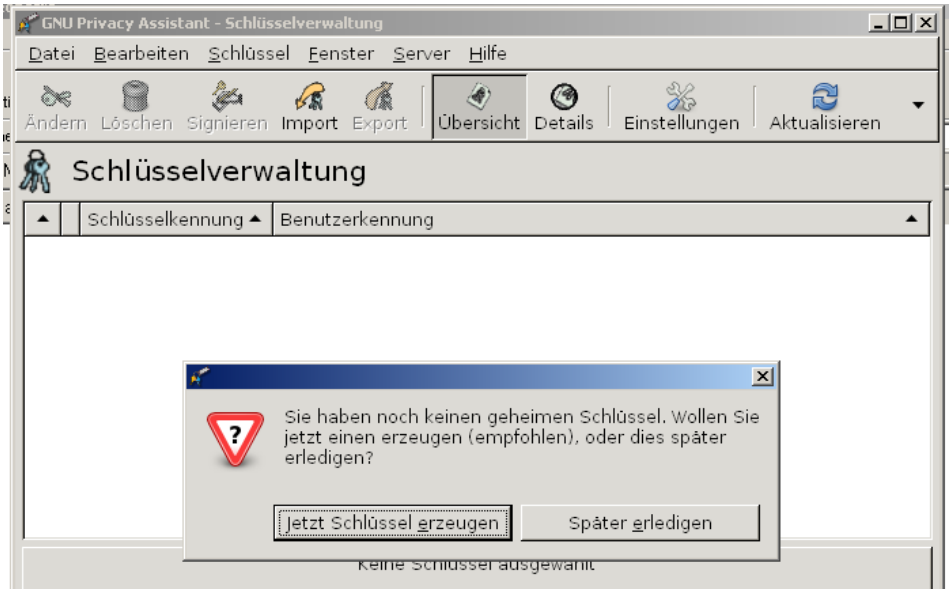
Gpg4Win - Anleitung

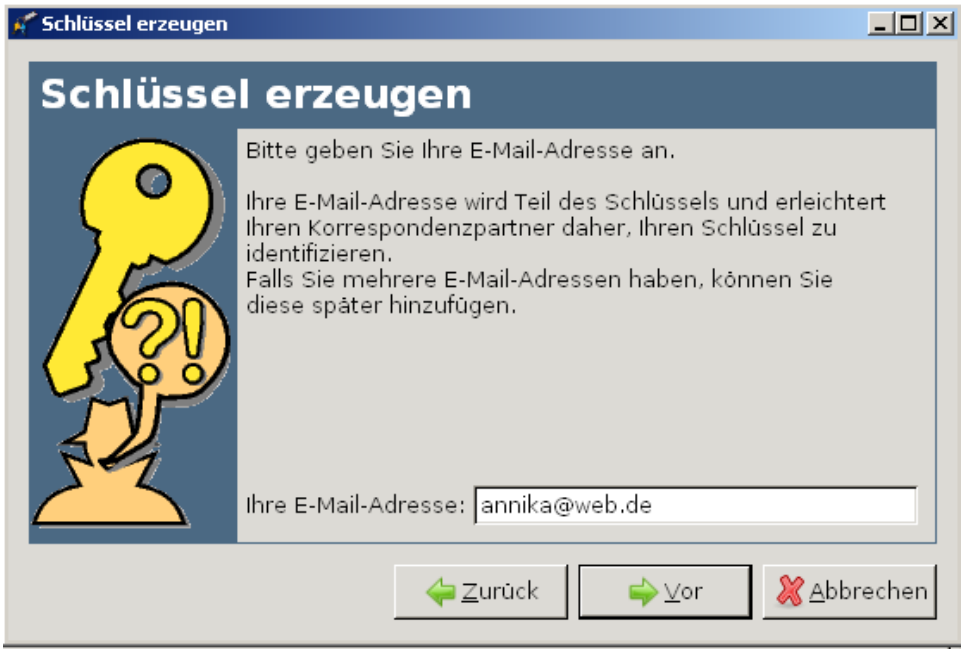
1. Schlüssel erzeugen

Wenn Sie den *GNU Privacy Assistant* (*GPA*) das erste Mal starten, werden Sie aufgefordert, ein Schlüsselpaar zu erzeugen. Klicken Sie auf *„Jetzt Schlüssel erzeugen“*



Geben Sie bei *„Ihr Name“* Ihren Vor- oder Nachnamen ein, damit man bei Ihrem öffentlichen Schlüssel später leicht erkennen kann, dass er Ihnen gehört.

