

Hinweis: Bitte achten Sie darauf, dass das Verzeichnis, in das **GnuPG** installiert werden soll, leer ist.

Nach erfolgreicher Installation wird der Pfad automatisch in die Einstellungen übernommen und Sie können mit der Konfiguration fortfahren.

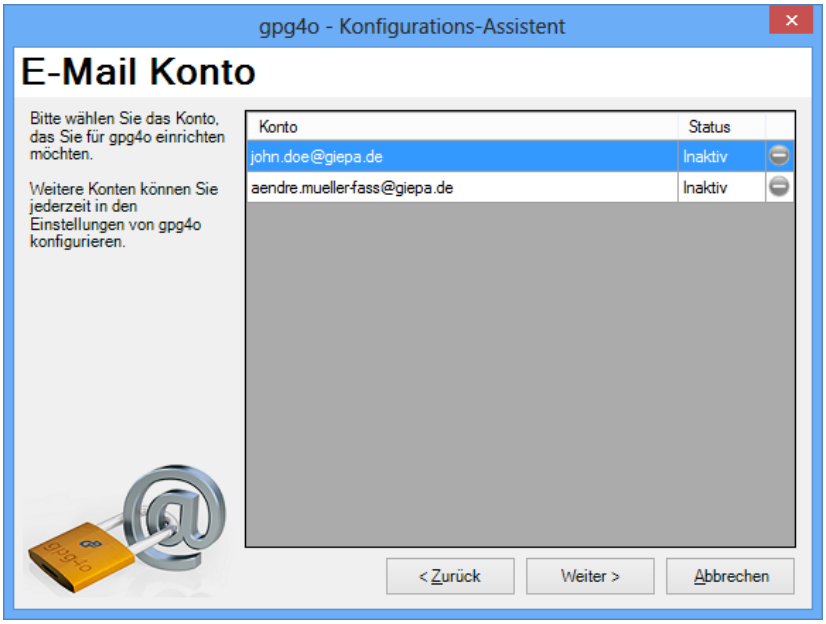


5.1.3 E-Mail Konto

Sind in Microsoft Outlook mehrere E-Mail Konten eingerichtet, können Sie hier das Konto auswählen, für das **gpg4o** initial eingerichtet wird. Wir empfehlen hier das E-Mail Konto auszuwählen, mit dem Sie hauptsächlich arbeiten.

Hinweis: Nach Abschluss des Assistenten können jederzeit weitere Konten zur Verwendung mit **gpg4o** eingerichtet werden.

Sollte nur ein einziges E-Mail Konto in Outlook vorhanden sein, wird diese Seite übersprungen und **gpg4o** automatisch für das vorhandene Konto eingerichtet.



Wählen Sie das Konto aus, mit dem Sie **gpg4o** benutzen wollen und klicken Sie anschließend auf Weiter >.

5.1.4 Schlüsselerstellung

Sie erhalten nachfolgenden Dialog für die Konfiguration des neuen Schlüsselpaares.

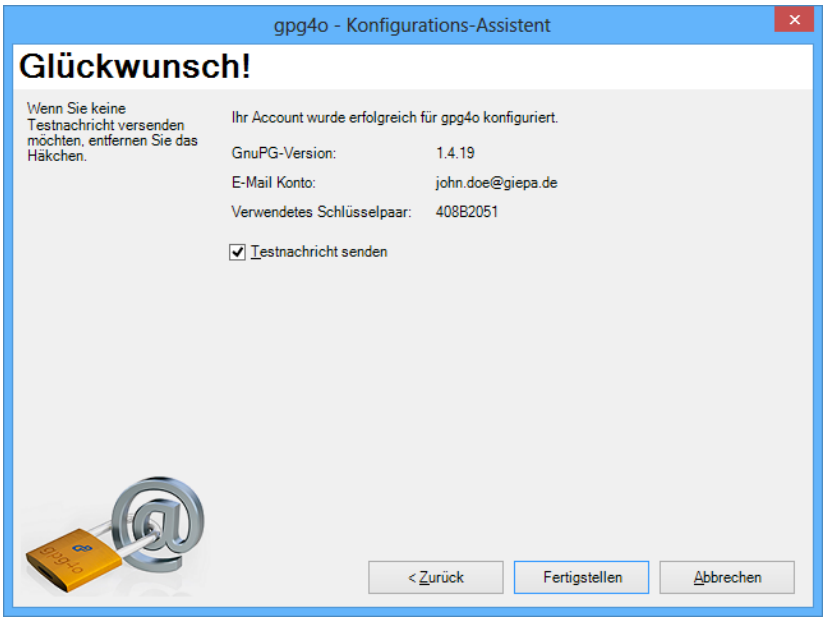
Geben Sie zur Erstellung eines neuen Schlüsselpaares zunächst Ihren Namen sowie eine Passphrase ein. Die Passphrase wird später regelmäßig benötigt, um E-Mails zu entschlüsseln und zu unterschreiben.

Achtung: Merken Sie sich **unbedingt** die eingegebene Passphrase, da ohne diese keine Entschlüsselung Ihrer E-Mails möglich ist!
Weder **gpg4o** noch **Giegerich & Partner** kennen Ihre geheime Passphrase und es besteht keine Möglichkeit eine vergessene Passphrase wiederherzustellen!

Nachdem Sie alle benötigten Felder ausgefüllt haben, klicken Sie auf Generieren und Ihr neues Schlüsselpaar wird erstellt.

5.1.5 Zusammenfassung

Nachdem Sie nun ein Schlüsselpaar erstellt haben, erscheint die Zusammenfassung Ihrer Einrichtung.



Wenn Sie den Haken bei Testnachricht senden belassen, wird Ihnen automatisch eine verschlüsselte Testnachricht zugestellt, mit der Sie die Konfiguration von **gpg4o** überprüfen können.

Klicken Sie auf Fertigstellen, um die Einrichtung abzuschließen und mit der Verwendung von **gpg4o** zu beginnen. In Kapitel 6 werden die ersten Schritte mit **gpg4o** erklärt.

5.2 Fortgeschrittene Einrichtung

In diesem Kapitel erhalten Sie detailliertere Informationen zu den fortgeschrittenen Möglichkeiten im Konfigurations-Assistenten. Als Erstanwender können Sie dieses Kapitel überspringen und direkt mit Kapitel 6 fortfahren.

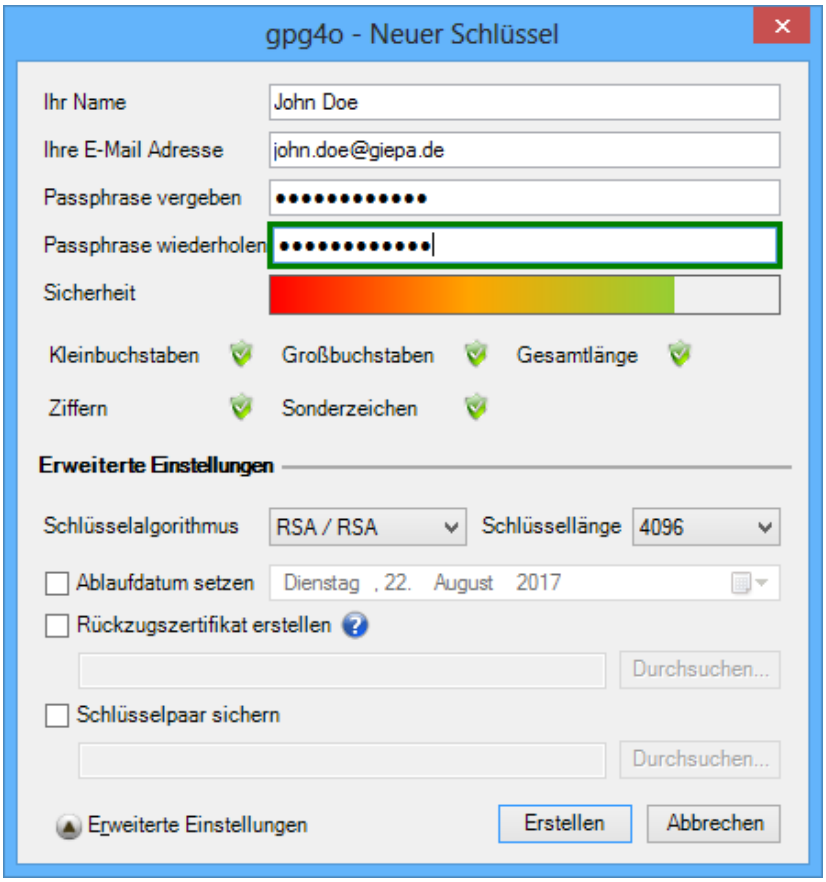
5.2.1 GnuPG

Auf dieser Seite haben Sie, zusätzlich zur Installation von **GnuPG**, die Möglichkeit eine Datensicherung einzuspielen. Dies ist hilfreich, um nach einer Neuinstallation des Betriebssystems oder nach einem Wechsel des Computers die vorherige Konfiguration von **gpg4o** und die Schlüssel wiederherzustellen.

Informationen zur Erstellung einer Datensicherung finden Sie in Kapitel 11.8.1.

5.2.2 Schlüsselerstellung

In der Maske zur Schlüsselerstellung können Sie über die Schaltfläche Erweitert... zusätzliche Einstellmöglichkeiten aufrufen.



Hier haben Sie die Möglichkeit, die Algorithmen und die Länge des Schlüssels zu beeinflussen. Die Standardeinstellung stellen jedoch schon ein hohes Maß an Sicherheit dar.

Außerdem können Sie ein Ablaufdatum für den Schlüssel festlegen. Nach diesem Zeitpunkt kann der Schlüssel nicht mehr zum Signieren oder Verschlüsseln von Nachrichten genutzt werden, das Entschlüsseln bleibt davon unberührt.

Ebenfalls möglich ist die Erstellung eines Rückzugzertifikates, das für den Fall wichtig ist, dass Sie die Passphrase vergessen, Sie den Zugriff auf das Schlüsselpaar verlieren (Datenverlust) oder es einer anderen Person in die Hände fällt.

Achtung: Bitte verwahren Sie dieses Zertifikat besonders gut geschützt, da für das einspielen des Zertifikates **keine** Passphrase notwendig ist.
Somit kann jede beliebigen Person, die im Besitz dieses Zertifikates ist, das Schlüsselpaar dauerhaft und unwiderruflich unbenutzbar machen!

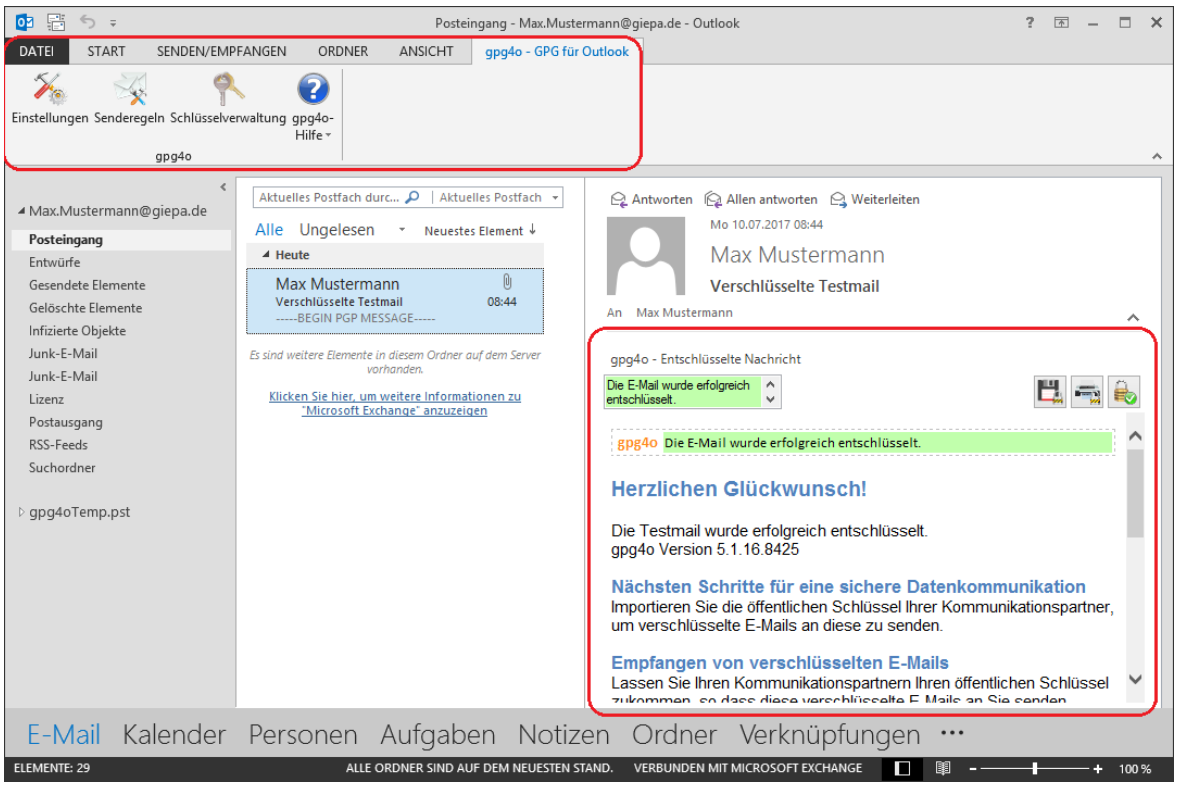
Nähere Informationen zu Rückzugszertifikaten finden Sie in Kapitel 8.12.

Zuletzt haben Sie noch die Möglichkeit, das Schlüsselpaar zu exportieren. Diese Datensicherung sollte sehr sicher verwahrt werden. Beachten Sie auch, dass das exportierte Schlüsselpaar nur mit der Passphrase benutzt werden kann, die bei der Erstellung eingegeben wurde.

6 Erste Schritte mit gpg4o

6.1 Übersicht

Nach erfolgreicher Installation von **gpg4o** sehen Sie in Microsoft Outlook einen neuen Reiter namens gpg4o - GPG für Outlook. Dort finden Sie die Einstellungen von **gpg4o**, die Senderegeln, die Schlüsselverwaltung und die gpg4o-Hilfe.



Ist die E-Mail Vorschau in Outlook aktiviert, wird in diesem Bereich die verschlüsselte oder entschlüsselte E-Mail angezeigt. Dieser Vorschaubereich wird von **gpg4o** um einen Bereich für zusätzliche Informationen und Aktionen erweitert.

Am linken Rand der Vorschau werden Detailinformationen zur Entschlüsselung und Signaturen angezeigt. Die Textbox ist grün eingefärbt, wenn die Entschlüsselung/Signaturprüfung erfolgreich war.

Am rechten Rand können sich, je nach angezeigter E-Mail, unter anderem die folgenden Schaltflächen/Symbole befinden:

Diskette

Entschlüsselt die angezeigte E-Mail dauerhaft.

Drucker

Druckt die entschlüsselt angezeigte E-Mail.

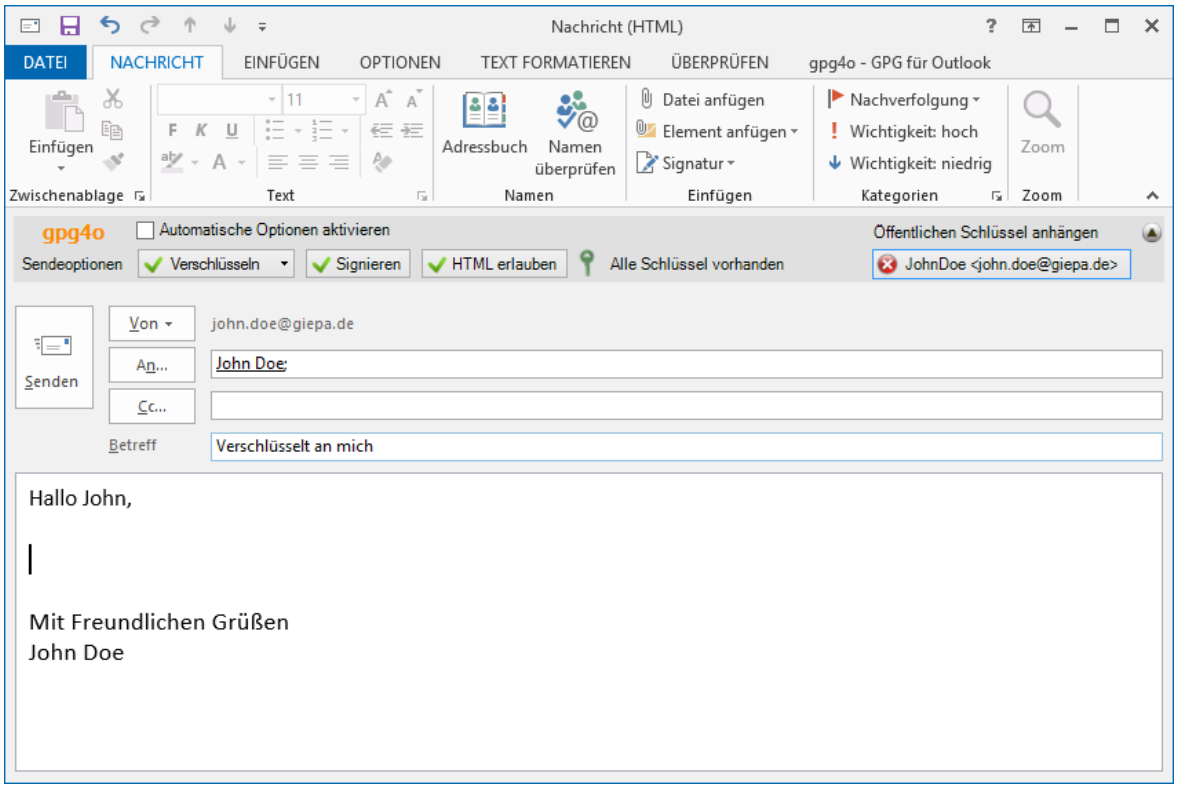
Schloss

E-Mail wird verschlüsselt angezeigt / Eingegebene Passphrase wird vergessen.

Mehr Informationen zu den Symbolen finden Sie ab Kapitel 7.5.1.

6.2 Verschlüsselte E-Mail senden und lesen

Um eine verschlüsselte oder signierte E-Mail zu senden, erstellen Sie eine neue E-Mail. In dem sich öffnenden Fenster wird am oberen Rand durch **gpg4o** eine Leiste mit den **„Sendeoptionen“** für diese E-Mail angezeigt.



Mit den Schaltflächen Verschlüsseln und Signieren in der Leiste können Sie für diese E-Mail festlegen ob diese verschlüsselt und/oder signiert versendet werden soll.

Mit der Schaltfläche HTML erlauben legen Sie fest, ob die E-Mail im **„HTML“** oder **„Nur Text“** Format gesendet werden soll.

Mit der Schaltfläche Öffentlichen Schlüssel anhängen können Sie dem Empfänger Ihren öffentlichen Schlüssel zukommen lassen. (siehe Kapitel 1.4)

Verfassen Sie eine E-Mail an sich selbst, aktivieren die Verschlüsselung über die Schaltfläche Verschlüsseln und senden die E-Mail ab. Wenn Sie zusätzlich die Option Signieren aktiviert haben, werden Sie kurz vor dem Versand der E-Mail nach der Passphrase gefragt.

Ist die E-Mail angekommen, können Sie diese in der Outlook Vorschau lesen oder per Doppelklick öffnen. Haben Sie die E-Mail ohne die Option Signieren gesendet, werden Sie jetzt zur Eingabe Ihrer Passphrase aufgefordert, um die Entschlüsselung durchzuführen. Haben

Sie die E-Mail signiert versandt, befindet sich Ihre Passphrase noch im Arbeitsspeicher des Computers, so dass sie diese hier nicht nochmal eingeben müssen.

Achtung: Bei Anzeige bestimmter E-Mails können Sie von gpg4o eine nicht abschaltbare Warnung angezeigt bekommen, die auf Probleme in der Integrität der E-Mail hinweist. Im Mai 2018 wurde eine „Efail“ getaufte Sicherheitslücke veröffentlicht, bei der Angreifer Inhalte von verschlüsselten E-Mails verändern konnten, ohne dass Sie als Empfänger dies erkennen können. Ein Angreifer kann durch Änderungen an einer, ohne MDC verschlüsselten, E-Mail (Modification Detection Code) unter bestimmten Umständen auch einen Teil Ihres privaten Schlüssels erraten. gpg4o erkennt solche E-Mails und verhindert dies, indem es bei einer Antwort/Weiterleitung die möglicherweise veränderten Daten entfernt. Damit kann ein Angreifer durch eine Antwort/Weiterleitung solcher E-Mails keine Rückschlüsse mehr auf Ihren privaten Schlüssel ziehen.

6.3 Verschlüsseln und Signieren

Wenn Sie eine E-Mail verschlüsseln, kann nur die Person den Text der E-Mail lesen, der im Besitz des dazu gehörigen Schlüssels ist. Dies betrifft auch die Anhänge der E-Mail.

Hinweis: Bitte beachten Sie, dass bei der Verschlüsselung von E-Mails keine Anonymisierung stattfindet, sondern nur die Inhalte für Dritte unlesbar gemacht werden. Wenn jemand Zugriff auf Ihre E-Mail erhält, kann er trotzdem noch sehen, mit wem Sie kommunizieren.

Wenn Sie eine E-Mail signieren, wird über Ihren Text und eventuell vorhandene Anhänge eine Prüfsumme berechnet und in die E-Mail eingebettet. Dadurch kann der Empfänger mit **gpg4o** oder einem ähnlichen Programm überprüfen, ob der Text der E-Mail während der Übertragung verändert wurde oder nicht.

7 Verwenden von gpg4o

Sie haben **gpg4o** eingerichtet und entsprechende Schlüsselpaare für Ihre E-Mail Konten erzeugt, müssen Sie nun Ihren Kommunikationspartnern Ihren öffentlichen Schlüssel zusenden. Ein Schlüsselpaar besteht aus zwei Teilen: Einem privaten Schlüssel (Private-Key) und einem öffentlichen Schlüssel (Public-Key). Bei der Erstellung des Schlüsselpaares wurden Sie gebeten, eine Passphrase (Passwort) für das Schlüsselpaar einzugeben.

Achtung: Geben Sie **niemals** Ihre Passphrase oder Ihren privaten Schlüssel weiter. Jede Person, die in den Besitz Ihres privaten Schlüssels kommt, kann Ihre E-Mails entschlüsseln und neue Nachrichten in Ihrem Namen unterschreiben.
Die Passphrase sollten Sie ebenso sicher aufbewahren, wie Ihre anderen Passwörter, und **niemandem sonst mitteilen**.

Zur generellen Verwendung von **gpg4o** hier ein kurzes Beispiel:

Sie möchten mit Person B verschlüsselt kommunizieren. Daher schicken Sie eine E-Mail mit Ihrem öffentlichen Schlüssel an Person B und fragen dessen öffentlichen Schlüssel an. Dieser Schlüsselaustausch ist für jeden Kontaktpartner einmalig nötig.

Person B ist nun im Besitz Ihres öffentlichen Schlüssels und kann Ihnen daher sofort verschlüsselt antworten. Person B antwortet also auf die Anfrage, hängt seinen öffentlichen Schlüssel an und verschlüsselt die Antwort mit dem öffentlichen Schlüssel von Ihnen.

Sie erhalten nun die verschlüsselte E-Mail von Person B und entschlüsseln diese mit Ihrem eigenen privaten Schlüssel. Den öffentlichen Schlüssel von Person B importieren Sie, und können nun auch an Person B verschlüsseln.

Hinweis: Um die eigenen selbst versendeten E-Mails noch lesen zu können, wird stets auch mit dem eigenen öffentlichen Schlüssel verschlüsselt.

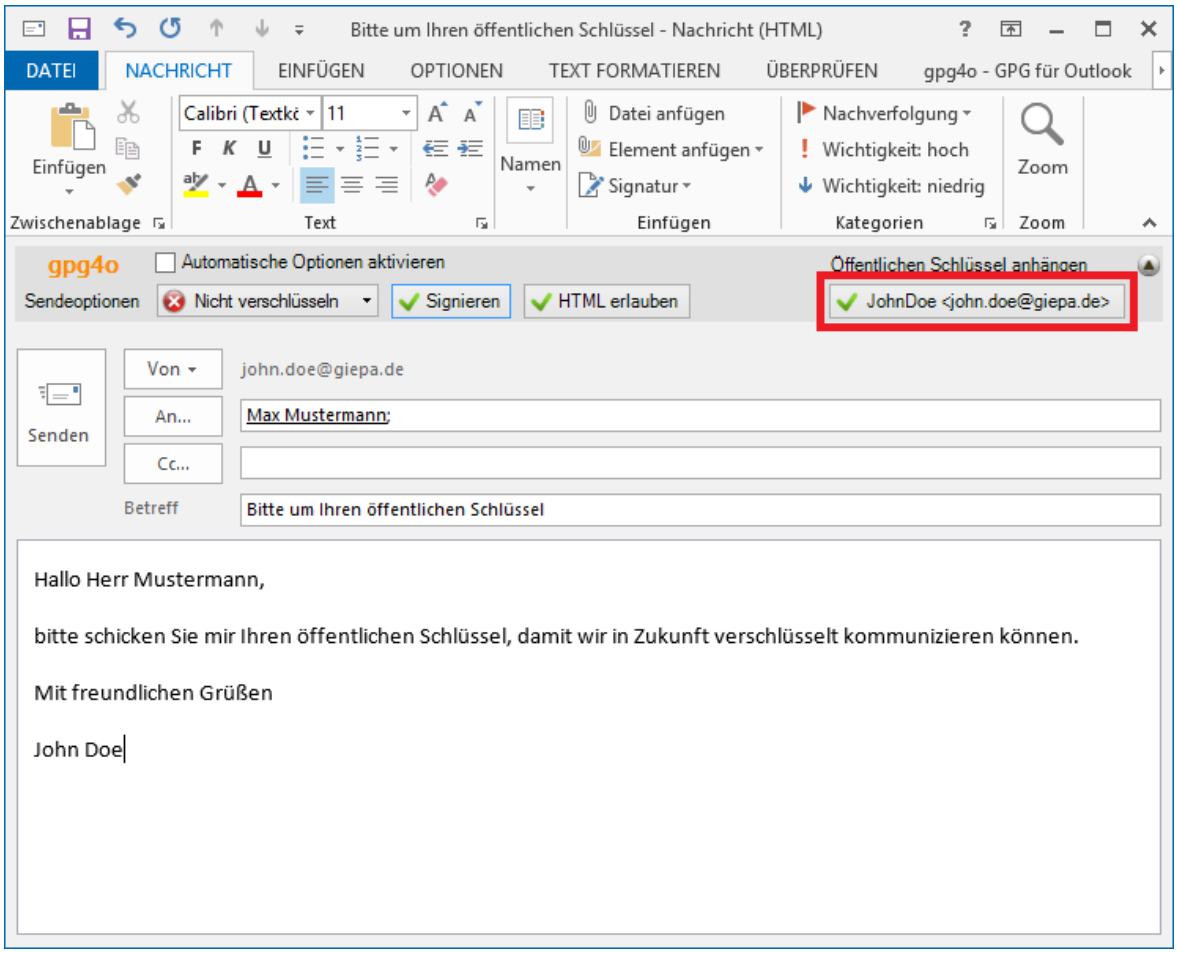
7.1 Versenden von öffentlichen Schlüsseln

Um Nachrichten an jemanden verschlüsseln zu können, benötigen Sie den öffentlichen Schlüssel des Empfängers der Nachricht. Damit Ihnen verschlüsselte E-Mails geschickt werden können, benötigen Ihre Kommunikationspartner also zuerst Ihren öffentlichen Schlüssel.

Dazu erstellen Sie bitte eine neue E-Mail und klicken auf die Schaltfläche

Öffentlichen Schlüssel anhängen

. Damit wird Ihr öffentlicher Schlüssel vor dem Senden als Anhang an diese E-Mail angefügt. Wenn Ihr Kommunikationspartner Ihren öffentlichen Schlüssel bereits importiert hat, ist es normalerweise nicht nötig, den Schlüssel ein weiteres Mal zu versenden.



Bitte beachten Sie dass beim Versand von E-Mails die gewählten Standardeinstellungen verwendet werden, sofern keine davon abweichenden Senderegeln definiert wurden (siehe Kapitel 10).

Hinweis: Achten Sie vor dem Versenden von E-Mails immer darauf, ob diese verschlüsselt werden sollen oder nicht.

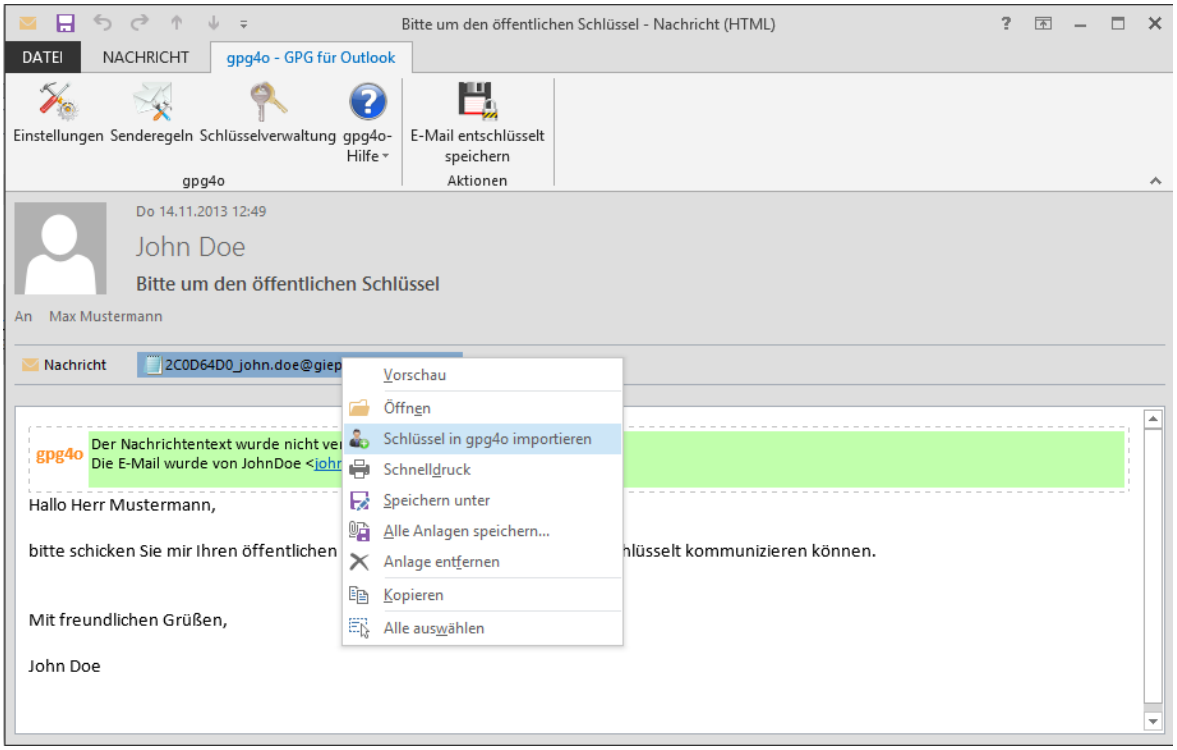
Der öffentliche Schlüssel kann von allen gängigen Verschlüsselungstools importiert werden, die den **OpenPGP**-Standard unterstützen. Er beinhaltet nur den öffentlichen Teil des Schlüsselpaares, nicht den privaten Teil.

7.2 Importieren von öffentlichen Schlüsseln

Wenn Ihnen Ihr Kommunikationspartner einen öffentlichen Schlüssel im Anhang einer E-Mail zusendet, wird Ihnen der Import automatisch angeboten, sobald Sie die E-Mail zur Ansicht öffnen. (siehe Kapitel 11.4.4).

Wird Ihnen der Dialog nicht angezeigt, können Sie den Anhang auch weiterhin mit der rechten Maustaste anklicken und im erscheinenden Kontext-Menü auf den Eintrag Schlüssel in gpg4o importieren klicken, um den Schlüssel in Ihre Schlüsselverwaltung zu

importieren.

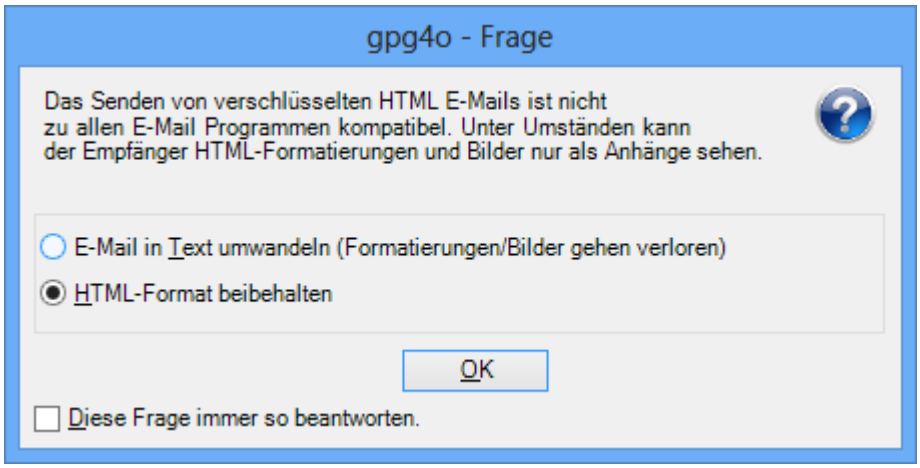


Alternativ haben Sie in der Schlüsselverwaltung die Möglichkeit, den Schlüssel von einem Schlüsselserver zu importieren (siehe Kapitel 8.11).

