Mail/Verschlüsselung einrichten

Grundsätzliche Hinweise

Notebooks:

Grundsätzlich sollte man eine Notebookfestplatte verschlüsseln.

Es geht über das Bios moderner Computer (dort Festplattenverschlüsselung suchen) oder über die Freie Software Truecrypt.

Achtung! Man benötigt während des Verschlüsselns einen angeschlossenen DVD-Brenner und eine leere DVD (kann auch eine wiederbeschreibbare DVD sein). Ein starkes Passwort sollte man sich im Vorfeld auch schon mal überlegen (mind. 12 Zeichen/Buchstaben/Groß-Kleinschreibung)

www.truecrypt.org

Passwöter!

Empfehlung: Man merkt sich nur noch eines, vergibt aber stets unterschiedliche Passwörter! Da immer wieder die Passwörter bei einzelnen Shops o. ä. abgefischt werden, sollte man sein Passwort nicht „wiederverwenden“. Stets ein neues vergeben, am besten eine wilde Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.

Man kann sich einen Passwortsafe installieren (Software zum sicheren Ablegen von Passwörtern), die dann über das Passwort zum Safe die weiteren Passwörter sichtbar macht.

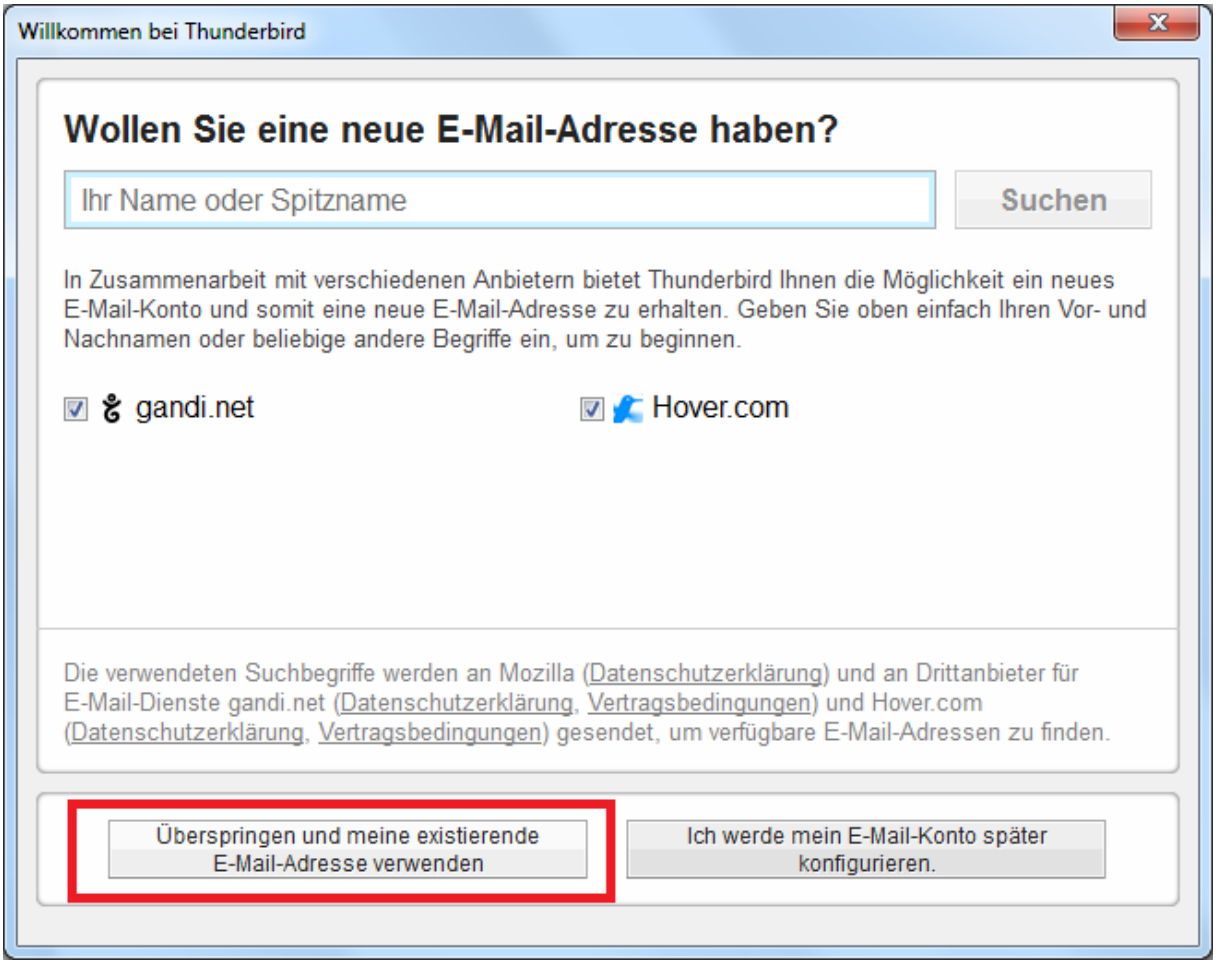
Eine Freie und zur Zeit als sicher eingeschätzte Software ist KeePass.

Aktuelle Version Keepass 2.20 (www.keepass.info)

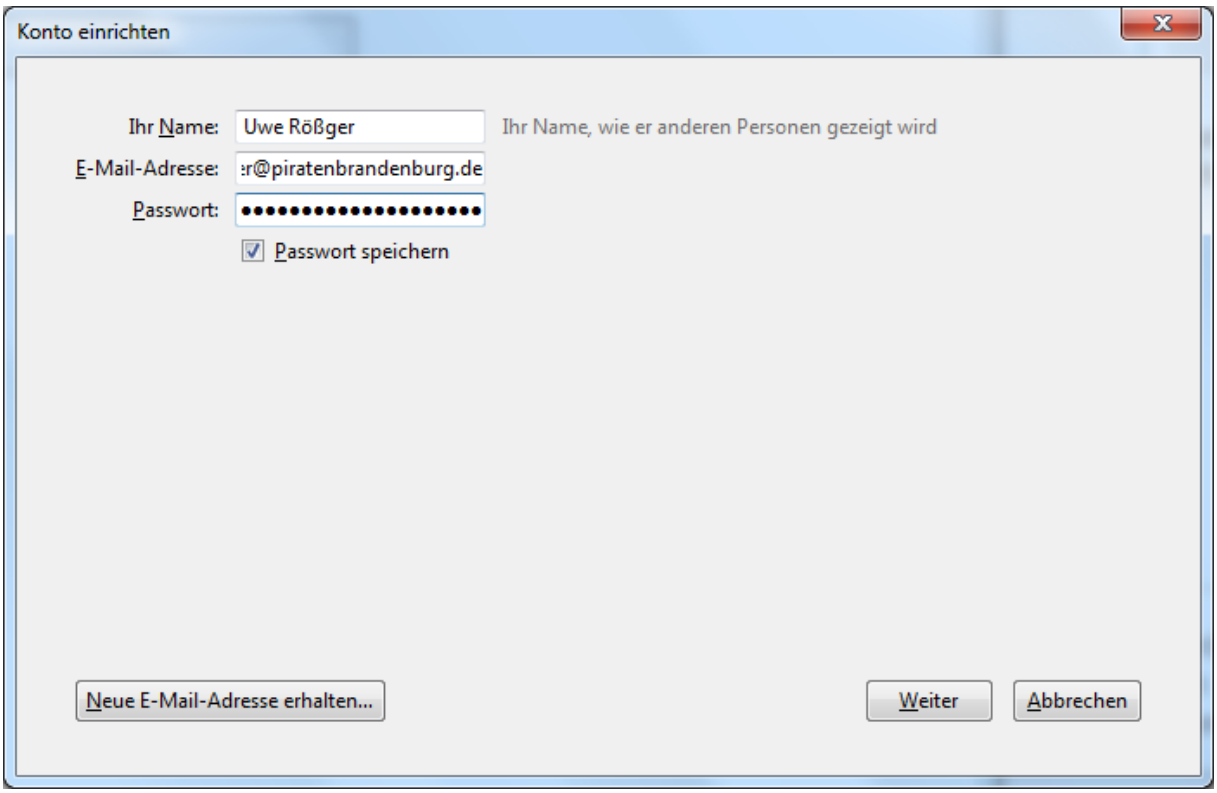
Mail

Eine freie und PGP/GPG-verschlüsselung unterstützende Version des Mailprogramms ist Thunderbird Mail. Download unter: http://www.mozilla.org/de/thunderbird

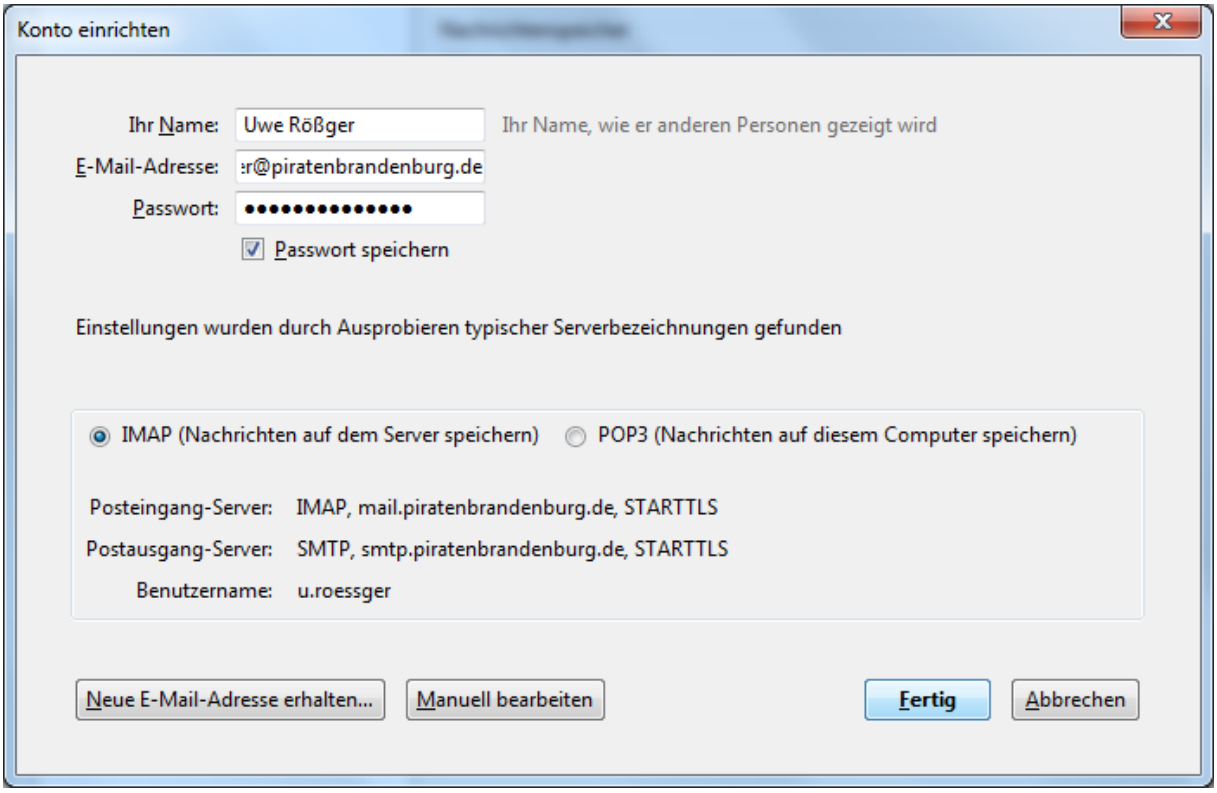
„Thunderbird Setup 15.0.1.exe“ ausführen, am Ende der Installation starten.