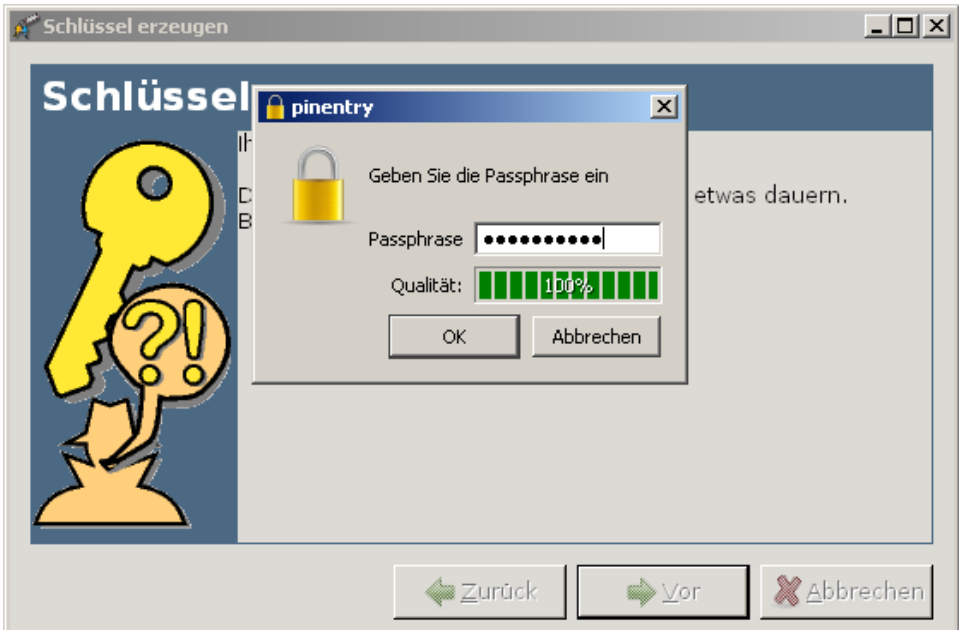
Die Email-Adresse, die Sie bei *Ihre E-Mail-Adresse* eingeben, muss nicht echt sein. Für unsere Testzwecke muss hier nur irgendeine Adresse eintragen werden. Sie können aber natürlich auch einen Schlüssel für Ihre echten Daten erzeugen. Am übersichtlichsten wird es, wenn auch die E-Mail-Adresse Ihren Namen enthält.



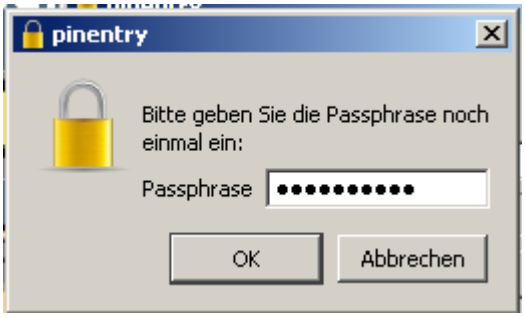
Zur Sicherheit können Sie eine Sicherheitskopie von Ihrem Schlüssel anlegen lassen.

Jetzt kommt der wichtigste Teil, die Passphrase. Dies ist ein Passwort, das Sie später jedes Mal eingeben müssen, wenn Sie Ihren privaten Schlüssel verwenden möchten. Anhand des Passwortes überprüft der Rechner, ob Sie auch tatsächlich der Eigentümer des privaten Schlüssels sind.

