Thunderbird Portable + GPG/Enigmail

Bedienungsanleitung für die Programmversion 17.0.2

Kann heruntergeladen werden unter
https://we.riseup.net/assets/125110/versions/1/ThunderbirdPortableGPG17.0.2.zip

Grundsätzliches

Thunderbird Portable + GPG/Enigmail ist ein Programm, mit dem ihr eure E-Mails verschlüsseln könnt. Ein PGP-Schlüssel besteht aus zwei Teilen: Den **öffentlichen Schlüssel (public key)** benötigt man, um an den Besitzer dieses Schlüssels eine verschlüsselte Mail zu schicken. Den **privaten Schlüssel (private key)** braucht der Empfänger, um eine verschlüsselte Mail wieder zu öffnen. Jeder Schlüssel ist einer bestimmten E-Mailadresse zugeordnet. Wenn ihr eine verschlüsselte Mail an eine bestimmte E-Mailadresse versenden wollt, benötigt ihr zunächst den *öffentlichen* Schlüssel, der dieser E-Mailadresse zugeordnet ist. Der Empfänger kann diese E-Mail nur dann entschlüsseln, wenn er erstens im Besitz des dazugehörigen *privaten* Schlüssels ist und zweitens die **Passphrase** zu dem privaten Schlüssel kennt.

Wichtig: Bitte führt **keine Aktualisierungen/Updates** des Programms durch, auch dann nicht, wenn Thunderbird euch dazu auffordert. Es kann passieren, dass nach einem Update die Verschlüsselungsfunktion nicht mehr vorhanden ist.

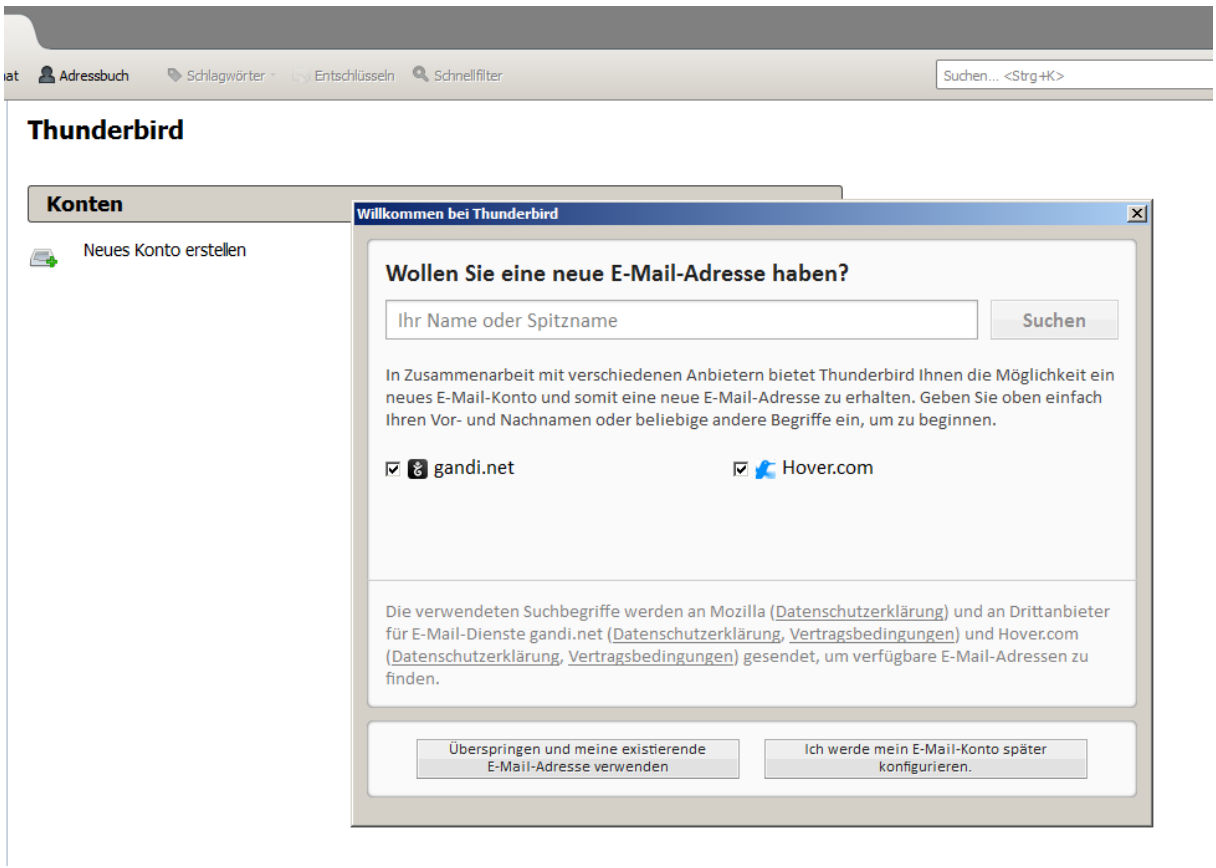
organize.blogsport.eu

Vorbereitung

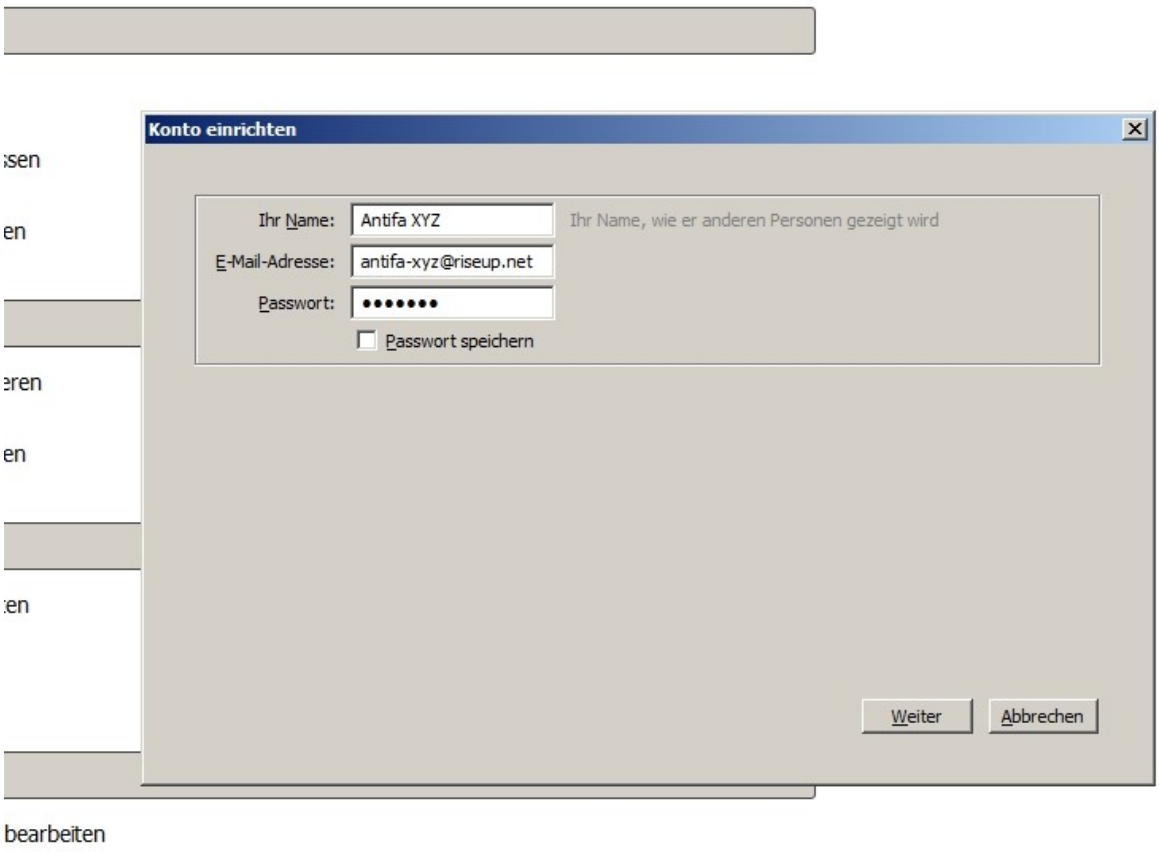
- Programm herunterladen
- Doppelklick auf die Datei ThunderbirdPortable+GPG 17.0.2.zip
- Datei entpacken und den darin enthaltenen Ordner auf einen beliebigen Datenträger kopieren (entweder auf eure Festplatte oder auf einen USB-Stick)