Sobald Sie den öffentlichen Schlüssel importiert haben, können Sie Nachrichten an diese Person verschlüsselt versenden, als auch von dieser Person empfangene, signierte E-Mails verifizieren. Dieser Austausch des öffentlichen Schlüssels muss einmalig mit jedem Kommunikationspartner erfolgen, mit dem Sie verschlüsselte E-Mails austauschen möchten.

7.3 Versenden von verschlüsselten/signierten Nachrichten

Sie können nun verschlüsselte und/oder signierte E-Mails versenden. Damit größtmögliche Kompatibilität zu allen gängigen E-Mail Programmen gewährleistet werden kann, sollten Sie ihre E-Mails im **„Nur Text“**-Format verfassen. Es besteht natürlich trotzdem die Möglichkeit, E-Mails im HTML-Format zu versenden, wodurch Sie zum Beispiel Grafiken innerhalb eines Textes platzieren können. Eine entsprechende Auswahlmöglichkeit erscheint, sobald Sie die Option Verschlüsseln oder Signieren wählen.

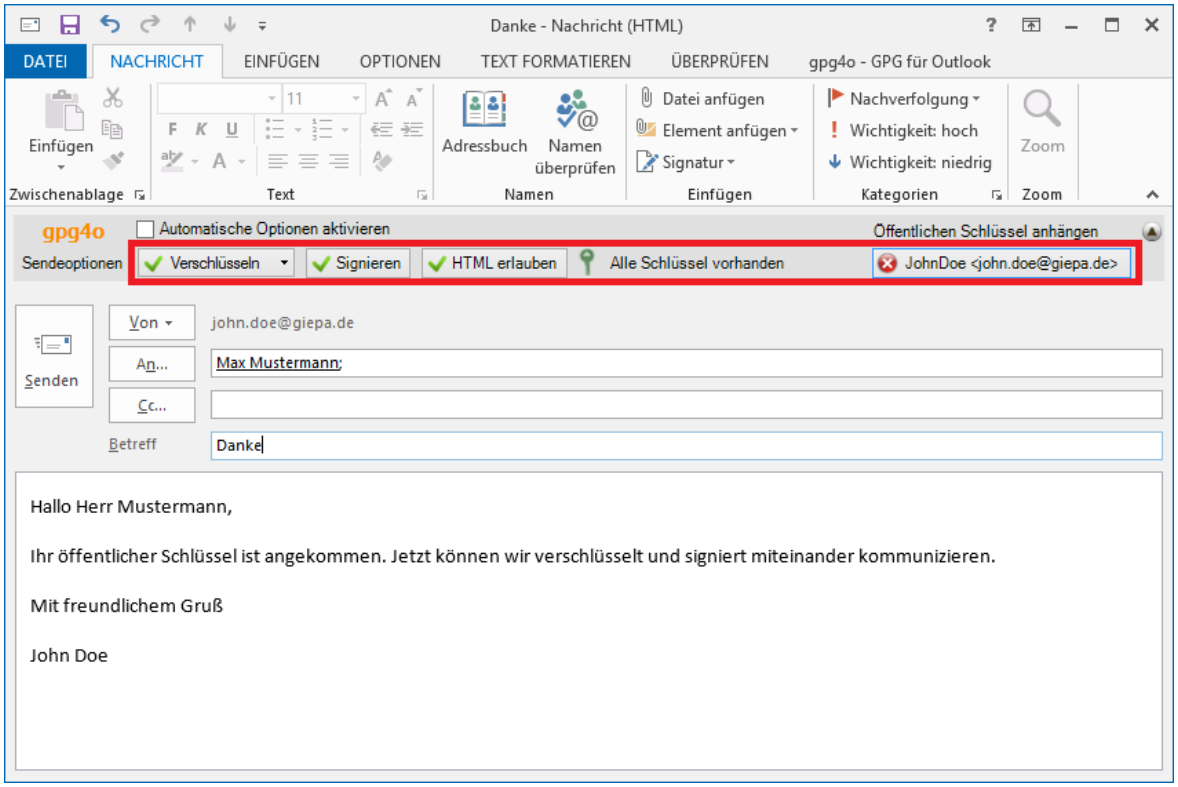


Möchten Sie ihre Auswahl als Standard festlegen, so aktivieren Sie den Haken

Diese Frage immer so beantworten.

Hinweis: In den Konten-Einstellungen (siehe Kapitel 11.3) können Sie diese Option jederzeit wieder ändern.

Wenn Sie eine E-Mail verfassen, werden Ihnen unter dem Menüband die **gpg4o** Sendeoptionen angezeigt.



Hier können Sie festlegen, ob Ihre E-Mail verschlüsselt und/oder signiert werden soll und ob Ihr

öffentlicher Schlüssel an die E-Mail angehängt wird.

Bevor Sie eine E-Mail versenden, aktivieren Sie die Schaltfläche Signieren, wenn Sie diese signiert versenden möchten, oder Verschlüsseln, wenn Sie diese verschlüsselt versenden wollen. Wenn Sie beide Schaltflächen aktivieren, wird Ihre E-Mail verschlüsselt und signiert versendet.

Beachten Sie auch den Zustand Verschlüsseln (nur Anhänge), welcher durch nochmaliges Drücken der Schaltfläche Verschlüsseln ausgewählt wird. Dieser Zustand ist ebenfalls kombinierbar mit Signieren, jedoch wird in diesem Fall die Nachricht nur signiert, während die Anhänge verschlüsselt und signiert werden.

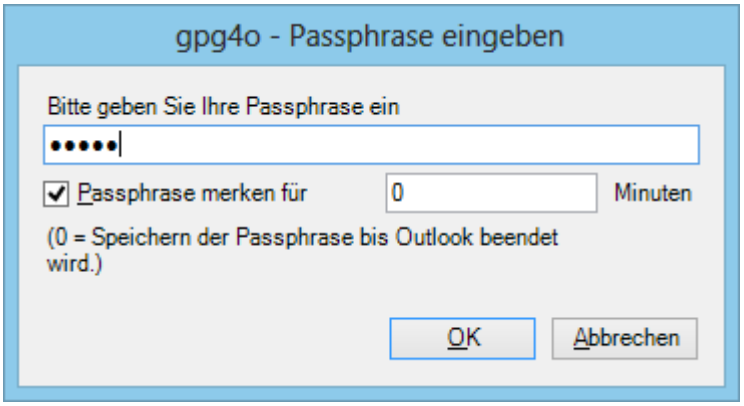
Des weiteren bekommen Sie in der Leiste mit den Sendeoptionen angezeigt, ob Sie alle benötigten öffentlichen Schlüssel für die Empfänger der E-Mail verfügen. Dies geschieht jedoch nur wenn die Sendeoption Verschlüsseln oder Verschlüsseln (nur Anhänge) aktiv ist.

Sind alle öffentlichen Schlüssel für die eingetragenen Empfänger vorhanden, wird dies durch einen grünen Schlüssel in der Leiste symbolisiert. Verfügen Sie nicht über alle öffentlichen Schlüssel, wird Ihnen dies durch einen roten Schlüssel symbolisiert.

Sollten Sie in der Einstellung **„Autoimport“** (siehe Kapitel 11.6.2) einen Schlüsselserver eingetragen haben, dann werden die fehlenden Schlüssel auf dem angegebenen Server gesucht und automatisch in Ihren Schlüsselring importiert.

Wenn Sie die Nachricht vollständig verfasst und die Sendeoptionen gewählt haben, klicken Sie wie gewohnt auf Senden. Sollte es Probleme mit dem Versenden der E-Mail geben, werden Sie mit einer Nachricht darauf hingewiesen.

Wenn Sie ausgewählt haben, dass die Nachricht signiert versendet werden soll, werden Sie nun dazu aufgefordert, Ihre Passphrase (Passwort) einzugeben. Dazu verwenden Sie bitte das Passwort, das Sie bei der Einrichtung von **gpg4o** für Ihren Schlüssel gewählt haben.



Hinweis: Sie werden bei allen Aktionen, die Ihren privaten Schlüssel erfordern, nach Ihrer Passphrase gefragt. Wenn Sie **gpg4o** erlauben, sich die Passphrase zu merken, werden Sie nur dann erneut danach gefragt, wenn seit der letzten Nutzung des privaten Schlüssels die angegebene Zeit verstrichen ist.

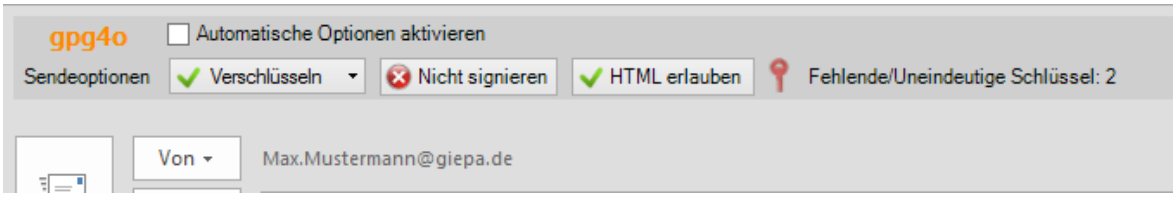
Aktionen, die den privaten Schlüssel benötigen sind:

- Signieren von Nachrichten, Anhängen oder Schlüsseln
- Entschlüsseln von Nachrichten und Anhängen
- Erzeugen von Rückzugszertifikaten
- Ändern der Passphrase
- Identitäten hinzufügen
- Primäre Identität festlegen

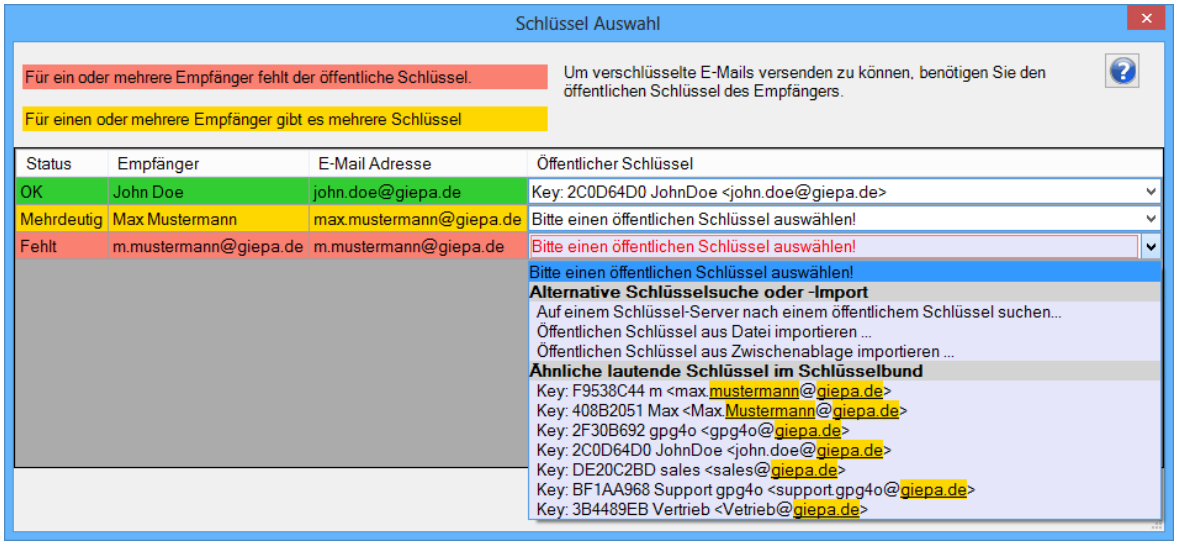
7.3.1 Manuelle Zuordnung der Schlüssel

Beim Erstellen einer verschlüsselten E-Mail wird Ihnen angezeigt, ob für jeden Empfänger ein passender Schlüssel vorhanden ist. Ist ein Autoimport-Schlüsselserver konfiguriert, wird dieser ebenfalls für die Schlüsselsuche herangezogen und dort vorhandene Schlüssel automatisch importiert.

Wird weder im Schlüsselbund noch auf dem Schlüsselserver ein passender Schlüssel gefunden, so wird dies dem Benutzer durch einen roten Schlüssel in den Sendeoptionen visualisiert. Ist der Schlüssel grün, dann wurde für jeden Empfänger ein passender Schlüssel ermittelt.



Durch anklicken des Schlüssel-Symbols oder den erklärenden Text rechts daneben, gelangt man in den Schlüsselauswahl-Dialog. Dort ist es nun möglich eine manuelle Zuordnung von Empfänger zu Schlüssel vorzunehmen.

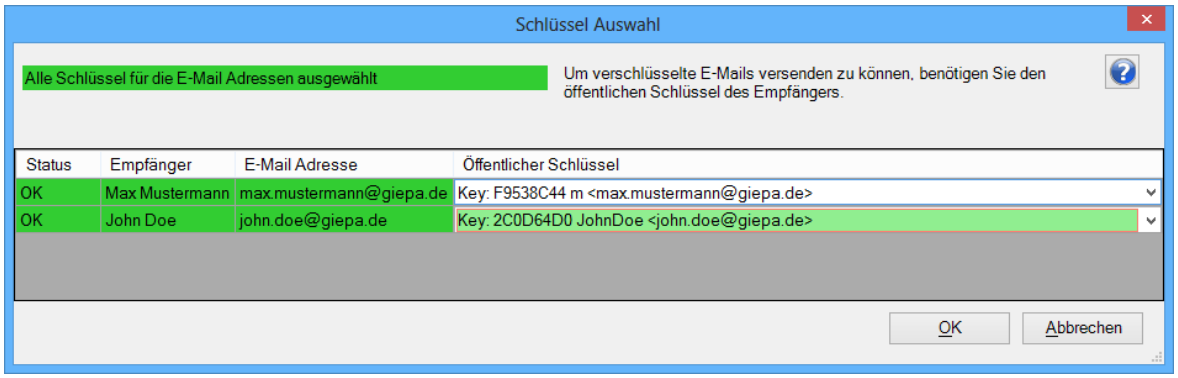


Hier helfen Ihnen die farbigen Hinterlegungen der E-Mail Adressen nach dem Ampelprinzip:

- Grün: Es ist ein passender Schlüssel vorhanden
- Gelb: Es sind mindestens zwei passende Schlüssel vorhanden
- Rot: Es ist kein passender Schlüssel vorhanden

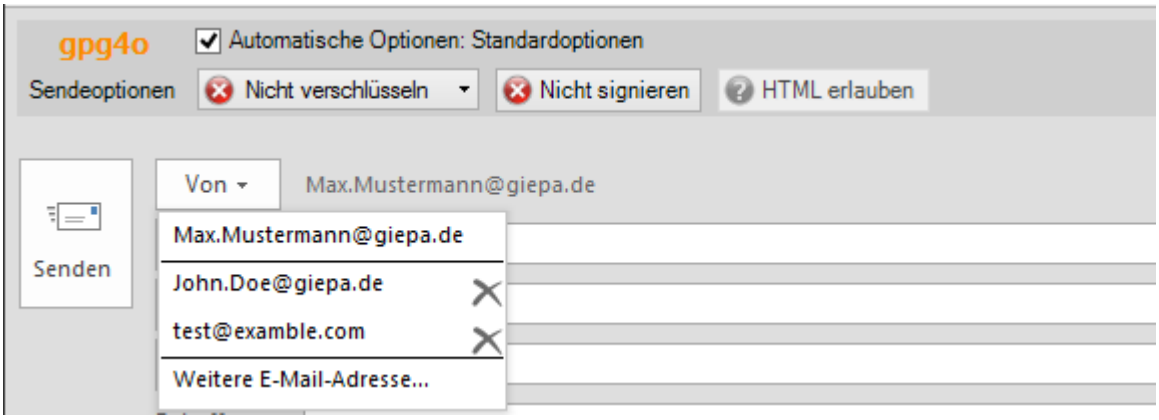
Jetzt können Sie den einzelnen E-Mail Adressen einen passenden Schlüssel zuweisen.

Beim Versand einer verschlüsselten E-Mail an eine Verteilerliste kann entweder der gesamten Liste oder jedem einzelnen Mitglied manuell ein Schlüssel zugewiesen werden.



Wenn Sie jeder E-Mail Adresse ein Schlüssel zugewiesen haben, sind nun alle Zeilen, wie im Bild zu sehen, grün hinterlegt und Sie können den Dialog durch einen Klick auf die Schaltfläche OK verlassen. Die E-Mail kann jetzt verschlüsselt versendet werden.

7.3.2 Virtuelle Konten

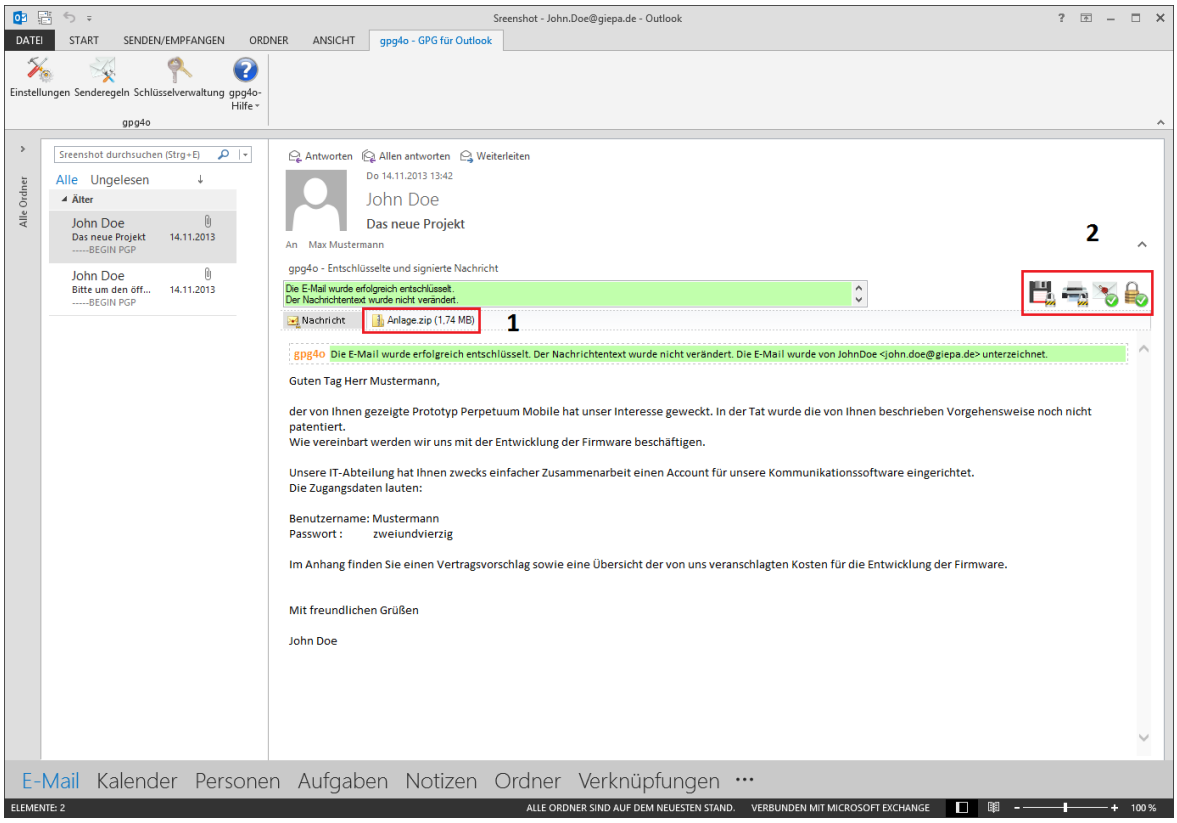


Beim Erstellen einer neuen E-Mail können Sie durch Drücken der Von -Schaltfläche den Absender auswählen. Für jede zusätzlich dort angelegte E-Mail Adresse wird in **gpg4o** ein virtuelles Konto angelegt. Dieses können Sie über die Kontoverwaltung konfigurieren. (siehe Kapitel 11.3) Somit kann jedes virtuelle Konto **gpg4o** benutzen. Die E-Mail Adresse eines virtuelles Kontos kann nicht für die Registrierung einer Lizenz genutzt werden.

Hinweis: Wird im Von Feld eine E-Mail Adresse entfernt, wird das entsprechende virtuelle Konto gelöscht.

7.4 Empfangen von verschlüsselten/signierten Nachrichten

Wenn Sie eine verschlüsselte und/oder signierte E-Mail erhalten, wird unterhalb der Leseansicht ein weiterer Bereich angezeigt. Hier können Sie nun die E-Mails entschlüsselt, beziehungsweise ohne Signatur-Blöcke lesen.



1. *Entschlüsselter Anhang*
2. *Aktionen und Verschlüsselungsstatus*
   - *E-Mail entschlüsselt speichern*
   - *Druckvorschau*
   - *Signiert*
   - *Verschlüsselt / Eingegebene Passphrase vergessen*

Die Symbole zeigen an, ob die E-Mail verschlüsselt oder signiert empfangen wurde. Hier stehen Ihnen bestimmte Aktionen zur Verfügung. Sie können zum Beispiel die Nachricht dauerhaft entschlüsselt speichern oder die Druckvorschau der entschlüsselten Nachricht öffnen (siehe Kapitel 7.5). Klicken Sie dafür einfach auf das jeweilige Symbol.

7.5 Mit entschlüsselten E-Mails arbeiten

7.5.1 Dauerhaft entschlüsselt speichern

Zur einfacheren Archivierung bietet **gpg4o** auch die Möglichkeit, Nachrichten dauerhaft entschlüsselt zu speichern.

Klicken Sie dazu auf das Entschlüsselt speichern Symbol in der Leseansicht von **gpg4o**.

Achtung: Sollte sich die E-Mail in einem synchronisierten Ordner befinden, wird die Nachricht auch auf dem Server lesbar. Benutzen Sie diese Funktion daher mit entsprechender Vorsicht.

Hinweis: Beachten Sie, dass diese Funktionalität nicht mit **gpg4o *Free*** zur Verfügung steht.

7.5.2 Drucken von verschlüsselten Nachrichten

Um eine verschlüsselte Nachricht zu drucken, muss diese zuvor entschlüsselt werden (siehe Kapitel 7.4).

Danach haben Sie zwei Möglichkeiten Ihre entschlüsselte Nachricht zu drucken. Wenn Sie den Lesebereich in Outlook aktiviert haben, können Sie die E-Mail mit einem Klick auf das Druckvorschau Symbol in der Vorschau ausdrucken.

Anderenfalls können Sie die E-Mail auch per Doppelklick öffnen und dort wie gewohnt mit der Tastenkombination Strg + P oder per Datei und Drucken ausdrucken.

Hinweis: In der Testversion ist das Drucken von verschlüsselten Nachrichten nicht über die oben beschriebene Schaltfläche möglich.

7.5.3 Verschlüsselt anzeigen

Die E-Mail wird in verschlüsseltem Zustand angezeigt, so als wäre keine Passphrase für die Entschlüsselung eingegeben worden. Zusätzlich wird die aktuell im Arbeitsspeicher befindliche Passphrase entfernt, so dass diese zur erneuten Entschlüsselung wieder eingegeben werden muss.

7.6 Verschlüsselungsstatus einer E-Mail

Die farbige Box links neben den Aktionssymbolen zeigt Informationen über die Gültigkeit der Signatur und den Status zur Entschlüsselung an.

Für eine schnelle Erfassung des Status, werden vier Farben zur Anzeige verwendet:

- **Grün** bedeutet, dass die E-Mail korrekt entschlüsselt wurde. Wurde die E-Mail signiert, gibt diese Farbe an, dass die Nachricht und eventuell vorhandene Anhänge während der Übermittlung nicht verändert wurden.
- **Türkis** bedeutet, dass der unterschreibende Schlüssel nicht bekannt ist, oder der Schlüssel noch nicht bestätigt/unterschrieben wurde. (siehe Kapitel 8.10.4)
- **Rot** bedeutet, dass die E-Mail nicht entschlüsselt werden konnte oder die Nachricht beziehungsweise ihre Anhänge während der Übermittlung verändert wurden.
- **Gelb** bedeutet, dass die Absender-Adresse nicht in den Identitäten des Schlüssels vorhanden ist.

Zur Ermittlung des Status der Signatur überprüft **gpg4o** nicht nur ob die Nachricht verändert wurde, sondern auch ob der Absender der E-Mail zum unterschreibenden Schlüssel passt. Diese Überprüfung findet anhand der E-Mail Adresse des Absenders und den im unterschreibenden Schlüssel vorhandenen Identitäten statt.

Hinweis: In den Einstellungen haben Sie die Möglichkeit, den Verschlüsselungsstatus in verschiedenen Bereichen von gpg4o anzuzeigen oder auszublenden. Mehr Informationen finden Sie hierzu in Kapitel 11.1.2

7.7 Import unbekannter Schlüssel

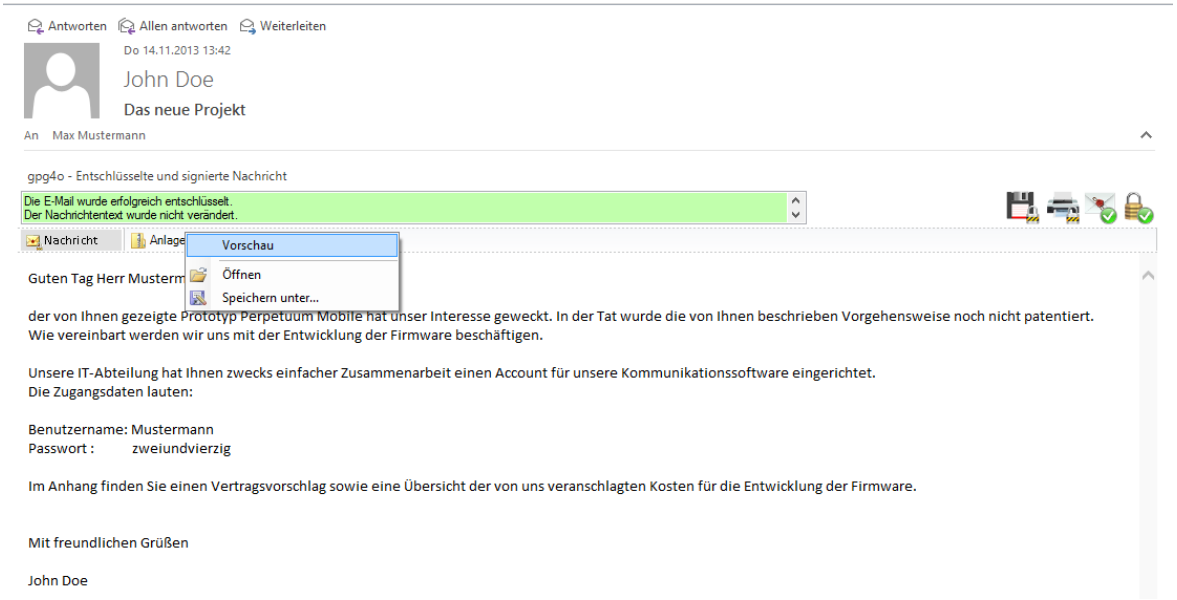
Wird bei Anzeige und Überprüfung einer signierten E-Mail festgestellt, dass kein passender Schlüssel im eigenen Schlüsselbund vorhanden ist, wird dessen Schlüssel-ID angezeigt. Durch Anklicken dieser ID wird der fehlende Schlüssel auf allen **gpg4o** bekannten Schlüsselservern gesucht, die das Protokoll HKP oder HKPS beherrschen. Die Bearbeitung der Schlüsselserver-Liste können Sie in Kapitel 11.6 nachlesen.

Die Schlüssel-ID wird nur angezeigt, wenn Sie den Verschlüsselungsstatus für die E-Mail Vorschau von **gpg4o** aktiviert haben (siehe Kapitel 11.1.2).

7.8 Versenden/Empfangen von verschlüsselten Anhängen

Sobald Sie eine verschlüsselte E-Mail versenden, die einen Anhang enthält, erledigt **gpg4o** den Rest für Sie ganz automatisch. Sie können wie gewohnt Dateien an Ihre E-Mails anhängen, ohne dass Sie sich um Details kümmern müssen. Sobald der Haken bei Verschlüsseln gesetzt ist, werden neben dem Text der E-Mail auch alle Anhänge verschlüsselt.

Wenn Sie eine verschlüsselte E-Mail mit Anhang erhalten haben, können Sie den entschlüsselten Anhang entweder speichern oder direkt öffnen. Dazu stehen Ihnen im Kontextmenü (Rechtsklick auf den Anhang) die Optionen Vorschau, Öffnen und Speichern unter... zur Verfügung.



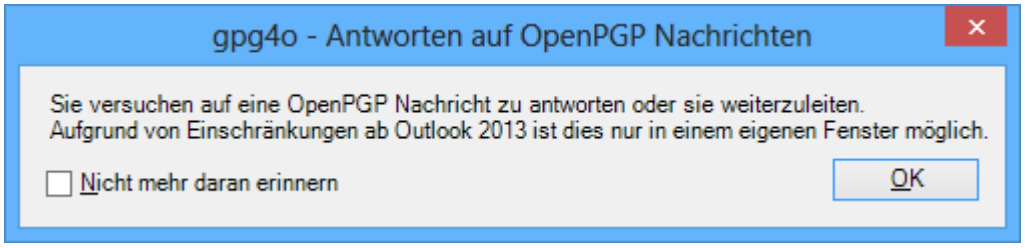
Alternativ können Sie die Anlage auch per Drag and Drop in einem Ordner abspeichern.

Mit der Option Vorschau oder einem einfachen Klick auf den Anhang wird dieser in der Anzeige dargestellt, so wie Sie es von Microsoft Outlook gewohnt sind.

7.9 Antworten/Weiterleiten von E-Mails ab Outlook 2013

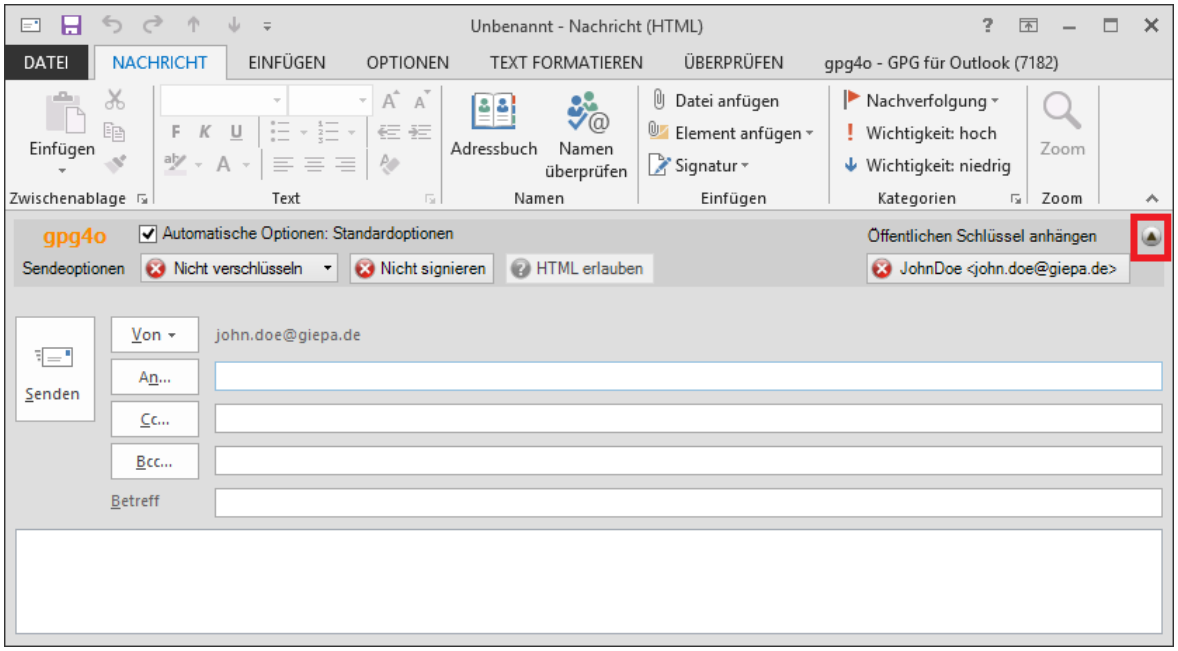
Wenn Sie in Microsoft Outlook 2013 (oder späteren Versionen) auf eine verschlüsselte E-Mail antworten oder diese weiterleiten möchten, öffnet sich die zu schreibende Antwort standardmäßig nicht in einem eigenen Fenster, sondern in einer sogenannten Inline-Antwort.

Leider kann **gpg4o** in diesem Fall die originale Nachricht nicht immer korrekt entschlüsseln. Daher erzwingt **gpg4o** das **„Abdocken“** von Antworten auf verschlüsselte beziehungsweise signierte E-Mails in ein eigenes Fenster. Wenn dieser Fall eintritt, wird **gpg4o** Sie darauf hinweisen.



Wenn Sie nicht erneut darauf hingewiesen werden möchten, setzen Sie den Haken bei Nicht mehr daran erinnern. Über die Schaltfläche OK setzen Sie den Vorgang fort.

7.10 Sendeoptionen verstecken



Um Ihnen mehr Platz für den E-Mail Editor zur Verfügung zu stellen, können Sie die Sendeoptionen verkleinern oder ganz ausblenden.

Ist **gpg4o** zur Verwendung mit einem Konto aktiviert, können Sie die Sendeoptionen über die Schaltfläche mit dem Pfeil, in der rechten oberen Ecke der Leiste, verkleinern und auch wieder vergrößern.