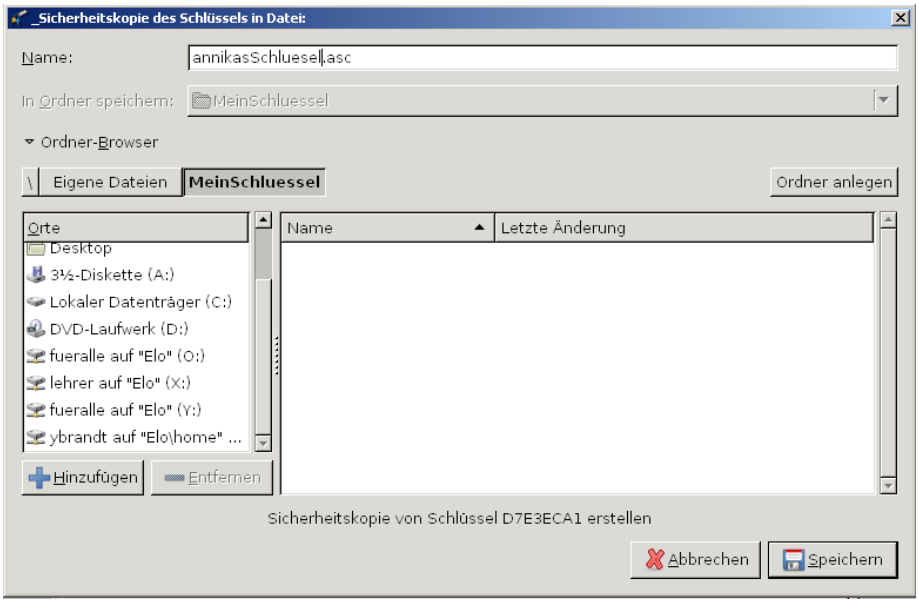
Das Passwort muss Sonderzeichen, Klein- und Großbuchstaben enthalten, damit es wirklich sicher ist. Anhand des Balkens sieht man, wann das Passwort sicher genug ist.



Um sicher zu gehen, dass sich keine Tippfehler eingeschlichen haben, muss das Passwort noch einmal bestätigt werden.

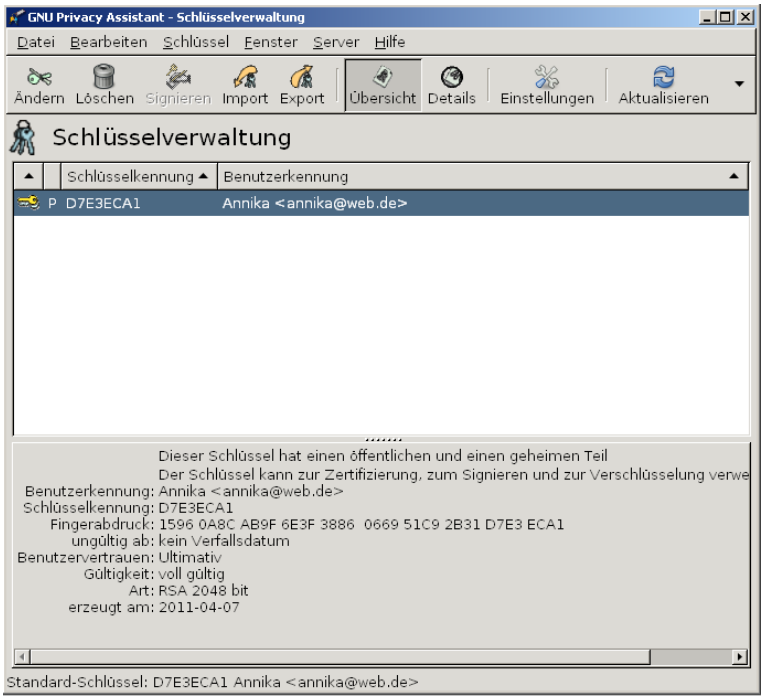


Wenn Sie sich dafür entschieden haben, eine Sicherheitskopie anlegen zu lassen, müssen Sie noch den Ort auswählen, an dem die Sicherheitskopie abgelegt wird. Normalerweise sollte der Schlüssel nicht auf dem Rechner, sondern auf einem externen Datenträger, wie einem USB-Stick gespeichert werden. Für unsere Testzwecke kann aber auch z. B. unter *ÄEigene Dateien*ñein Ordner für den Schlüssel anlegt werden.