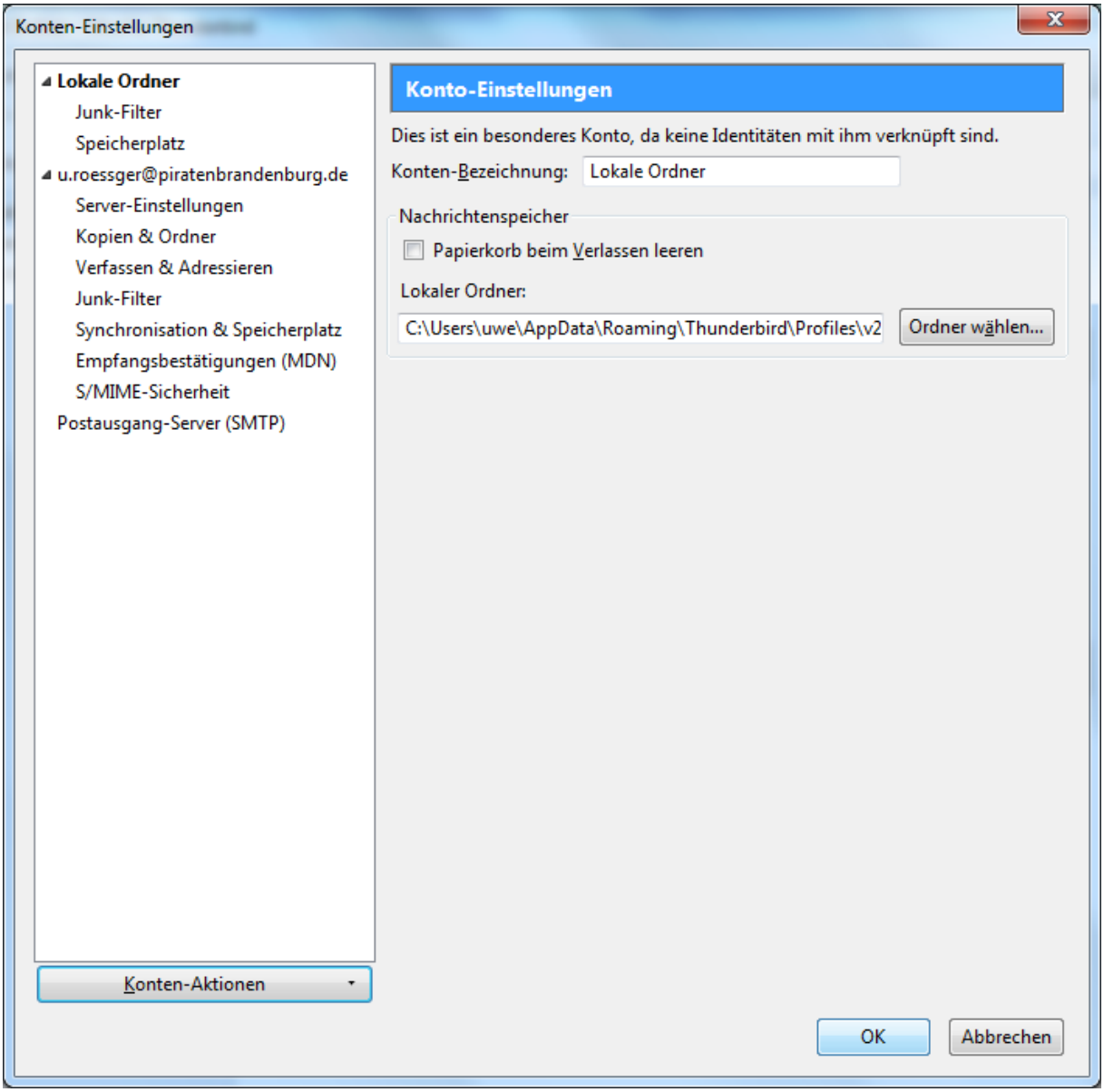
Bei Konto einrichten, Klarnamen, Mailadresse und Passwort eintragen!



Das System überprüf mehre ISP-Datenbanken und schlägt ff. vor / **Weiter …**


Konto einrichten
Ihr Name:
Uwe Rößger
Ihr Name, wie er anderen Personen gezeigt wird
E-Mail-Adresse:
:r@piratenbrandenburg.de
Passwort:
Passwort speichern
Einstellungen wurden durch Ausprobieren typischer Serverbezeichnungen gefunden
IMAP (Nachrichten auf dem Server speichern)
POP3 (Nachrichten auf diesem Computer speichern)
Posteingang-Server:
IMAP, mail.piratenbrandenburg.de, STARTTLS
Postausgang-Server:
SMTP, smtp.piratenbrandenburg.de, STARTTLS
Benutzername:
u.roessger
Neue E-Mail-Adresse erhalten...
Manuell bearbeiten
Fertig
Abbrechen

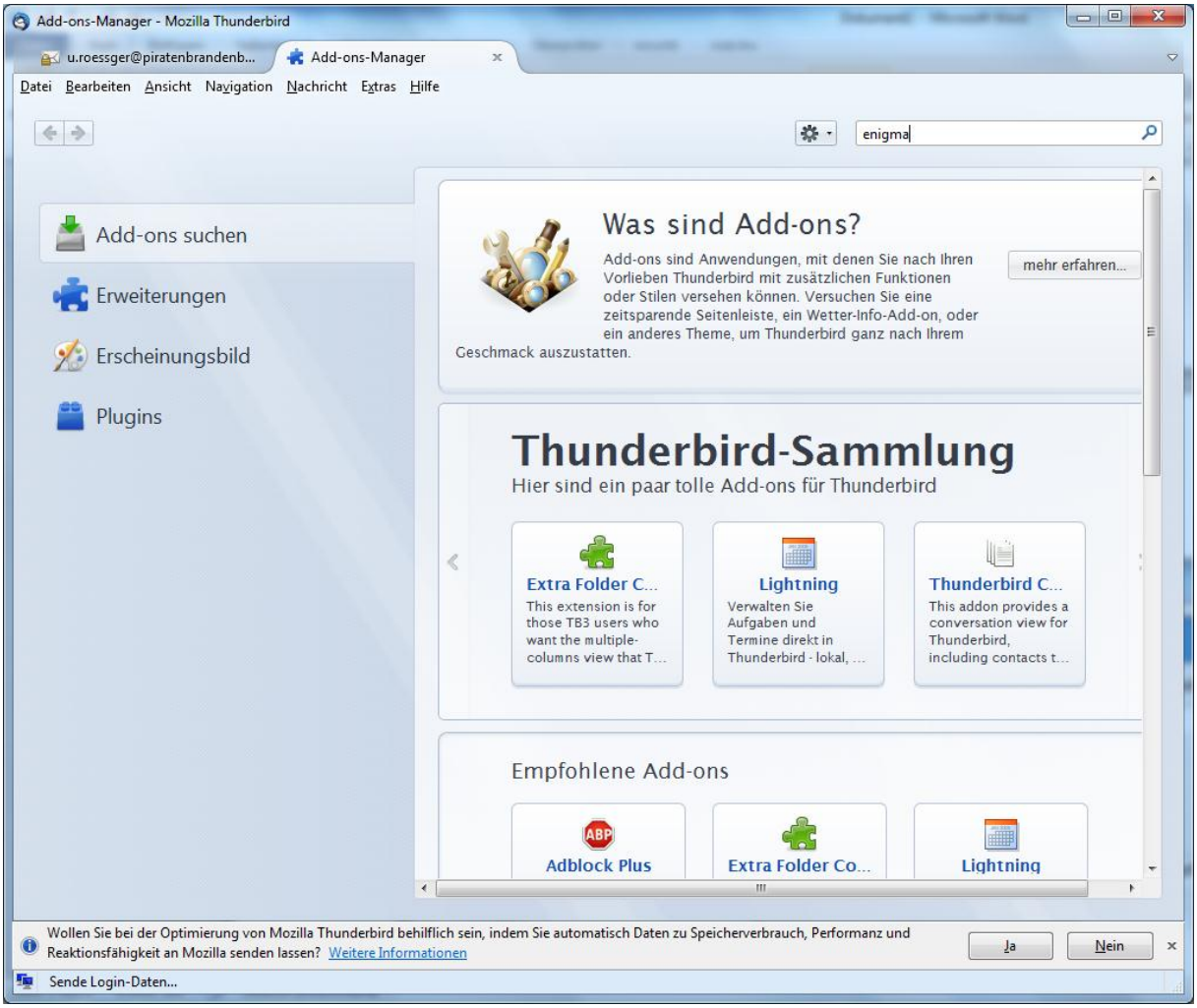
und … **Fertig**!



Mailen geht damit schon!