Programm einrichten

- Anschließend den Ordner ThunderbirdPortable öffnen.
- Programm starten durch Doppelklick auf ThunderbirdPortable.exe
- Nun auf „Überspringen und meine existierende E-Mail-Adresse verwenden“ klicken

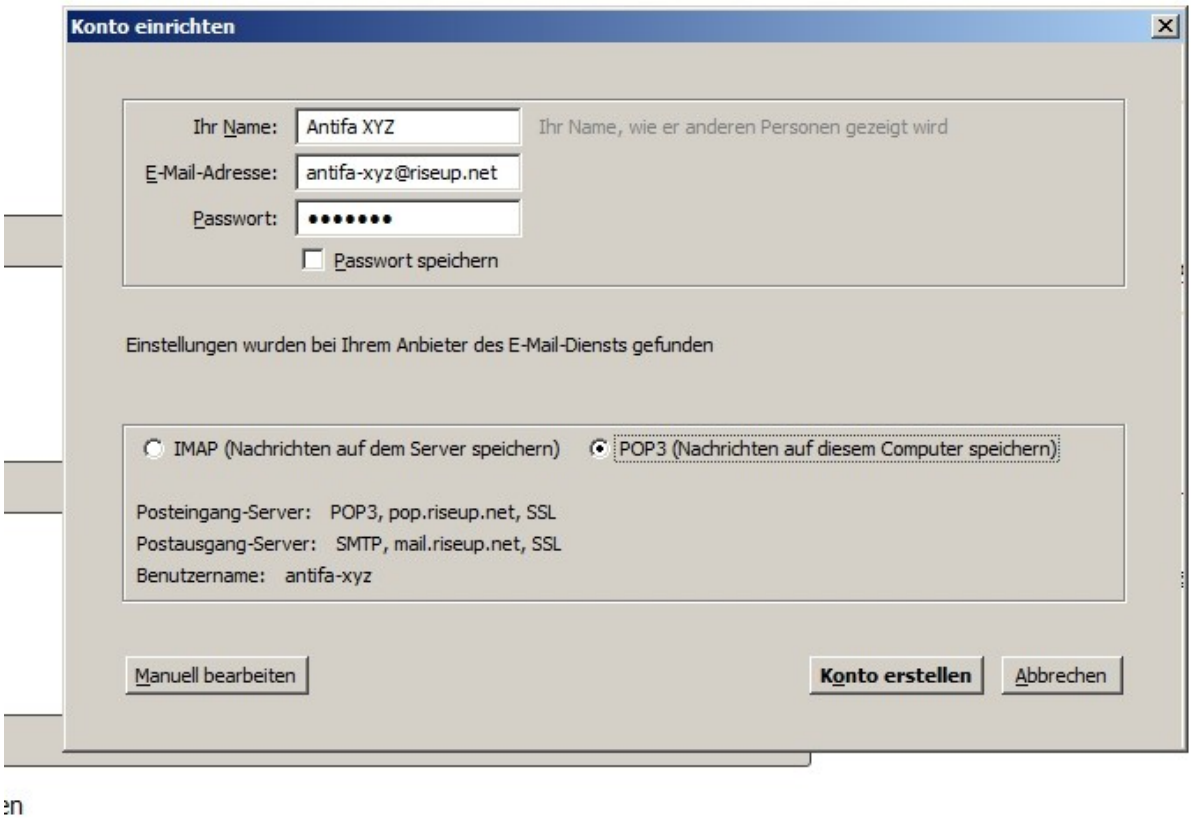


- Benutzernamen und E-Mailadresse auswählen, Passwort eures E-Mail-Kontos eingeben
- anschließend auf „Weiter“ klicken