Die Sendeoptionen merken sich den letzten Zustand, so dass sie Ihnen bei Verfassen einer weiteren E-Mail im selben Zustand wie zuvor angezeigt wird.

Ist das Konto nicht zur Verwendung mit **gpg4o** konfiguriert, wird anstelle des Pfeils eine Schaltfläche mit einem X angezeigt. Klicken Sie auf dieses, wird die Leiste versteckt bei inaktiven Konten in Zukunft auch nicht mehr angezeigt.

Sie können dies in den Einstellungen auf der Seite **„Ansicht“** (siehe Kapitel 11.1.3) wieder rückgängig machen.

8 Schlüsselverwaltung

Mit der Schlüsselverwaltung von **gpg4o** können Sie Ihre erzeugten und importierten Schlüssel verwalten, sich alle Details der Schlüssel ansehen, neue Schlüssel erzeugen, alte Schlüssel zurückziehen, Schlüssel löschen und vieles mehr.

8.1 Allgemeine Informationen zu Schlüsseln

Da in der Schlüsselverwaltung oft einige **OpenPGP** spezifische Begriffe verwendet werden, möchten wir Ihnen diese zunächst kurz erläutern.

Jedes **„Schlüsselpaar“** besteht aus einem privaten und einem öffentlichen Schlüssel. Der öffentliche Schlüssel errechnet sich aus dem privaten Schlüssel, umgekehrt ist dies jedoch nicht möglich. Daher besitzen Sie als Schlüsselinhaber immer den öffentlichen und den privaten Schlüssel, Ihre Kommunikationspartner aber nur Ihren öffentlichen Schlüssel.

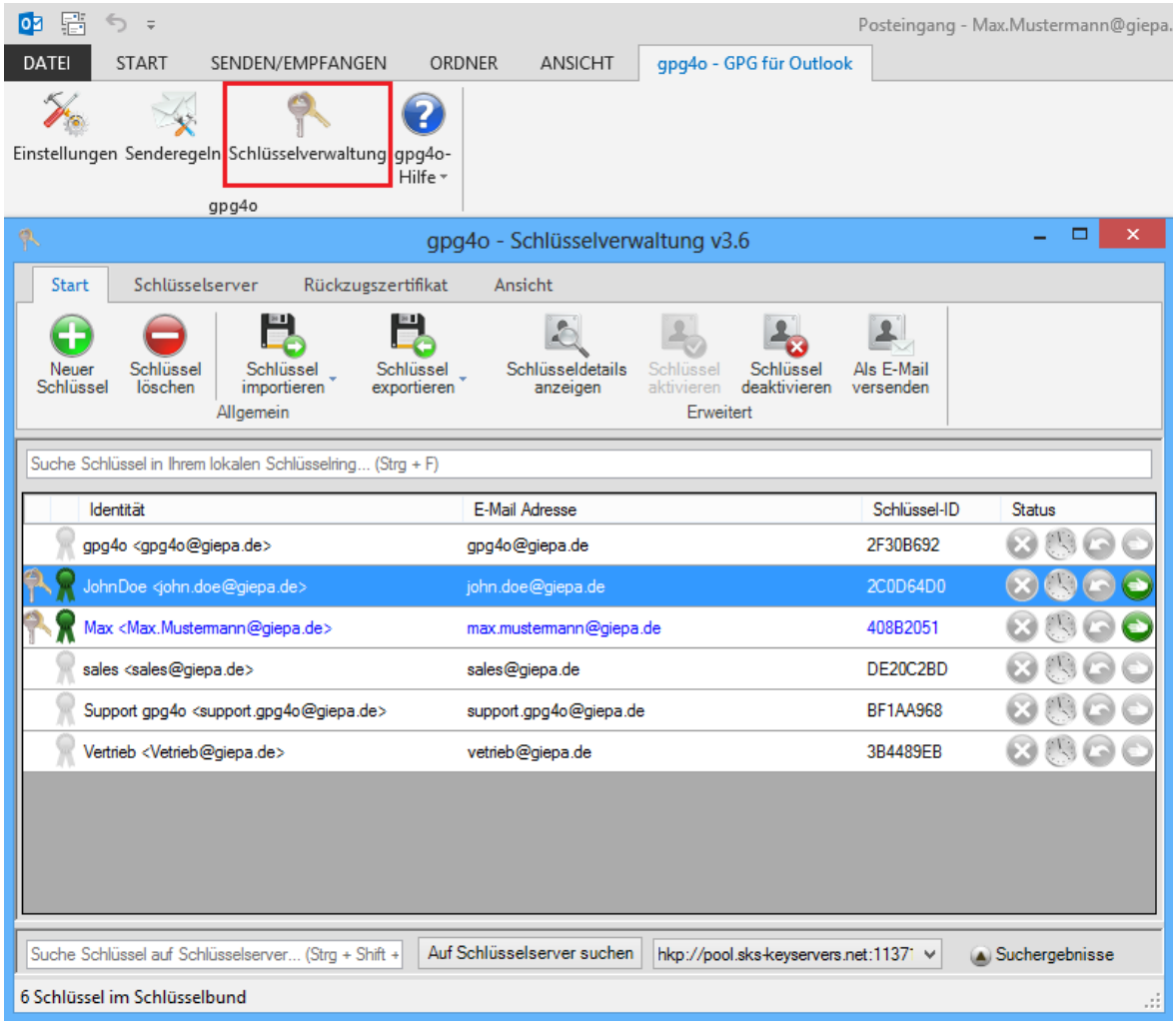
Ihre Kommunikationspartner verschlüsseln Nachrichten an Sie mit Ihrem öffentlichen Schlüssel. Sie entschlüsseln diese E-Mails dann wieder mit ihrem eigenen privaten Schlüssel. Bei Signaturen funktioniert das Prinzip genau umgekehrt. Sie signieren eine Nachricht mit Ihrem eigenen, privaten Schlüssel. Der Empfänger prüft ihre Signatur mit Ihrem öffentlichen Schlüssel.

Jeder Schlüssel enthält einen **„Hauptschlüssel“** und beliebig viele **„Unterschlüssel“**. Wenn Sie einen neuen Schlüssel mit **gpg4o** erzeugen, wird immer ein Hauptschlüssel und immer ein Unterschlüssel erzeugt. Andere **OpenPGP** Anwendungen können allerdings weitere Unterschlüssel erzeugen. Sie werden in **gpg4o** nur der Vollständigkeit halber angezeigt, haben für Sie als Anwender aber kaum eine Bedeutung. **GnuPG** wählt in der Regel automatisch den benötigten Schlüssel für die jeweilige Operation aus.

Zudem wird ein Schlüssel mit einer oder mehreren **„Benutzer-ID(s)/Identität(en)“** versehen, welche einer für Menschen lesbaren Darstellung des Schlüssels entspricht. Solch eine Benutzer-ID besteht üblicherweise aus dem vollständigen Namen des Inhabers und seiner E-Mail Adresse. Weil ein Schlüssel mehr als eine Benutzer-ID haben kann, kann er auch für mehrere E-Mail Adressen verwendet werden.

8.2 Übersicht

Um die Schlüsselverwaltung von **gpg4o** zu öffnen, klicken Sie bitte im Menüband von Microsoft Outlook auf `gpg4o - GPG für Outlook` und dann auf `Schlüsselverwaltung`.

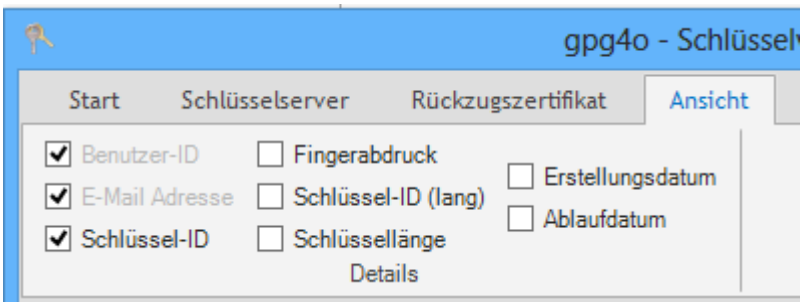


In der Übersicht sehen Sie alle Schlüssel, die in Ihrem Schlüsselring enthalten sind. Sowohl Ihre eigenen, als auch importierte Schlüssel werden Ihnen hier angezeigt.

Die meisten Aktionen können über mehrere Wege erreicht werden. Die zwei wichtigsten Methoden, um eine Aktion auszuführen sind das Menüband im oberen Bereich der Schlüsselverwaltung und das Kontextmenü, welches Sie über einen Rechtsklick auf den/die selektierten Schlüssel erhalten.

Außerdem können viele Aktionen auch auf mehrere Schlüssel gleichzeitig angewendet werden. Selektieren Sie dazu einfach mehrere Schlüssel, indem Sie bei gedrückter Strg Taste weitere Schlüssel an- oder abwählen.

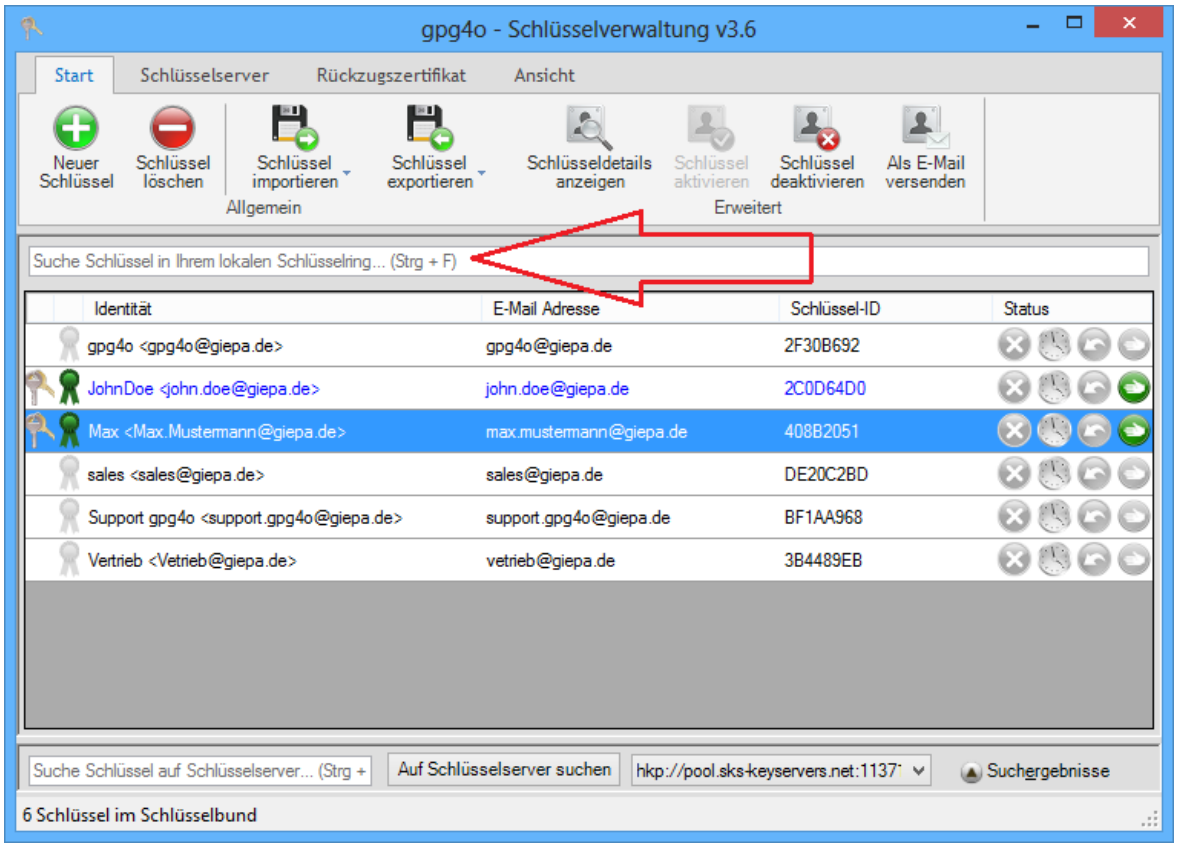
8.3 Ansicht ändern



Im Menüband der Schlüsselverwaltung können Sie unter Ansicht einstellen, welche Spalten Sie ein- beziehungsweise ausblenden möchten.

Zudem sind die Spalten sortierbar. Wenn Sie die Ansicht anhand einer Spalte sortieren möchten, klicken Sie einfach auf die Spaltenüberschrift. Jeder weitere Klick auf die gleiche Spalte kehrt die Sortierung um.

8.4 Schlüssel filtern

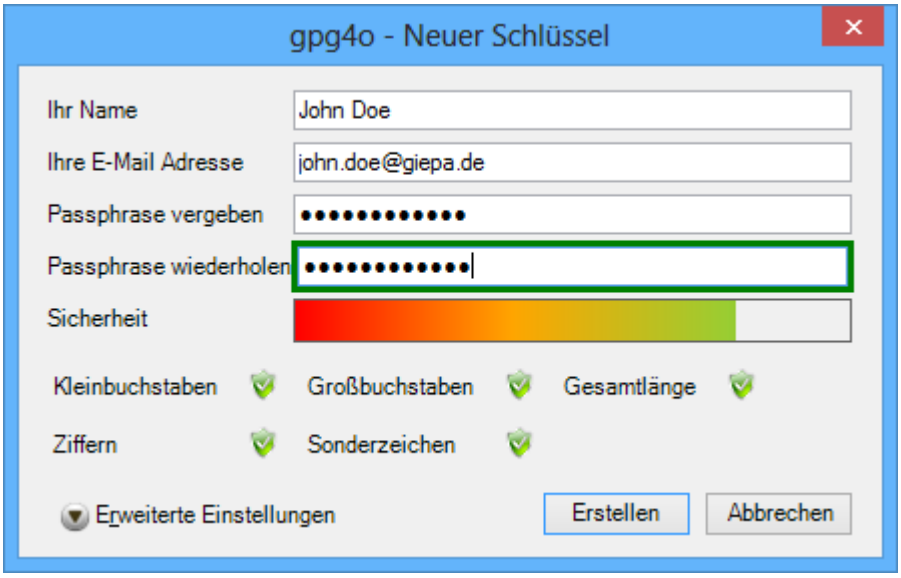


Außerdem haben Sie die Möglichkeit, die Ansicht der Schlüssel zu filtern. Geben Sie dazu einen Suchbegriff in das Feld **„Suche Schlüssel in Ihrem lokalen Schlüsselring...“** ein,

um nur noch passende Schlüssel anzuzeigen. Solch ein Suchbegriff kann zum Beispiel eine E-Mail Adresse oder ein Name sein, oder auch nur ein Teil davon.

8.5 Neue Schlüssel erzeugen

Um ein weiteres Schlüsselpaar zu erzeugen, klicken Sie bitte im Menüband Start auf Neuer Schlüssel. Im darauf erscheinenden Dialog geben Sie bitte die benötigten Daten ein, wie Sie es auch bei der Einrichtung von **gpg4o** gemacht haben.



Wenn Sie weitere Optionen wie das Ablaufdatum für den neuen Schlüssel setzen möchten, klicken Sie bitte auf Erweiterte Einstellungen. Sobald Sie alle benötigten Daten eingegeben haben, klicken Sie auf Erstellen.

Hinweis: Die Erzeugung des Schlüsselpaares kann einen Moment dauern.

8.6 Schlüssel löschen

Um einen Schlüssel zu löschen, selektieren Sie diesen und drücken im Menüband Start auf Schlüssel löschen. Alternativ können Sie die Taste Entf drücken.

Achtung: Durch das Löschen eines privaten Schlüssels verlieren Sie dauerhaft den Zugriff auf Ihre verschlüsselten E-Mails! Ohne die passenden Schlüssel können Ihre E-Mails nicht entschlüsselt werden.
Beachten Sie, dass das Löschen eines Schlüssels nicht rückgängig gemacht werden kann. Sie können jedoch einen zuvor exportierten Schlüssel wieder importieren.

Hinweis: Wenn Sie ein Schlüsselpaar löschen, wird sowohl der private als auch der öffentliche Schlüssel gelöscht. Wenn das zu löschende Schlüsselpaar in den **gpg4o** Einstellungen für ein Konto hinterlegt ist, wird diese Einstellung ungültig. In diesem Fall wird **gpg4o** nach dem Löschen den Einstellungen-Dialog öffnen, damit Sie ein anderes Schlüsselpaar auswählen oder dieses Konto deaktivieren können.

8.7 Schlüssel aktivieren/deaktivieren

Wenn Sie einen Schlüssel deaktivieren, wird er nicht mehr zum Verschlüsseln genutzt. Dies ist sinnvoll, wenn Sie mehr als einen öffentlichen Schlüssel für die gleiche E-Mail Adresse eines Kontaktes haben, Sie aber nur einen der öffentlichen Schlüssel zum Verschlüsseln nutzen. Alle weiteren Aktionen bleiben hiervon unberührt.

Um einen oder mehrere Schlüssel zu deaktivieren, wählen Sie diese aus und klicken im Menüband auf die Schaltfläche Schlüssel deaktivieren. Umgekehrt können Sie zuvor deaktivierte Schlüssel über die Schaltfläche Schlüssel aktivieren wieder aktivieren.

Hinweis: Wenn das zu deaktivierende Schlüsselpaar in den **gpg4o** Einstellungen für ein Konto hinterlegt ist, wird diese Einstellung ungültig. In diesem Fall wird **gpg4o** nach dem Deaktivieren den Einstellungen-Dialog öffnen, damit Sie ein anderes Schlüsselpaar auswählen können.

8.8 Schlüssel exportieren

Abgesehen vom Versenden Ihres eigenen öffentlichen Schlüssels (siehe Kapitel 7.1) können Sie Ihre eigenen Schlüssel, beziehungsweise die Ihrer Kontakte, auch in der Schlüsselverwaltung exportieren.

Wählen Sie dazu den/die zu exportierenden Schlüssel aus und klicken im Menüband auf Schlüssel exportieren. In dem darauf eingeblendeten Menü können Sie den Export in eine Datei durchführen oder den gewählten Schlüssel in die Zwischenablage exportieren.

Ein Export in die Zwischenablage ist sinnvoll, wenn Sie den/die Schlüssel in ein anderes Programm übertragen, auf einer Webseite oder einem Beitrag im Internet veröffentlichen möchten, ohne dabei eine Datei verwenden zu können.

Ein Export in das Dateisystem ist sinnvoll, wenn Sie den/die Schlüssel zu einem anderen Computer oder auf Ihr Smartphone übertragen möchten.

Haben Sie Schlüssel in Datei exportieren... gewählt, werden Sie gefragt, wo Sie die Schlüssel abspeichern möchten. Sobald Sie einen Ordner gewählt haben, in dem diese gespeichert werden sollen, klicken Sie bitte auf OK.

Haben Sie Schlüssel in die Zwischenablage exportieren angeklickt, befinden sich die gewählten Schlüssel kurz darauf in der Zwischenablage von Windows und Sie können diese mit der Tastenkombination Strg + V in ein beliebiges Textfeld einfügen.

Sollte einer der ausgewählten Schlüssel ein Schlüsselpaar sein (Sie im Besitz des privaten Schlüssels sind), werden Sie gefragt, ob Sie nur den öffentlichen Schlüssel exportieren möchten, oder auch den privaten Schlüssel. Diese Auswahl wird für alle Schlüsselpaare der Selektion übernommen.

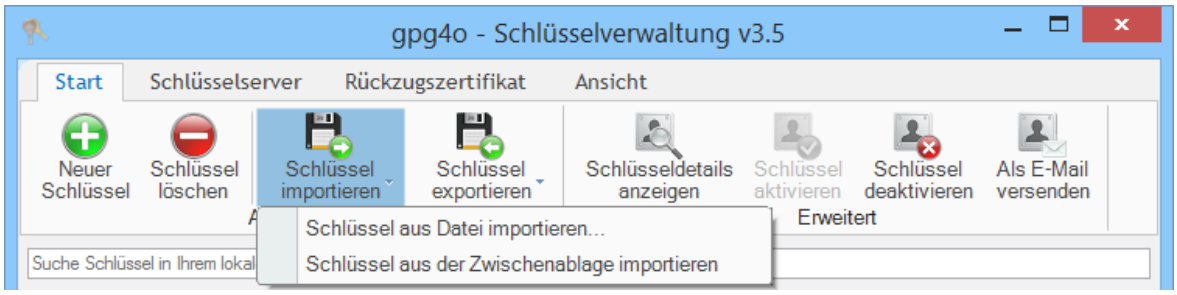
Achtung: Sie sollten niemals Ihren privaten Schlüssel an andere Personen weitergeben. Nutzen Sie diese Funktion also nur als Datensicherung oder zum Transport Ihres Schlüsselpaares zu einem anderen Computer.

Tipp: Sie können Schlüssel auch per Drag and Drop ins Dateisystem oder in eine E-Mail exportieren.

8.9 Schlüssel importieren

Sie können in der Schlüsselverwaltung auch Schlüssel importieren. Klicken Sie dazu im Menüband die Schaltfläche Schlüssel importieren, und wählen die Option

Schlüssel aus Datei importieren... oder Schlüssel aus der Zwischenablage importieren aus um einen Schlüssel zu importieren.

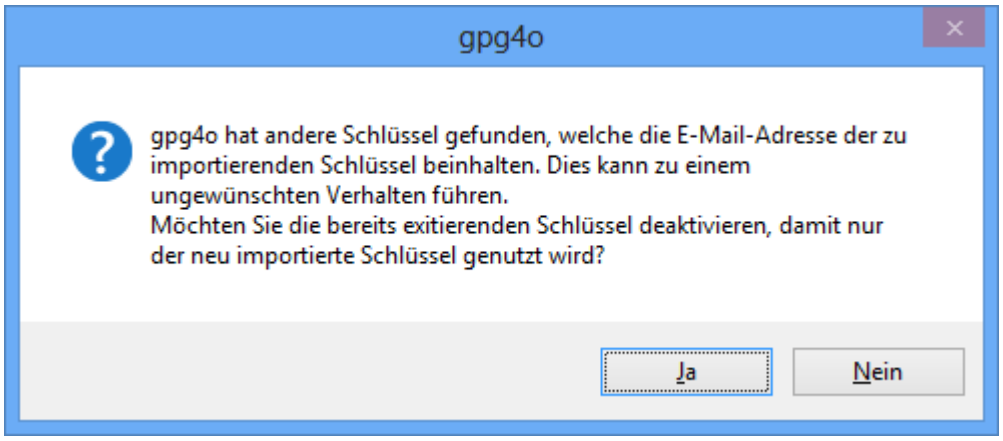


Öffentliche Schlüssel können in Textform auf Webseiten im Internet veröffentlicht werden. Um diese in Ihren Schlüsselring zu importieren, markieren Sie den Text und kopieren Ihn mit Strg + C in die Zwischenablage. Danach können Sie diesen ganz einfach über den Eintrag Schlüssel aus der Zwischenablage importieren importieren und verwenden.

Wenn Sie Schlüssel aus Datei importieren... ausgewählt haben, wird Ihnen ein Dialog zur Dateiauswahl angeboten, über den Sie den Schlüssel suchen können. Der so ausgewählte Schlüssel wird mit der Schaltfläche OK importiert.

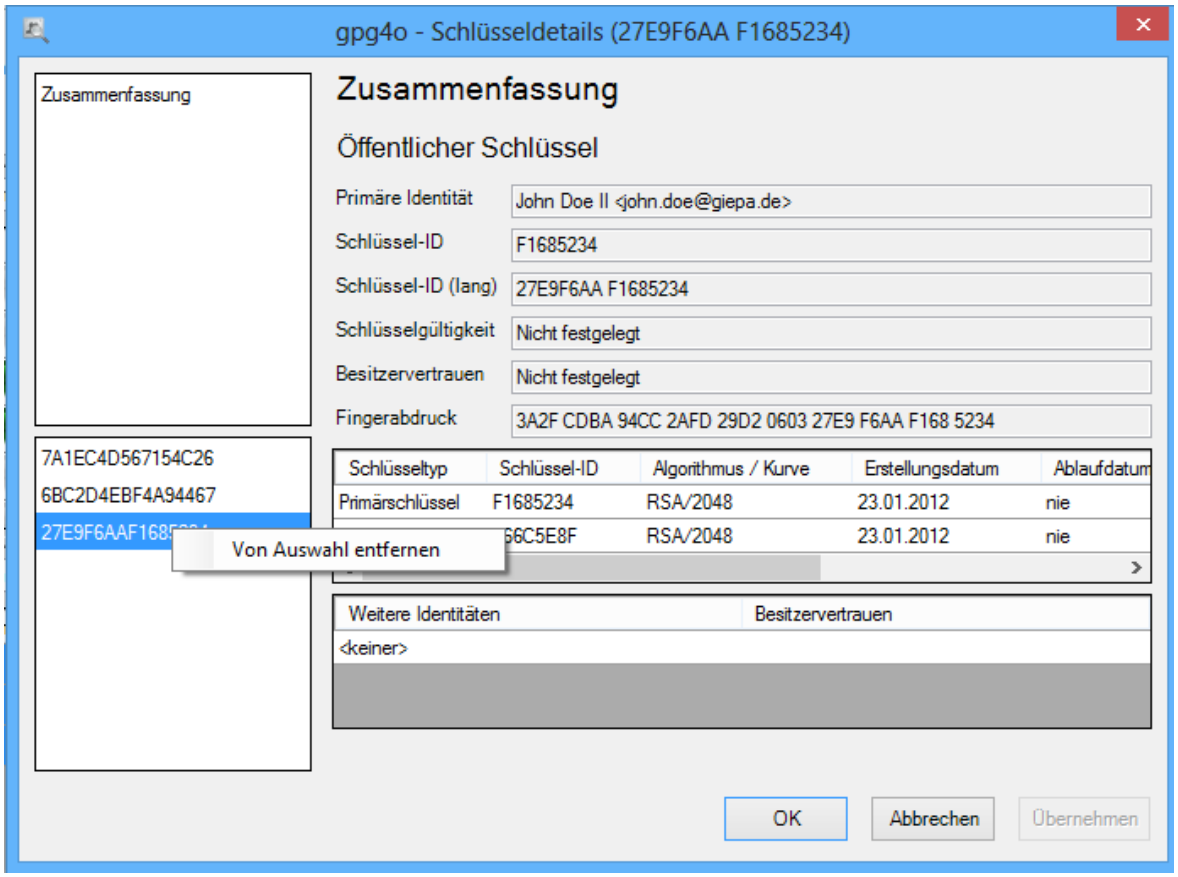
Tipp: Sie können Schlüssel auch per Drag and Drop aus dem Dateisystem importieren, indem Sie die Datei in die Liste ziehen.

Sollte einer der zu importierenden Schlüssel für eine E-Mail Adresse ausgestellt sein, zu der Sie schon einen Schlüssel importiert haben, werden Sie sicherheitshalber nochmal gefragt, ob Sie den bereits existierenden Schlüssel zuvor deaktivieren möchten.



Wenn es sich um den gleichen Schlüssel handeln sollte, brauchen Sie keine Bedenken zu haben, da Unterschiede der Schlüssel automatisch zusammengeführt werden.

Anschließend erscheint eine Übersicht über die zu importierenden Schlüssel, welche alle nötigen Informationen beinhaltet.



Hier können Sie gegebenenfalls noch einzelne Schlüssel vom Import ausschließen, indem Sie den entsprechenden Schlüssel rechtsklicken und Von Auswahl entfernen auswählen. Außerdem können Sie auch das Besitzervertrauen für die zu importierenden Schlüssel festlegen (siehe auch Kapitel 8.10.6). Klicken Sie dazu zuerst auf den Menüpunkt **„Besitzervertrauen“** und wählen dort das neue Besitzervertrauen für die Schlüssel aus.

Achtung: Bitte stellen Sie sicher, dass der zu importierende Schlüssel wirklich von der Person stammt, die als Schlüsselbesitzer angegeben ist. Nehmen Sie Kontakt zur dieser Person auf und fragen Sie nach deren Fingerabdruck des Schlüssels um absolut sicher zu sein. Lesen sie hierzu bitte Kapitel 8.10.4.

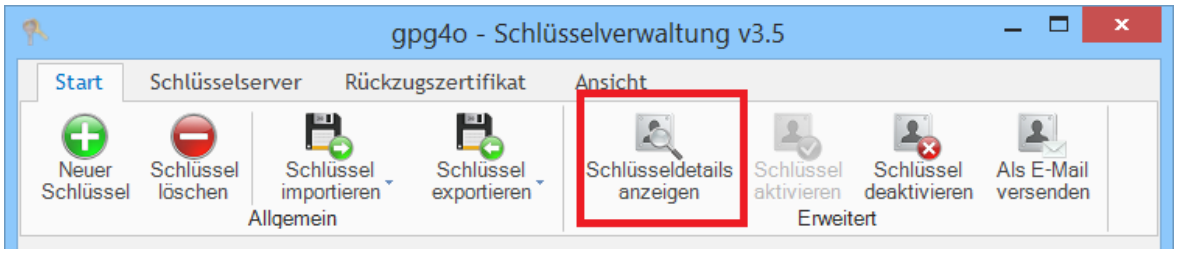
Um den Import des/der Schlüssel(s) abzuschließen, klicken Sie auf Import abschließen.

Im Anschluss an den Import können Sie dessen Identitäten bestätigen. Andere können so erkennen, dass Sie die Zugehörigkeit des Schlüssels zur Person überprüft haben. Weitere Informationen dazu finden Sie in Kapitel 8.10.4

8.10 Schlüsseldetails

Um sich einen oder mehrere Schlüssel im Detail anzusehen, können Sie im Menüband Start auf Schlüsseldetails anzeigen klicken, oder einen Rechtsklick auf den/die selektier-

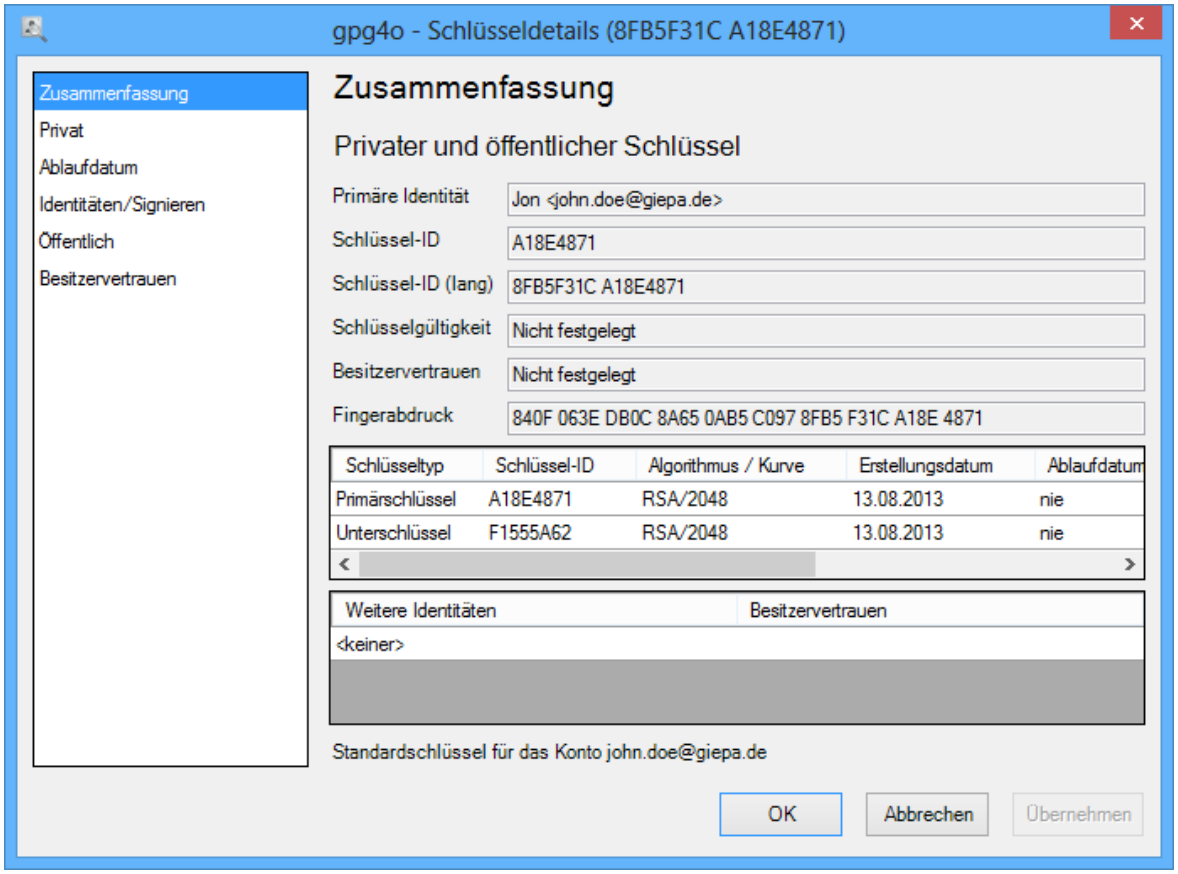
ten Schlüssel machen und im Kontextmenü auf Details... klicken.



Die Schlüsseldetails sind in mehrere Bereiche unterteilt, welche links im Menü aufgelistet sind. Der Bereich **„Privat“** ist nur bei Schlüsselpaaren sichtbar. Um in einen anderen Bereich zu wechseln, klicken Sie einfach auf den Namen des Bereiches.

8.10.1 Zusammenfassung

Auf der Seite **„Zusammenfassung“** sehen Sie die wichtigsten Informationen zu dem ausgewählten Schlüssel. Die **„Schlüssel-ID“** und der **„Fingerabdruck“** identifizieren den Schlüssel, wobei die Schlüssel-ID eine Kurzform des Fingerabdrucks ist. Der Fingerabdruck sollte beim Austausch der Schlüssel abgeglichen werden, am besten per Telefon (siehe auch Kapitel 8.10.4).