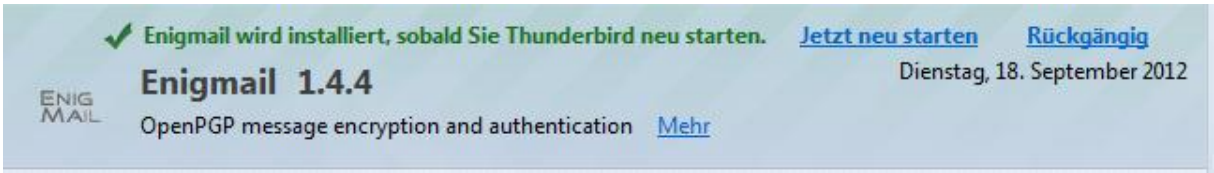
<u>Enigma Installieren</u>

Extras / Addons wählen



Ins Suchfenster das Wort **enigma** schreiben und und die **Lupe klicken**.

Es wird das Addon Enigmamail gefunden -> **installieren** klicken!



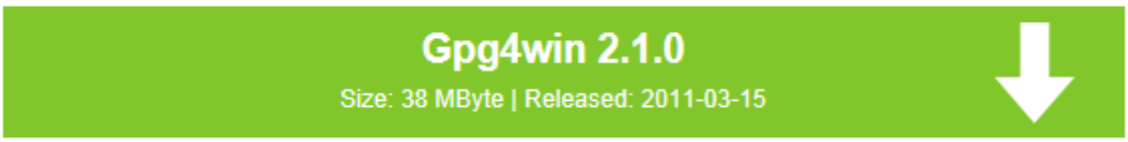
Jetzt neu starten

Laden Sie VOR der Einrichtung nun die GPG-Software auf ihren Rechner.

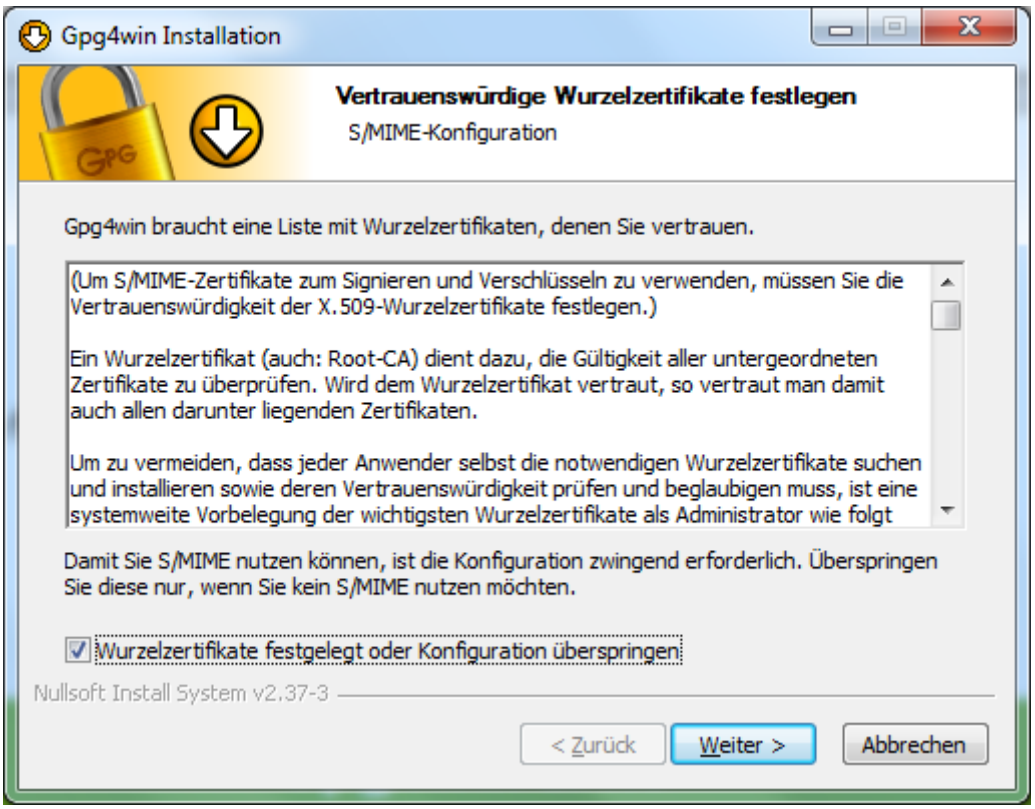
Für Windows-Systeme finden Sie die Version 2.1.0 oder 2.1.1 (Beta) unter

http://gpg4win.org/

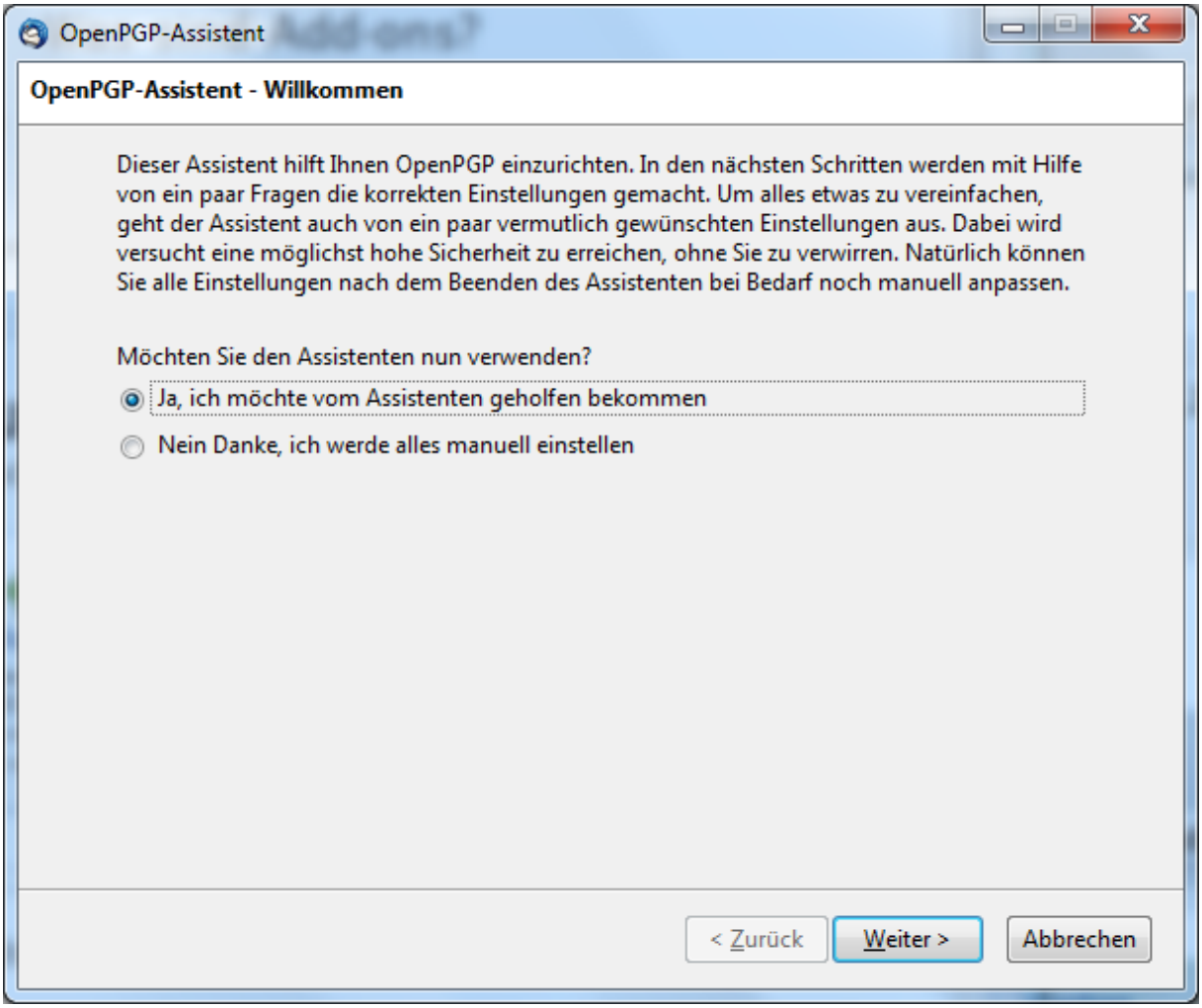
bsp:

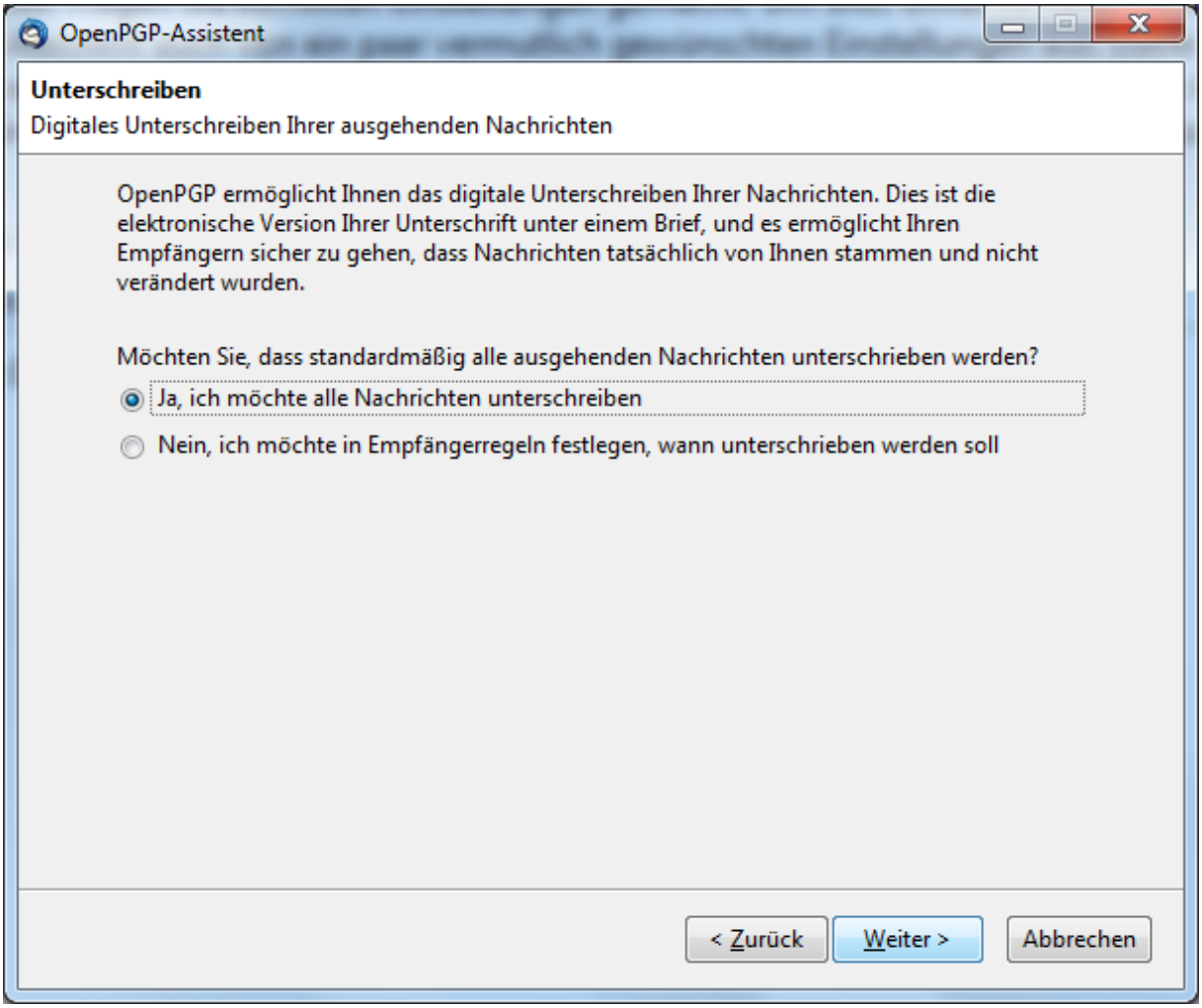


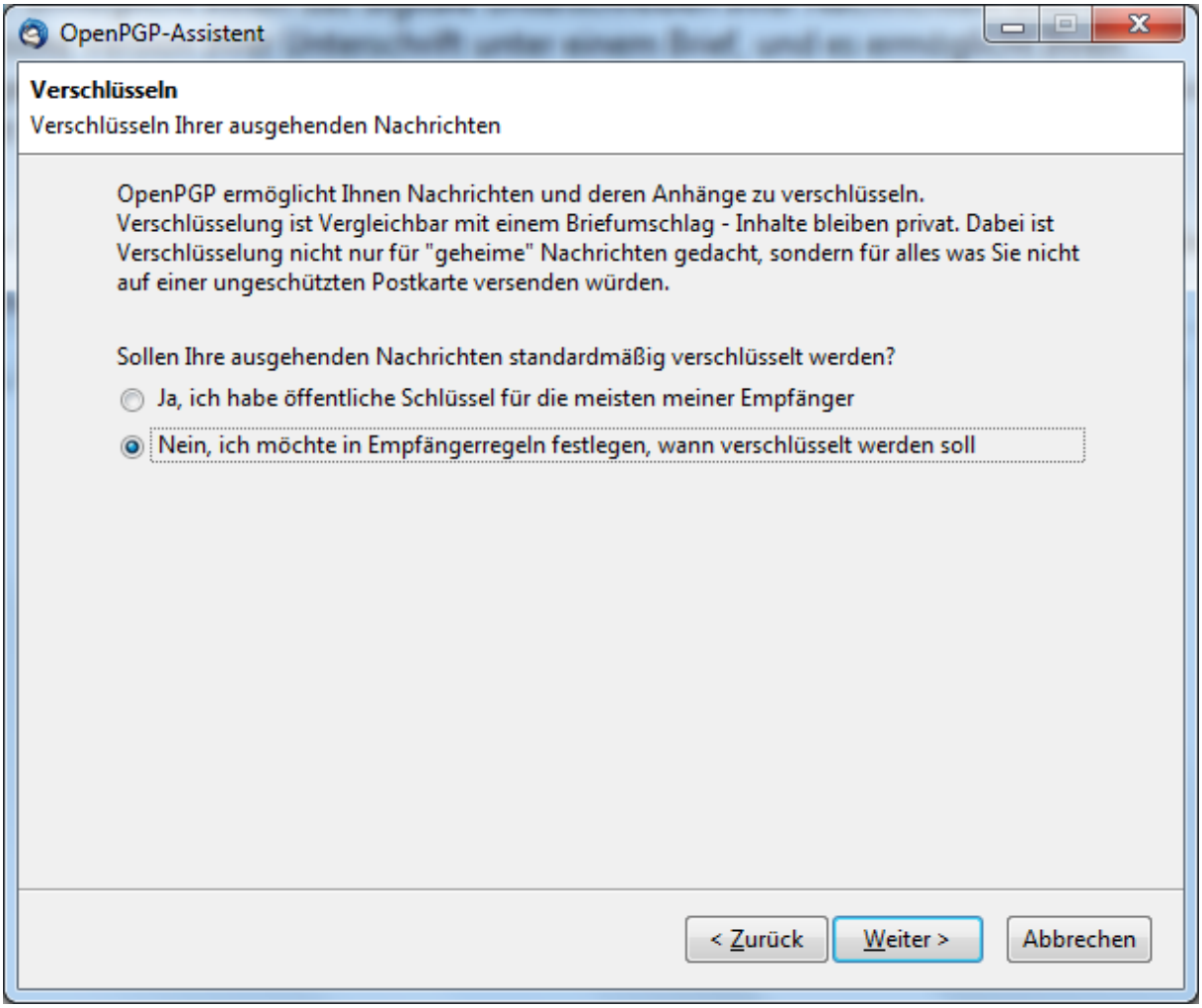
Deutsch->weiter->weiter->weiter->installieren

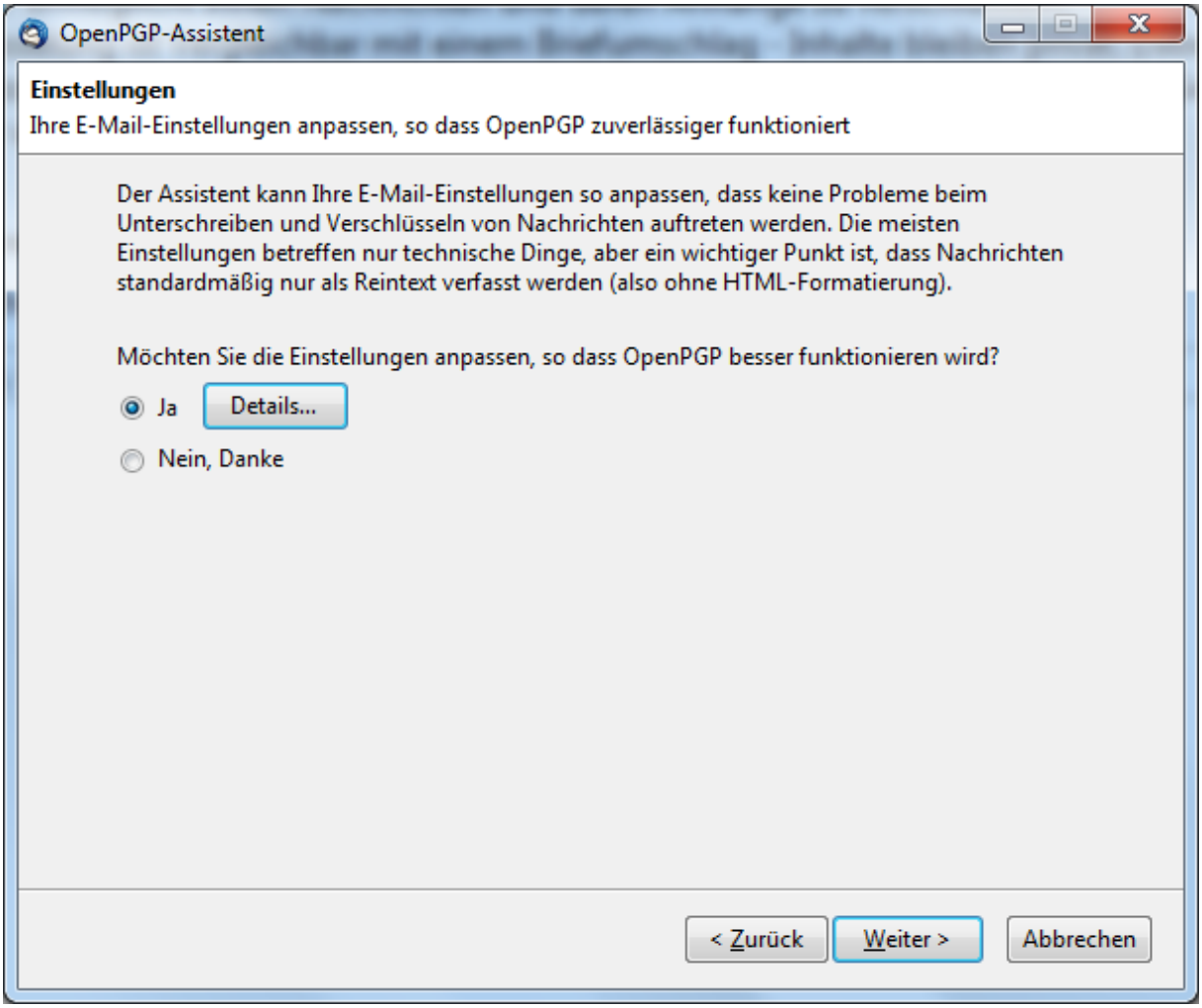


Starten des OpenPGP Assistenten


OpenPGP-Assistent
OpenPGP-Assistent - Willkommen
Dieser Assistent hilft Ihnen OpenPGP einzurichten. In den nächsten Schritten werden mit Hilfe von ein paar Fragen die korrekten Einstellungen gemacht. Um alles etwas zu vereinfachen, geht der Assistent auch von ein paar vermutlich gewünschten Einstellungen aus. Dabei wird versucht eine möglichst hohe Sicherheit zu erreichen, ohne Sie zu verwirren. Natürlich können Sie alle Einstellungen nach dem Beenden des Assistenten bei Bedarf noch manuell anpassen.
Möchten Sie den Assistenten nun verwenden?
Ja, ich möchte vom Assistenten geholfen bekommen
Nein Danke, ich werde alles manuell einstellen
< Zurück
Weiter >
Abbrechen