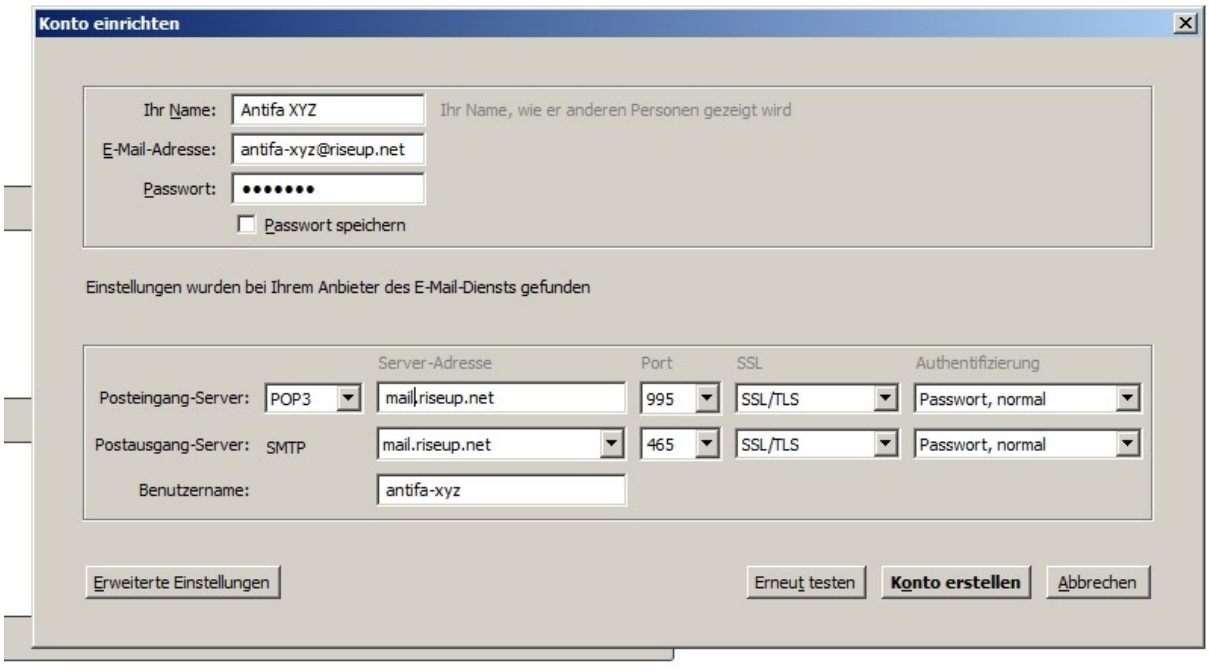
organize.blogsport.eu

- dann „Manuell bearbeiten“ wählen



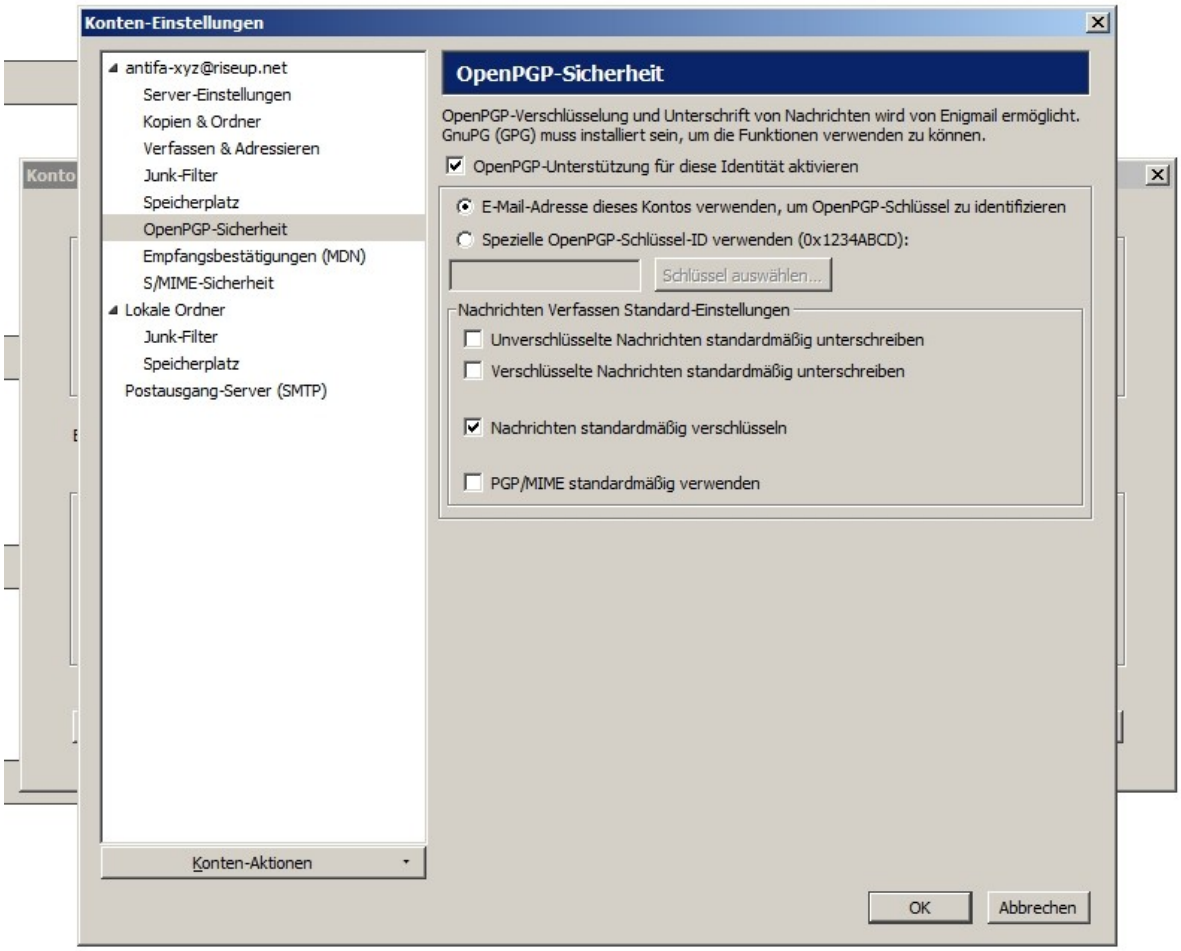
- prüfen, ob die Serveradresse bei **„Posteingang-Server“** und **„Postausgang-Server“** korrekt angegeben ist
- je nach Anbieter muss unter **„Benutzername“** entweder nur der Teil eurer E-Mailadresse vor dem „@“ („antifa-xyz“) oder die gesamte E-Mailadresse („antifa-xyz@riseup.net“) eingegeben werden
- die richtigen Angaben für euren E-Mail-Anbieter findet ihr unter http://www.patshaping.de/hilfen_ta/pop3_smtp.htm
- wenn euer Anbieter dort nicht aufgeführt ist, müsst Ihr nach dem Begriff „Thunderbird“ und eurem Anbieter googlen
- für E-Mailadressen bei **riseup.net** lauten die Daten:
  Posteingang-Server: mail.riseup.net
  Postausgang-Server: mail.riseup.net
  Benutzername: vorderer Teil eurer E-Mailadresse (Ohne „@riseup.net“)

- anschließend auf „Erweiterte Einstellungen“ klicken



organize.blogsport.eu

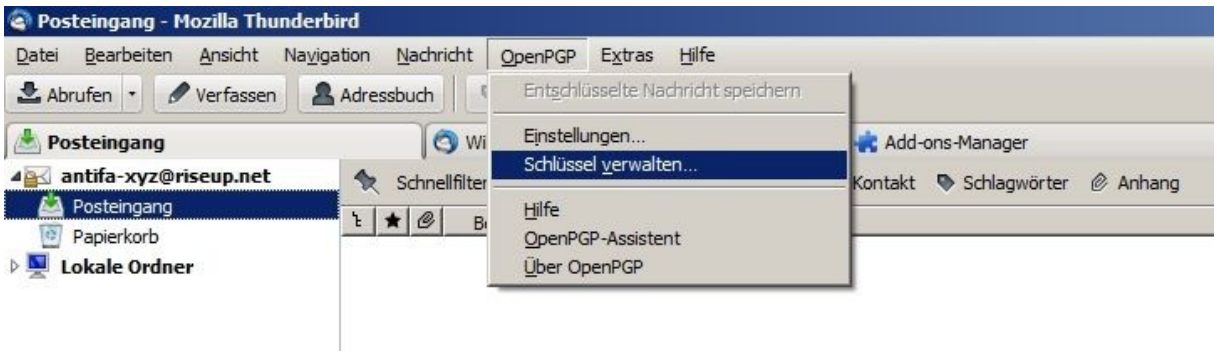
- hier **„OpenPGP-Sicherheit“** anklicken
- Häkchen bei **„OpenPGP-Unterstützung für diese Identität aktivieren“** und bei **„Nachrichten standardmäßig verschlüsseln“** setzen
- dann auf „OK“