Außerdem werden das **„Besitzervertrauen“** und die **„Schlüsselgültigkeit“** angezeigt. Das Besitzervertrauen können Sie selbst festlegen (siehe Kapitel 8.10.6), die Schlüsselgültigkeit wird anhand von schon vorhandenen Signaturen und dem Besitzervertrauen der Unterzeichner ermittelt.

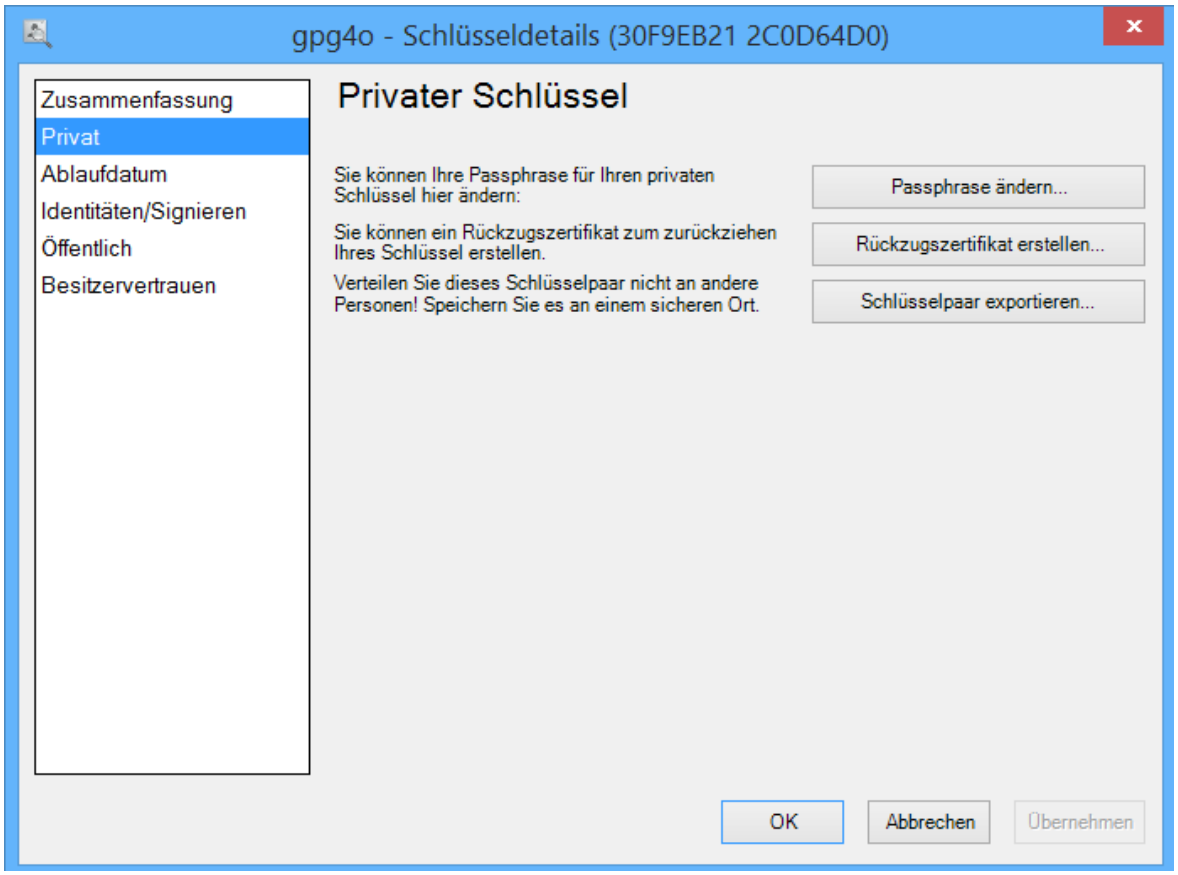
Unter der Schlüsselgültigkeit versteht man, ob ein Schlüssel durch eigene Signaturen oder die von vertrauten Schlüsseln als gültig markiert wurde. Hier spielt also auch das **„Web of Trust“** eine große Rolle.

Ein Schlüssel ist dann gültig, wenn er

- Von einem Ihrer eigenen Schlüssel signiert wurde
- Von einem anderen Schlüsselinhaber signiert wurde, dem Sie das vollständige Vertrauen ausgesprochen haben
- Von mindestens drei anderen Schlüsselinhabern signiert wurde, denen Sie ein marginales Vertrauen ausgesprochen haben

8.10.2 Privater Schlüssel

Wenn Sie in den Details eines Schlüsselpaares den Bereich **„Privat“** öffnen, können Sie die Passphrase des Schlüssels ändern, ein Rückzugszertifikat erzeugen oder das komplette Schlüsselpaar sichern.



Achtung: Geben Sie die Datensicherung mit Ihrem privaten Schlüssel oder das Rückzugszertifikat **an niemanden** weiter.

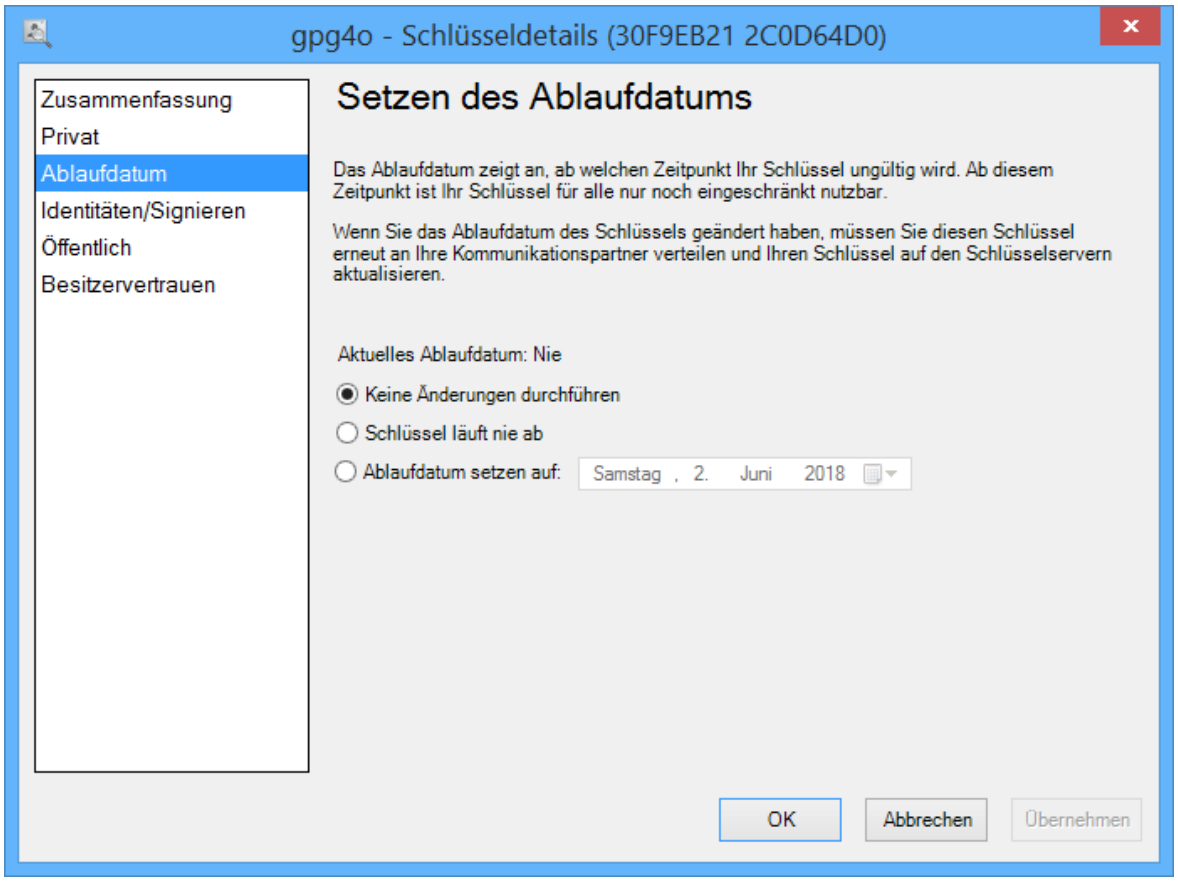
8.10.3 Ablaufdatum

Wenn ein Schlüsselpaar mit einem Ablaufdatum versehen wurde und dieses Datum verstrichen ist, können Ihre Kommunikationspartner diesen nicht mehr zur Verschlüsselung verwenden und Ihnen somit keine verschlüsselten E-Mails mehr schreiben.

Dies ist für den Fall hilfreich, wenn Sie die Passphrase eines Schlüsselpaares verloren haben und kein Rückzugszertifikat besitzen. (siehe Kapitel 8.12)

Hinweis: Wenn Sie einem Schlüsselpaar ein Ablaufdatum zuweisen, müssen Sie dieses Datum regelmäßig ändern und den aktualisierten öffentlichen Schlüssel Ihren Kommunikationspartnern zukommen lassen.

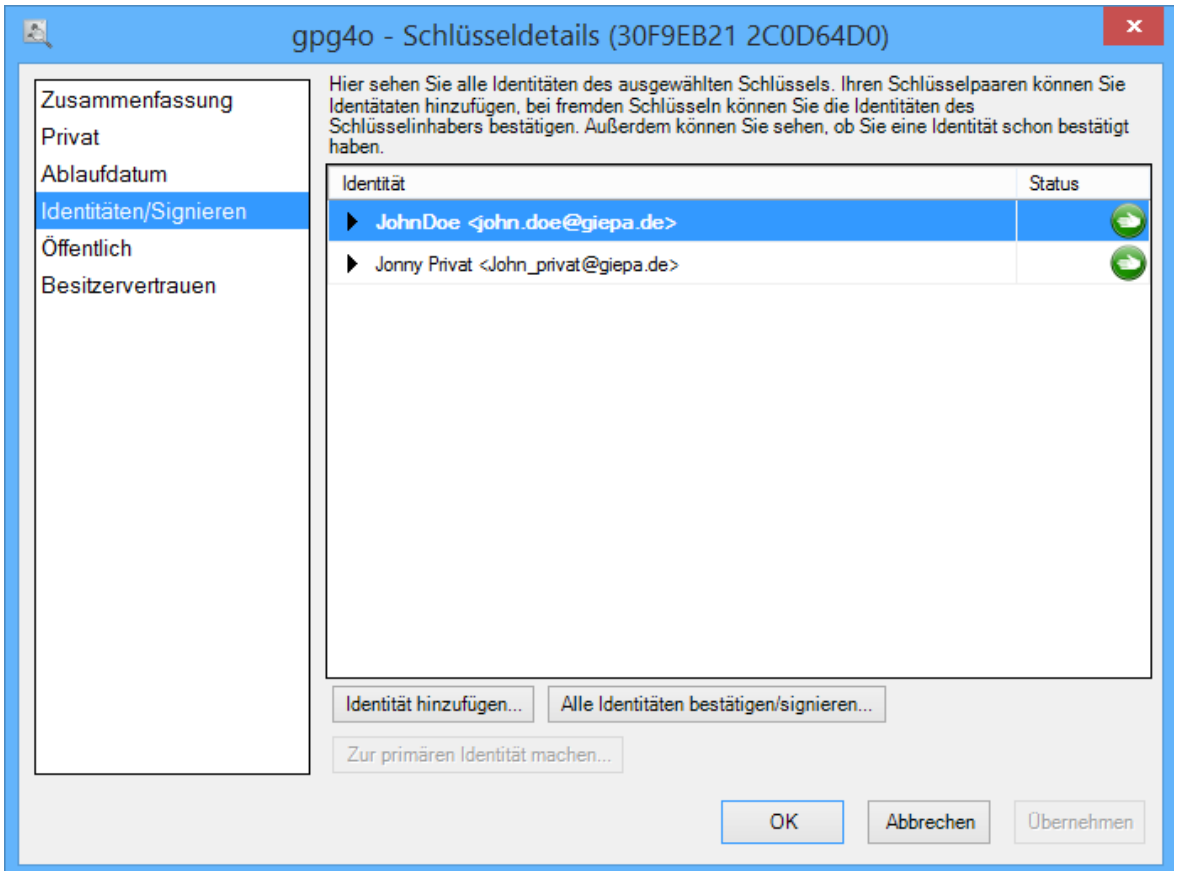
Sie können hier jedoch auch ein vorhandenes Ablaufdatum entfernen, indem Sie die Option Schlüssel läuft nie ab auswählen. Ihr Schlüsselpaar bleibt dann unbegrenzt lange zur Verschlüsselung fähig.



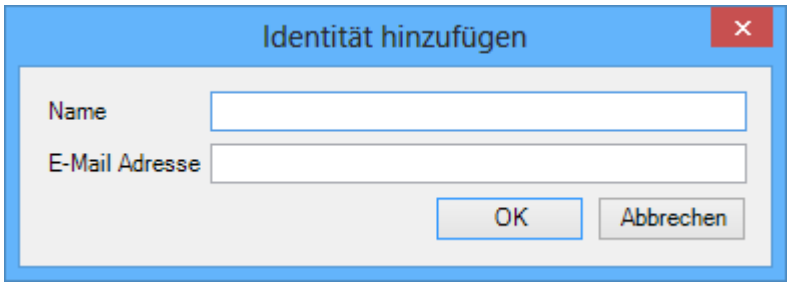
8.10.4 Identitäten/Signieren

Auf dieser Seite werden Ihnen alle im Schlüssel vorhandenen Identitäten (Benutzer-IDs) angezeigt. Bei Schlüsselpaaren können Sie Identitäten hinzufügen oder eine Haupt-Identität auswählen. Des weiteren können Sie hierüber Identitäten öffentlicher Schlüssel bestätigen (signieren, unterschreiben) und Schlüssel somit als gültig markieren.

Schlüssel können von jedermann mit beliebigen Namen und E-Mail Adressen erstellt werden. Es ist daher erforderlich, dass Sie vor der ersten Verwendung überprüfen, dass der Schlüssel wirklich von der angegebenen Person stammt. Details zur Vorgehensweise finden Sie nachfolgend.

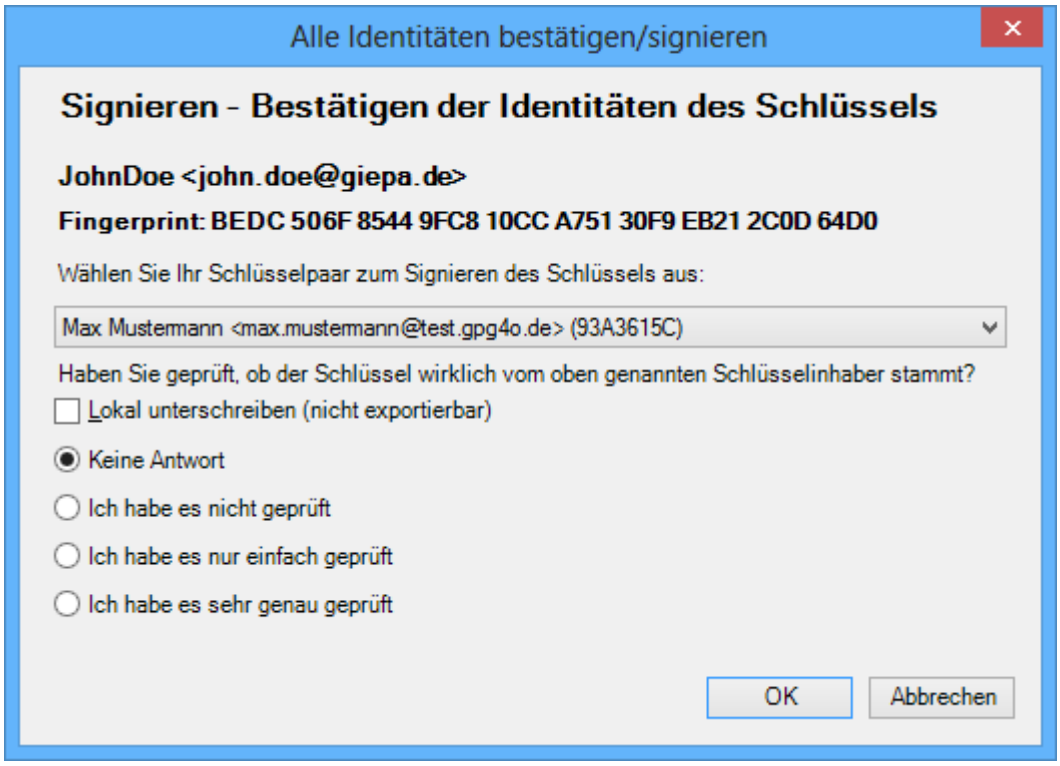


Eine neue Identität fügen Sie einem Schlüsselpaar hinzu, indem Sie auf die Schaltfläche Identität hinzufügen... klicken und in dem darauf folgenden Dialog den Namen und die E-Mail Adresse der zusätzlichen Identität eingeben. Durch klick auf OK wird diese dem Schlüssel hinzugefügt.



In der Regel wird in allen Programmen die mit GnuPG arbeiten, die primäre Identität dargestellt, wenn ein Schlüssel angezeigt wird. Mit der Funktion Zur primären Identität machen... können Sie die aktuell gewählte Identität in Ihrem Schlüssel zur primären machen, so dass in Zukunft nur noch diese angezeigt wird.

Wenn Sie einen öffentlichen Schlüssel und dessen Identitäten bestätigen möchten, klicken Sie auf die Schaltfläche Alle Identitäten bestätigen/signieren... .

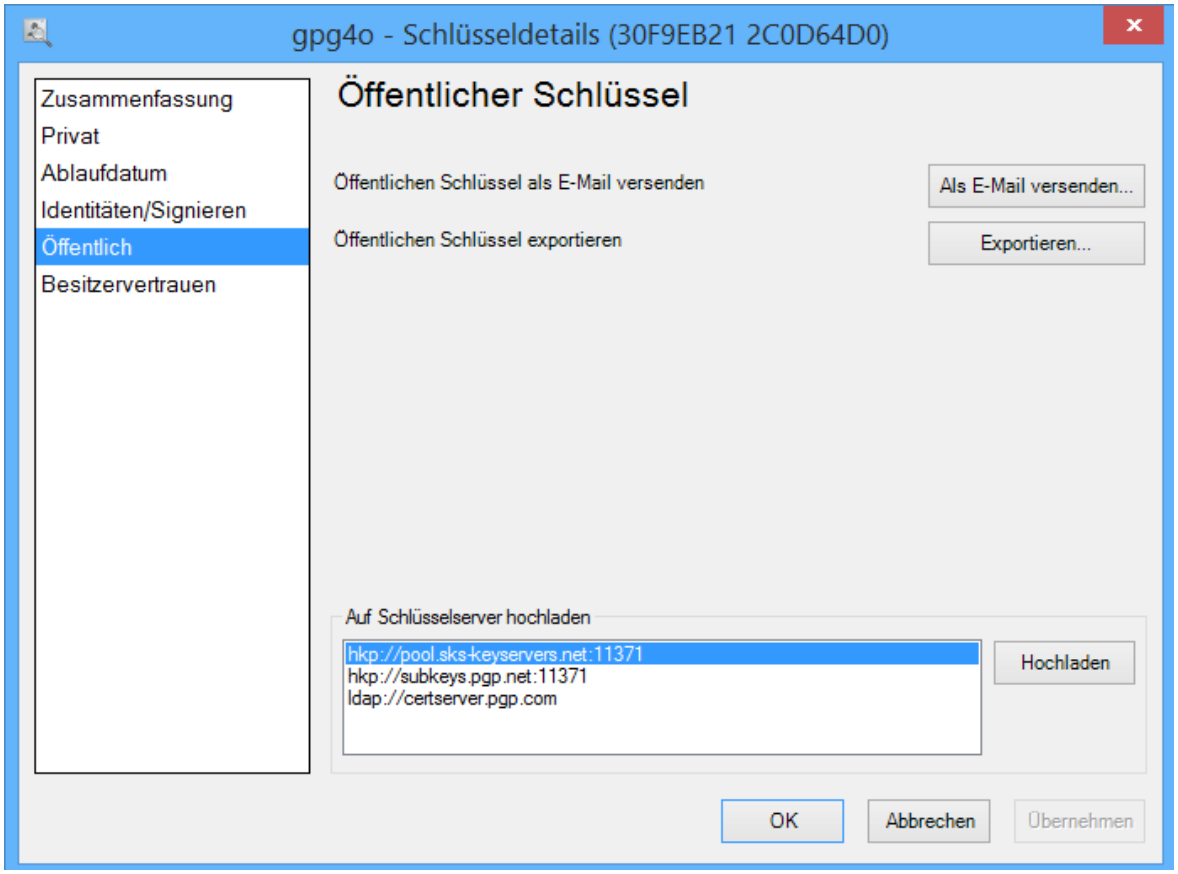


In diesem Dialog legen Sie zuerst fest, mit welchem Ihrer Schlüsselpaare Sie die Identitäten bestätigen möchten. Danach geben Sie an, wie sicher Sie sich über die Echtheit des zu unterschreibenden Schlüssels sind. Durch diese Auswahl wird die Stärke der Unterschrift (Signatur) festgelegt. Mit einem Klick auf OK wird die Signatur auf den Schlüssel angewendet.

Hinweis: Um sich ganz sicher zu sein, dass der Schlüssel wirklich von der Person ausgestellt wurde, für die sie sich ausgegeben hat, sollten Sie mindestens den Fingerabdruck mit dieser Person persönlich abgleichen.
Sie können den Ersteller per Telefon, Fax, SMS, Messenger, ... kontaktieren und miteinander den Fingerabdruck vergleichen. E-Mails sind für die Verifizierung ungeeignet, da sie über eine **„Man-in-the-Middle“** Attacke gefälscht werden können.
Nur wenn der vorliegende Fingerabdruck mit dem übereinstimmt, den Ihnen der Erstellers nennt, haben den selben Schlüssel erhalten und können diesen nutzen.
Unterscheidet sich der Fingerabdruck, wurde Ihnen ein gefälschter Schlüssel untergeschoben. In diesem Fall signieren und verwenden Sie diesen Schlüssel bitte nicht!

8.10.5 Öffentlicher Schlüssel

Auf dieser Seite stehen Ihnen Möglichkeiten zur Verfügung, mit denen Sie Ihren öffentlichen Schlüssel verteilen können.



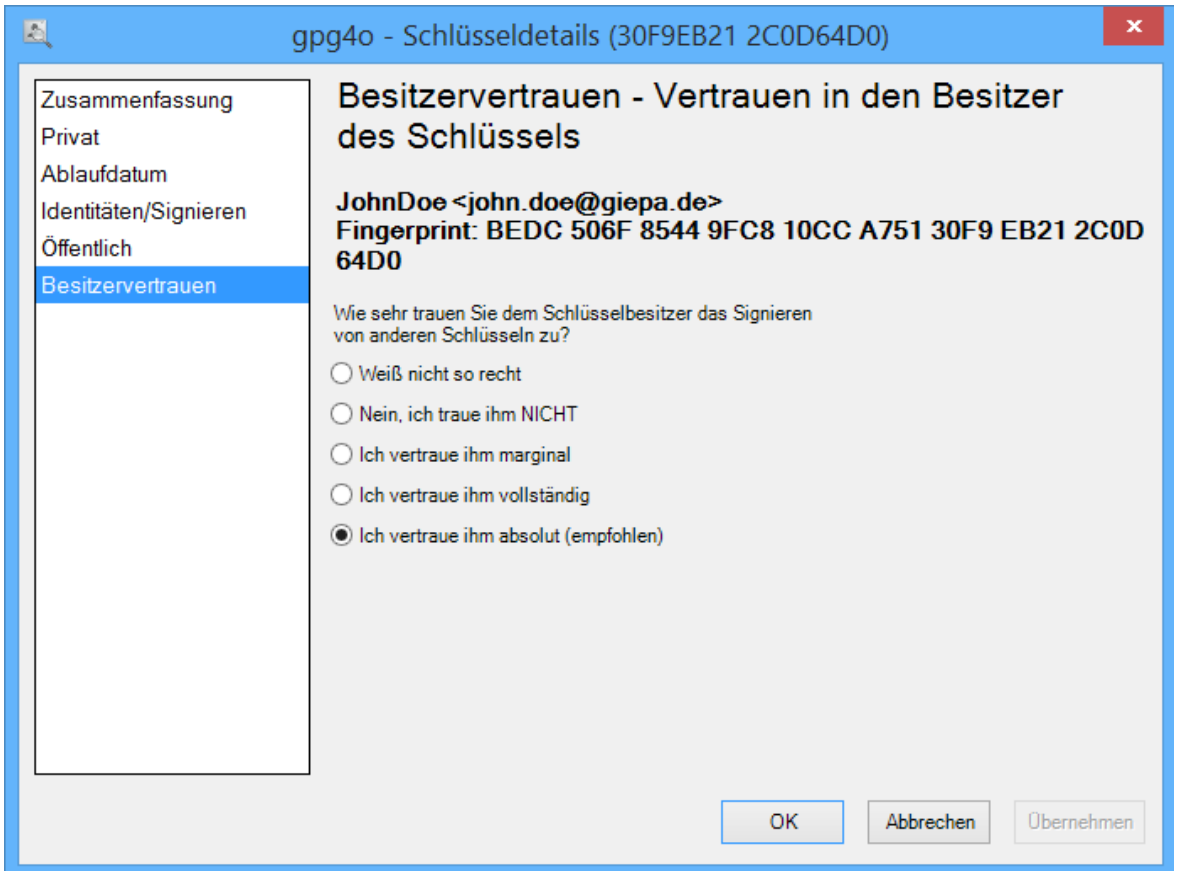
Sie können Ihren öffentlichen Schlüssel als Anhang in einer neuen E-Mail versenden, oder ihn auf einen Schlüsselserver hochladen. Von diesem Server kann er von Ihren Kontaktpartnern importiert und benutzt werden. Außerdem besteht mit der Export-Funktion die Möglich-

keit, den öffentlichen Schlüssel als Datei auf Ihren Computer oder einen Wechseldatenträger, wie z.B. einem USB-Stick, zu speichern.

Tipp: All diese Funktionen stehen Ihnen auch direkt in der Übersicht per Rechtsklick auf einen Schlüssel zur Verfügung.

8.10.6 Besitzervertrauen festlegen

Über das Besitzervertrauen legen Sie fest, wie sehr Sie Ihren Kontakten zutrauen, fremde Schlüssel zu signieren und als echt einzustufen. Dies ermöglicht die Ermittlung der Schlüsselgültigkeit anderer Schlüssel anhand seiner Signaturen. Wenn ein anderer Schlüssel vom Herausgeber desjenigen Schlüssel signiert wurde, dessen Besitzervertrauen Sie hier einstellen, wirkt sich das direkt auf die Schlüsselgültigkeit des anderen Schlüssel aus. Dieses Prinzip nennt sich **„Web of Trust“**. Beachten Sie dazu auch Kapitel 8.10.1.



Ihnen stehen mehrere Auswahlmöglichkeiten zur Verfügung, um das Vertrauen in diesen Kontakt festzulegen. Wählen Sie die Option Ich vertraue ihm absolut jedoch nur für eigene Schlüssel, da diese Option sich anders auf das Verhalten der Schlüsselgültigkeit auswirkt und nicht für fremde Schlüssel gedacht ist.

Die von Ihnen angegebene Vertrauensstufe bleibt ein Geheimnis von **GnuPG** und wird, abgesehen von der integrierten Backup Funktion, niemals exportiert oder an andere über-

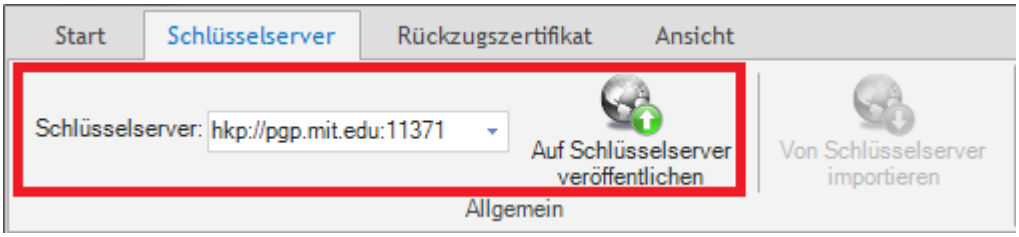
mittelt.

Tipp: Sie können das Besitzervertrauen auch direkt in der Übersicht per Rechtsklick auf einen Schlüssel ändern.

8.11 Verwenden von Schlüsselservern

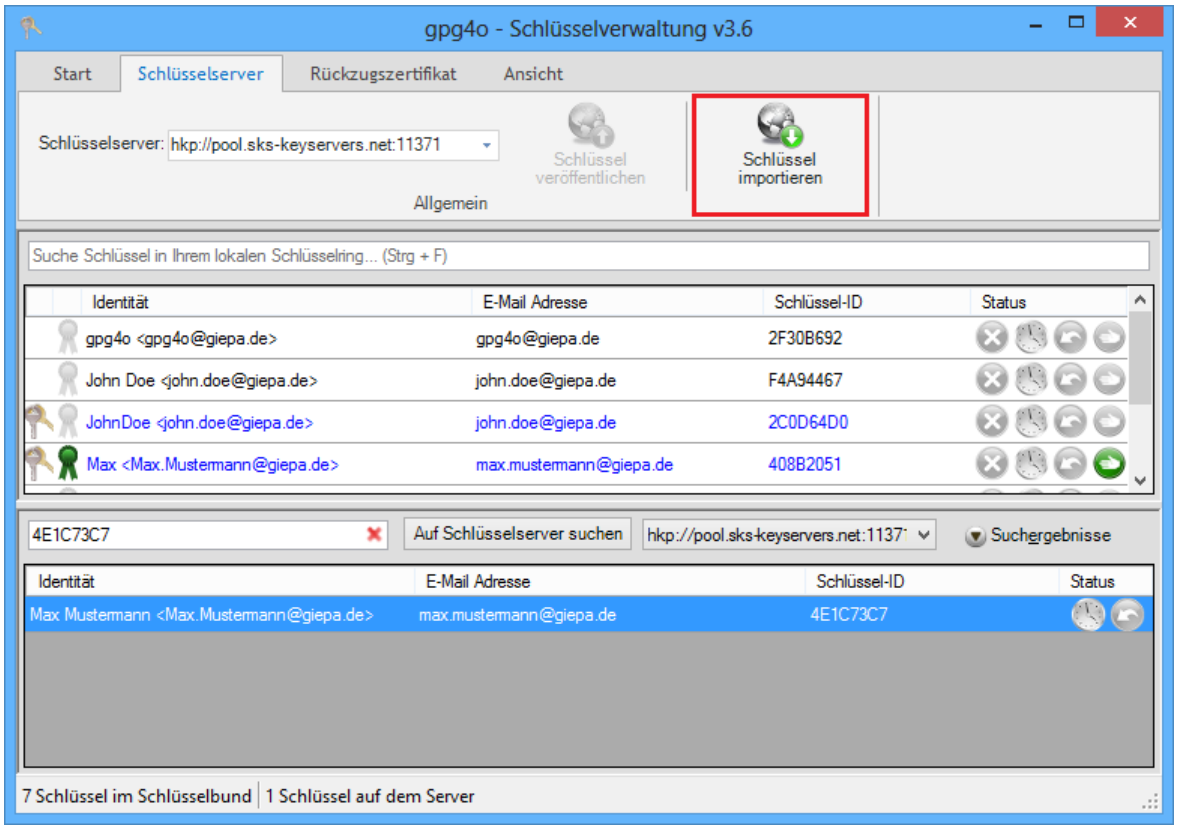
Zusätzlich zu den in den Kapiteln 7.1 und 7.2 erläuterten Möglichkeiten des Schlüsselversands per E-Mail können Sie Ihren öffentlichen Schlüssel auch auf einen Schlüsselserver im Internet hochladen und von dort auch öffentliche Schlüssel Ihrer Kommunikationspartner importieren.

Gehen Sie dazu zurück in die Übersicht der Schlüsselverwaltung und selektieren Sie Ihren Schlüssel. Wechseln Sie im Menüband auf den Reiter Schlüsselserver und wählen Sie den Schlüsselserver aus, auf den Sie Ihren Schlüssel hochladen möchten.



Klicken Sie nun auf die Schaltfläche Auf Schlüsselserver veröffentlichen, um den/die aktuell ausgewählten Schlüssel hochzuladen. Nun müssen Sie lediglich Ihrem Kommunikationspartner den ausgewählten Schlüsselserver mitteilen, damit er Ihren öffentlichen Schlüssel von dort importieren kann.

Um einen Schlüssel von einem Schlüsselserver zu importieren, können Sie den Namen oder die Schlüssel-ID Ihres Kommunikationspartners in das Suchfeld im unteren Bereich der Schlüsselverwaltung eingeben.



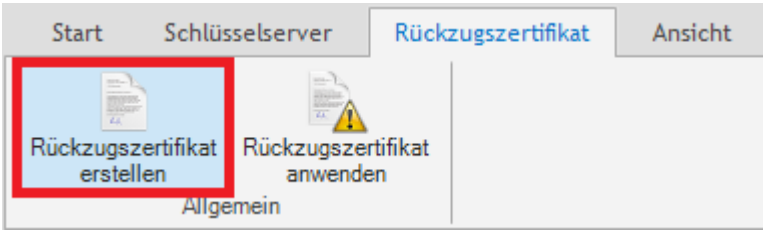
Wenn der gesuchte Schlüssel gefunden wurde, können Sie diesen auswählen und über die Schaltfläche Von Schlüsselserver importieren importieren.