OpenPGP-Assistent
Unterschreiben
Digitales Unterschreiben Ihrer ausgehenden Nachrichten
OpenPGP ermöglicht Ihnen das digitale Unterschreiben Ihrer Nachrichten. Dies ist die elektronische Version Ihrer Unterschrift unter einem Brief, und es ermöglicht Ihren Empfängern sicher zu gehen, dass Nachrichten tatsächlich von Ihnen stammen und nicht verändert wurden.
Möchten Sie, dass standardmäßig alle ausgehenden Nachrichten unterschrieben werden?
Ja, ich möchte alle Nachrichten unterschreiben
Nein, ich möchte in Empfängerregeln festlegen, wann unterschrieben werden soll
< Zurück
Weiter >
Abbrechen


OpenPGP-Assistent
Verschlüsseln
Verschlüsseln Ihrer ausgehenden Nachrichten
OpenPGP ermöglicht Ihnen Nachrichten und deren Anhänge zu verschlüsseln. Verschlüsselung ist Vergleichbar mit einem Briefumschlag - Inhalte bleiben privat. Dabei ist Verschlüsselung nicht nur für "geheime" Nachrichten gedacht, sondern für alles was Sie nicht auf einer ungeschützten Postkarte versenden würden.
Sollen Ihre ausgehenden Nachrichten standardmäßig verschlüsselt werden?
Ja, ich habe öffentliche Schlüssel für die meisten meiner Empfänger
Nein, ich möchte in Empfängerregeln festlegen, wann verschlüsselt werden soll
< Zurück
Weiter >
Abbrechen

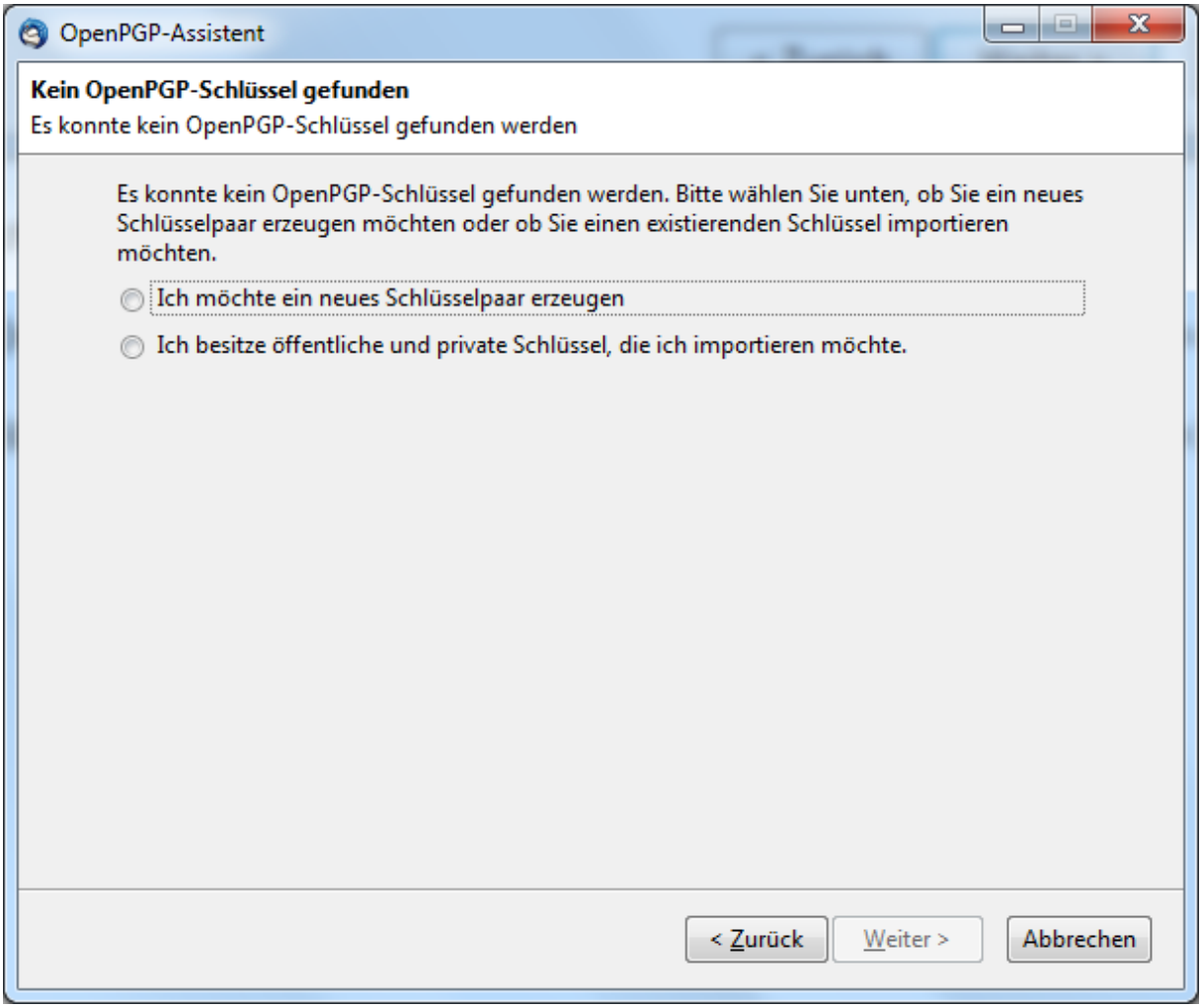


Bei der Suche nach gpg.exe stellen sie auf

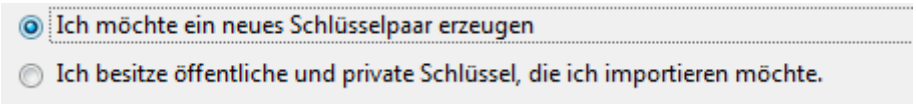
C:\Program Files (x86)\GNU\GnuPG\gpg2.exe 64 Bit System oder

C:\Programmme\GnuPG\gpg2.exe 32 Bit System (XP z.B.)

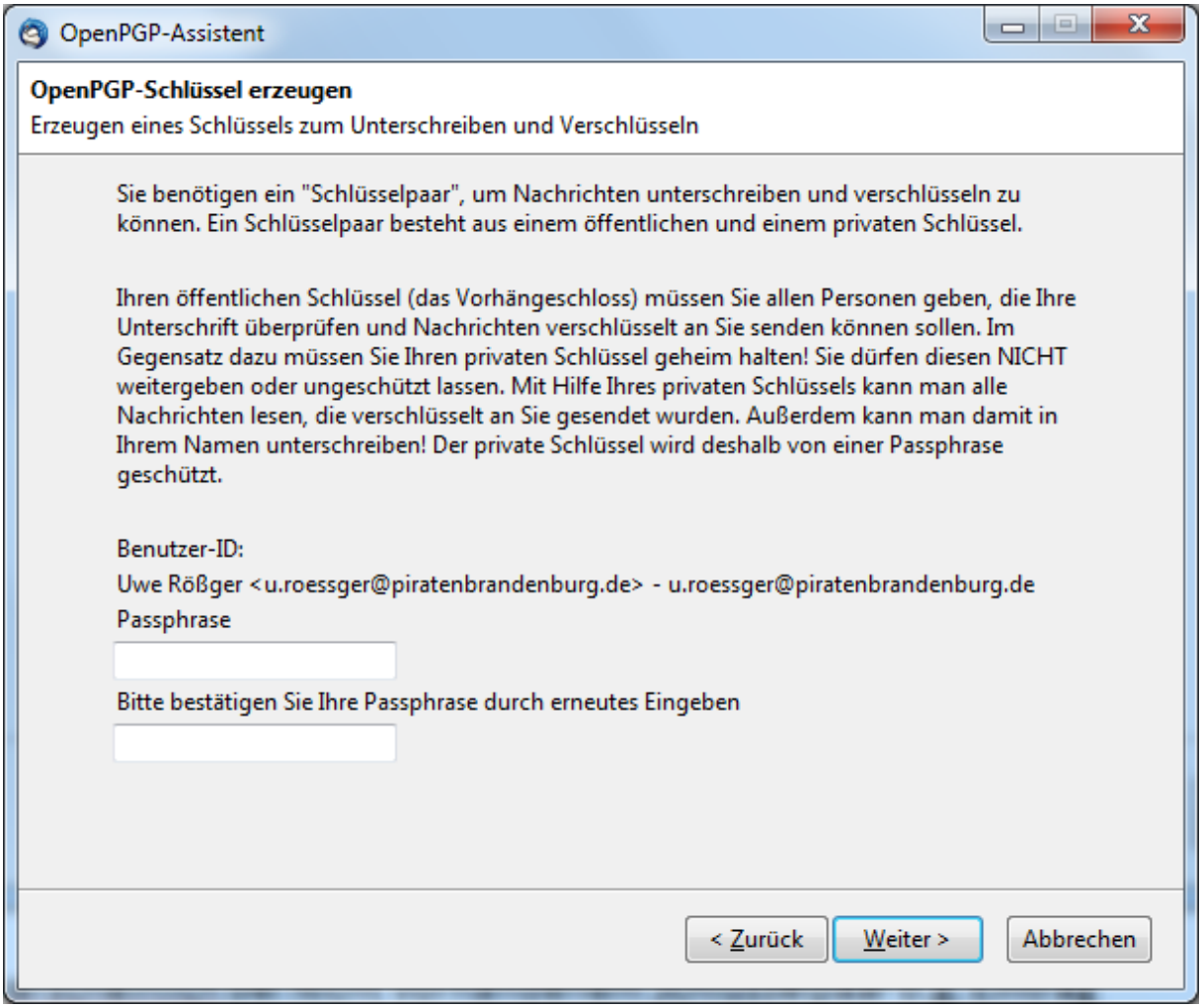
Je nachdem, ob es die Erstinstallation oder eine weitere ist und man schon einen PGP-Schlüssel hat wählt man:



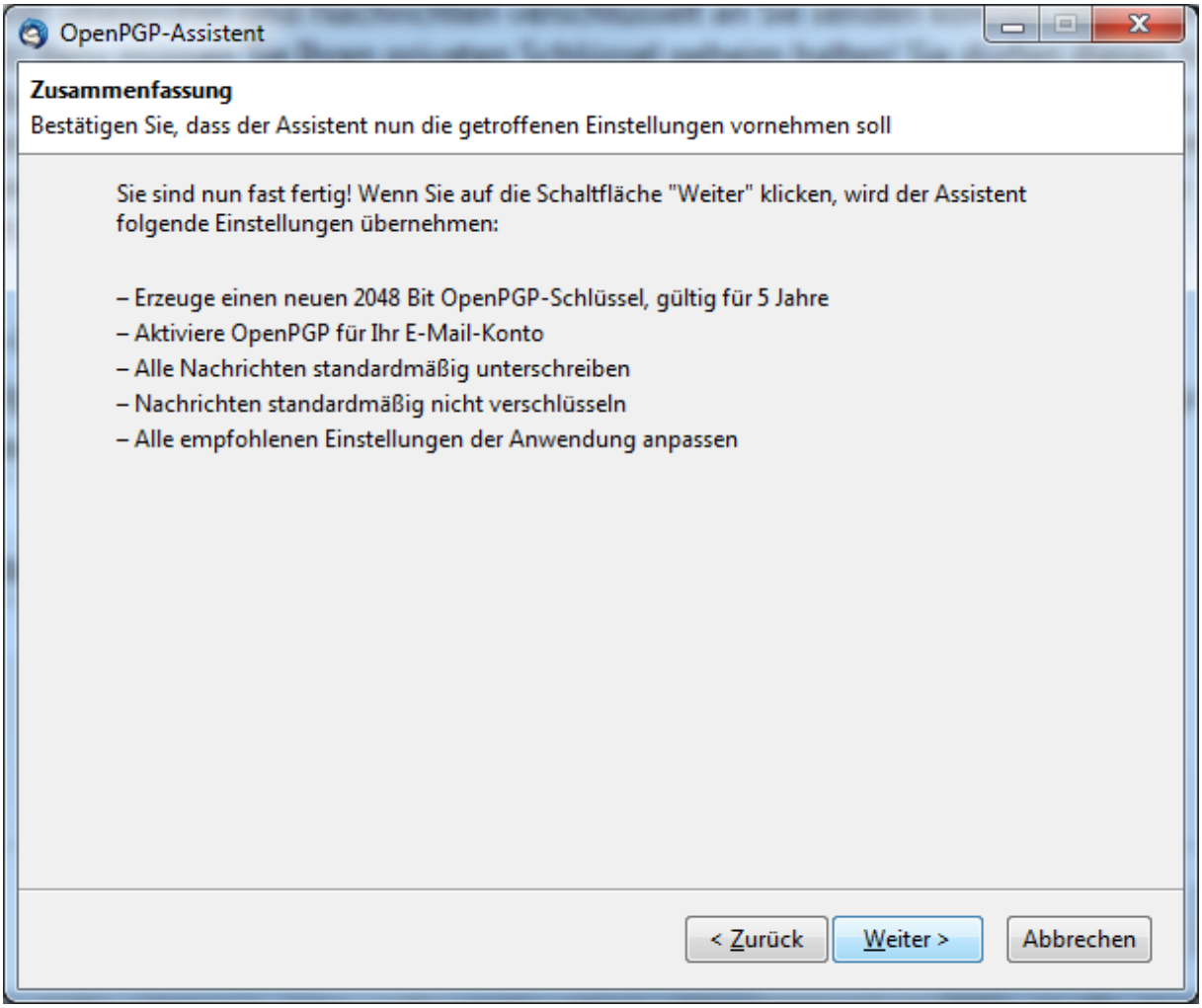
In unserem Fall warscheinlich bei Nicht vorhandenem Schlüsselpaar o.g. Eintrag

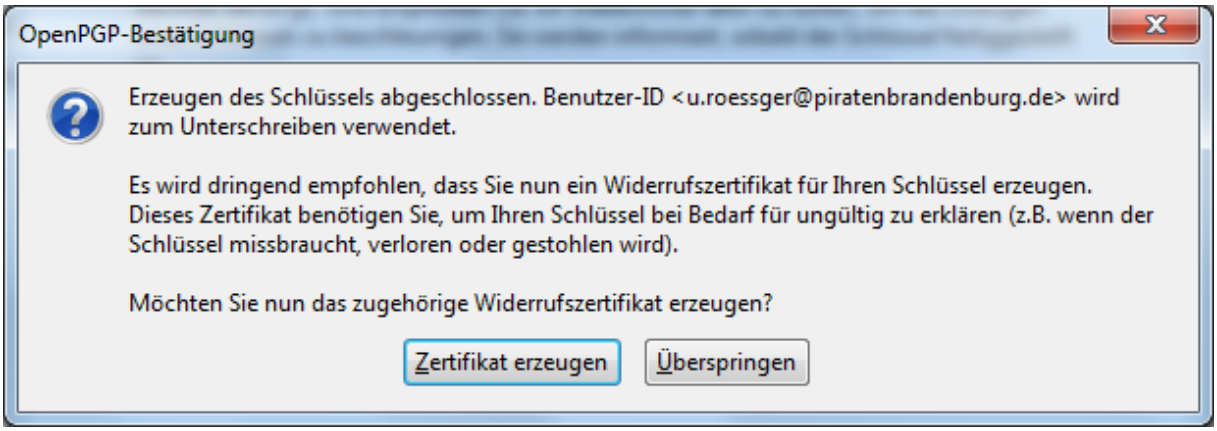


… weiter



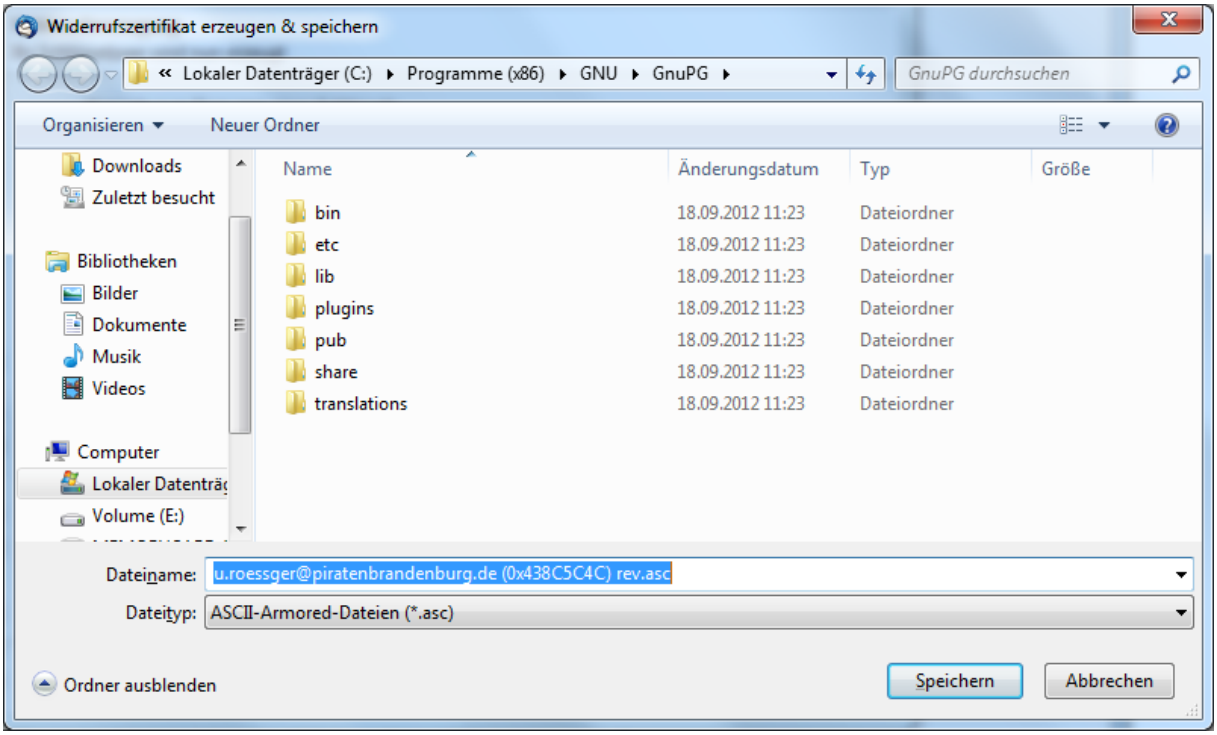
Die Passphrase ist ein Passwort (bitte ein SICHERES eingeben und gleich in Keepass eintragen!)