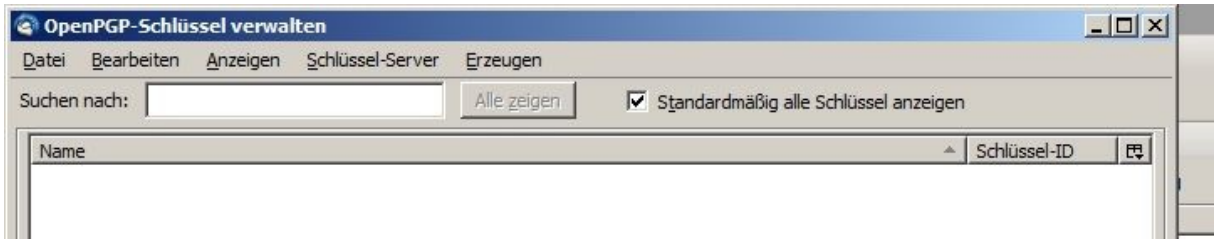
Eigenen PGP-Schlüssel erstellen

Um selbst verschlüsselte E-Mails von anderen Benutzern erhalten zu können, braucht ihr einen eigenen Schlüssel, der eurer E-Mailadresse zugeordnet ist.

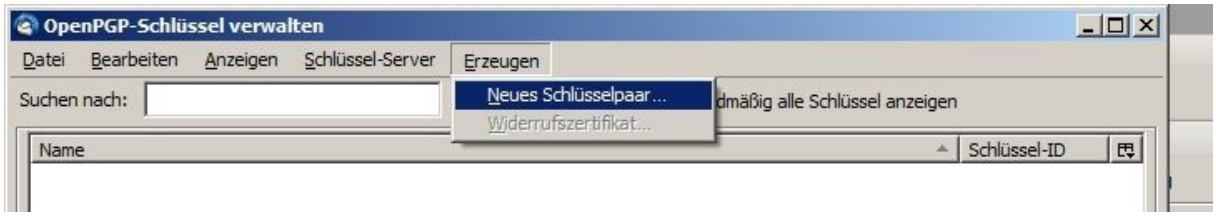
- „OpenPGP“ anklicken und „Schlüssel verwalten“ wählen