Tipp: Sie können den Schlüssel auch über einen Rechtsklick auf den gefundenen Schlüssel importieren oder ihn mit gehaltener linker Maustaste in die obere Liste ziehen.

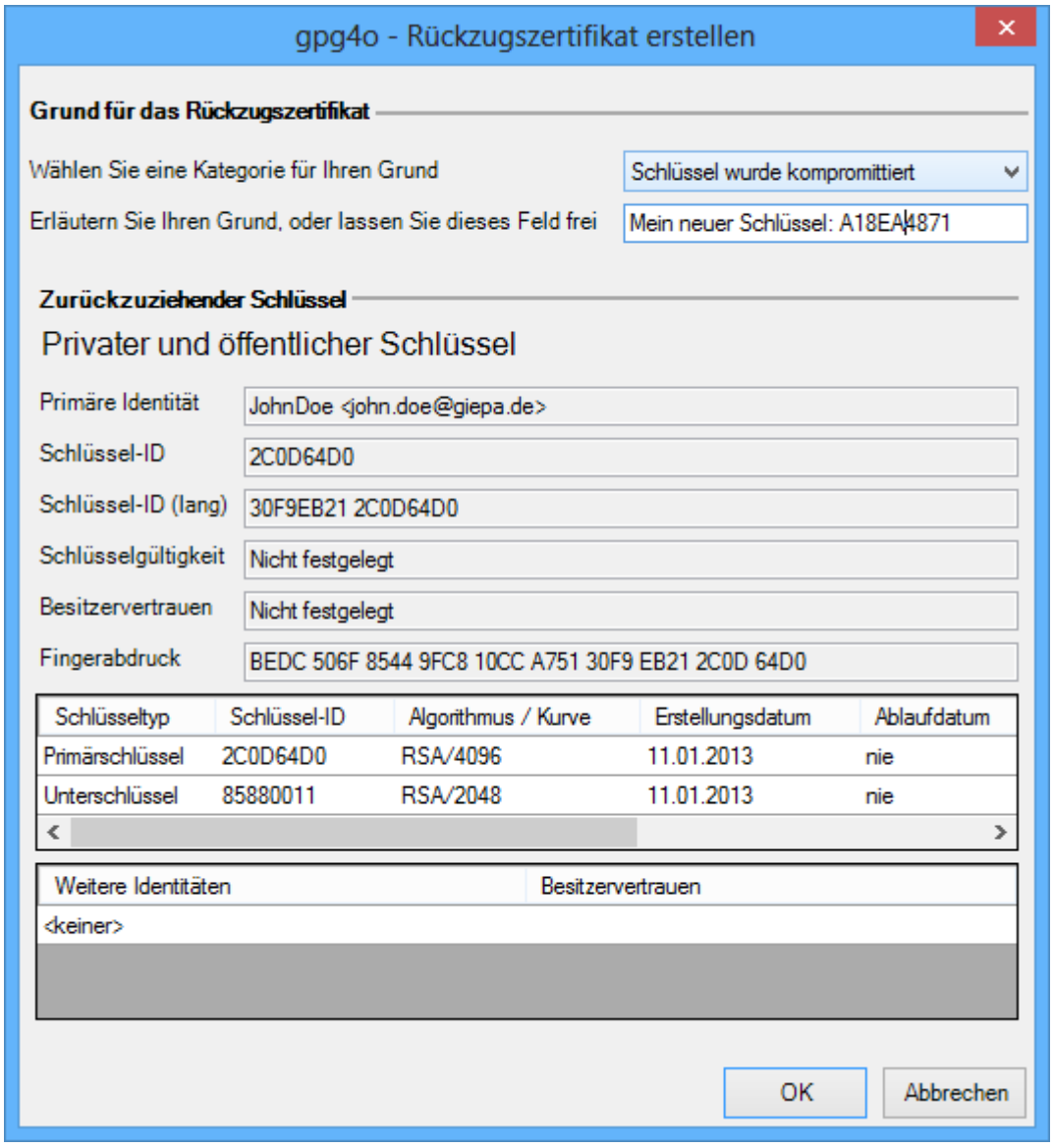
8.12 Rückzugszertifikat erstellen

Mit einem Rückzugszertifikat kann ein Schlüssel dauerhaft und unwiderruflich für ungültig erklärt werden. Mit einem für ungültig erklärten öffentlichen Schlüssel können Ihre Kommunikationspartner keine E-Mails mehr an Sie verschlüsseln. Dies ist zum Beispiel sinnvoll, wenn eine andere Person in den Besitz Ihres privaten Schlüssels gekommen ist und somit nicht sichergestellt werden kann, dass damit unterschriebene E-Mails wirklich von Ihnen stammen.

Um ein Rückzugszertifikat zu erzeugen, wählen Sie bitte den entsprechenden Schlüssel in der Übersicht der Schlüsselverwaltung aus. Dann wählen Sie über das Menüband im Reiter Rückzugszertifikat die Schaltfläche Rückzugszertifikat erstellen.



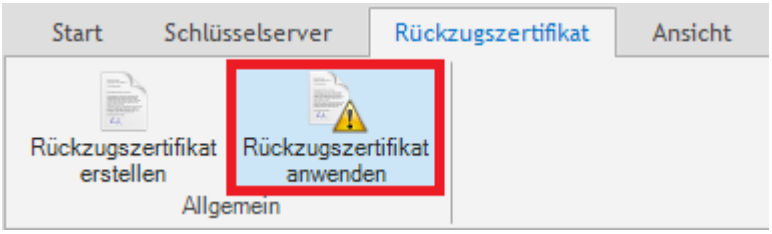
Im nachfolgenden Dialog spezifizieren Sie den Grund, warum Sie ein Rückzugszertifikat erstellen wollen. Sie können außerdem noch einen Kommentar dazu verfassen, der den Grund genauer erläutert oder weitere Informationen enthält. Das kann zum Beispiel die Schlüssel-ID des neuen Schlüssels sein, den Ihre Kontaktpartner anschließend verwenden sollen.



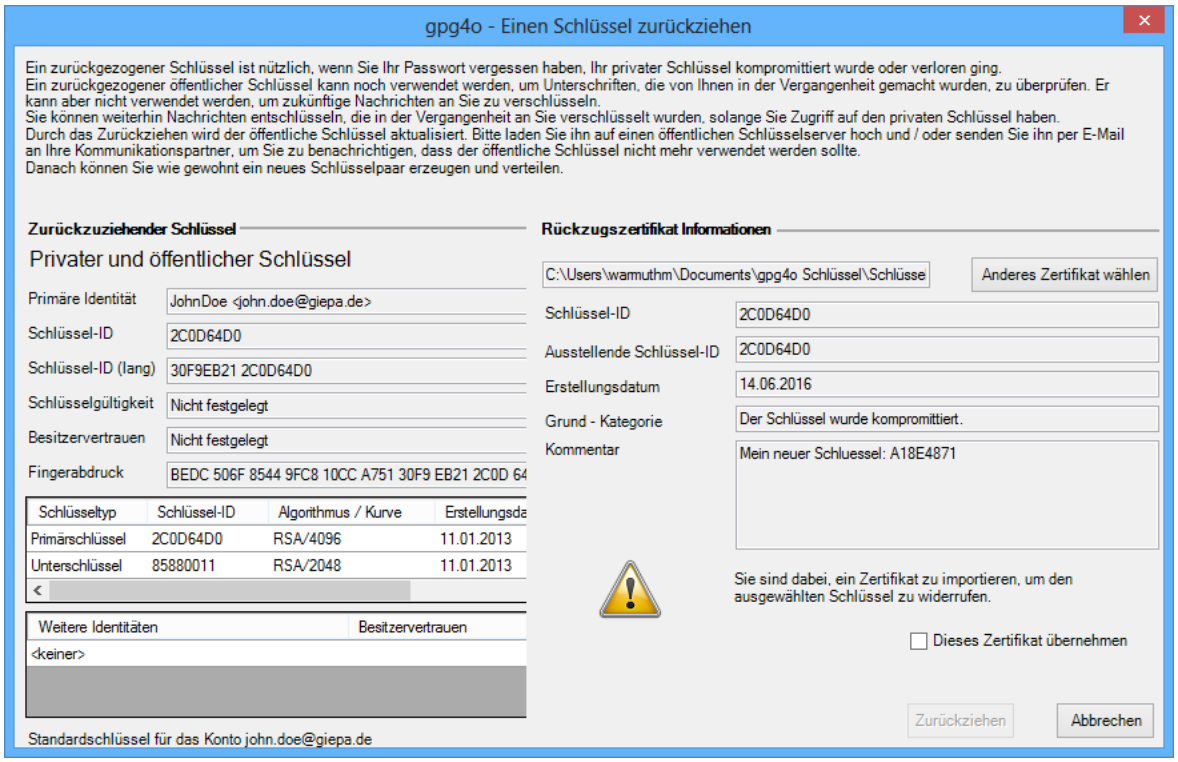
Nach Eingabe des Grundes klicken Sie auf OK und geben den Ordner an, in dem das Rückzugszertifikat gespeichert werden soll.

8.13 Rückzugszertifikat anwenden

Um einen Schlüssel zurückzuziehen, wählen Sie diesen bitte zuerst aus, und gehen dann im Menüband der Schlüsselverwaltung im Reiter Rückzugszertifikat auf Rückzugszertifikat anwenden.



Wählen Sie im erscheinenden Dateiauswahldialog das Rückzugszertifikat aus und klicken anschließend auf Öffnen.



Prüfen Sie zunächst die Angaben des Rückzugszertifikates. Wenn Sie sicher sind, dass Sie das Rückzugszertifikat anwenden möchten, setzen Sie einen Haken bei Dieses Zertifikat übernehmen und klicken anschließend auf Zurückziehen.

Achtung: Durch das Zurückziehen wird der Schlüssel dauerhaft unbrauchbar gemacht! Außerdem wird der öffentliche Schlüssel aktualisiert, und muss daher an Ihre Kommunikationspartner verteilt werden. Falls Sie den Schlüssel auch auf einem Schlüsselserver veröffentlicht hatten, müssen Sie den aktualisierten Schlüssel erneut hochladen.

9 Verwendung von GnuPG 2.1 und spätere Versionen

In diesem Kapitel sind die Änderungen im Verhalten von **gpg4o** angegeben, die sich durch die Verwendung von GnuPG 2.1 ergeben. Ferner gibt dieses Kapitel Anwendern wichtige Hinweise zur Verwendung von GnuPG 2.1.

gpg4o ab Version 5.0 unterstützt GnuPG 2.1 und somit die Verschlüsselung mittels sogenannter elliptischer Kurven (ECC). Da mit GnuPG 2.1 das Format des Schlüsselringes umstrukturiert wurde, können bei der Umstellung von früheren **GnuPG** Versionen Probleme in der Portierung Ihres Schlüsselringes auftreten, die von gpg4o nicht beeinflusst werden können.

Um die Portierung möglichst reibungslos zu gestalten und um Datenverlust in Ihrem Schlüsselring zu vermeiden, empfehlen wir folgende Schritte für die Umstellung auf GnuPG 2.1:

Erstellen Sie eine Sicherung von **gpg4o**. (siehe Kapitel 11.8)

Wechseln Sie nach erfolgreicher Installation von GnuPG 2.1 in die **gpg4o** Einstellungen und wählen Sie das Programm auf der Seite **„GnuPG“** aus.

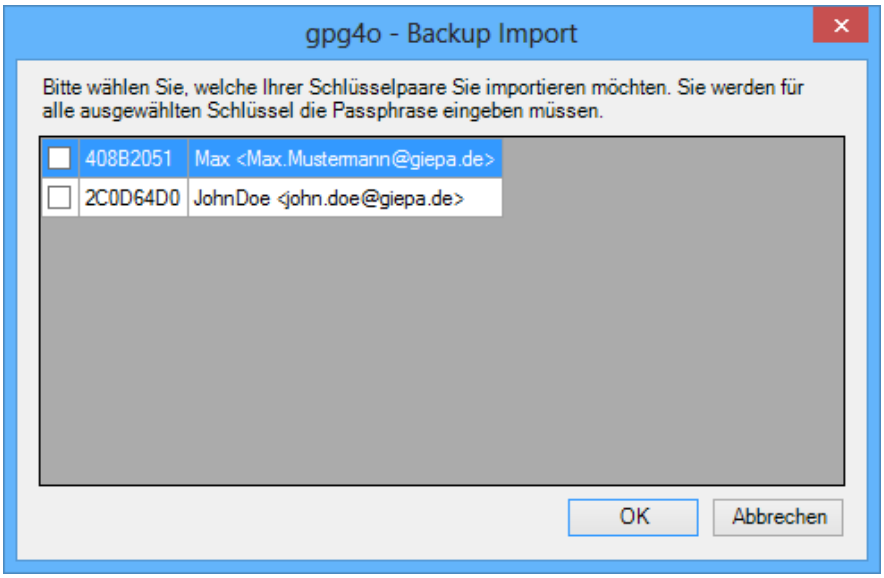
Importieren Sie die zuvor erstellte Datensicherung.

Hinweis: Beachten Sie bitte, dass Sie beim Import der Datensicherung die Passphrasen aller darin befindlichen privaten Schlüssel benötigen!

9.1 Import/Export von Schlüsselpaaren

GnuPG 2.1 verlangt beim Export oder Import eines Schlüsselpaares die Eingabe der Passphrase. Daher wird bei Export oder Import eines Schlüsselpaares in der Schlüsselverwaltung oder bei der Datensicherung (siehe Kapitel 11.8) ein entsprechender Dialog zur Eingabe der Passphrase angezeigt.

In beiden Fällen ist zu jedem Schlüsselpaar, das sich im Schlüsselring befindet, das entsprechende Passwort einzugeben. Bei Erstellung einer Datensicherung werden Ihnen alle Schlüsselpaare angezeigt und Sie haben die Möglichkeit, nicht mehr benötigte Schlüsselpaare von der Sicherung auszuschließen.



Beim Einspielen einer Sicherung können Sie die zu importierenden Schlüsselpaare mit Hilfe eines Dialogs auswählen.

Hinweis: Nach einem Wechsel zu GnuPG 2.1 kann es sein, dass nicht mehr alle Schlüssel/-paare in Ihrer Schlüsselverwaltung sichtbar sind. Dies liegt daran, dass GnuPG 2.1 Schlüsselpaare mit veralteten Sicherheitsmechanismen nicht mehr zur Verwendung anbietet. In so einem Fall sollten Sie ein neues Schlüsselpaar nach aktuellen Sicherheitsstandards erstellen und ihr altes Schlüsselpaar zurückziehen. (siehe Kapitel 8.12)

10 Senderegeln

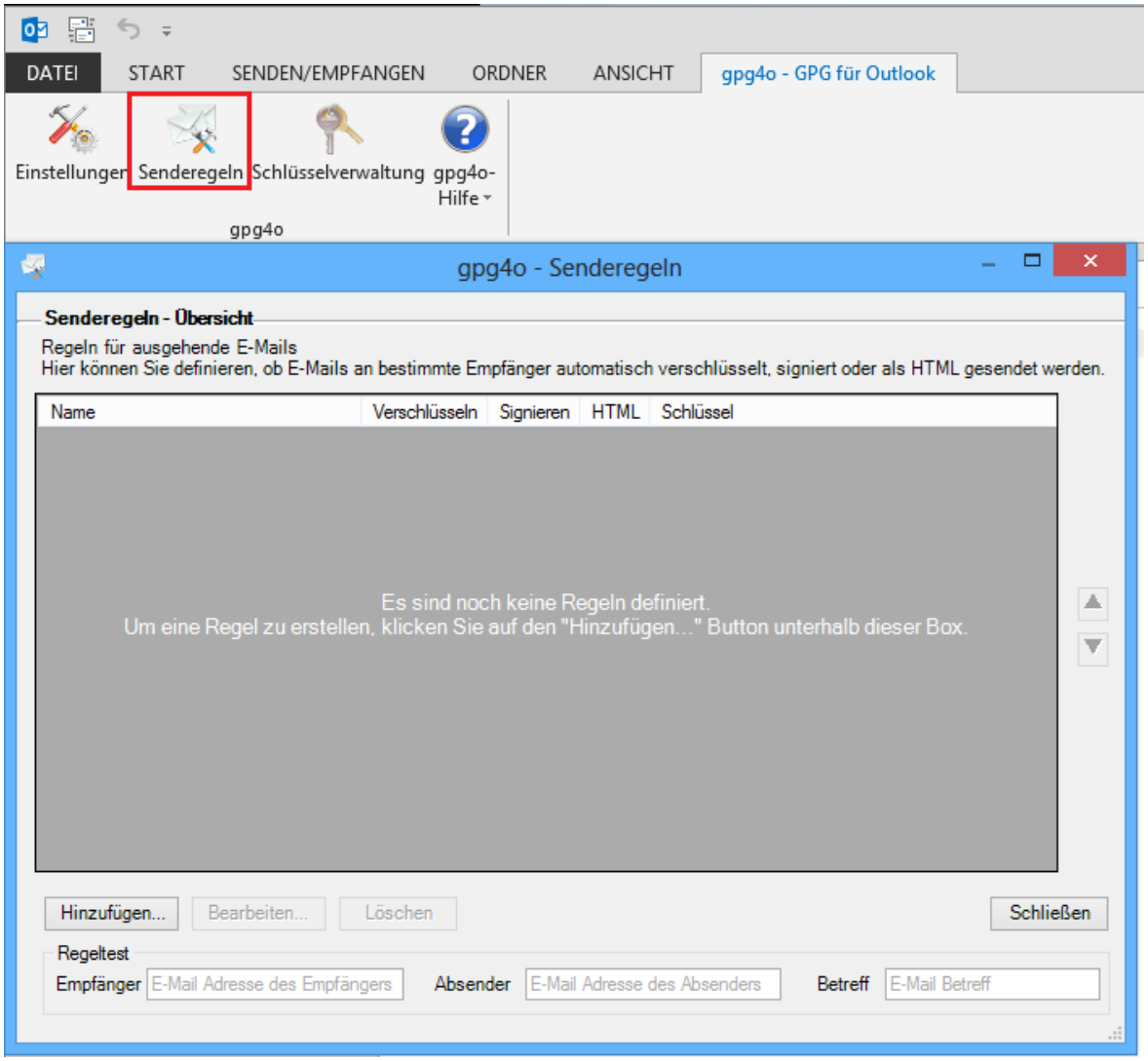
Damit Sie nicht für jede Ihrer E-Mails die Einstellungen für Verschlüsselung und Signierung manuell auswählen müssen, gibt es in **gpg4o** Senderegeln, die Ihnen diese Arbeit abnehmen.

Achtung: Beachten Sie, dass mit **gpg4o *Free*** die Senderegeln lediglich ausprobiert werden können, allerdings nicht aktiv nutzbar sind.

10.1 Senderegeln verwalten

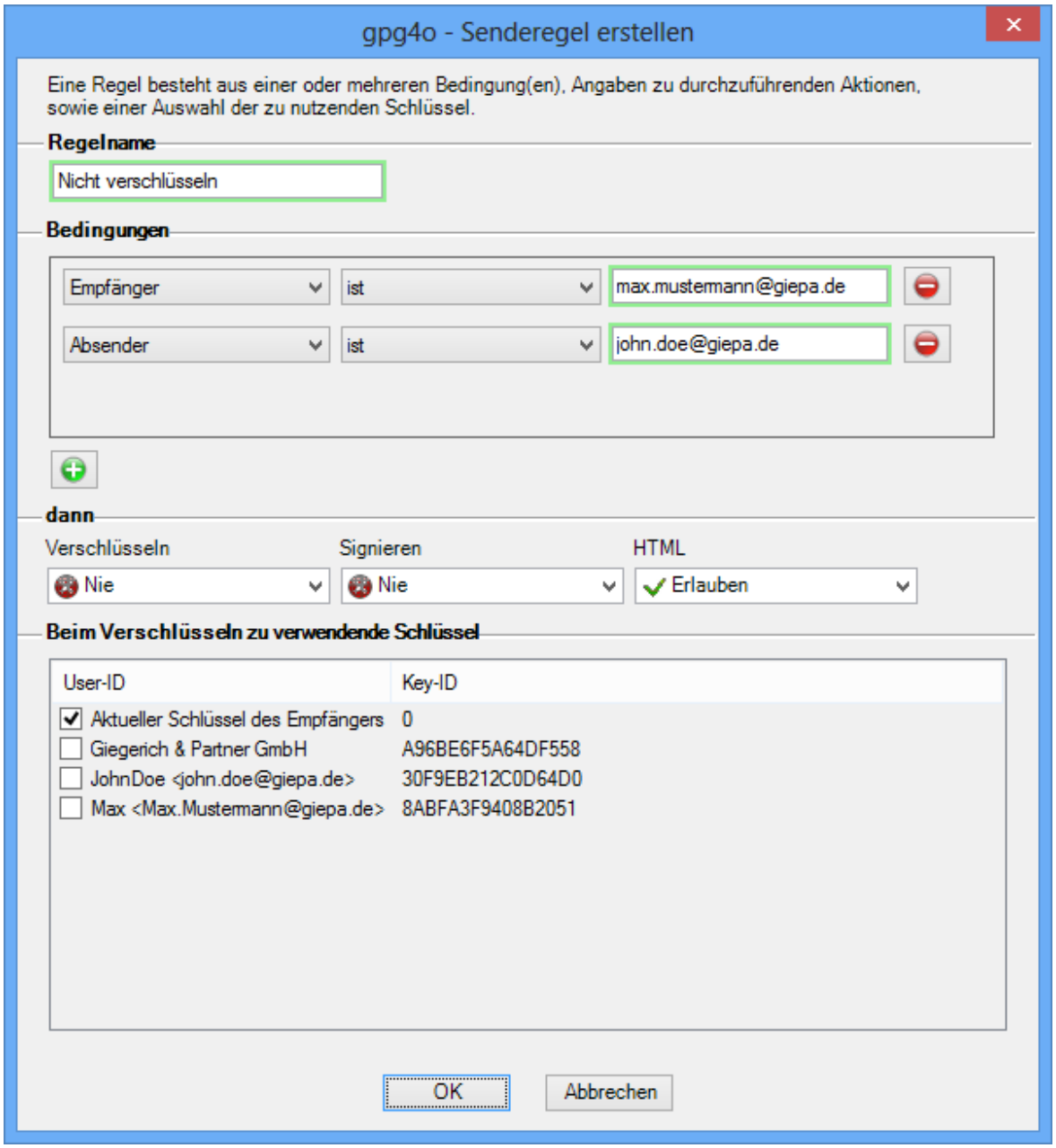
In der Übersicht der Senderegeln haben Sie die Möglichkeit, Ihre bestehenden Regeln, ohne Einfluss auf die Regelauswertung, zu sortieren und zu testen.

Klicken Sie dazu den Punkt Senderegeln im Menüband gpg4o - GPG für Outlook an.



Um eine neue Regel zu erstellen, klicken Sie in der Übersicht auf die Schaltfläche Hinzufügen.

Im Feld **„Regelname“** tragen Sie einen aussagekräftigen Namen für diese neue Regel ein. Ergänzen Sie danach die Bedingungen. Achten Sie beim Erstellen der Bedingungen darauf, diese so spezifisch wie möglich anzulegen, um spätere Konflikte zu vermeiden. Danach wählen Sie die zu verwendenden Verschlüsselungsoptionen und öffentliche Schlüssel des oder der Empfänger. Die Schlüssel werden später beim Versand der E-Mail zum Verschlüsseln genutzt, wenn die Regel verwendet wird. Wenn Sie möchten, dass **gpg4o** den passenden Schlüssel für Sie auswählt, belassen Sie die Auswahl auf Aktueller Schlüssel des Empfängers. Andernfalls wählen Sie hier die Schlüssel aus, welche für die E-Mail Verschlüsselung benutzt werden sollen.



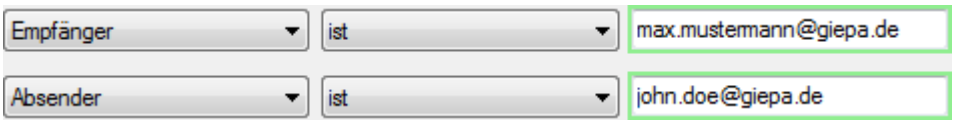
10.2 Regelauswertung

Damit eine Regel beim Versand einer E-Mail verwendet wird, müssen alle im Bereich **„Bedingungen“** angegebenen Voraussetzungen zutreffen.

Beim Verfassen einer neuen E-Mail werden alle Ihre Regeln durchsucht und alle passenden ausgewählt. Diese Auswahl basiert ausschließlich auf den Bedingungen der einzelnen Regeln und nicht auf der Anordnung in der Regelliste.

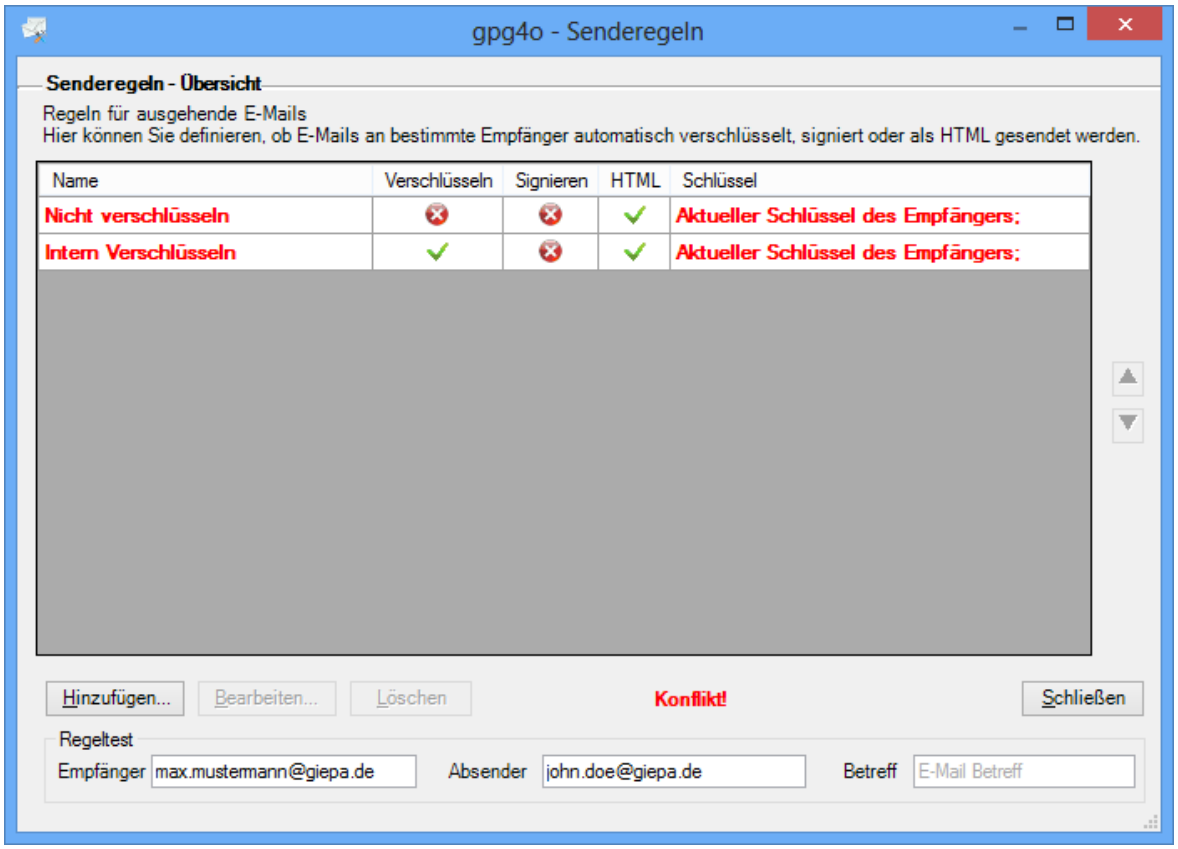
Im folgenden Beispiel sehen Sie zwei Regeln:

Die Regel **„Nicht verschlüsseln“** enthält zwei Bedingungen:



Die Regel **„Intern Verschlüsseln“** enthält eine Bedingung:

Wenn Sie jetzt eine E-Mail an max.mustermann@giepa.de schreiben und als Absender john.doe@giepa.de ausgewählt haben, greifen beide Ihrer Regeln. Dadurch erhalten Sie einen Konflikt, weil die Einstellungen für die Verschlüsselung innerhalb der Regeln gegensätzlich sind.



Um diesen Konflikt in Zukunft zu vermeiden, könnten Sie der Regel **„Intern Verschlüsseln“** weitere Bedingungen hinzufügen:

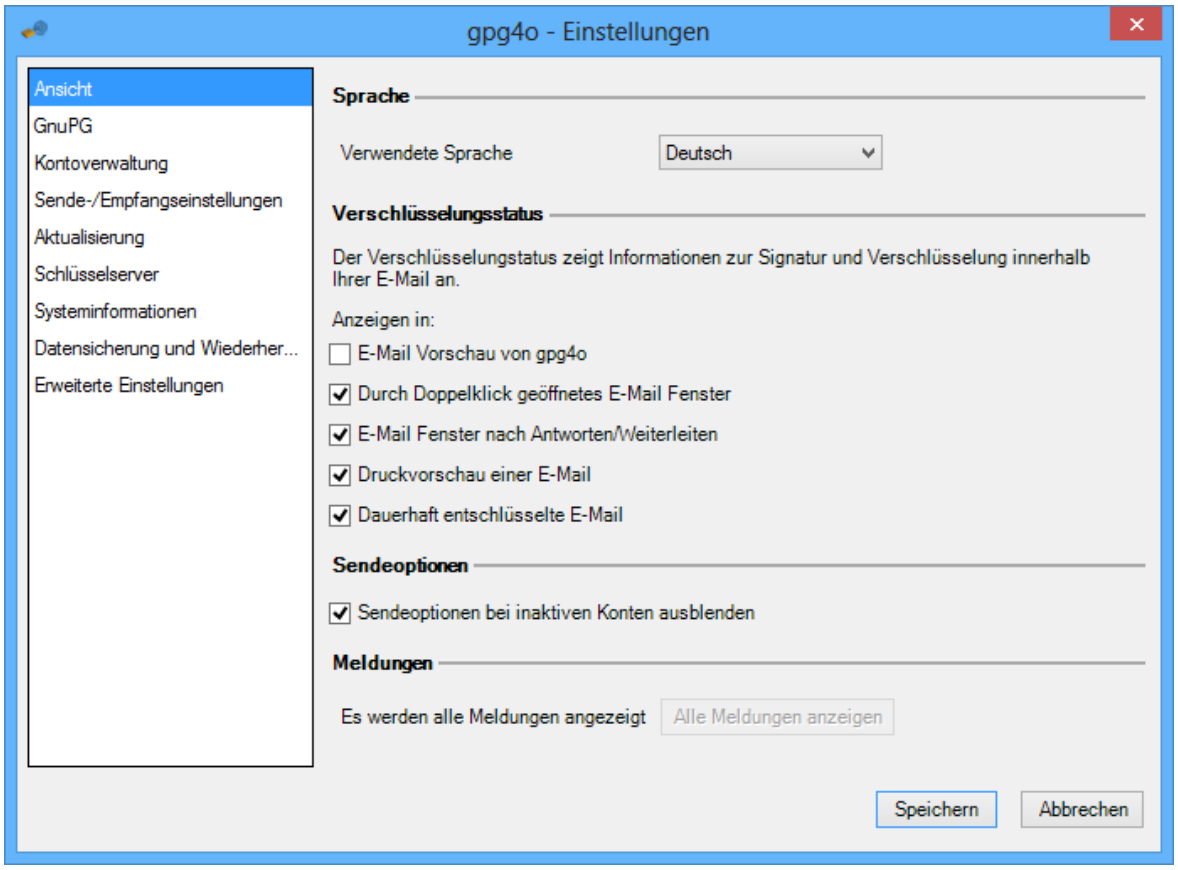
Empfänger	ist nicht	**max.mustermann@giepa.de**
Absender	ist nicht	**john.doe@giepa.de**

11 Einstellungen

Mit den Einstellungen können Sie wichtige Optionen von **gpg4o** verändern. Änderungen an den Optionen, auch wenn Menüpunkte gewechselt werden, werden erst nach dem Speichern wirksam.

11.1 Ansicht

Auf dieser Seite werden die allgemeinen Schalter angezeigt, mit denen das Aussehen von **gpg4o** und die Integration in Microsoft Outlook angepasst werden können.



11.1.1 Sprache

Die Sprache ist einstellbar zwischen Deutsch und Englisch. Bitte beachten Sie, dass bei Änderung der Sprache die Einstellungen geschlossen und erneut geöffnet werden müssen.

11.1.2 Verschlüsselungsstatus

Hier können Sie auswählen, in welchen Bereichen von **gpg4o** Ihnen innerhalb einer E-Mail die Information zur Entschlüsselung und Signatur angezeigt werden soll. Standardmäßig ist die Anzeige nur in der normalen E-Mail Vorschau abgestellt.

11.1.3 Sendeoptionen

Ist dieser Schalter aktiv, wird bei Verfassen einer E-Mail die Leiste mit den Sendeoptionen ausgeblendet, wenn das gewählte Absenderkonto nicht zur Verwendung mit **gpg4o** aktiviert wurde.