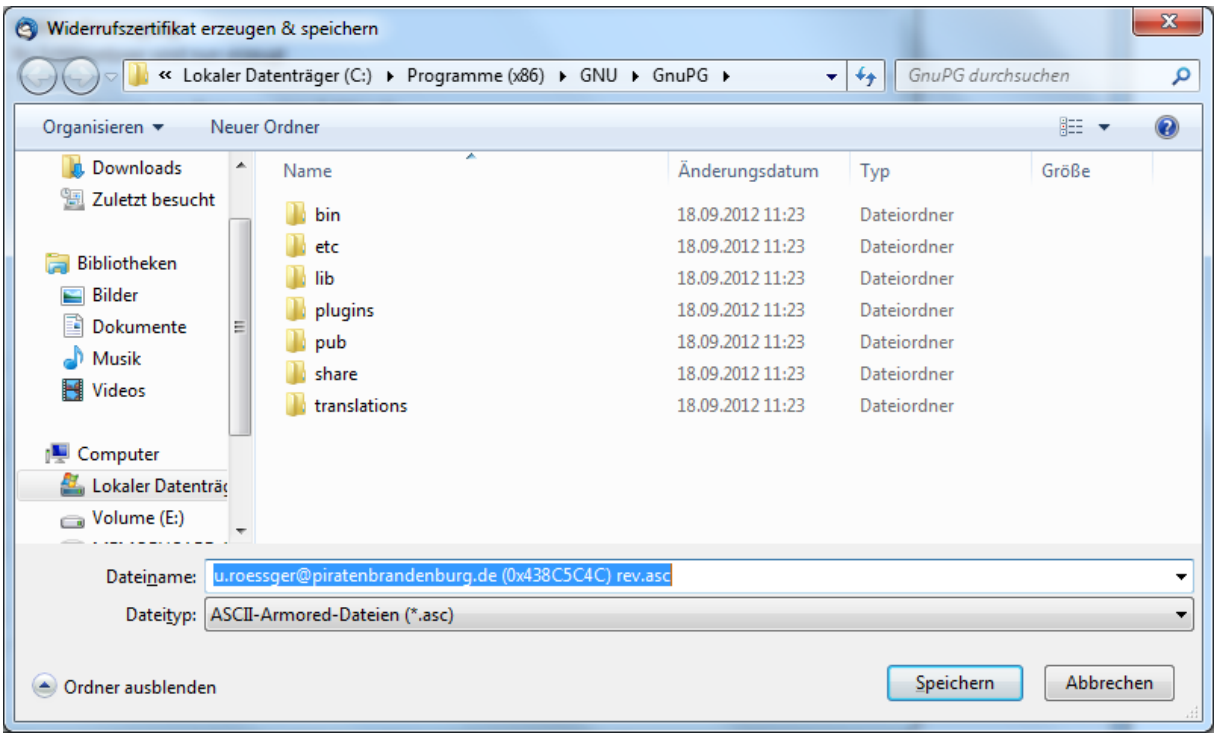




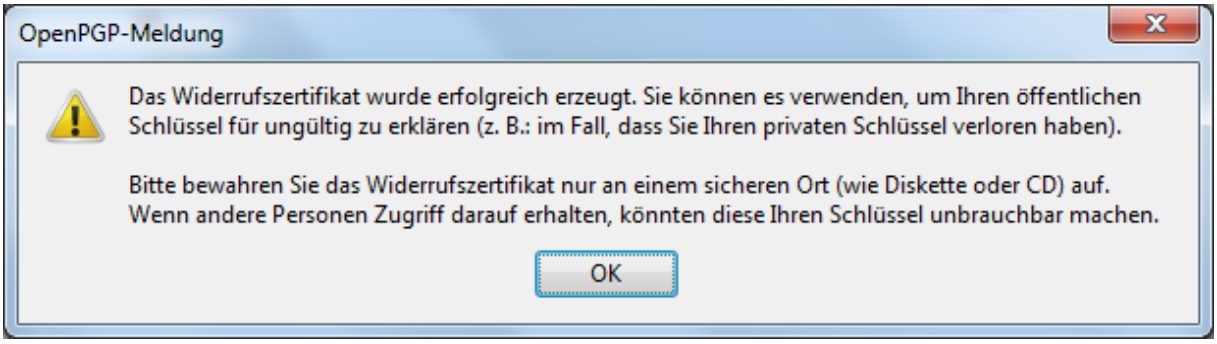
Erzeugen sie auch dieses!

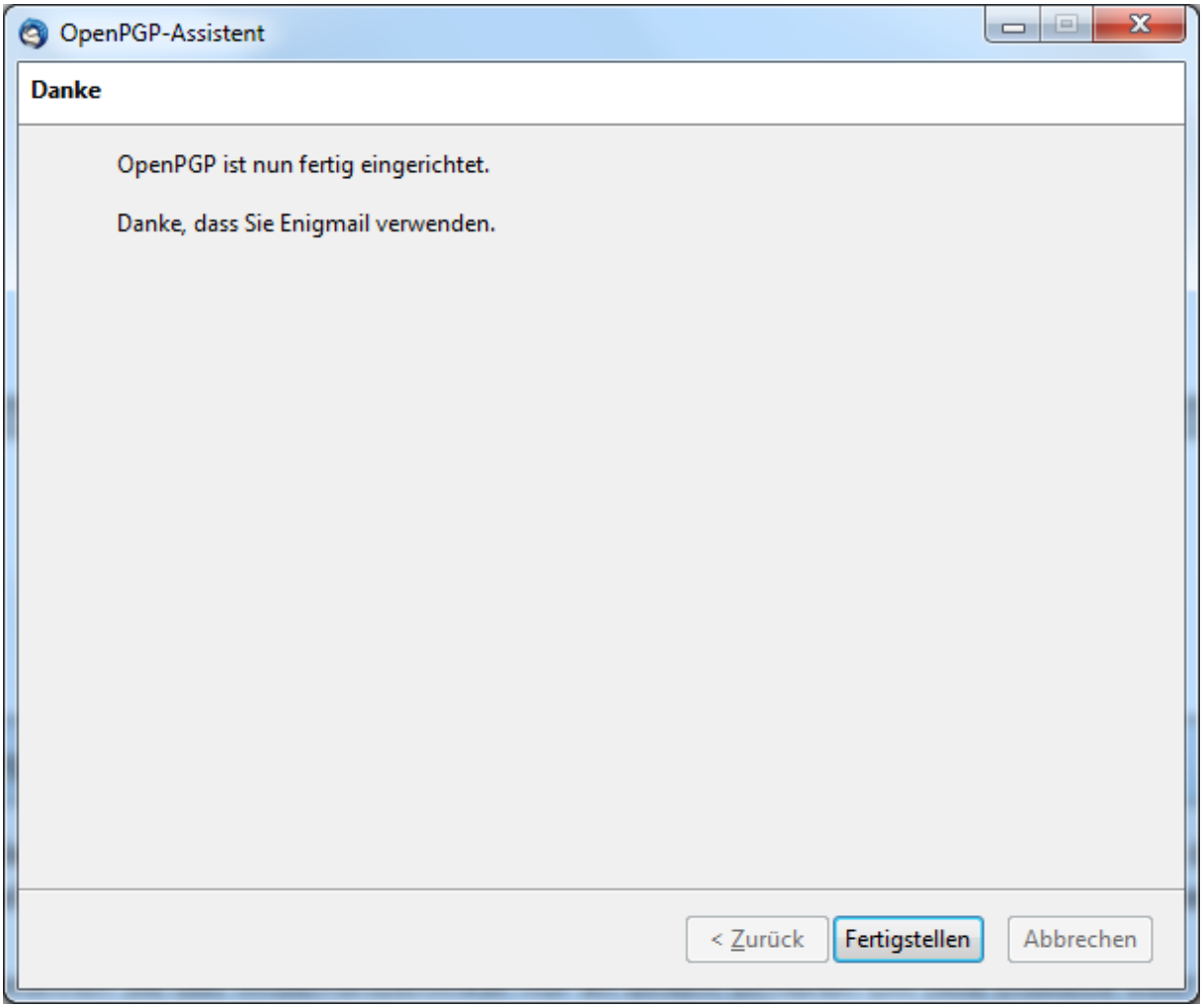
Legen sie es im Filesystem sicher ab (ggf. nochmals auf USB Stick o.ä.)





Passphrase eingeben für Entsperrung:



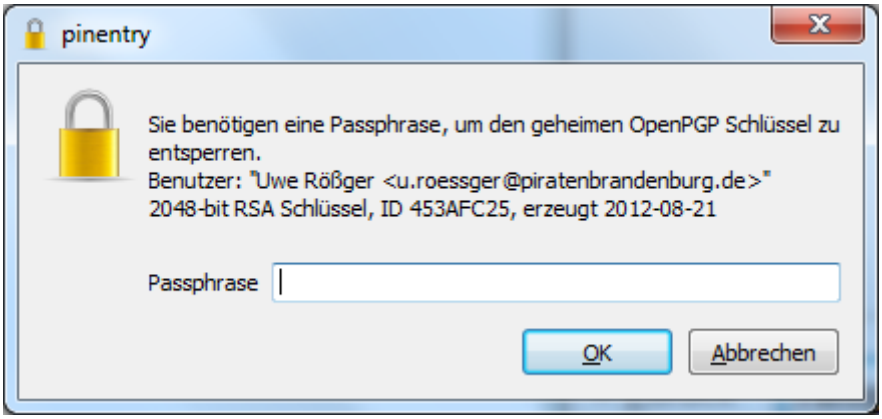


Wenn Sie eine neue Nachricht senden, ist per Default für OpenPGP „unterschreiben“ eingestellt.

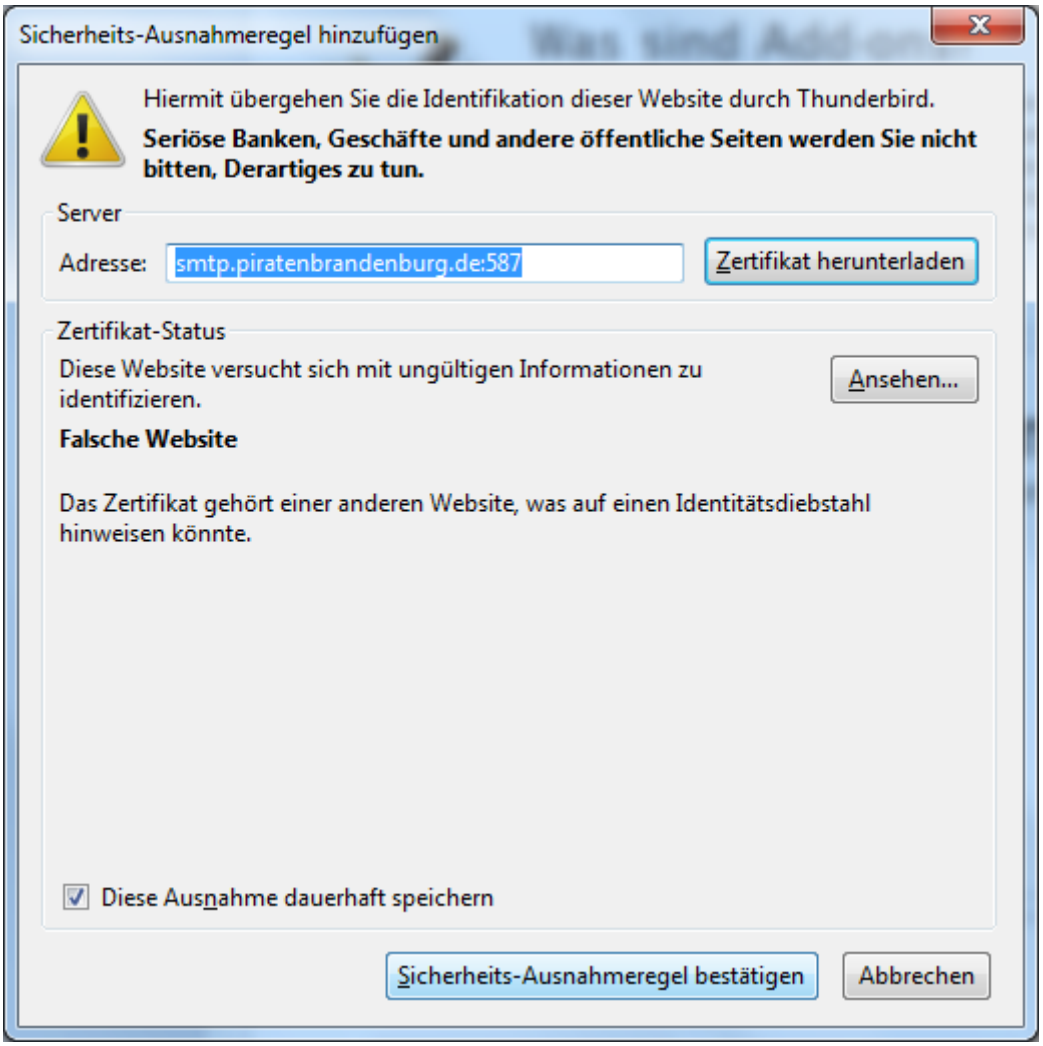
Sollte die Nachricht verschlüsselt werden, benötigen Sie eine Mail des Empfängers, die eine unterschriebene Nachricht enthält.