- Häkchen setzen bei „Standardmäßig alle Schlüssel anzeigen“

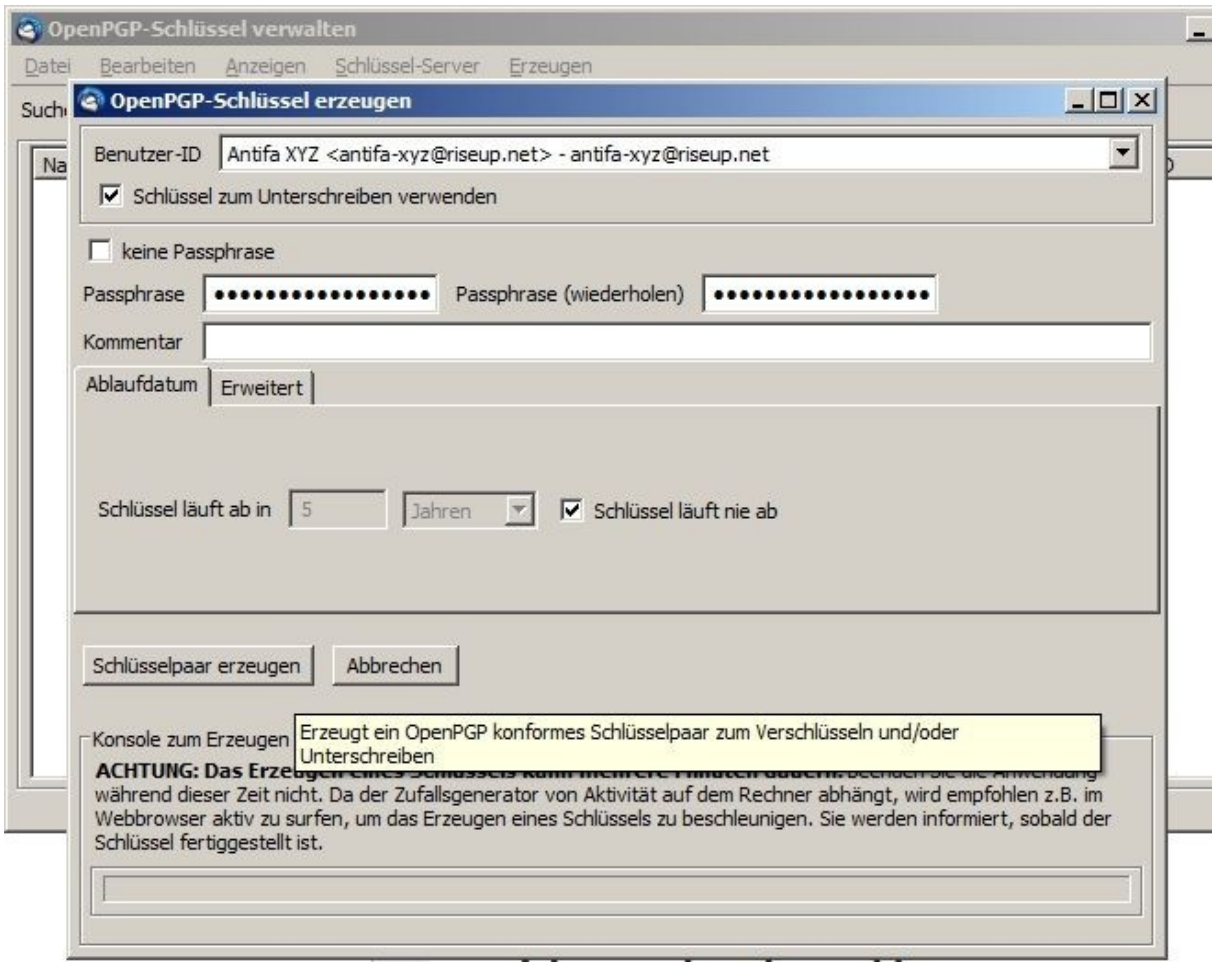


- dann auf „Erzeugen“ klicken und „Neues Schlüsselpaar…“ wählen



organize.blogsport.eu

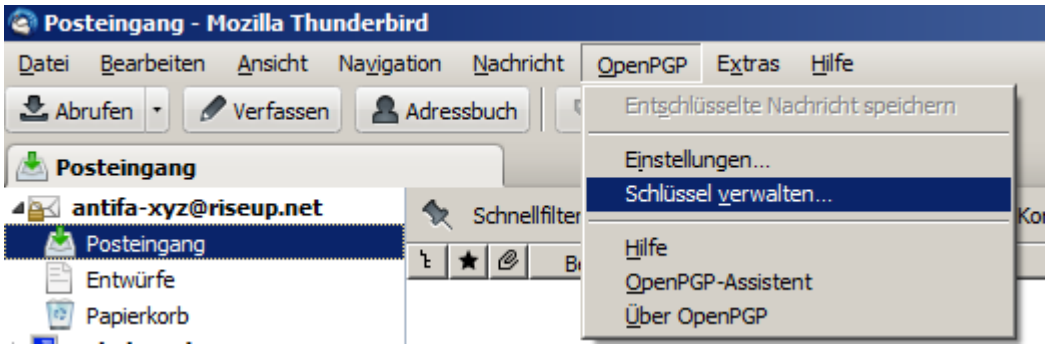
- Passphrase überlegen und eingeben
- dann auf „Schlüsselpaar erzeugen“ klicken
- anschließende Nachfrage bestätigen („Schlüssel erzeugen“)



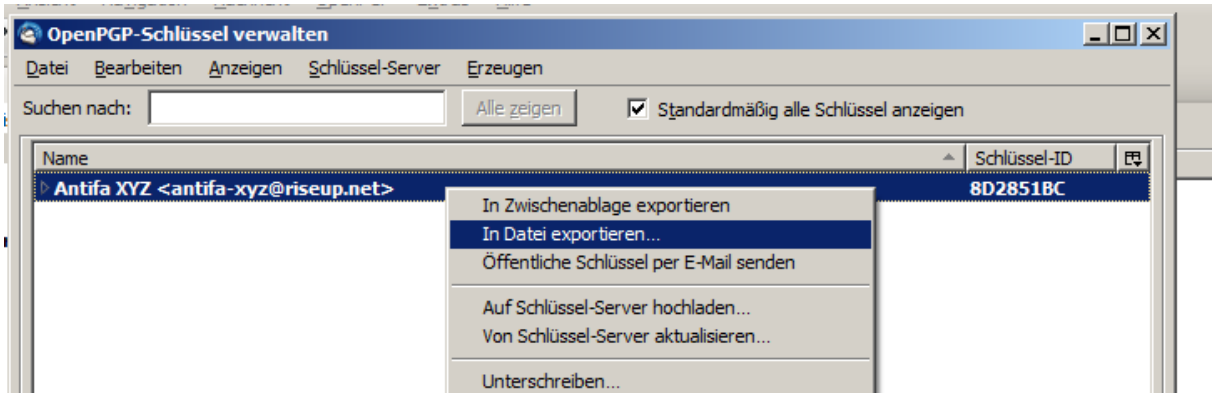
Eigenen PGP-Schlüssel sichern

Wenn euer privater Schlüssel einmal verloren geht, etwa weil euer Computer kaputt ist, könnt ihr die Mails, die mit diesem Schlüssel verschlüsselt wurden, nie wieder lesen. Deshalb ist es sinnvoll, eine Kopie seines privaten Schlüssels anzulegen und auf einem externen Speichermedium (z.B. USB-Stick) aufzubewahren.

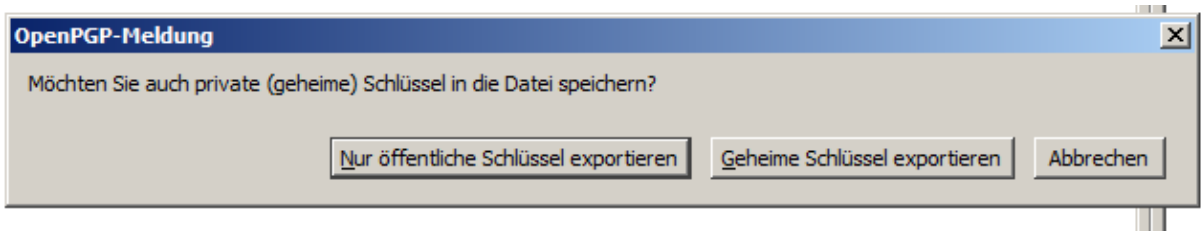
- auf „OpenPGP“ klicken und „Schlüssel verwalten“ wählen



- dann den eigenen Schlüssel per Rechtsklick anwählen und „In Datei exportieren“ anklicken



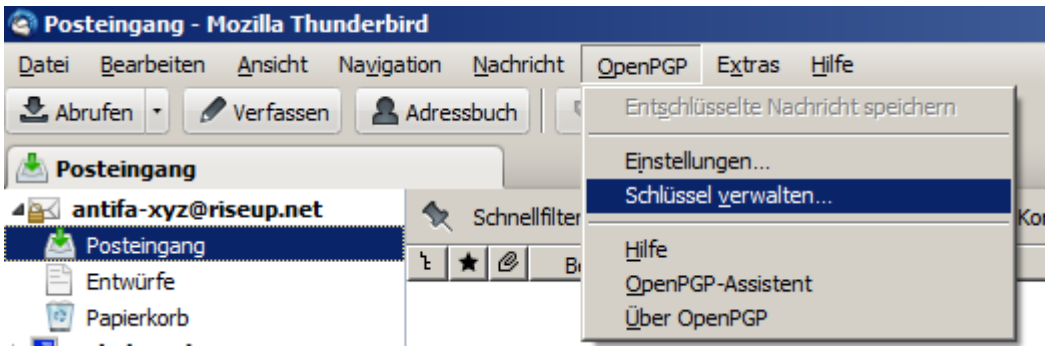
- anschließend auf **„Geheime Schlüssel exportieren“** klicken