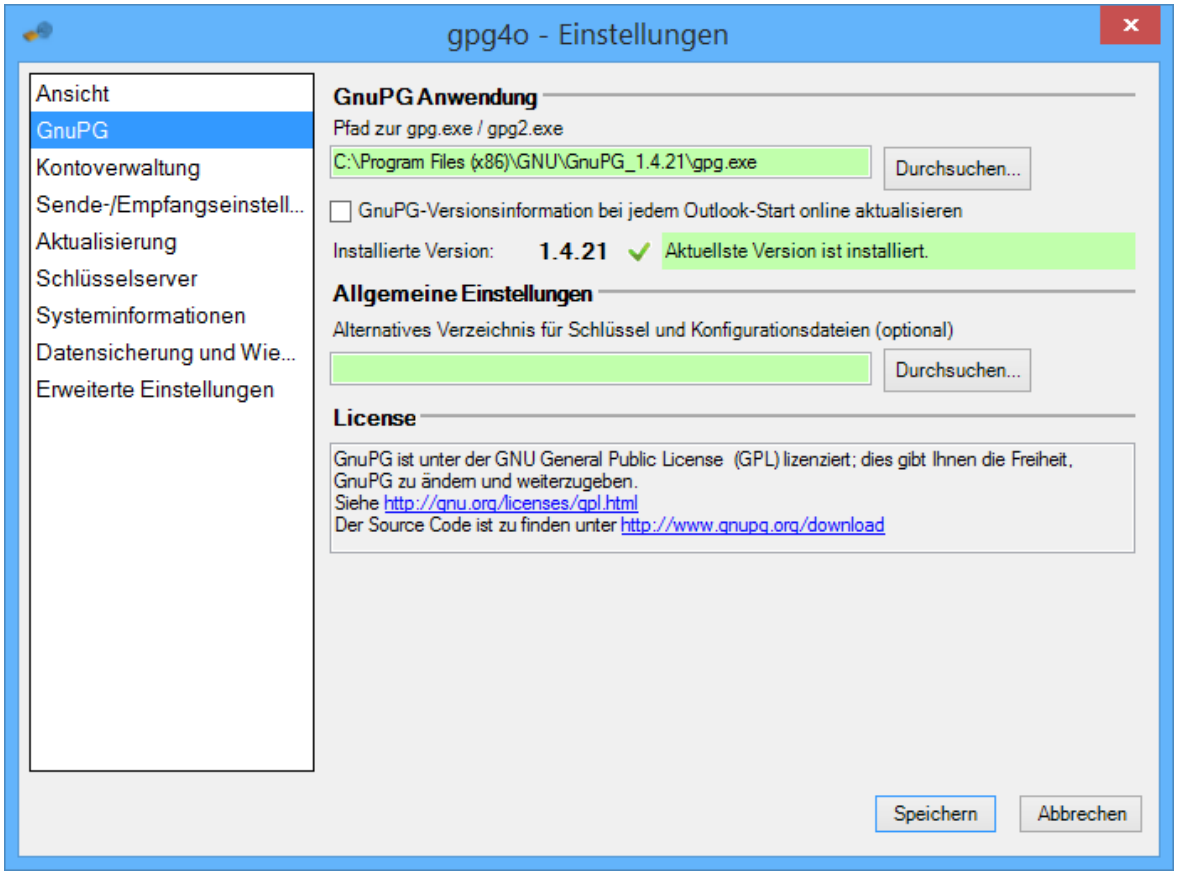
Ist der Schalter nicht gesetzt, werden die Sendeoptionen auch bei inaktiven Konten angezeigt.

11.1.4 Meldungen

Als Benutzer können Sie bestimmte, immer wiederkehrende Abfragen deaktivieren, so dass Ihnen diese nicht mehr angezeigt werden. Dazu gehört beispielsweise die Abfrage zur Aktualisierung des installierten **GnuPG** beim Programmstart von Outlook. Durch betätigen dieser Schaltfläche werden alle so deaktivierten Meldungen wieder angezeigt.

11.2 GnuPG

Auf der Seite **GnuPG** werden Ihnen die Versionsnummer und der Installationspfad Ihrer **GnuPG** Installation angezeigt.



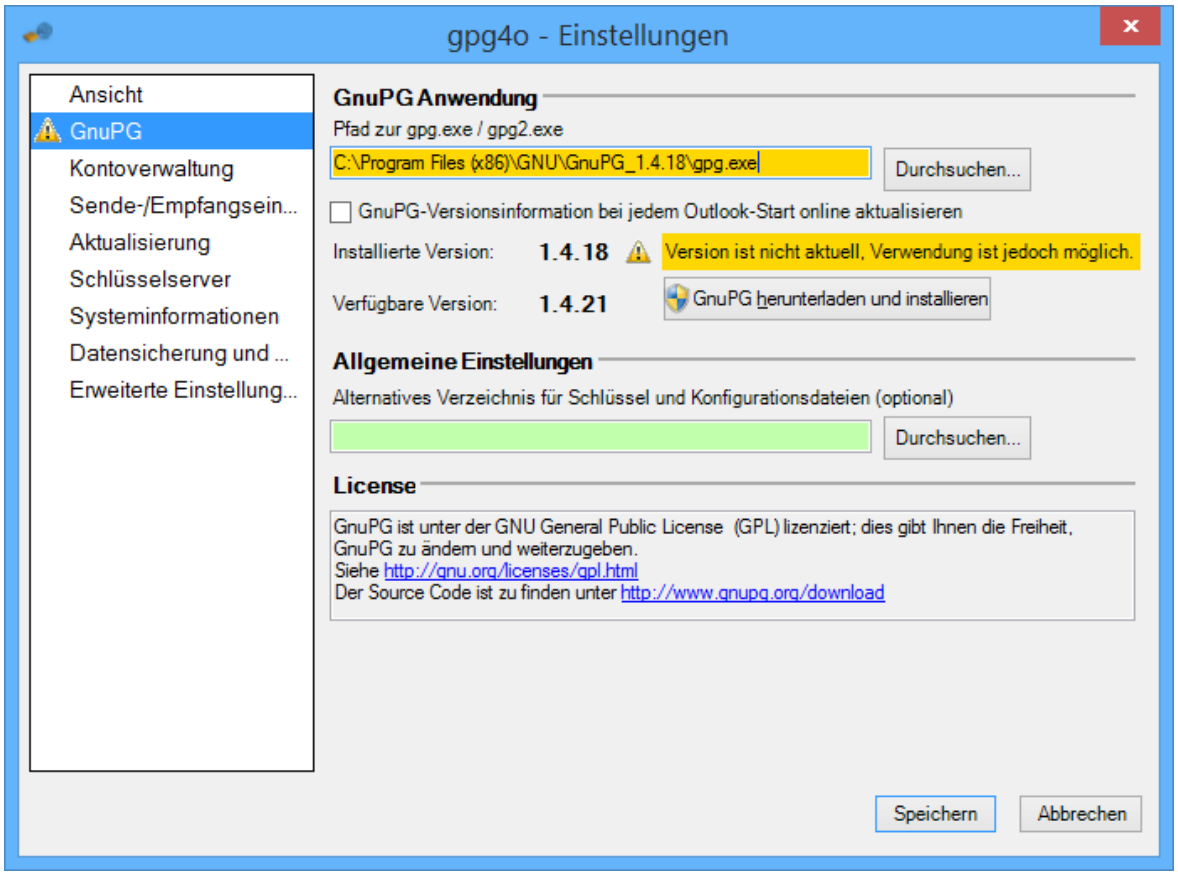
11.2.1 Pfad zu GnuPG

Sie können bei Bedarf über die Schaltfläche Durchsuchen... auch auf andere Installationen von **GnuPG** umstellen.

Sollten Sie **GnuPG** noch nicht installiert haben, wird Ihnen weiter unten im Dialog die Schaltfläche GnuPG herunterladen und installieren angezeigt, mit der Sie **GnuPG** aus dem Internet herunterladen und installieren können. Der Ablauf ist hierbei der gleiche wie auch bei der Installation durch den Konfigurations-Assistenten.

Hier finden Sie auch die Informationen zur Lizenz von **GnuPG** und haben die Möglichkeit, über die Links weitere Informationen zu erhalten.

11.2.2 Versionsüberprüfung von GnuPG



gpg4o verwendet für Verschlüsselung das Programm **GnuPG**. Dieses wird aktiv weiterentwickelt und erhält immer wieder Aktualisierungen und Erweiterungen. Um auch mit GnuPG immer auf dem neuesten Stand zu sein, aktivieren Sie bitte die Option GnuPG-Versionsinformation bei jedem Outlook-Start online aktualisieren. Wird eine neue GnuPG Version veröffentlicht, bekommen Sie beim Programmstart von Outlook einen Hinweis angezeigt und Sie können entscheiden, ob Sie diese Version installieren möchten, oder nicht. Bestätigen Sie die Frage mit Ja, wird Ihnen die Seite **„GnuPG“** der

gpg4o Einstellungen aufgerufen. Dort können Sie über einen Klick auf die Schaltfläche GnuPG herunterladen und installieren die Aktualisierung von GnuPG durchführen.

Hinweis: Beachten Sie, dass diese Funktionalität nicht mit **gpg4o *Free*** zur Verfügung steht.

11.2.3 GnuPG Datenverzeichnis

Standardmäßig speichert **GnuPG** seinen Schlüsselbund im Anwendungsordner Ihres Benutzerprofiles. Möchten Sie stattdessen ein anderes Verzeichnis nutzen, können Sie hier ein alternatives Verzeichnis auswählen. Dieses wird dann zukünftig anstelle des Standardverzeichnisses von **GnuPG** genutzt.

Hinweis: Bereits importierte oder erstellte Schlüssel werden hierbei nicht kopiert und sind im neuen Verzeichnis nicht mehr verfügbar. Im alten Verzeichnis bleiben diese dennoch weiterhin bestehen. Um auf diese Schlüssel zugreifen zu können, müssen Sie diese zuvor exportieren und nach der Umstellung auf ein alternatives Verzeichnis wieder importieren (siehe Kapitel 8).

11.2.4 Zwischenspeichern der Passphrase

Wenn Sie **GnuPG** 2.x einsetzen, werden die von Ihnen eingegebenen Passphrasen durch den **„GnuPG Agent“** zwischengespeichert. Wie lange diese zwischengespeichert werden sollen, können Sie hier einstellen. Die Mindestdauer, wie lange die Passphrasen zwischengespeichert werden, beträgt eine Minute.

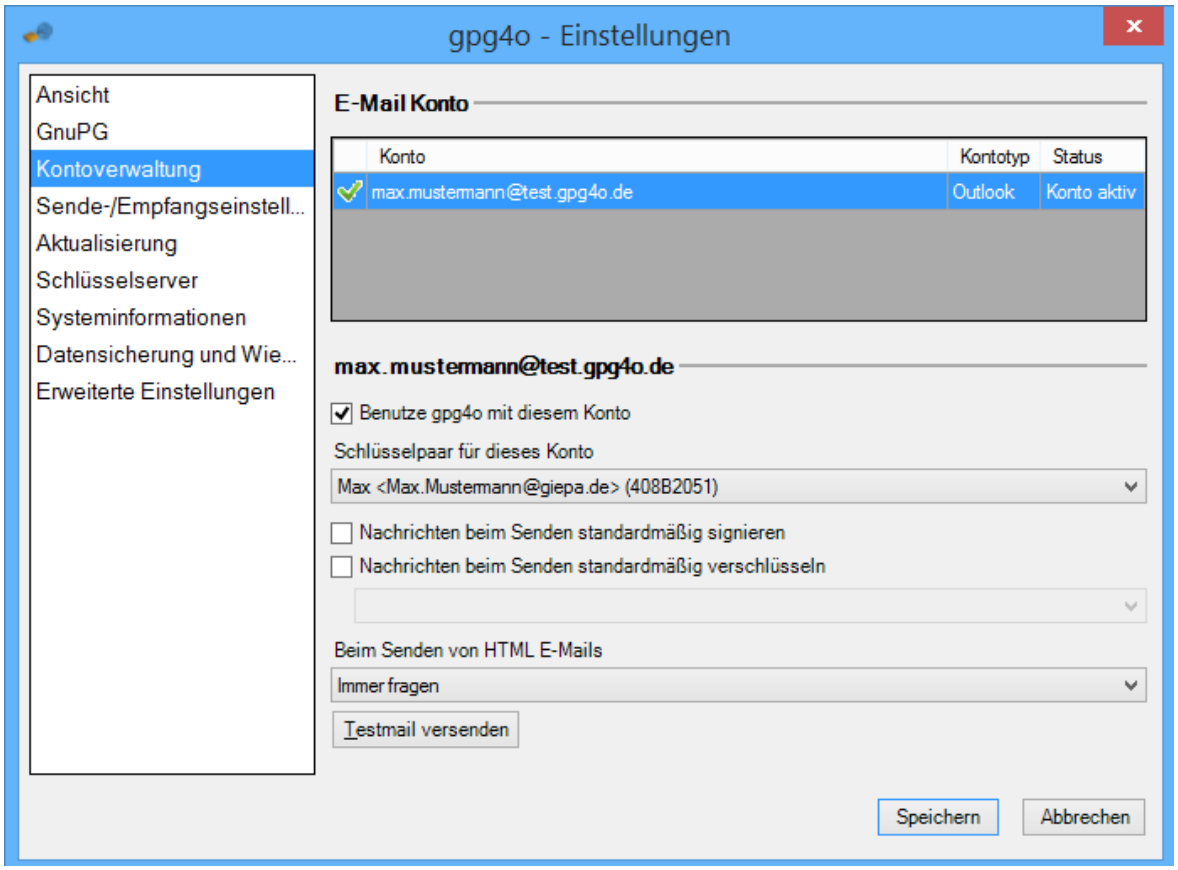
11.2.5 GnuPG Agent

Seit **GnuPG** 2.0 wird der **„GnuPG Agent“** eingesetzt, um die Passphrase zwischen zu speichern. Der **GnuPG** Agent wird automatisch gestartet, sobald eine **GnuPG** Aktion in **gpg4o** ausgeführt wird. Jedoch wird der **GnuPG** Agent beim Schließen von Microsoft Outlook nicht standardmäßig beendet. Dadurch werden zwischengespeicherte Passphrasen nicht zurückgesetzt, was ein Sicherheitsrisiko darstellen kann. Wenn Sie diese Option aktivieren, wird der **GnuPG** Agent automatisch mit Microsoft Outlook beendet, wodurch zuvor eingegebene Passphrasen aus dem Speicher entfernt werden.

Hinweis: Das Starten des **GnuPG** Agent kann ein paar Sekunden dauern. Dies ist besonders dann zu spüren, wenn Sie die erste E-Mail zum Entschlüsseln auswählen.

11.3 Kontoverwaltung

Auf dieser Seite erfolgt die Konfiguration der einzelnen E-Mail-Konten (üblicherweise entspricht eine E-Mail-Adresse einem Konto in Microsoft Outlook).



Unter dem Namen des ausgewählten E-Mail Kontos finden Sie die dazugehörigen Einstellungen. Setzen Sie den Haken bei Benutze gpg4o mit diesem Konto, wenn Sie Nachrichten in diesem E-Mail Konto entschlüsseln möchten, oder Nachrichten verschlüsselt und/oder signiert senden möchten.

Hinweis: Wenn Sie in einem E-Mail Konto überhaupt nicht verschlüsseln oder signieren möchten, sollten Sie **gpg4o** für dieses Konto deaktivieren.

Mit der Auswahlbox **„Schlüsselpaar für dieses Konto“** legen Sie fest, welches Schlüsselpaar zum Signieren von Nachrichten verwendet werden soll.

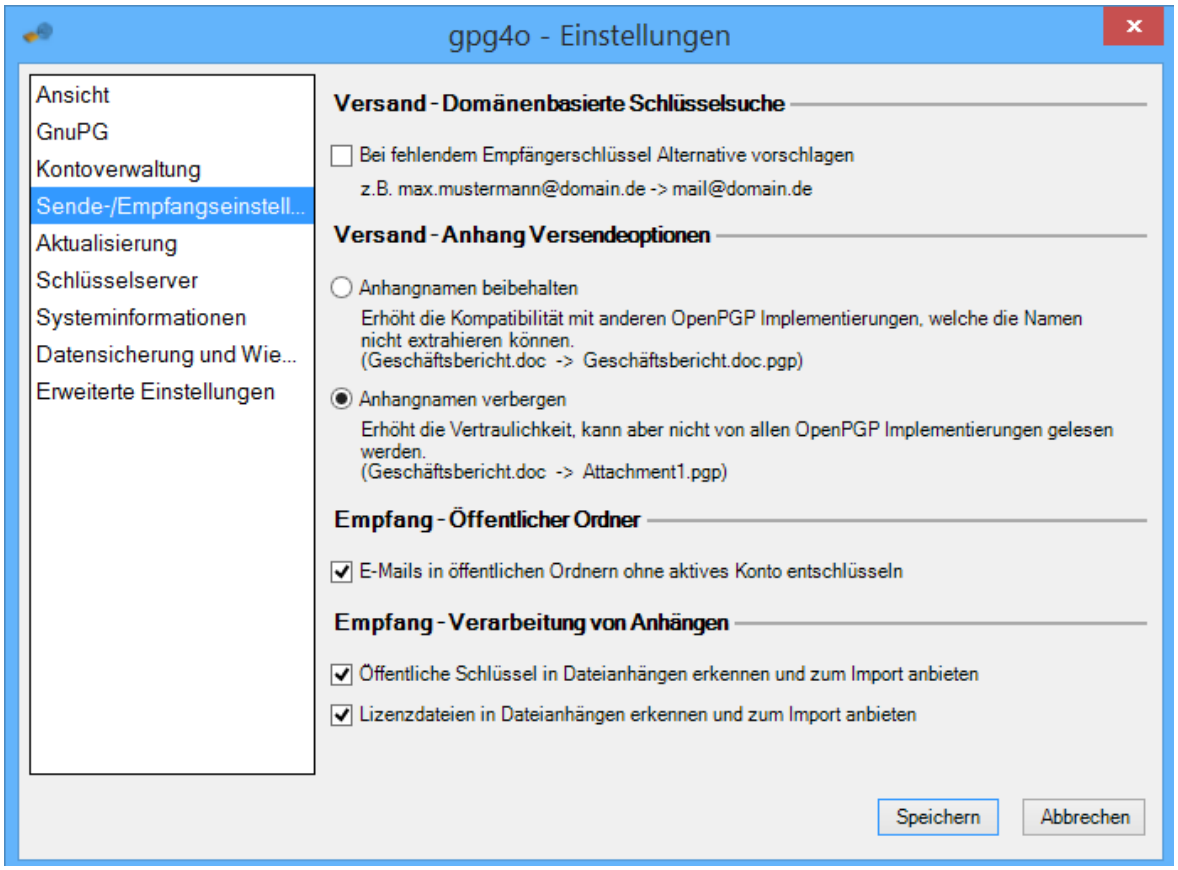
Mit den beiden nächsten Kontrollkästchen wird das Standardverhalten von **gpg4o** bezüglich des E-Mail-Versands festgelegt. Wenn Sie auswählen, dass Nachrichten standardmäßig verschlüsselt werden sollen, müssen Sie auch festlegen, ob nur die Anhänge oder die ganze Nachricht verschlüsselt werden soll.

Sollten Sie für bestimmte Situationen regelmäßig andere Einstellungen benötigen, können Sie diese mithilfe der Senderegeln (siehe Kapitel 10) einstellen.

Die Auswahlbox **„Beim Senden von HTML E-Mails“** dient dazu festzulegen, ob beim Versenden von E-Mails im HTML-Format standardmäßig nachgefragt werden soll, ob das HTML-Format genutzt werden darf, oder ob diese vor dem Senden in das **„Nur Text“**-Format umgewandelt werden sollen.

Für das ausgewählte Konto können Sie eine Testmail schicken. Bei der empfangenen Testmail können Sie überprüfen, ob die Verschlüsselung und Entschlüsselung mit Ihren Einstellungen funktioniert.

11.4 Sende-/Empfangseinstellungen



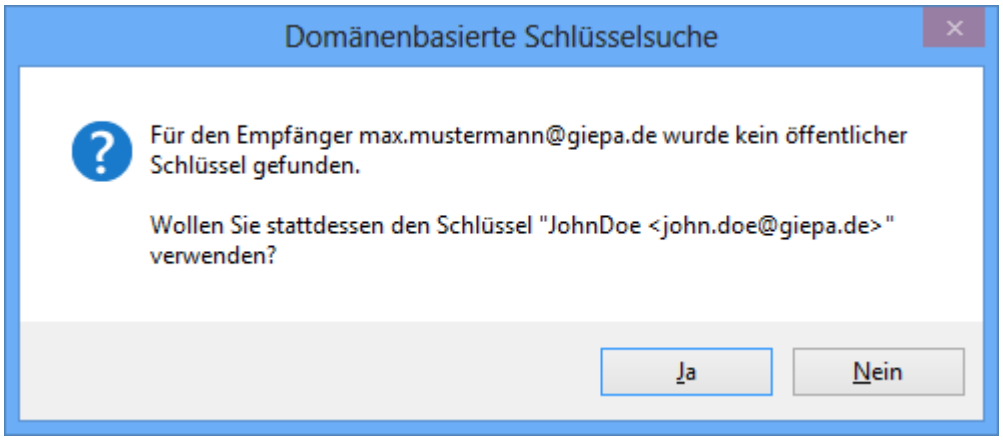
11.4.1 Versand - Domänenbasierte Schlüsselsuche

Sie können die **„Domänenbasierte Schlüsselsuche“** aktivieren, wenn Sie nicht für jeden fehlenden Schlüssel einen entsprechenden Schlüssel suchen müssen oder wenn Sie für eine Firma einen globalen Schlüssel besitzen. Dadurch wird Ihnen bei einem fehlenden Schlüssel automatisch ein möglicher passender Schlüssel, aus der Domäne des Empfängers, von Ihrer Schlüsselliste vorgeschlagen.

Um die Domänenbasierte Schlüsselsuche zu aktivieren, setzen Sie bei

Bei fehlendem Empfängerschlüssel Alternative vorschlagen einen Haken. Den Rest erledigt **gpg4o** für Sie.

Wenn Sie eine E-Mail an **„Max.Mustermann@giepa.de“** schreiben, aber keinen Schlüssel für diesen Empfänger besitzen, kann Ihnen **gpg4o** jetzt einen alternativen Schlüssel aus der jeweiligen Domäne anbieten.



Wenn Sie den hier vorgeschlagenen Schlüssel ablehnen, können Sie anschließend im Schlüsselauswahldialog die Zuordnung von Empfänger und Schlüssel für die Verschlüsselung der E-Mail manuell vornehmen.

11.4.2 Versand - Anhang Versendeoptionen

Viele OpenPGP-Anwendungen verschlüsseln nicht nur die E-Mail und die Anhänge, sondern auch die Dateinamen der Anhänge. Auch **gpg4o** beherrscht diese Technik und nutzt sie standardmäßig. Jedoch ist nicht jede OpenPGP-Anwendung mit dieser Technik kompatibel. Stellen Sie die Option daher um, wenn ein Empfänger die Dateinamen nicht entschlüsseln kann.

11.4.3 Empfang - Öffentlicher Ordner

Standardmäßig können Sie nur E-Mails entschlüsseln, welche sich im Ordner eines in **gpg4o** aktivierten Kontos befinden.

Mit dieser Option weisen Sie **gpg4o** an E-Mails in öffentlichen Ordnern, unabhängig Ihrer aktiven Konten, zu entschlüsseln. Voraussetzung dafür ist lediglich, dass Sie den privaten Schlüssel des Empfängers besitzen, an welchen die E-Mail versandt wurde. Sie können sich nun wie gewohnt Ihre E-Mails anzeigen lassen.

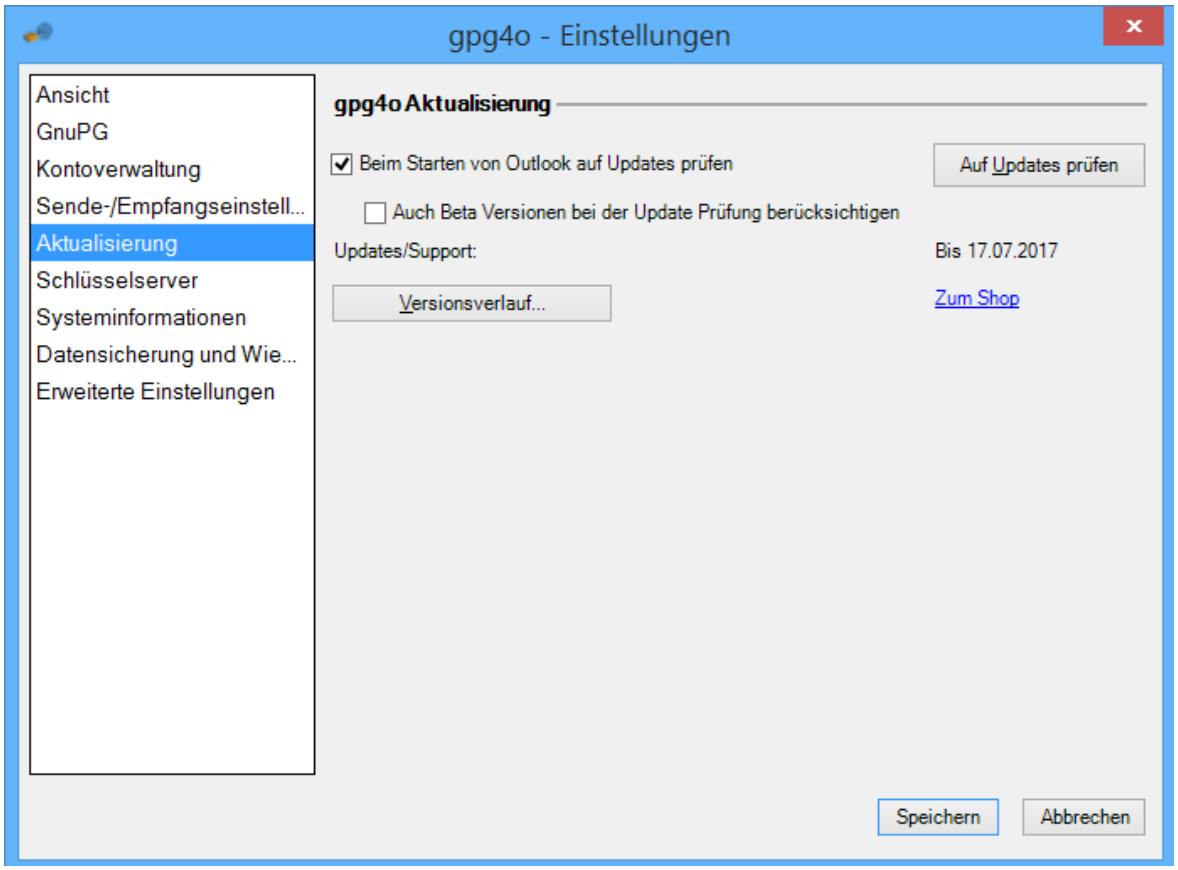
Beachten Sie bitte, dass diese Option lediglich in öffentlichen Ordnern genutzt wird. Für die Entschlüsselung von E-Mails in anderen Ordnern muss das entsprechende Konto aktiviert werden (siehe Kapitel 11.3).

11.4.4 Empfang - Verarbeitung von Anhängen

Sie können die Verarbeitung von Anhängen aktivieren, um einen automatischen Hinweis beim Empfang von E-Mails auf Schlüssel und/oder Lizenzen zu bekommen. Der Hinweis zeigt Ihnen zum einen, dass Schlüssel und/oder Lizenzen in der E-Mail vorhanden sind und zum anderen wird Ihnen direkt ein Import der entsprechenden Datei angeboten.

11.5 Aktualisierung

Auf dieser Seite kann die Überprüfung auf Updates von **gpg4o** eingestellt oder manuell ausgeführt werden.



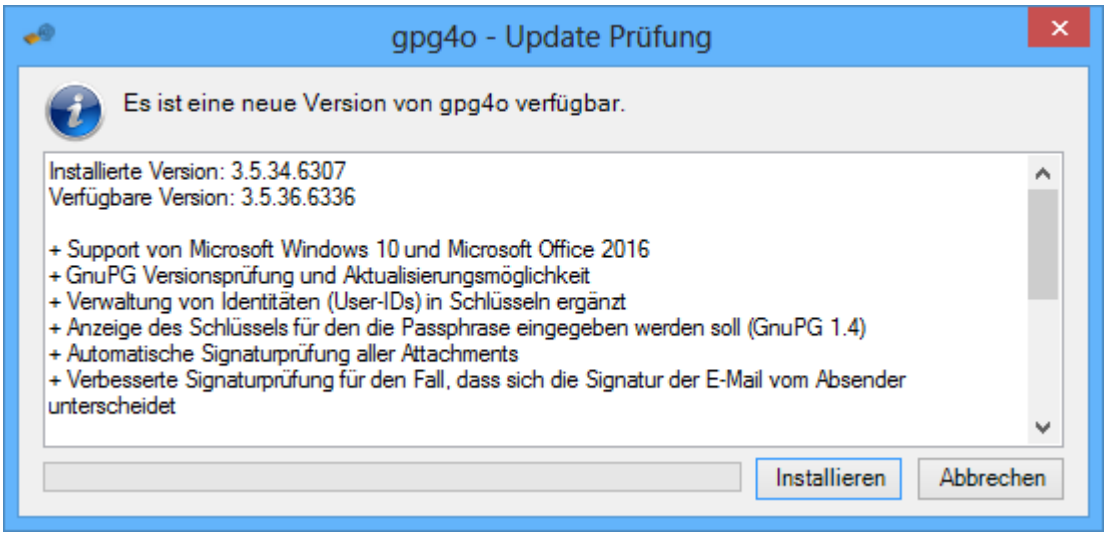
11.5.1 Update von gpg4o

Die Entwickler von **gpg4o** erweitern die Software regelmäßig, verbessern die Bedienbarkeit und fügen neue Funktionen hinzu.

Auf dieser Seite können Sie eine manuelle Überprüfung auf Updates durchführen, indem Sie auf die dortige Schaltfläche Auf Updates prüfen klicken. Soll diese Überprüfung automatisch stattfinden, setzen Sie den Haken bei Beim Starten von Outlook auf Updates prüfen. Sobald eine neuere Version von **gpg4o** erscheint, wird Ihnen diese zur Installation angeboten.

Durch aktivieren von Auch Beta Versionen bei der Update Prüfung berücksichtigen, erhalten Sie die Möglichkeit eine Vorabversion des kommenden **gpg4o** zu installieren. Sie erhalten hierdurch einen Ausblick auf die Verbesserungen und neuen Funktionen der kommenden Version und können durch Ihre Rückmeldung aktiv an der Entwicklung von **gpg4o** mitarbeiten. Beta Versionen werden in der Regel ein paar Wochen vor Veröffentlichung einer neuen **gpg4o** Version zur Verfügung gestellt und bis dahin immer wieder aktualisiert.

Hinweis: Bitte beachten Sie, dass es sich bei Beta Versionen naturgemäß um Versionen handelt, die noch Fehler beinhalten können. Sie sollten diese Option daher nicht in einer Produktivumgebung aktivieren.



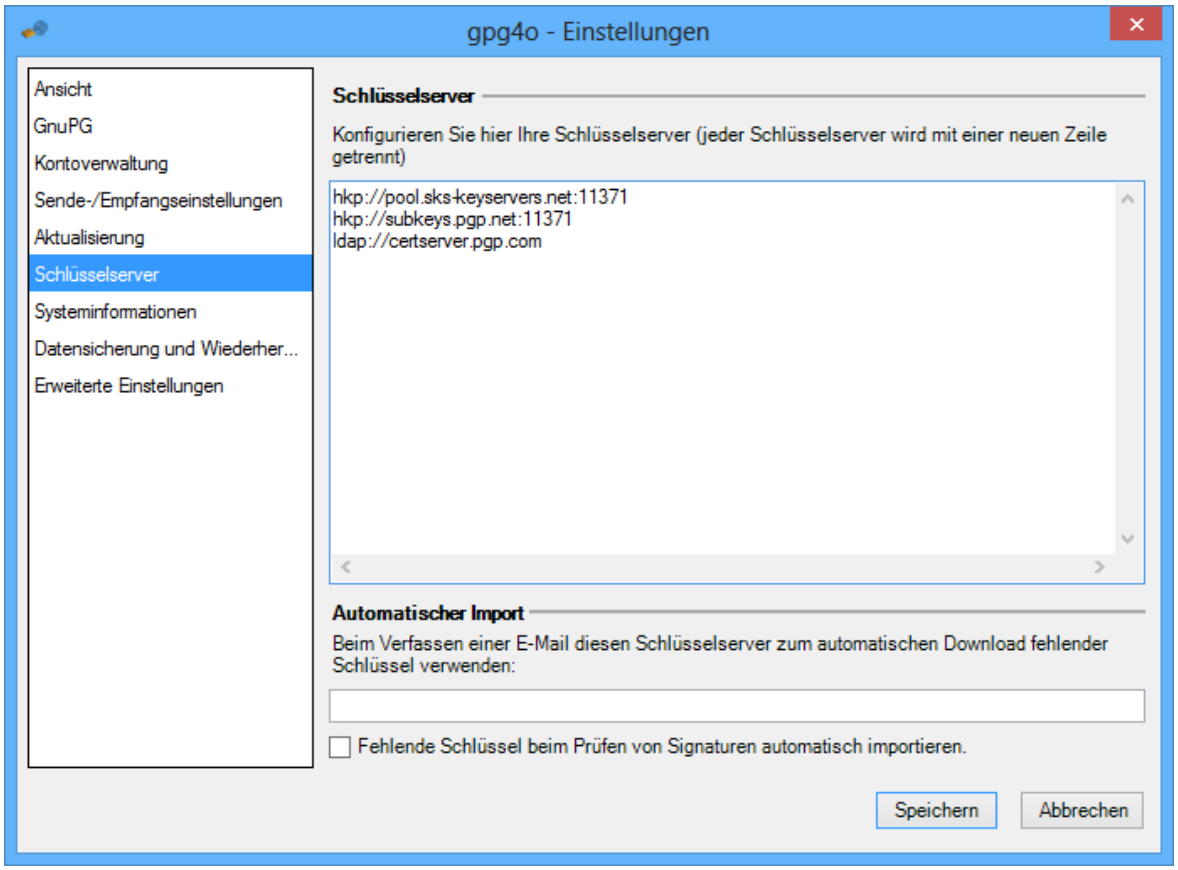
Mit Klick auf Installieren wird die Installation gestartet. In Kapitel 4 können Sie dessen Ablauf nachlesen. Nach Abschluss der Installation sollten Sie Microsoft Outlook neu starten, damit die Änderungen wirksam werden.