Wählen Sie dann zusätzlich unter OpenPGP „Nachricht Verschlüsseln“

Nach Drücken des „Senden“ Buttons wird die Eingabe des Passwortes notwendig



Danach erfolgt das Senden an die Zieladresse



Sollte dieser Dialog mal kommen, „sicherheits-Ausnahmeregel bestätigen“

Man sieht die Mail noch kurz verschlüsselt

-----BEGIN PGP MESSAGE-----

Charset: ISO-8859-15

Version: GnuPG v2.0.17 (MingW32)

Comment: Using GnuPG with Mozilla - http://www.enigmail.net/

hQEMA1E0sLv0sBXTAQf+NitDDTLEmbIQnMyDlzknsqdu+6vitnAjIrT7ctxnGtJI

rLBEPEl/TJ/xilZoesZY6lXUI7zFOp7Mw39FEEDDShURze89kpOq5N1WjOAQwM0R

SGvLYeHbPeDDW9y8vQwWM4G0B2I7j75WtcYFZzlfLr1PrC/aBG9ioKM78XsK+Cy8

CAN4aO7xndyehUl7AN9mXjIZT5jPMPLaoIXPA1spKC72VwPyso1GzCoAcHiy3LlG

M+6swbbJX/eN+aQCKkxXZi2RzvwSraNwXKPyBxeETtDyqbzCGnjCT/1YP/39dUP5

21TrUa5KeWU6KFPy7PX2M6rqyMP8x4sAjdmeN3mAmdLAsgHY6H3IbKsEfLxMApcO

4DyKiwdfES6ZMhLfmSOqPg3FlgRGcRKyvjiGiOA78I0N90xV4+HK6m/9M2tJu4HU

k1nrHs88R15HqN1e2dTZIgtZQ6sALG6+H+Ll1ejYVGDglkmdLTRaY5+kB3ua4jr7

RUCcaWW/gPOSo79Hs52T1g4bUGcZfUU2X+q9GyeHHP2ICdHl2SZRrxnLLOM30xHs

N1B5Yq6ZprlgmBJmwkg2VgSTNNNQYnzZTbXZkhDoAPQ7yhX5u6G9iW9rBUEdP5dU

dRAO9ac5cu81z0B9Orr+zB6piUGtNb7qRe/PMzyeYdGkrFgajb+UvG3WF7f0CWr6

CafkVK1ubw1LnsCLekBhaUlO2KXX1f6JkS3RLUpUkfR//jaSk/MZPUq503KV46d7

PNnRJyj7/ocblXwmx/cY9KXmLy2zrA+C0+5Yp+QDcP5CqeS25frZkLt2vXVQGnUv

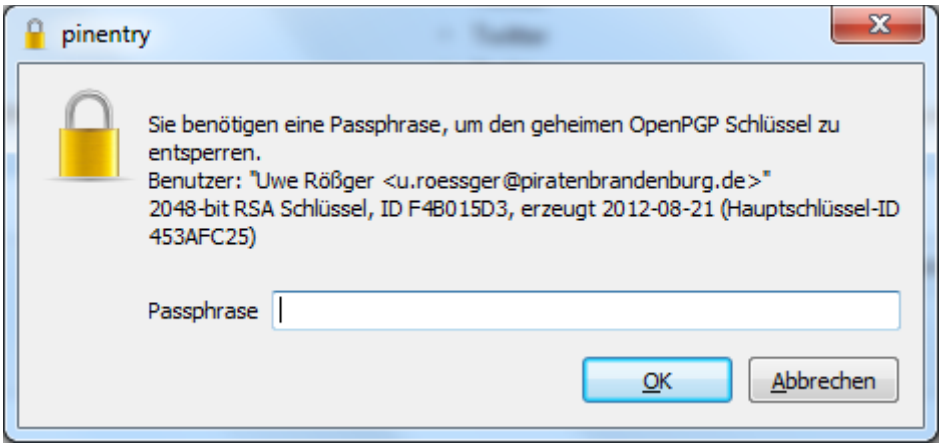
3icYkyM7ZcYX0WHdS1DY0UfTHQ4=

=1qKu

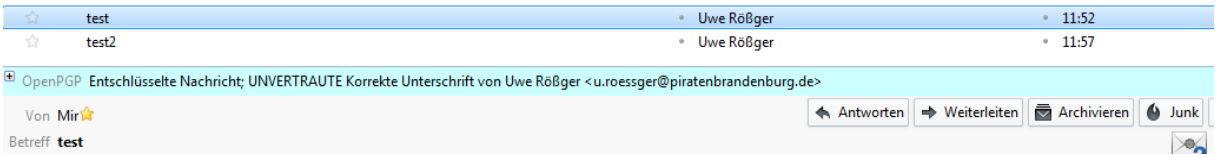
-----END PGP MESSAGE-----

Verschlüsselte Mails lesen

Sobald Du eine verschlüsselte Mail lesen willst, wirst du nach deiner Passphrase gefragt

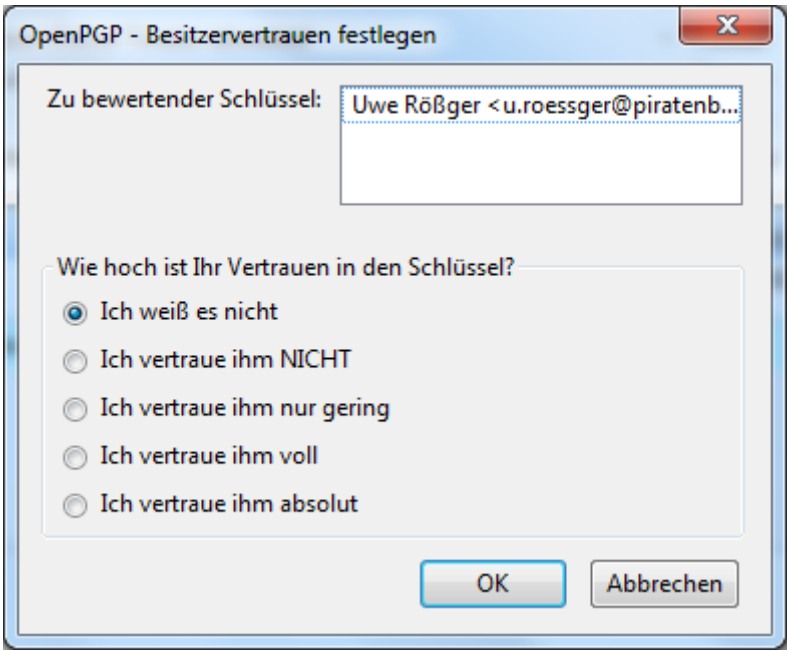


Das Passwort bleibt im Cache, so dass du auch beim Blättern nicht immer wieder das Passwort eingeben musst. Verschlüsselte Mails sind gekennzeichnet!



Über „Details“ ganz rechts auf dieser grünen Leiste kannst du ein Popup-Menü öffnen.

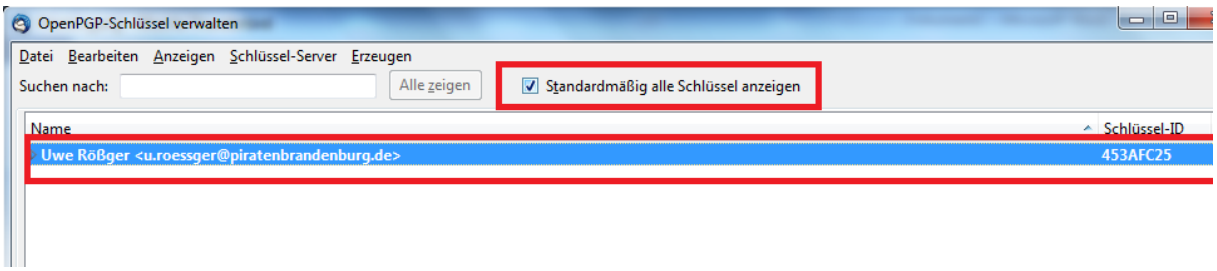
Dort regelst Du das Besitzvertrauen des Absenders:



Je nachdem was Du dort einstellst, wirst Du einen Eintrag bekommen.

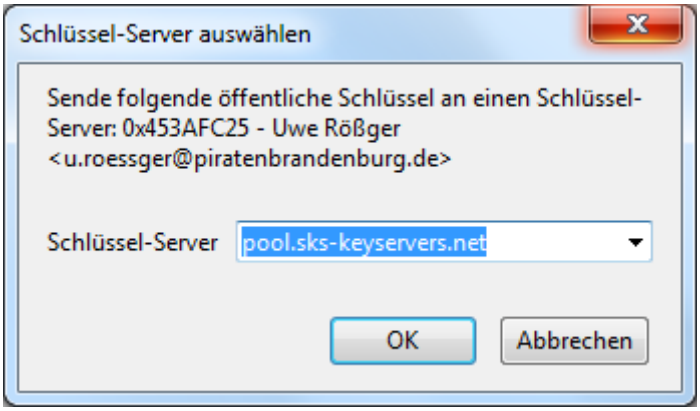
So, damit Du nun nicht jedem der dir was verschlüsselt senden will, deinen Öffentlichen Schlüssel senden musst, gibt es noch die Schlüsselserver, auf denen Du diesen speichern kannst.

Dazu gehst Du auf OpenPGP / Schlüssel verwalten.



setze das Häkchen, damit du Deinen Key siehst und markiere deinen eignen Key

Dort im Menü auf „Schlüssel –Server „ und „ Schlüssel hochladen“



Der erste ist okay!

Dann OK und „fertig“