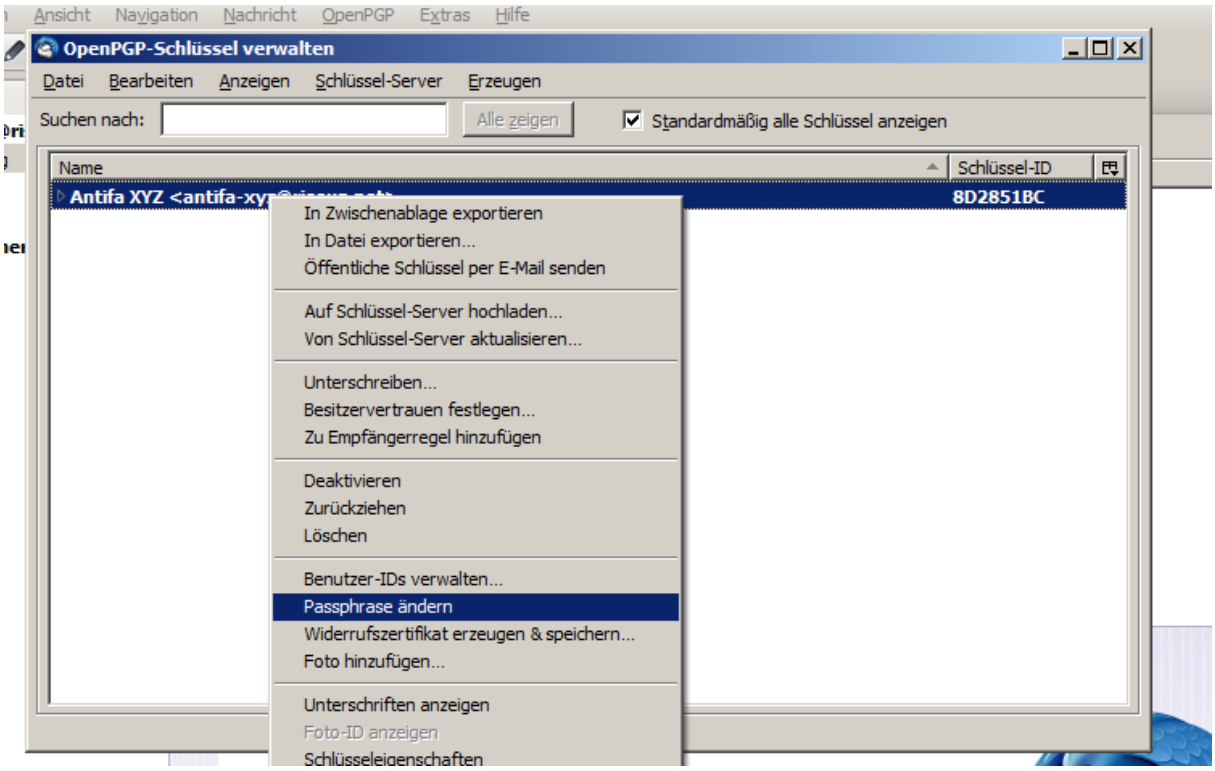
organize.blogsport.eu

Passphrase des eigenen Schlüssels ändern

- auf „OpenPGP“ klicken und „Schlüssel verwalten“ wählen



- den eigenen Schlüssel per Rechtsklick anwählen und „Passphrase ändern“ anklicken



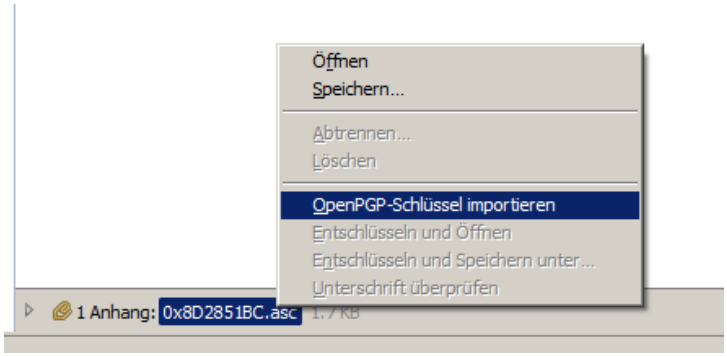
organize.blogsport.eu

Neue Schlüssel in die eigene Liste aufnehmen

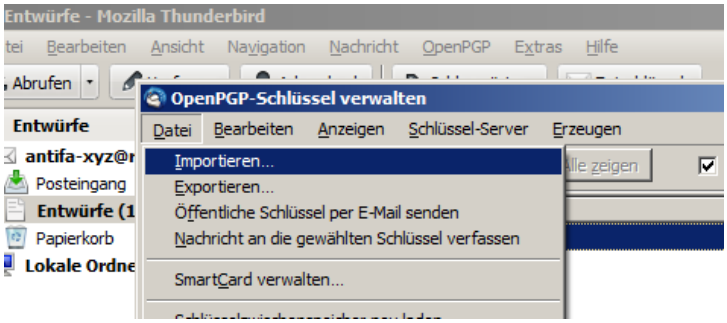
Um verschlüsselte Mails an einen bestimmten Empfänger schicken zu können, benötigt ihr den öffentlichen Schlüssel (public key) dieses Empfängers.

Öffentliche Schlüssel können in Form eines Textblocks oder einer **asc-Datei** vorliegen.

Am einfachsten ist das Importieren neuer Schlüssel, wenn euch diese per Mail zugeschickt werden. wenn der Schlüssel in der Mail als Textblock vorliegt, klickt ihr einfach auf entschlüsseln, dann wird der Schlüssel automatisch importiert. Ist er als asc-Datei angehängt, klickt ihr den anhang mit der rechten Maustaste an und wählt „OpenPGP-Schlüssel importieren“.



Wenn Ihr einen öffentlichen Schlüssel beispielsweise als asc-Datei oder txt-Datei von einer Website heruntergeladen und auf der Festplatte gespeichert habt, müsst ihr wieder auf „OpenPGP“ und „Schlüssel verwalten“ gehen. Dann geht ihr auf „Datei“ und klickt „importieren“ an. Nun wählt ihr die Datei mit dem zu importierenden Schlüssel auf eurer Festplatte aus und klickt auf „Öffnen“.