Über den Link Zum Shop können Sie eine Lizenz für **gpg4o** beziehungsweise eine Verlängerung der Produktwartung von **gpg4o** kaufen.

Über Versionsverlauf... können Sie die einzelnen Veröffentlichungen von **gpg4o** und deren Verbesserungen nachlesen.

11.6 Schlüsselserver

Unter dem Menüpunkt Schlüsselserver haben Sie die Möglichkeit, die von **gpg4o** genutzten Schlüsselserver anzuzeigen und zu editieren.



11.6.1 Schlüsselserver

Um einen neuen Schlüsselserver hinzuzufügen, tragen Sie dessen Adresse als neue Zeile in das Textfeld ein. Beachten Sie hierbei, dass die Adresse der Schlüsselserver nicht auf Gültigkeit geprüft wird und ein falscher Server nicht erreicht werden kann.

Um einen Schlüsselserver zu entfernen, entfernen Sie dessen Eintrag im Textfeld. Damit wird dieser Schlüsselserver nicht mehr in **gpg4o** verwendet.

Die hier aufgeführten Schlüsselserver werden dazu verwendet, fehlende Schlüssel bei der Überprüfung von E-Mail Signaturen manuell zu importieren. Bitte beachten Sie, dass nur die Server verwendet werden, die über Protokoll HKP oder HKPS angesprochen werden.

11.6.2 Automatischer Import von fehlenden Schlüssel

Hier können Sie den Schlüsselserver eintragen, von dem automatisch Schlüssel in den lokalen Schlüsselring importiert werden, während Sie eine E-Mail verfassen. Dies ist beispielsweise sinnvoll, wenn Sie selbst einen privaten Schlüsselserver betreiben und dort nur gültige Schlüssel hochladen. Der in diesem Feld angegebene Server muss nicht in der Liste aller Schlüsselserver eingetragen sein, um verwendet werden zu können.

Durch aktivieren von `Fehlende Schlüssel beim Prüfen von Signaturen automatisch importieren`, werden fehlende Schlüssel schon bei Anzeige einer signierten E-Mail automatisch in den

lokalen Schlüsselring importiert.

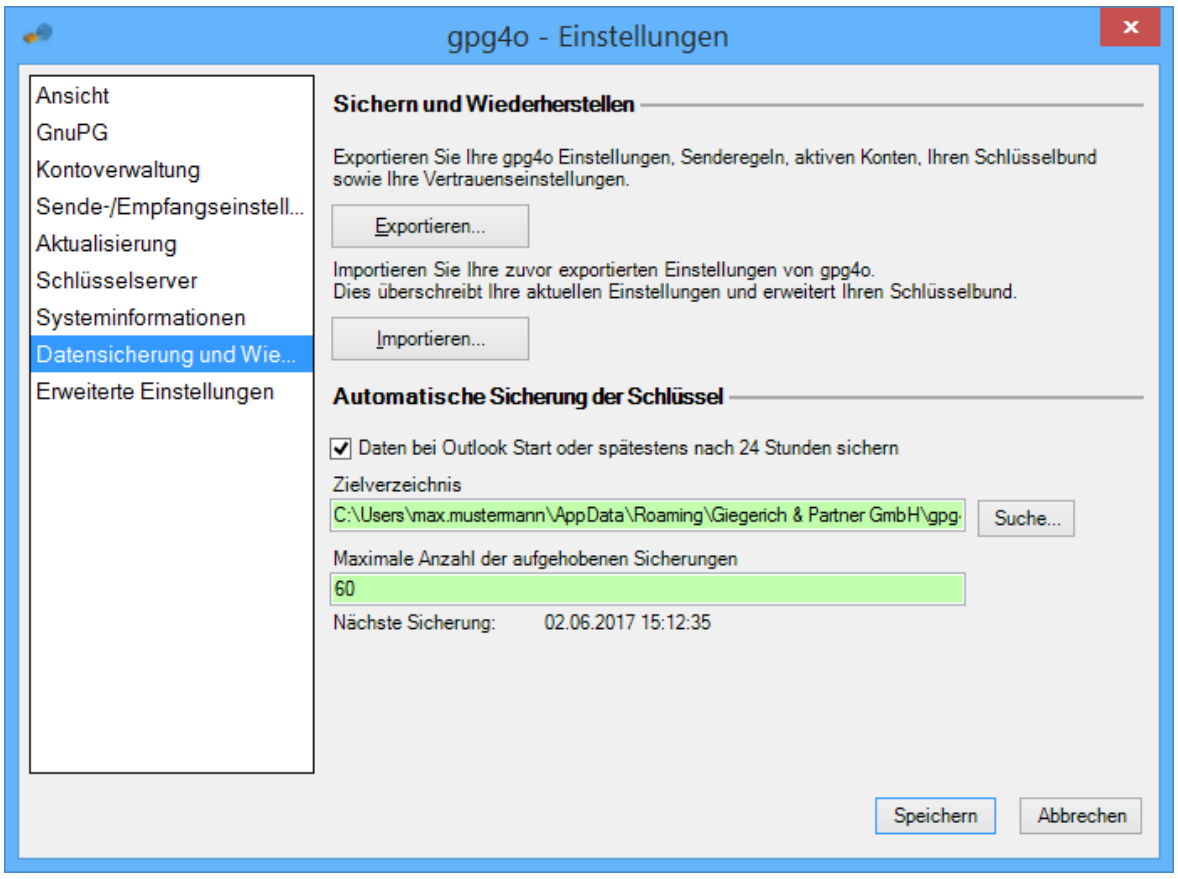
Hinweis: Beachten Sie, dass diese Funktionalität nicht mit **gpg4o *Free*** zur Verfügung steht.

11.7 Systeminformation

In den Systeminformationen stehen Einzelheiten über das Produkt **gpg4o**, der Lizenz, dem Betriebssystem und zu **GnuPG**. Dort sehen Sie unter anderem die Installationspfade der verschiedenen Produkte.

11.8 Datensicherung und Wiederherstellung

Auf dieser Seite können Sie die Einstellungen von **gpg4o** und Ihre Schlüssel sichern und eine Sicherung wiederherstellen. Diese Funktion kann auch dazu verwendet werden alle Einstellungen auf einen neuen Computer zu übertragen.



11.8.1 Sichern und Wiederherstellen

Hier können Sie eine manuelle Datensicherung durchführen oder eine vorhandene Datensicherung importieren. Diese Sicherung schützt Sie vor dem Verlust Ihrer Schlüssel und

aktuellen **gpg4o**-Konfiguration, wenn zum Beispiel die Daten nicht mehr von der Festplatte gelesen werden können. Hierfür müssen Sie die Sicherung auf einem externen Medium (bspw. USB-Stick, externe Festplatte, CD/DVD) abspeichern und sicher verwahren.

Über die Schaltfläche Exportieren erstellen Sie eine neue Sicherung mit den folgenden Daten:

- Alle Schlüssel, sowohl öffentliche Schlüssel als auch Schlüsselpaare
- Die Vertrauenseinstellungen zu den Schlüsseln
- Die komplette Konfiguration von **gpg4o** inkl. aller Konten-Einstellungen
- Alle definierten Senderegeln
- Die **gpg4o** Lizenzdatei

Mit der Schaltfläche Importieren laden Sie Ihre zuvor exportierten Einstellungen von **gpg4o** und überschreiben damit Ihre aktuellen. Ihr Schlüsselbund wird mit den neu hinzugefügten Schlüsseln erweitert und Schlüssel, die seit dem letzten Backup gelöscht wurden, werden wieder eingefügt.

Tipp: Eine Datensicherung kann auch genutzt werden, um **gpg4o** auf einen anderen Rechner umzuziehen.

Achtung: Speichern Sie die Datensicherung nur auf Ihren eigenen physikalischen Datenträger ab. **Niemals** sollten Sie die Sicherung in eine Cloud hochladen.

11.8.2 Automatische Sicherung der Schlüssel

Durch aktivieren von Daten bei Outlook Start oder spätestens nach 24 Stunden sichern wird direkt nach dem Speichern der Einstellung eine Sicherung des kompletten Schlüsselrings durchgeführt. Die Daten werden im Zip Format im angegebenen Zielverzeichnis abgelegt.

Die Sicherungsdatei wird in dem angegebenen Zielverzeichnis erstellt und sollte nur verän-

dert werden, wenn Sie sich der möglichen Konsequenzen bewusst sind, die sich beispielsweise dadurch ergeben können, wenn das Verzeichnis nicht zugreifbar ist oder ein anderes Problem damit auftritt.

Ist die maximale Anzahl der Sicherungen erreicht, wird die älteste Sicherung gelöscht um ein neues Backup zu erstellen.

„Nächste Sicherung“ zeigt Ihnen den Zeitpunkt an, zu der die nächsten Sicherung durchgeführt wird.

Hinweis: Bitte beachten Sie, dass aktuell noch keine Wiederherstellung dieser automatischen Sicherungen über die Benutzeroberfläche von **gpg4o** möglich ist. Die auf diese Art erstellten Sicherungen müssen bei Bedarf von Hand wiederhergestellt werden. Bitte wenden Sie sich bei Bedarf an Ihren technischen Betreuer oder an den Support von **gpg4o**.

11.9 Erweiterte Einstellungen

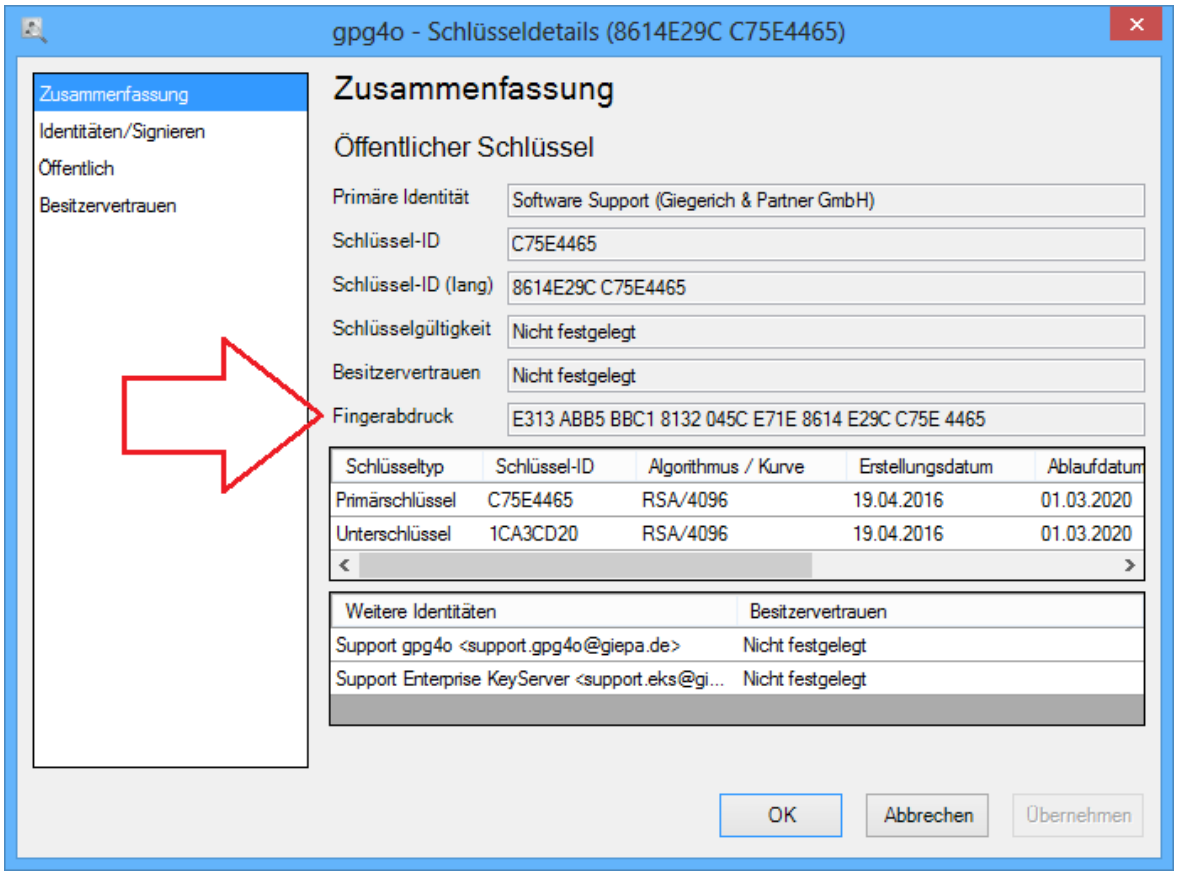
Auf dieser Seite befinden sich Einstellungen, die im Normalfall keiner Änderung bedürfen, oder ein höheres Verständnis über die **OpenPGP**-Verschlüsselung erfordern. Bitte ändern Sie hier nichts, wenn Sie sich nicht darüber im Klaren sind, welche Auswirkungen dies hat.

11.9.1 Immer alle Schlüssel als gültig betrachten

Diese Option zu deaktivieren erhöht zwar die Sicherheit, jedoch auch die Komplexität und erfordert einen deutlichen Mehraufwand bei der Schlüsselverwaltung. Sollten Sie diese Option deaktivieren, können Sie nur noch an Empfänger verschlüsseln, deren Schlüssel Sie signiert haben, oder der durch das **„Web of Trust“** als gültig erkannt wurde.

Beispiel:

Anhand des Schlüssels für die **gpg4o** Support Adresse von Giegerich & Partner wird hier erklärt, wie Sie die Echtheit des Schlüssels überprüfen und diesen Schlüssel gültig machen. Bitte öffnen Sie die Schlüsselverwaltung und suchen Sie den Schlüssel **„Software Support (Giegerich & Partner GmbH)“**. Markieren Sie den Schlüssel und lassen Sie sich die Schlüsseldetails anzeigen.



Bitte vergleichen Sie den Fingerabdruck in den Schlüsseldetails mit dem hier angegebenen Fingerabdruck:

```
E313 ABB5 BBC1 8132 045C E71E 8614 E29C C75E 4465
```

Stimmt der hier angegebene Fingerabdruck mit dem Fingerabdruck in Ihren Schlüsseldetails überein, verfügen Sie über den echten Supportschlüssel von Giegerich & Partner und können diesen nun bestätigen. Danach kann der Schlüssel zur sicheren Kommunikation verwendet werden.

Um einen Schlüssel gültig zu machen, lesen Sie bitte den Abschnitt zu **„Identitäten/Signieren“** (siehe Kapitel 8.10.4).

Hinweis: Wenn Sie den Schalter Immer alle Schlüssel als gültig betrachten deaktivieren, müssen Sie diese Überprüfung und Bestätigung mit jedem einzelnen Schlüssel durchführen, bevor Sie Ihn verwenden können.

11.9.2 Ablaufdatum von Schlüsselpaaren beim Programmstart prüfen

Wenn Sie diese Option aktivieren, werden Sie beim Programmstart darauf hingewiesen, wenn ein Schlüsselpaar das einem E-Mail Konto zugeordnet ist, in den nächsten 30 Tagen abläuft oder bereits abgelaufen ist.

Der Hinweis zeigt Ihnen die betroffenen Schlüsselpaare an und bietet Ihnen diese zur Verlängerung an. Stimmen Sie der Verlängerung zu, werden alle diese Schlüssel um ein Jahr verlängert.

Tipp: In den Schlüsseldetails können Sie das Ablaufdatum Ihrer Schlüsselpaare festlegen (siehe Kapitel 8.10.3)

11.9.3 GnuPG und gpg4o Informationen in ausgehende E-Mails einfügen

Wenn Sie eine E-Mail verfassen und verschlüsseln und/oder signieren, werden bei aktivierter Option die **GnuPG**-Version und die **gpg4o**-Version in die **GnuPG** Kopfzeilen eingefügt. Da dies auch bei anderen **OpenPGP**-Lösungen so realisiert wurde, ist diese Option standardmäßig aktiviert. Wenn Sie diesen Schalter deaktivieren und einer Ihrer Empfänger Probleme mit der Darstellung der E-Mail haben, kann er jedoch nicht ablesen, mit welcher Software die E-Mail verschlüsselt wurde.

11.9.4 Erweiterte Signatur-Prüfung aktivieren

Diese Option ist standardmäßig ausgeschaltet. Beim Auswählen einer PGP/MIME signierten E-Mail können Sie die erweiterten Singnaturprüfung aktivieren. Die Aktivierung bleibt für jede weitere PGP/MIME signierten E-Mail aktiv.

11.9.5 Automatischer Export von Schlüsseländerungen

Hier können Sie den Schlüsselserver eintragen, auf den öffentliche Schlüssel hochgeladen werden, sobald daran Änderungen stattfinden. Dies ist beispielsweise sinnvoll, wenn Sie selbst einen Schlüsselserver betreiben. Änderungen sind beispielsweise das Importieren eines Schlüssels von einem anderen Server oder aus einer Datei, das zurückziehen eines Schlüsselpaares, das hinzufügen oder bearbeiten einer Identität, oder das Unterschreiben eines fremden Schlüssels. Damit stellen Sie sicher, dass auf dem eingestellten Schlüsselserver immer die aktuellen öffentlichen Schlüssel liegen.

Hinweis: Beachten Sie, dass diese Funktionalität nicht mit **gpg4o *Free*** zur Verfügung steht.

11.9.6 Protokollierungsstufe von gpg4o

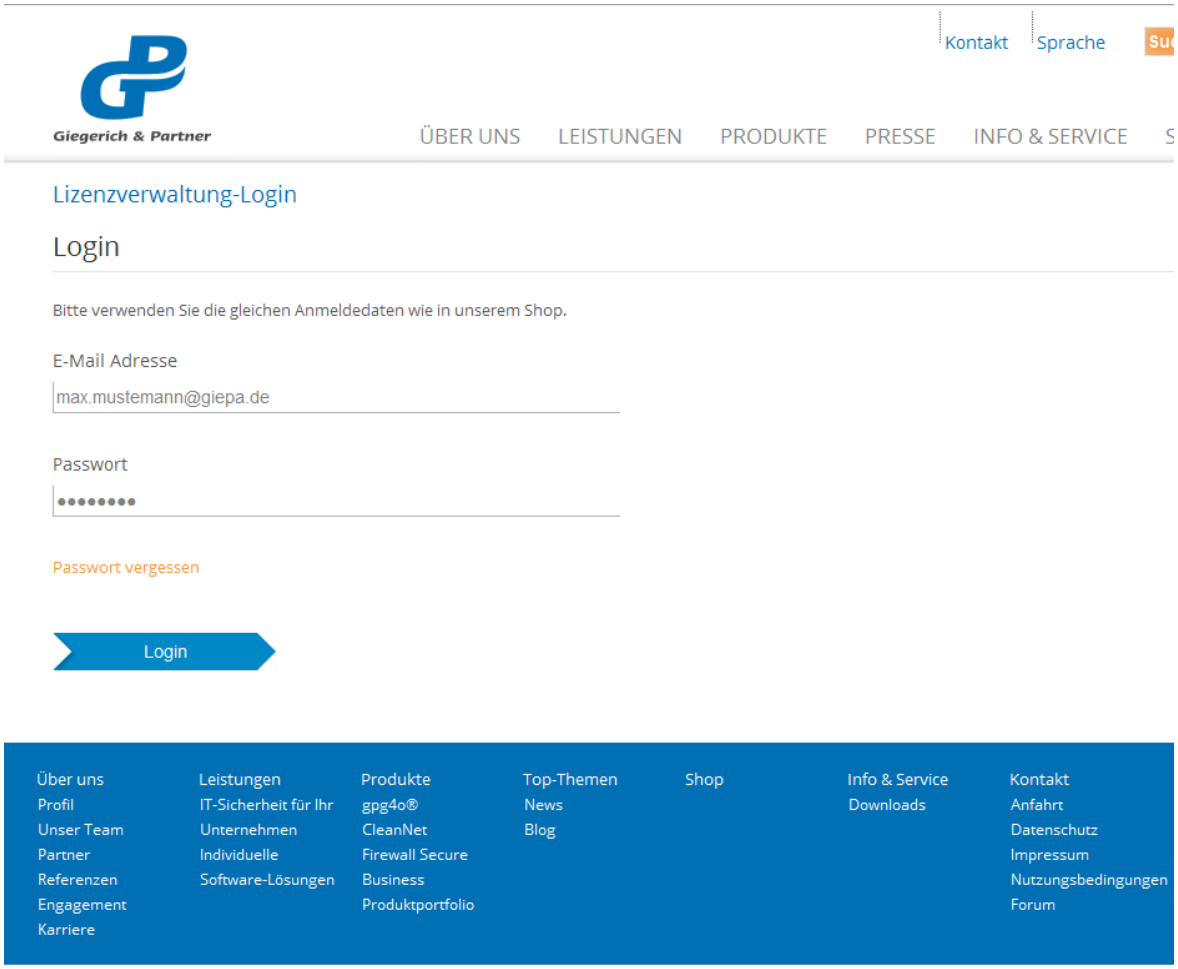
Hier können Sie die Detailstufe der Logdateien bestimmen. Standardmäßig ist hier die Stufe **„Normal“** eingestellt. Stellen Sie hier die Stufe **„Keine“** ein, werden ab diesem Zeitpunkt keine Logdateien mehr angelegt. Zusätzlich wird beim Kontaktieren des Supports (siehe Kapitel 13.2) keine Zip-Datei mit Logdateien automatisch an die E-Mail angehängt.

Hinweis: Beachten Sie bitte, dass bei der Protokolierungsstufe **„None“** die Arbeit des Supports deutlich erschwert wird.

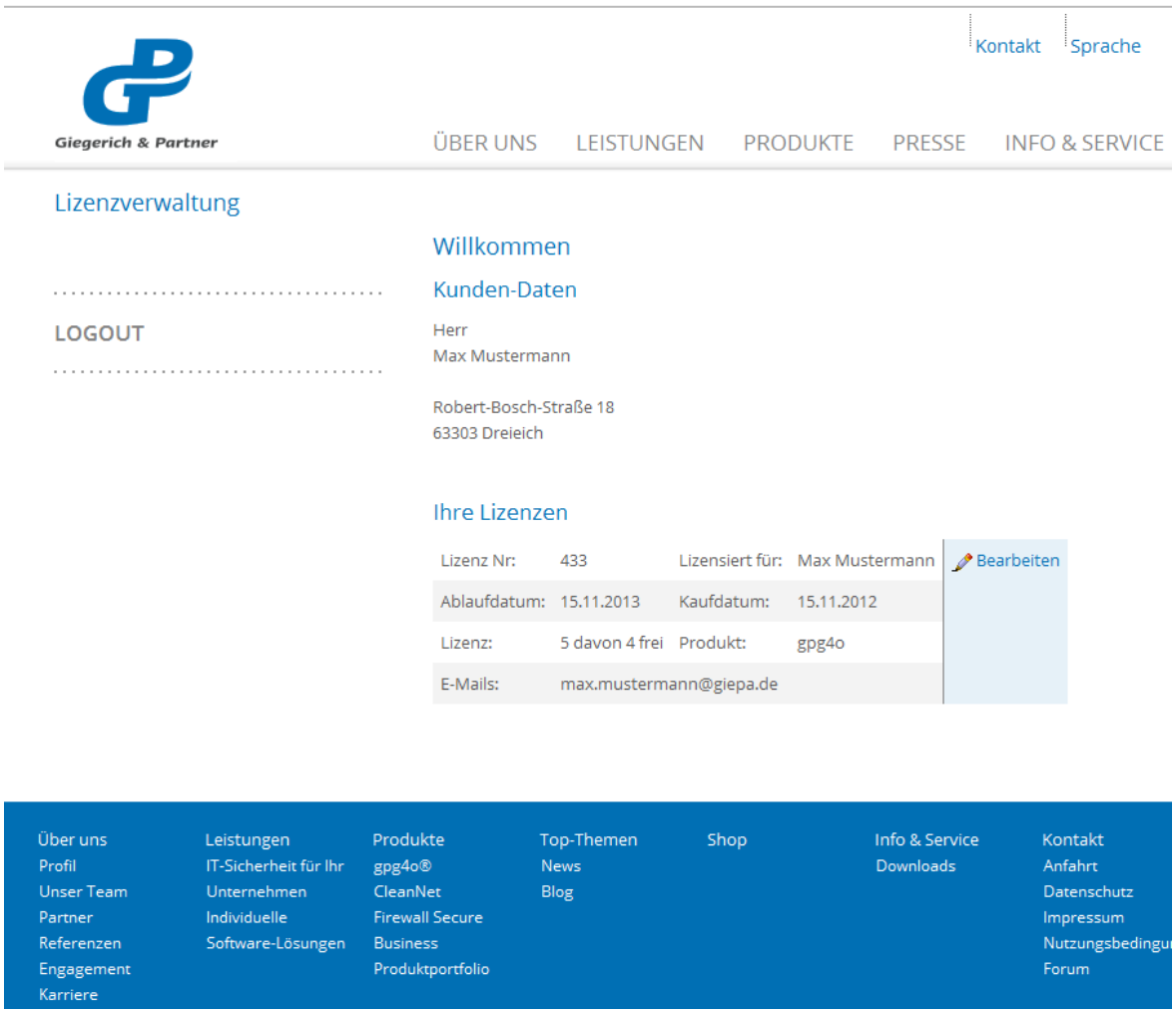
12 Lizenzdateien

12.1 Erzeugen und importieren von Lizenzdateien

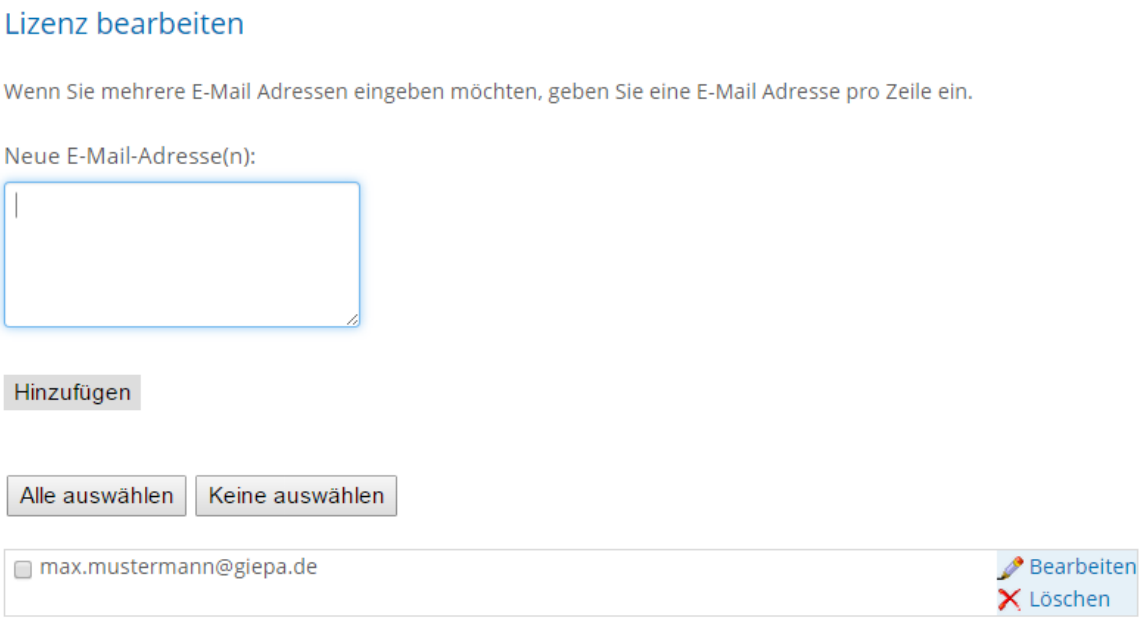
Nach Abwicklung der Online-Bestellung von **gpg4o** können Sie Ihre Lizenzen über unsere Lizenzverwaltung https://licmgmt.giepa.de/ beziehen.



Zur Anmeldung verwenden Sie die gleichen Zugangsdaten, die Sie auch in unserem Shop angegeben haben.

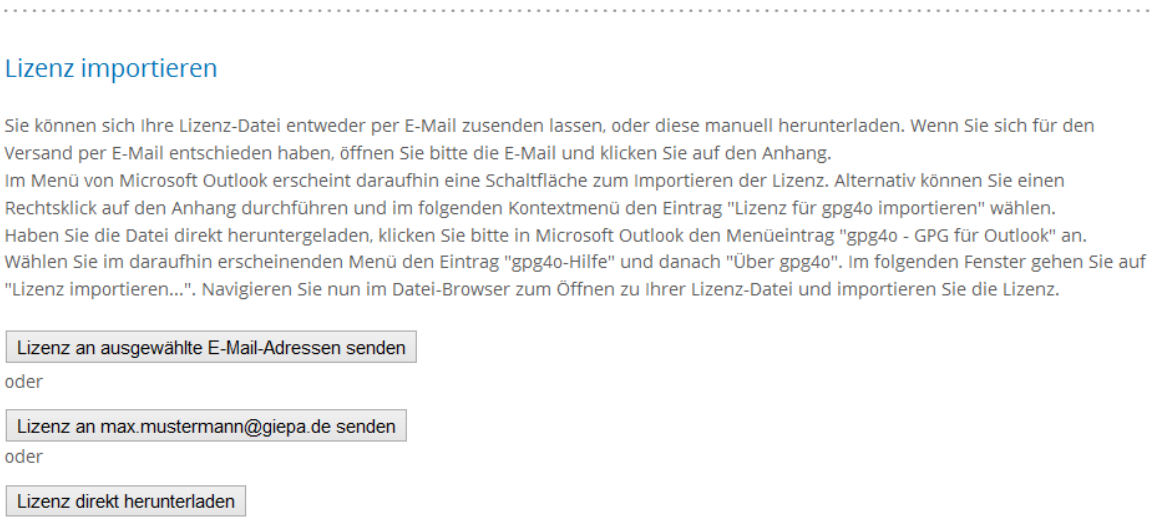


Nachdem Sie sich angemeldet haben, sehen Sie eine Übersicht Ihrer Bestellungen. Sie können einsehen, wie viele Lizenzen Ihnen zur Verfügung stehen und wie viele davon bereits benutzt werden, beziehungsweise noch verfügbar sind. Um Änderungen an Ihrer Lizenz vorzunehmen, klicken Sie auf die Schaltfläche Bearbeiten.



Tragen Sie nun die E-Mail-Adresse ein, die Sie für die Nutzung mit **gpg4o** lizenzieren wollen. Um mehrere E-Mail-Adressen auf einmal einzutragen, trennen Sie diese bitte jeweils in einer neuen Zeile.

Bereits eingetragene E-Mail-Adressen können über die Schaltflächen Bearbeiten und Löschen entsprechend angepasst werden.



Im Anschluss daran können Sie wählen, ob Sie die Lizenzdatei herunterladen oder per E-Mail geschickt bekommen möchten. Alternativ können Sie die Lizenz auch an die lizenzierten E-Mail-Adressen verschicken lassen. Wählen Sie dazu alle E-Mail Adressen aus, welchen die Lizenz zugestellt werden soll.

Um die Lizenz zu importieren, öffnen Sie Microsoft Outlook und wählen Sie im Menüband

gpg4o – GPG für Outlook die Schaltfläche gpg4o-Hilfe und Über gpg4o. Im erscheinenden Fenster klicken Sie auf Lizenz importieren... . Es erscheint ein Dateiauswahl-Dialog, in dem Sie bitte die heruntergeladene Lizenz auswählen und Öffnen wählen. Nach erfolgreicher Prüfung der Lizenz durch **gpg4o** wird Ihre Lizenzdatei importiert. Es erscheint eine entsprechende Meldung, die Sie mit einem Klick auf OK bestätigen können.

Wenn Sie die Lizenzdatei als Dateianhang per E-Mail erhalten haben, wird Ihnen **gpg4o** ab Version 5.1 den Import anbieten, falls diese Lizenz besser als die aktuell eingespielte ist. (siehe Kapitel 11.4.4) Es ist ebenfalls möglich, die Lizenzdatei direkt zu importieren. Klicken Sie dazu mit der rechten Maustaste auf den Anhang der E-Mail und wählen Sie im Kontext-Menü den Punkt Lizenz für gpg4o importieren .

12.2 Laufzeit der Lizenz

Die Lizenz von **gpg4o** berechtigt Sie zur zeitlich nicht limitierten Nutzung von **gpg4o** mit der lizenzierten E-Mail Adresse. Die Laufzeit der Lizenz beginnt mit dem ersten Download der Lizenzdatei. **gpg4o** wird pro reale Person lizenziert. Daher funktioniert **gpg4o** auch mit nur einer Lizenz an mehreren Computern, sowie mit weiteren E-Mail Adressen innerhalb der gleichen Installation, solange die lizenzierte E-Mail Adresse in Microsoft Outlook eingerichtet ist.