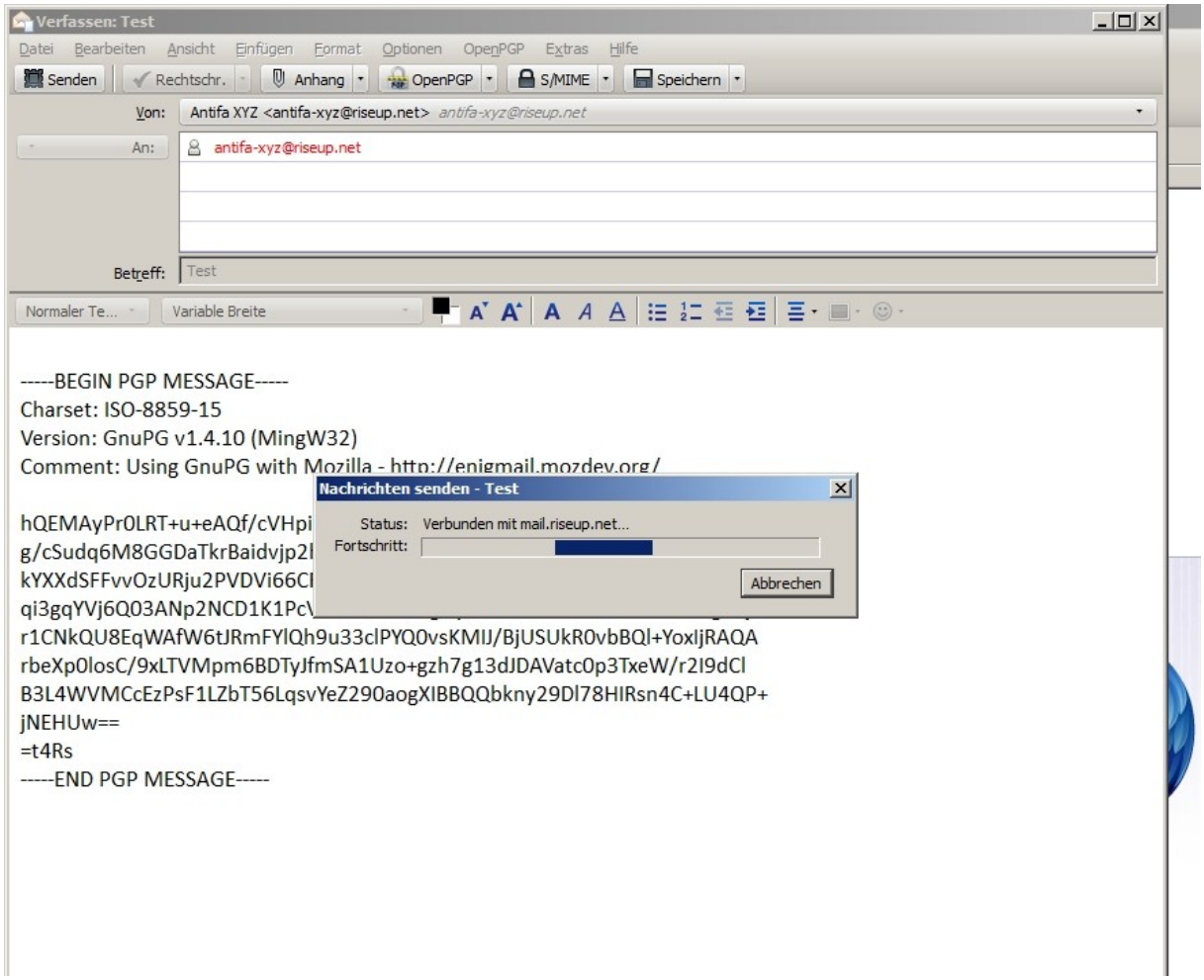


Liegt der Schlüssel als Textblock vor, muss dieser in die Zwischenablage kopiert werden. Dann geht ihr auf „OpenPGP“ und „Schlüssel verwalten“, klickt nun „Bearbeiten“ an geht auf „Aus Zwischenablage importieren“.

Verschlüsselte E-Mails schreiben

- oben auf „Verfassen“ klicken

- Mail verfassen
- auf „Senden“ klicken
- Mail wird automatisch verschlüsselt, wenn der öffentliche Schlüssel (public key) des Empfängers vorhanden ist



organize.blogsport.eu

Anhänge verschlüsseln

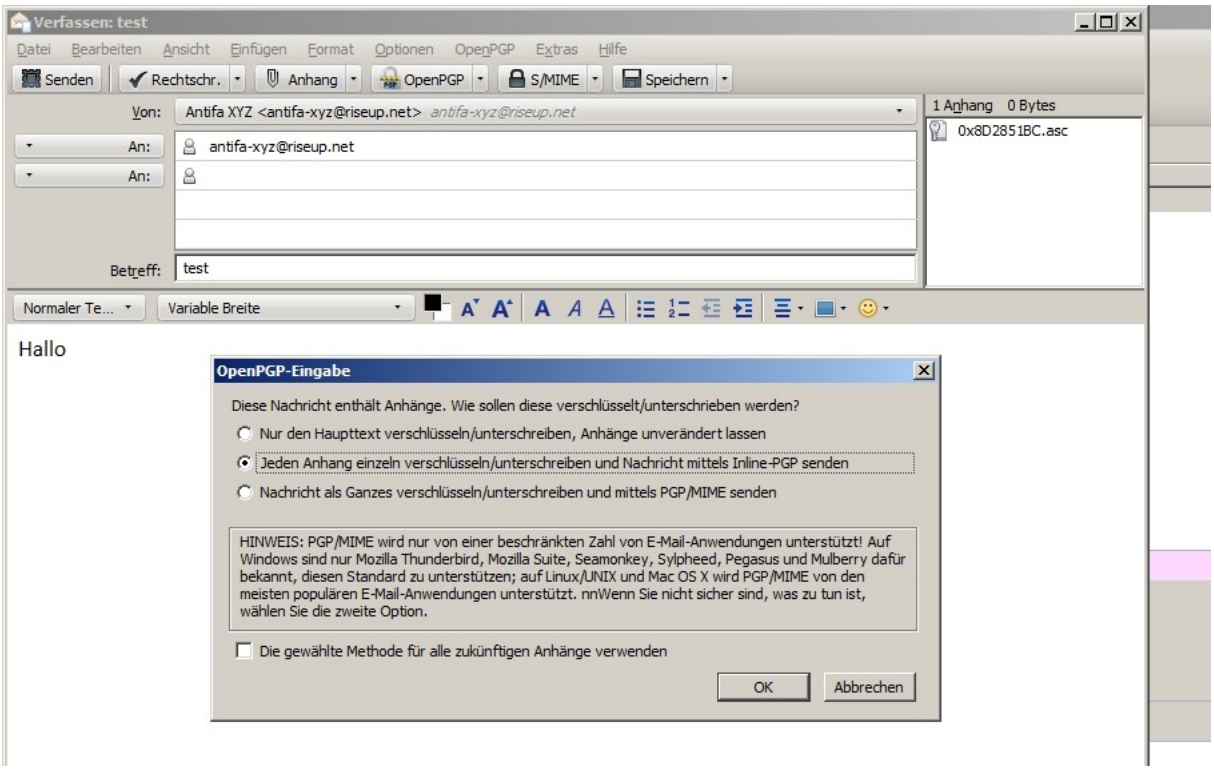
Wenn man versucht, Mails mit Anhängen zu verschicken, bietet Thunderbird drei verschiedene Möglichkeiten an, das zu tun:

1. Nur den Haupttext verschlüsseln/unterschreiben, Anhänge unverändert lassen (sollte man nicht tun)

2. Jeden Anhang einzeln verschlüsseln

3. Die ganze Mail als Paket verschlüsseln (PGP/MIME). Das ist für den Empfänger am praktischsten, hat aber den Nachteil, dass diese Mails nur von Empfängern entschlüsselt werden können, die ihrerseits auch Thunderbird zum ver- und entschlüsseln ihrer Mails benutzen.

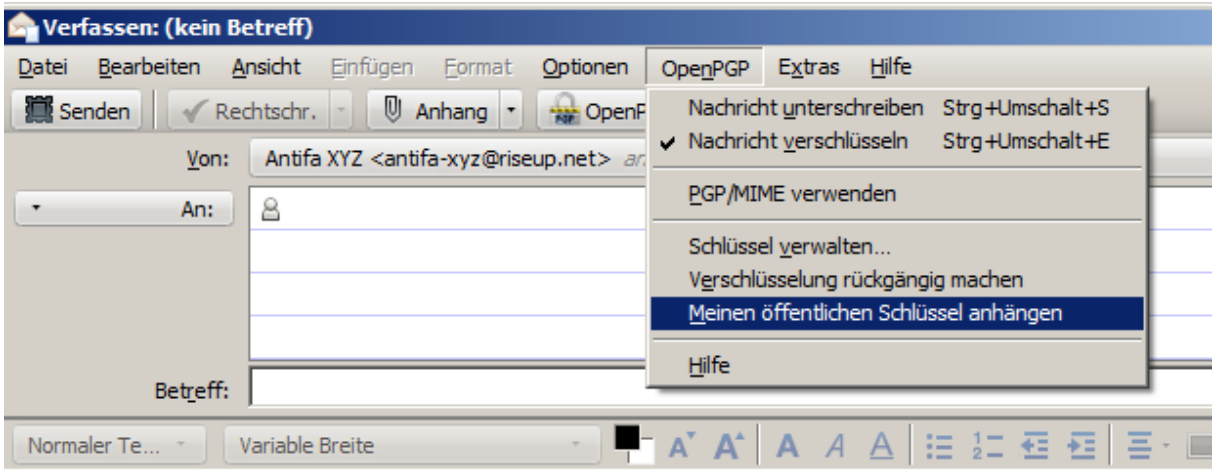
Im Zweifelsfall sollte ihr also die zweite Option wählen.



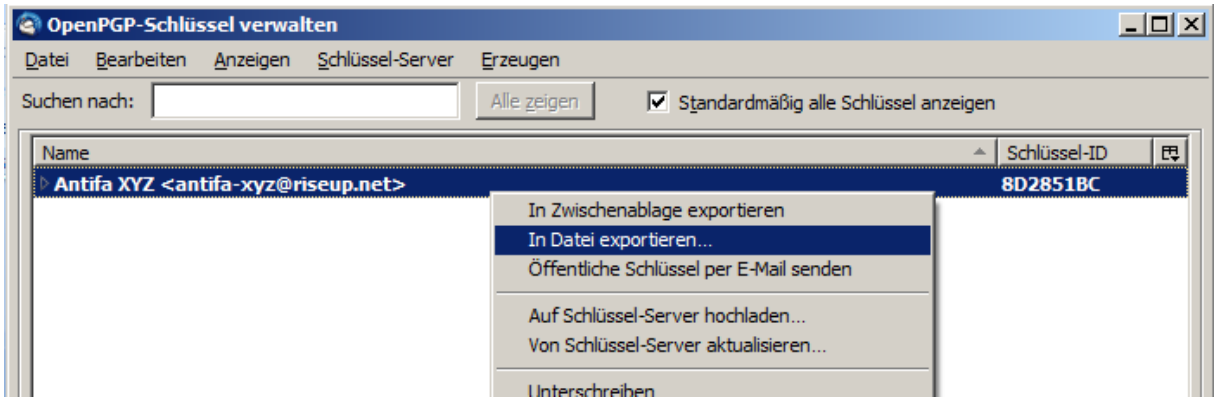
Anderen Benutzern euren öffentlichen Schlüssel mitteilen

Damit andere Benutzer euch eine verschlüsselte E-Mail schreiben können, benötigen sie euren öffentlichen Schlüssel (public key).

- entweder eine Mail an den betreffenden Benutzer verfassen und unter „OpenPGP“ **„Meinen öffentlichen Schlüssel anhängen“** auswählen



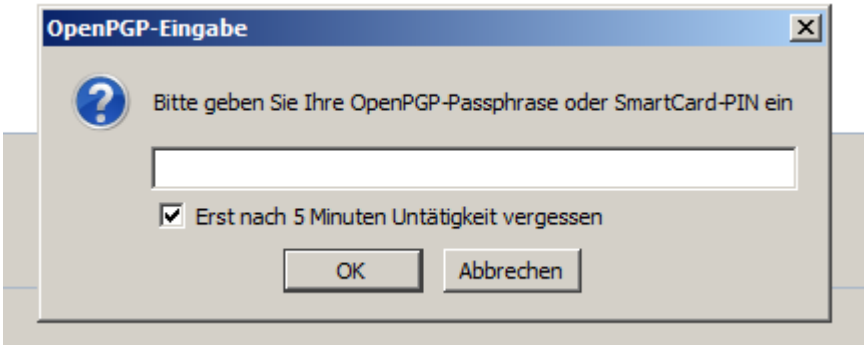
- …oder direkt auf „OpenPGP“ und „Schlüssel verwalten“, dort den eigenen Schlüssel per Rechtsklick anwählen und auf „In Datei exportieren…“ klicken. Die folgende Frage unbedingt mit **„Nur öffentliche Schlüssel exportieren“** beantworten
- dann kann der öffentliche Schlüssel als asc-Datei auf der Festplatte gespeichert und anschließend beispielsweise auf einer Website hochgeladen werden



organize.blogsport.eu

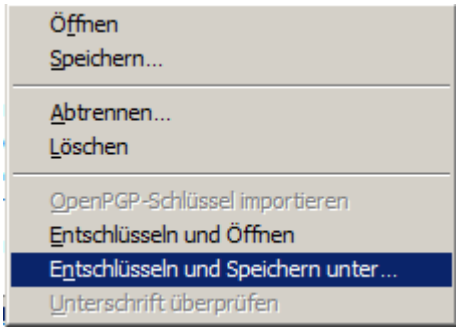
Verschlüsselte Mails lesen

Wenn ihr eine Mail, die mit eurem öffentlichen Schlüssel verschlüsselt wurde, öffnet, werdet ihr dazu aufgefordert, eure PGP-Passphrase einzugeben. Sobald ihr das getan habt, wird die Nachricht im Klartext angezeigt.



Verschlüsselte Anhänge öffnen

Anhänge werden am Ende der E-Mail angezeigt. Um verschlüsselte Anhänge zu öffnen klickt ihr sie mit der rechten Maustaste an und wählt dann „Entschlüsseln und speichern unter…“.



organize.blogsport.eu