12.3 Laufzeit der Produktwartung/Support

Während der Laufzeit der Produktwartung/Support erhalten Sie Produktupdates mit zahlreichen neuen Funktionalitäten für **gpg4o**. Des Weiteren haben Sie die Möglichkeit, bei Fragen oder Problemen den Support per E-Mail support.gpg4o@giepa.de in Anspruch zu nehmen.

Wenn die Laufzeit der Produktwartung/Support abgelaufen ist, kann **gpg4o** weiterhin genutzt werden. Das heißt, Sie können weiterhin E-Mails verschlüsselt/signiert versenden und verschlüsselte/signierte E-Mails lesen. Sie verlieren damit den Anspruch auf künftige Updates und auf den Support.

12.4 Verlängerung der Produktwartung/Support

Das Entwicklerteam von **gpg4o** verbessert das Programm stetig und integriert Anregungen von Kunden in neue Versionen. Mit einer Verlängerung der Produktwartung können Sie neue Versionen von **gpg4o** beziehen, die nach Ablauf Ihrer Produktwartung veröffentlicht wurden. Außerdem verlängern Sie damit auch die Möglichkeit, den Support via E-Mail zu kontaktieren. Die Laufzeit der Produktwartung wird um die Anzahl der gekauften Jahre der Verlängerung erhöht. Damit wird das Ablaufdatum der Produktwartung um die gekauften Jahre verlängert.

Beispiel 1:

Ursprüngliches Ablaufdatum: 01.04.2019

Sie kaufen am 01.02.2019, im ersten Jahr nach dem Kauf von **gpg4o**, eine Verlängerung von einem Jahr.

Neues Ablaufdatum nach dem Kauf der Verlängerung: 01.04. 2020

Beispiel 2:

Ursprüngliches Ablaufdatum: 01.04.2019

Sie kaufen am 01.06.2019, zwei Monate nach Ablauf der Produktwartung, eine Verlängerung von einem Jahr.

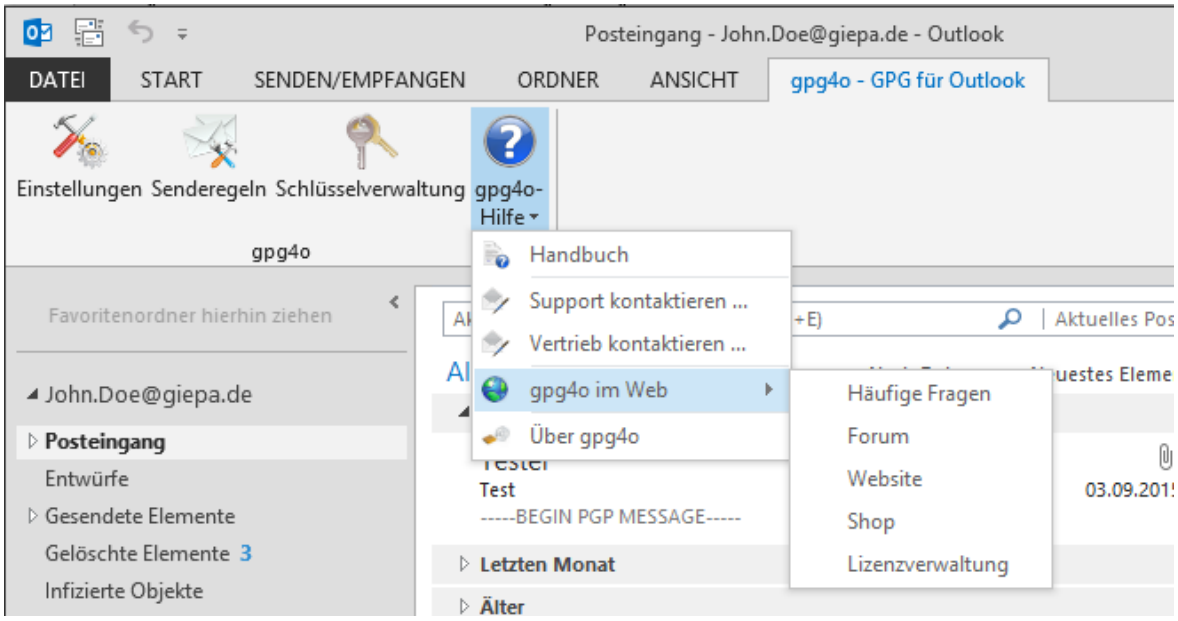
Neues Ablaufdatum nach dem Kauf der Verlängerung: 01.04. 2020

Hier haben Sie einen Verlust von 2 Monate Support.

Hinweis: Nach Kauf einer Verlängerung muss diese neue, veränderte Lizenzdatei einmalig in **gpg4o** importiert werden.

13 Hilfecenter

Über das Hilfecenter erhalten Sie einen einfachen und schnellen Zugriff auf alle wichtigen Informationen zur Verwendung von **gpg4o**.

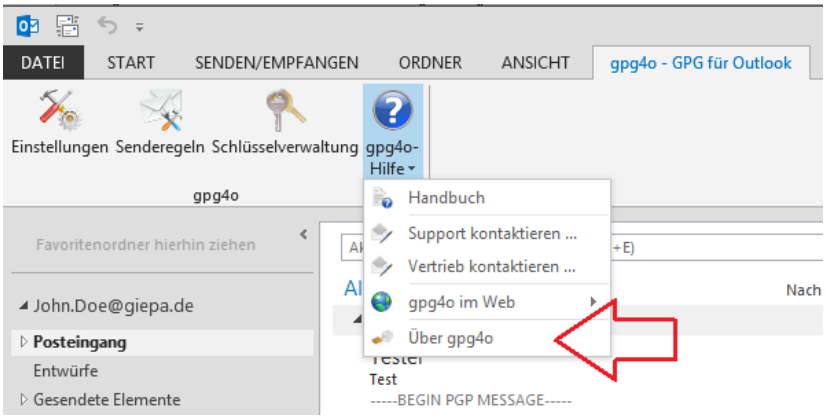


Sie können hier das Handbuch öffnen, eine E-Mail an den technischen Support oder den Vertrieb schreiben oder sich im Internet über **gpg4o** informieren.

Über den Menüeintrag gpg4o im Web erhalten Sie Zugriff auf die folgenden Webseiten:

- Häufige Fragen
- Forum
- Webseite
- Shop
- Lizenzverwaltung

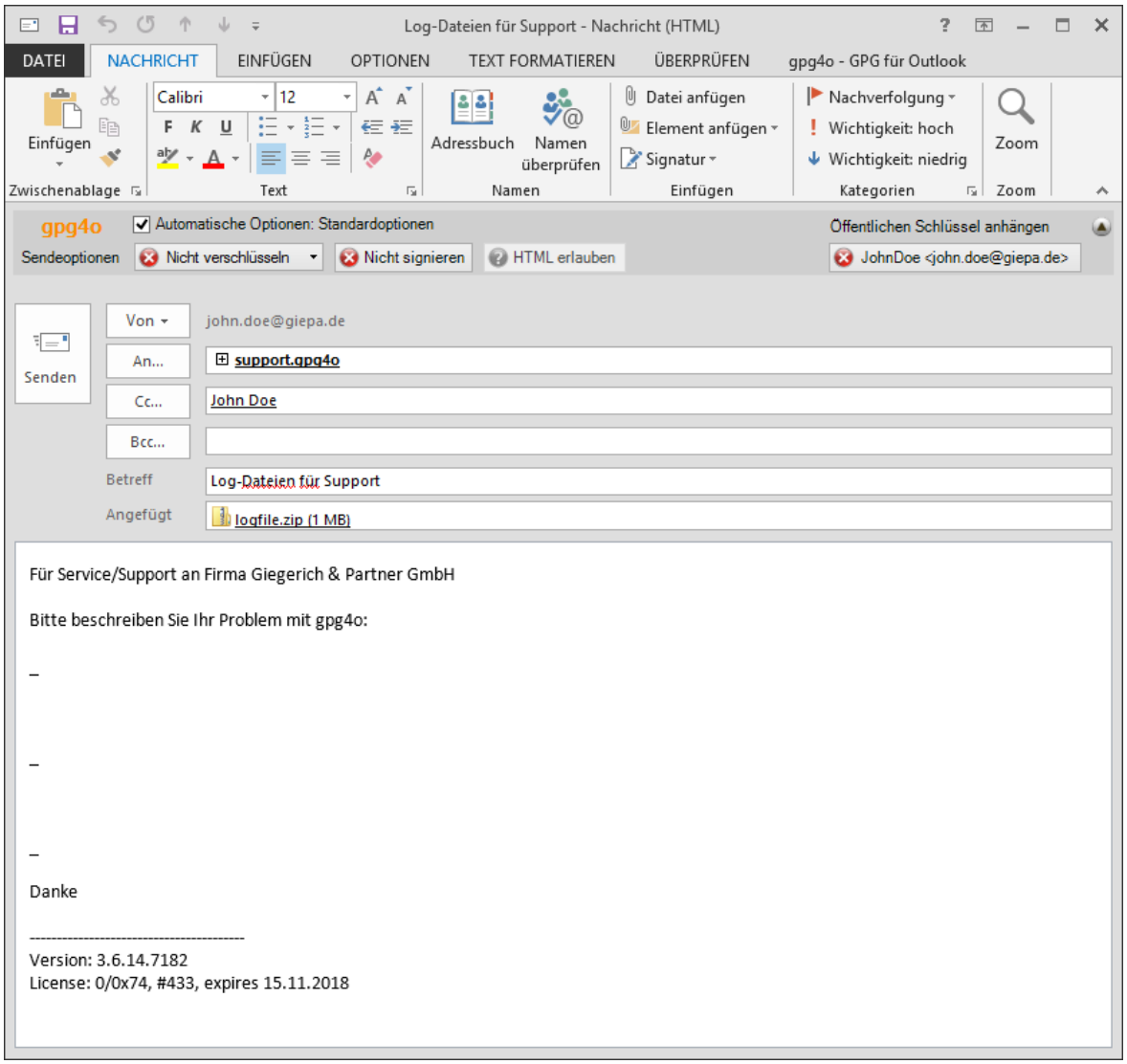
13.1 Informationen zu gpg4o



Um weitere Informationen zu **gpg4o** zu erhalten, klicken Sie bitte auf gpg4o-Hilfe und Über gpg4o. Im daraufhin erscheinenden Fenster können Sie Informationen zu Ihrer Lizenz und der aktuell verwendeten Version einsehen.

13.2 Versenden von Log-Dateien

Um die Log-Dateien an unseren Support zu senden, klicken Sie im Menüband von Microsoft Outlook auf gpg4o – GPG für Outlook. Wählen Sie hier die Schaltfläche gpg4o-Hilfe und klicken dann auf den Eintrag Support kontaktieren ... . Es öffnet sich nun automatisch eine vorkonfigurierte E-Mail mit den Log-Dateien als Anhang.



Bitte beschreiben Sie den aufgetretenen Fehler und die Schritte, die Sie kurz davor ausgeführt haben möglichst genau. Sie helfen uns damit die Fehlerquelle einzugrenzen und Ihnen möglichst schnell eine Lösung anbieten zu können.

13.3 Inhalt von Log-Dateien

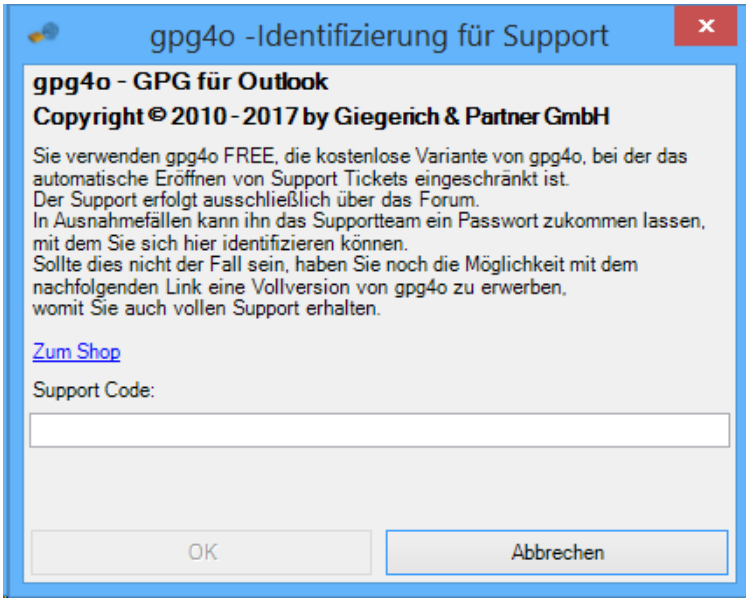
Damit unsere Entwicklungsabteilung möglichst effizient eventuell auftretende Fehler beseitigen kann, werden Statusmeldungen von **gpg4o** in so genannte Log-Dateien geschrieben. Diese Statusmeldungen enthalten weder persönliche Informationen, Passwörter noch Inhalte von E-Mails. Vor dem Senden der E-Mail mit den Log-Dateien können Sie die übermittelten Informationen einsehen, indem Sie die angehängte Zip-Datei entpacken. Alle darin enthaltenen Dateien bestehen aus Klartext.

13.4 Hilfe in gpg4o *Free*

Die **Free Version** von **gpg4o** wird ohne den Anspruch auf Support zur Verfügung gestellt.

Die erste Anlaufstelle für Sie sollte das Forum von **Giegerich & Partner** sein. Dies erreichen Sie ebenfalls über das Hilfecenter von **gpg4o**.

In Ausnahmefällen kann Ihnen das Supportteam ein Passwort zukommen lassen, mit dem Sie eine Supportanfrage über **gpg4o** stellen können. Durch Eingabe dieses Passwortes können Sie sich im nachfolgenden Dialog identifizieren und bei gültigem Passwort den Support für zehn Tage in Anspruch nehmen.



14 Sonstiges

14.1 Was tun bei Fehlern?

Bitte helfen Sie uns, Fehler aufzudecken und zu beseitigen.

Um auftretende Fehler schnell beheben zu können, benötigen wir möglichst detaillierte Informationen zu dem aufgetretenen Fehler. Bitte senden Sie uns die Fehlerberichte sowie die Log-Dateien über die dafür vorgesehene E-Mail aus **gpg4o** heraus. (siehe Kapitel 13.2)

Sollten Sie Fragen, Kritik oder Verbesserungsvorschläge haben, schicken Sie uns diese bitte auf gleichem Wege zu oder schreiben uns in unser gpg4o & GnuPG Forum (siehe Kapitel 13), denn auch hierfür haben wir immer ein offenes Ohr.

14.2 Hilfsprogramme

Für bestimmte Probleme bringt **gpg4o** Programme zu Analyse und Korrektur mit sich. Diese Programme werden in den Installationspfad von gpg4o abgelegt und können dort aufgerufen werden.

14.2.1 Maintenance_Registry

Verwenden Sie dieses Programm, wenn **gpg4o** nach jedem Start von Outlook manuell geladen werden muss und nicht aktiviert bleibt. Bitte beachten Sie, dass dieses Programm zur korrekten Ausführung Administrator-Rechte benötigt.

14.2.2 Maintenance_LogFiles

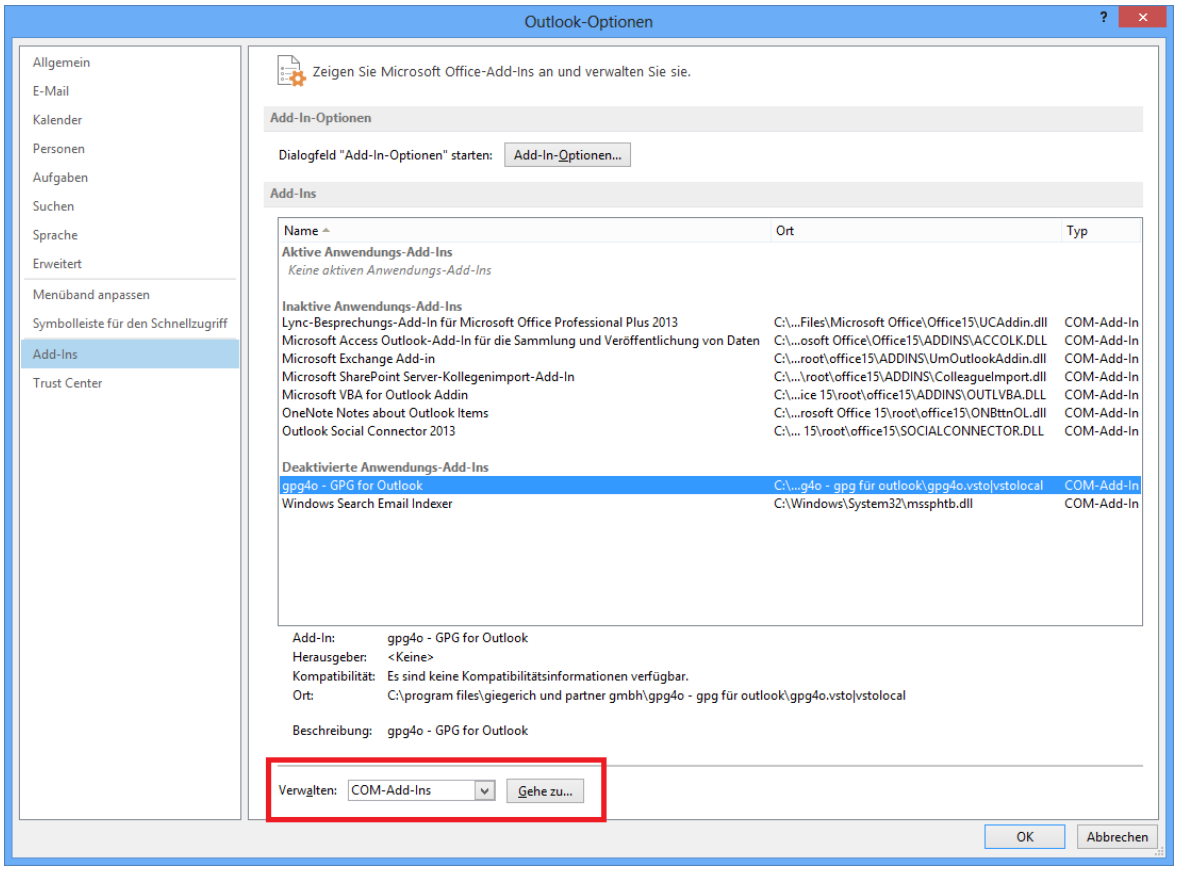
Erstellt aus den Log Dateien von **gpg4o** eine Zip Datei und hängt diese an eine neue E-Mail an, die Sie an den Support senden können.

14.2.3 Maintenance_Outlook

Diese Anwendung liefert Informationen, die bei Problemen mit der Lizenzierung von **gpg4o** auftreten können. Dazu werden grundlegende Informationen über die eingerichteten E-Mail Konten ausgegeben. Diese Ausgaben beinhalten beispielsweise die E-Mail Adresse und das verwendete E-Mail Protokoll.

14.3 gpg4o startet nicht

Sollte **gpg4o** nicht mehr angezeigt werden, gibt es mehrere Möglichkeiten, das Add-In wieder zu aktivieren. Öffnen Sie zunächst bitte Ihre Outlook Optionen, indem Sie im Menüband auf Datei klicken und dort den Menüpunkt Optionen auswählen. Klicken Sie im folgenden Fenster auf der linken Seite auf Add-Ins.



Suchen Sie nun auf der rechten Seite den Eintrag gpg4o – GPG for Outlook. Sollte **gpg4o** unter **„Deaktivierte Anwendungs-Add-Ins“** stehen, lesen Sie bitte das Kapitel 14.3.1.

Steht **gpg4o** unter **„Inaktive Anwendungs-Add-Ins“**, lesen Sie bitte das Kapitel 14.3.2.

14.3.1 Deaktivierte Anwendungs-Add-Ins

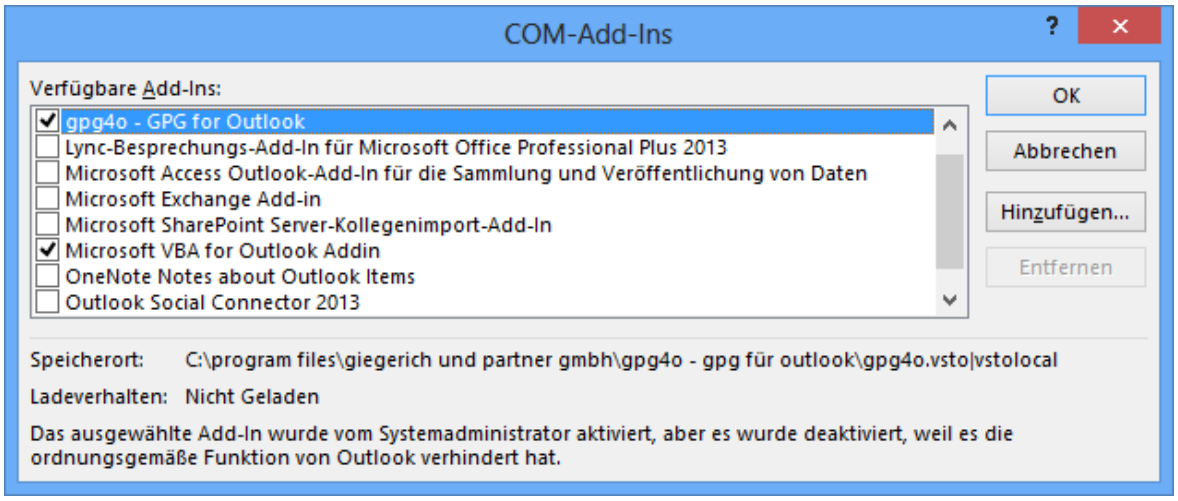
Wählen Sie im unteren Bereich neben der Schaltfläche Gehe zu... den Eintrag **„Deaktivierte Elemente“** in der Auswahl aus und klicken Sie danach auf die Schaltfläche Gehe zu... Im nun geöffneten Fenster wählen Sie den Eintrag gpg4o – GPG for Outlook aus und klicken anschließend auf die Schaltfläche Aktivieren. Schließen Sie danach das Fenster mit einem Klick auf Schließen. Nach einem Moment sollte **gpg4o** wieder geladen werden. Wenn nicht, kann es nötig sein, **gpg4o** über den in Kapitel 14.3.2 beschriebenen Weg nachträglich zu aktivieren.

14.3.2 COM-Add-Ins

Bitte beachten Sie, dass Outlook als Administrator gestartet werden muss, damit die folgende Änderung dauerhaft wirksam wird.

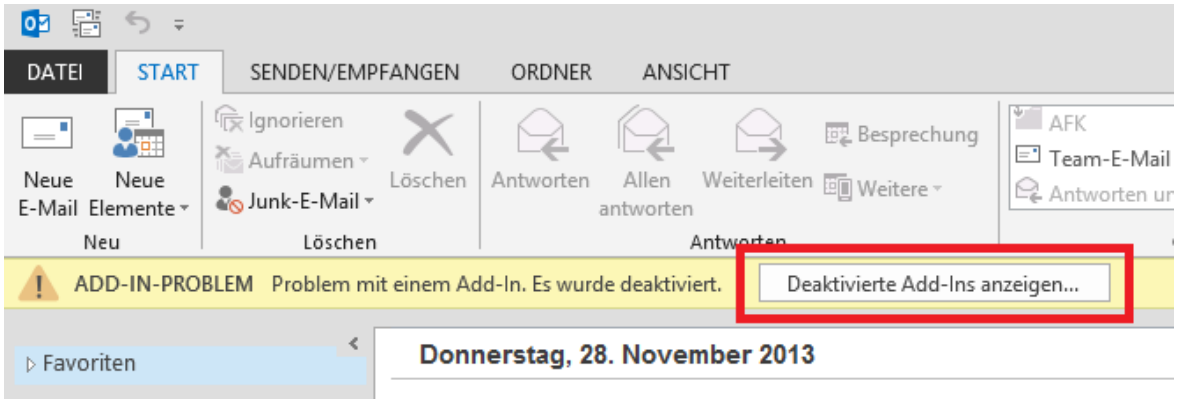
Wählen Sie im unteren Bereich neben der Schaltfläche Gehe zu... den Eintrag **„COM-Add-Ins“** in der Auswahl aus und klicken Sie danach auf die Schaltfläche Gehe zu... Im nun

geöffneten Fenster suchen Sie den Eintrag gpg4o – GPG for Outlook und setzen davor einen Haken. Schließen Sie danach das Fenster mit einem Klick auf OK. Nach einem Moment sollte **gpg4o** wieder geladen werden. Sollte dies nicht der Fall sein, kann es sein, dass ein grundlegendes Problem vorliegt. In diesem Fall kontaktieren Sie bitte den Support (siehe Kapitel 13.2).

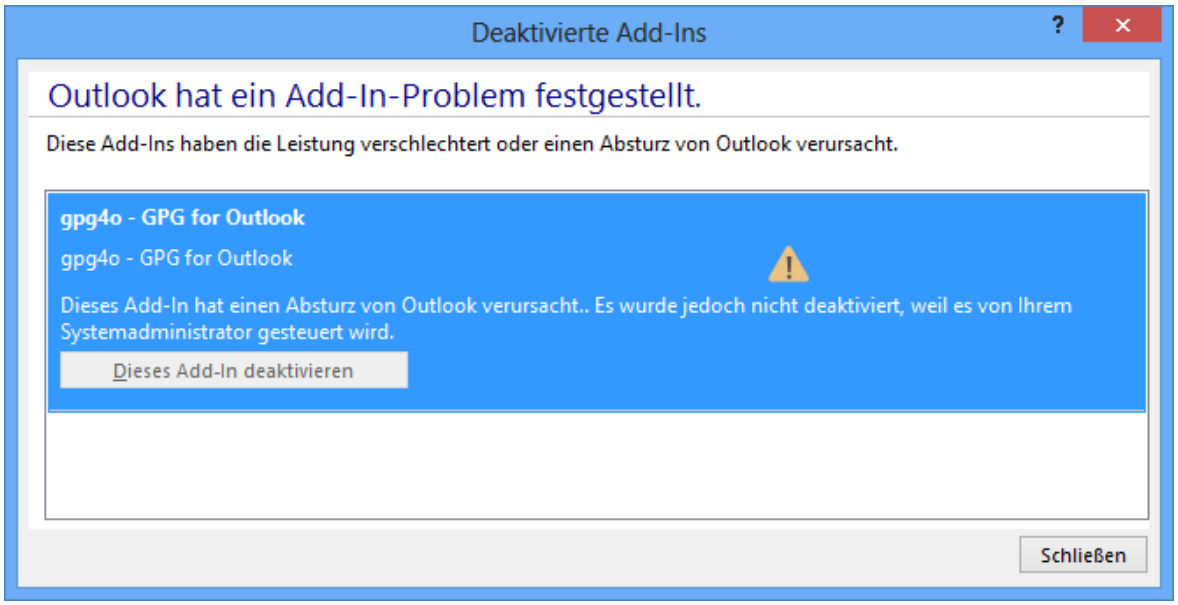


14.3.3 Outlook 2013 und Outlook 2016

Microsoft Outlook 2013 und 2016 analysieren die Ladezeiten von Add-Ins und deaktiviert Add-Ins mit durchschnittlich längeren Ladezeiten automatisch.



Wenn dies bei Ihnen der Fall sein sollte, gehen Sie bitte im Menüband auf Datei und dort auf Add-Ins verwalten.



Wählen Sie **gpg4o** aus und drücken Sie auf die Schaltfläche Dieses Add-In aktivieren. Anschließend klicken Sie bitte auf die Schaltfläche Schließen.

15 Deinstallation

Wenn Sie **gpg4o** und/oder **GnuPG** deinstallieren, bleiben alle angelegten und importierten Schlüssel erhalten und stehen Ihnen nach einer erneuten Installation wieder zur Verfügung.

15.1 Löschen der persönlichen Daten

Falls Sie Ihre Schlüssel komplett löschen möchten, sollten Sie dies über die Schlüsselverwaltung von **gpg4o** erledigen und erst im Anschluss daran **gpg4o** deinstallieren.

Alternativ löschen Sie das Datenverzeichnis von **GnuPG**. Dort befinden sich sämtliche persönlichen Daten, welche durch **GnuPG** verwaltet werden (Schlüsselbünde, Vertrauenseinstellungen und Programmkonfigurationen).

Des Weiteren sollten Sie auch das **gpg4o** Benutzerverzeichnis und das Microsoft Outlook Konfigurationsverzeichnis löschen. Dort befinden sich die persönlichen Einstellungen von **gpg4o**.

15.1.1 GnuPG Datenverzeichnis

```
%AppData%\gnupg
```

Achtung: Bitte beachten Sie, dass nicht nur das Programm **gpg4o** auf **GnuPG**-Schlüssel zugreift. Ein Löschen der Daten kann andere Programme beeinträchtigen.
Durch das Löschen der Schlüsseldateien verlieren Sie dauerhaft den Zugriff auf Ihre verschlüsselten E-Mails! Ohne die passenden Schlüssel können Ihre E-Mails nicht entschlüsselt werden.

15.1.2 gpg4o Benutzerverzeichnis

```
%AppData%\Giegerich & Partner GmbH\gpg4o\
```

15.1.3 Microsoft Outlook Konfigurationsverzeichnis

```
%AppData%\Local\Microsoft_Corporation\gpg4o.vsto_...
```

Dieser Pfad variiert je nach Computer und kann in ähnlicher Form mehrfach vorhanden sein.

15.2 Deinstallation von gpg4o

Um **gpg4o** zu deinstallieren, klicken Sie im Windows Startmenü auf Systemsteuerung und navigieren Sie dort zum Punkt Programme und anschließend zu Programm deinstallieren. Sie sehen nun die Liste aller auf Ihrem Rechner installierten Programme. Wählen Sie gpg4o – GPG für Outlook aus und klicken Sie im Menü auf Deinstallieren.

15.3 Deinstallation von GnuPG

Um **GnuPG** zu deinstallieren, klicken Sie im Windows Startmenü auf Systemsteuerung und navigieren Sie dort zum Punkt Programme und anschließend zu Programm deinstallieren. Sie sehen nun die Liste aller auf Ihrem Rechner installierten Programme. Wählen Sie das installierte **GnuPG** aus und klicken Sie im Menü auf Deinstallieren.

16 Firmen- und Kontaktinformationen

16.1 Über Giegerich & Partner GmbH

Firmenprofil

Giegerich & Partner ist Ihr zuverlässiger IT-Lösungsanbieter. Wir schaffen effiziente IT-Infrastrukturen, sorgen für IT-Sicherheit, erstellen effiziente Softwarelösungen und veredeln Standardprodukte. Die individuellen Bedürfnisse unserer Kunden geben dabei den Rahmen jedes Projekts vor. Unsere Dienstleistung geht jedoch weit über die Abnahme hinaus. Wir bieten unseren Kunden zu jedem Produkt auch den persönlichen Support an. Durch kompetente Ansprechpartner statt anonymer Callcenter.

Wer und Wo

Mit knapp 40 Mitarbeitern in der Nähe von Frankfurt am Main – Deutschland betreuen wir über 1300 Kunden weltweit in über 70 Länder, wenn es um IT Sicherheit, Softwareentwicklung und E-Mail Verschlüsselung geht. Als ein Mitglied des TeleTrust Verbandes in Deutschland haben wir uns verpflichtet sichere IT Lösungen ohne Hintertüren zu entwickeln. Dies erlaubt uns ein Mitglied der „IT Security made in Germany“ Gruppe zu sein.

Unsere Mission

Setzen Sie auf zuverlässige IT-Lösungen nach Maß. Wir widmen uns seit 1993 mit Energie, Leidenschaft und Kompetenz der Realisierung dieser individuellen Bausteine Ihres Unternehmenserfolgs. Mit uns als Partner können Sie sich auf ihr Kerngeschäft konzentrieren. Wir kümmern uns um passende Softwarelösungen und die nötige Sicherheit Ihrer Unternehmens-IT. Wir bieten Ihnen aus einer Hand: IT nach Maß.

Unsere Werte

Fachliche Kompetenz ist wichtig. Sie alleine ist uns als inhabergeführtes Unternehmen jedoch noch nicht genug. Verlässlichkeit, Nachhaltigkeit, Persönlichkeit und Partnerschaft bilden die Grundlage für ein funktionierendes Miteinander und gegenseitiges Vertrauen. Der Mensch und seine unverwechselbare Persönlichkeit stehen daher stets im Mittelpunkt unseres Handelns. Wir stellen Ihnen darum einen festen Ansprechpartner zur Seite, der Sie langfristig kompetent begleitet. So sorgen wir auf der persönlichen und der technischen Ebene dafür, dass Ihre Hard- und Software auf Dauer zukunftsfähig bleibt. Denn wir wollen, dass Sie sich jederzeit guten Gewissens auf uns verlassen können.

Besuchen Sie unsere Website auf https://www.giepa.de

16.2 Supportinformationen

Bitte nutzen Sie die nachfolgenden E-Mail Adresse um den Support bezogen auf **gpg4o** von **Giegerich & Partner** GmbH:

support.gpg4o@giepa.de

Sie können ebenfalls unser Kontaktformular verwenden:

https://www.giepa.de/kontakt/

Kontaktinformationen:

Giegerich & Partner GmbH

Rober-Bosch-Str. 18

D-63303 Dreieich

Deutschland

Telefon: +49 (0)6103-5881-0

Internet: https://www.giepa.de