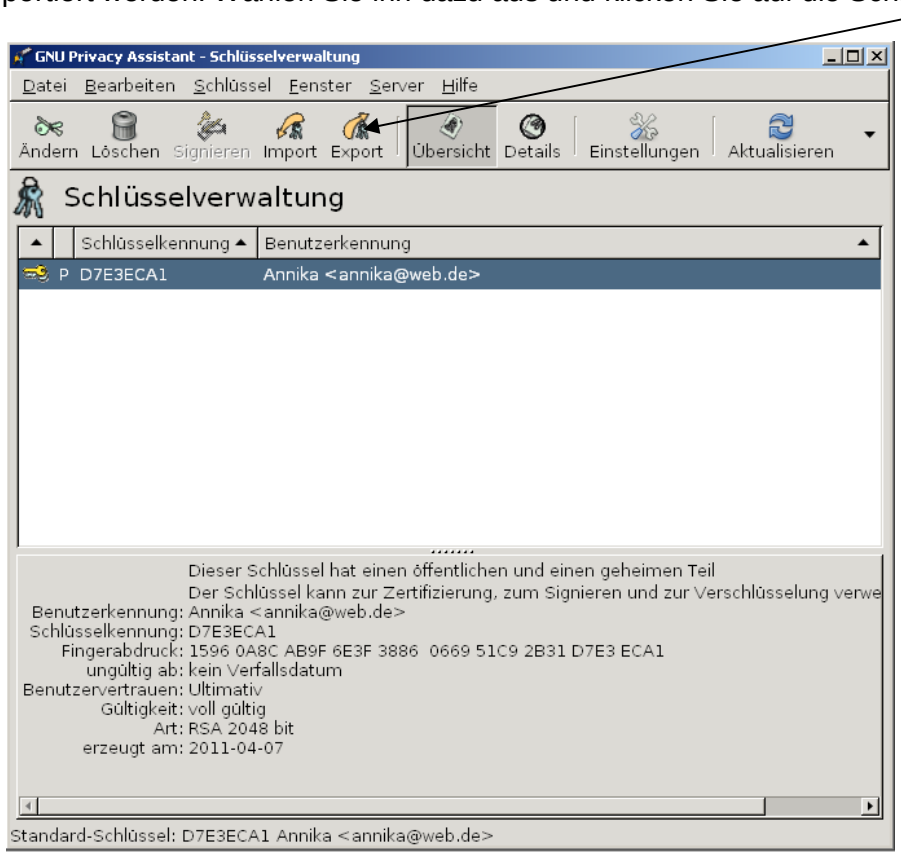
Da es sehr aufwändig ist, sichere Schlüssel zu erzeugen, werden Sie einen Moment warten müssen, während der Rechner arbeitet. Anschließend müsste Ihr Schlüsselpaar in der Schlüsselverwaltung angezeigt werden. Dass es sich um ein Paar aus privatem und öffentlichem Schlüssel handelt, erkennt man an dem doppelten Schlüsselsymbol.

Manchmal tritt beim Erzeugen der Sicherheitskopie eine Fehlermeldung auf. Das ist aber nicht so schlimm, da das Schlüsselpaar trotzdem erzeugt wird. Wenn das Programm wieder gestartet wird, sollte das Schlüsselpaar wie unten angezeigt werden.

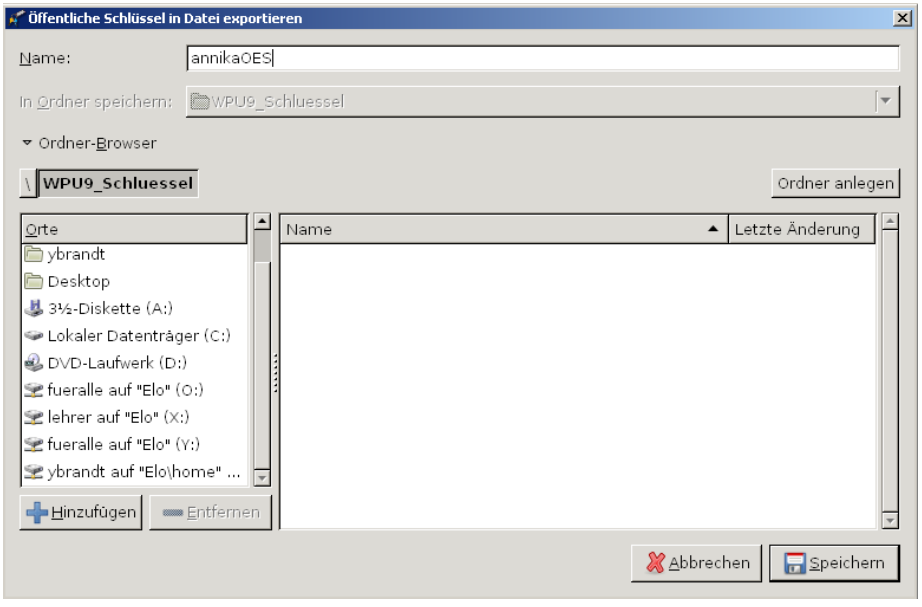


2. Exportieren des Schlüssels

Damit Ihnen die anderen Kursteilnehmer verschlüsselte Nachrichten schicken können, benötigen sie Ihren öffentlichen Schlüssel. Um ihn übergeben zu können, muss er zunächst exportiert werden. Wählen Sie ihn dazu aus und klicken Sie auf die Schaltfläche ÄExportñ

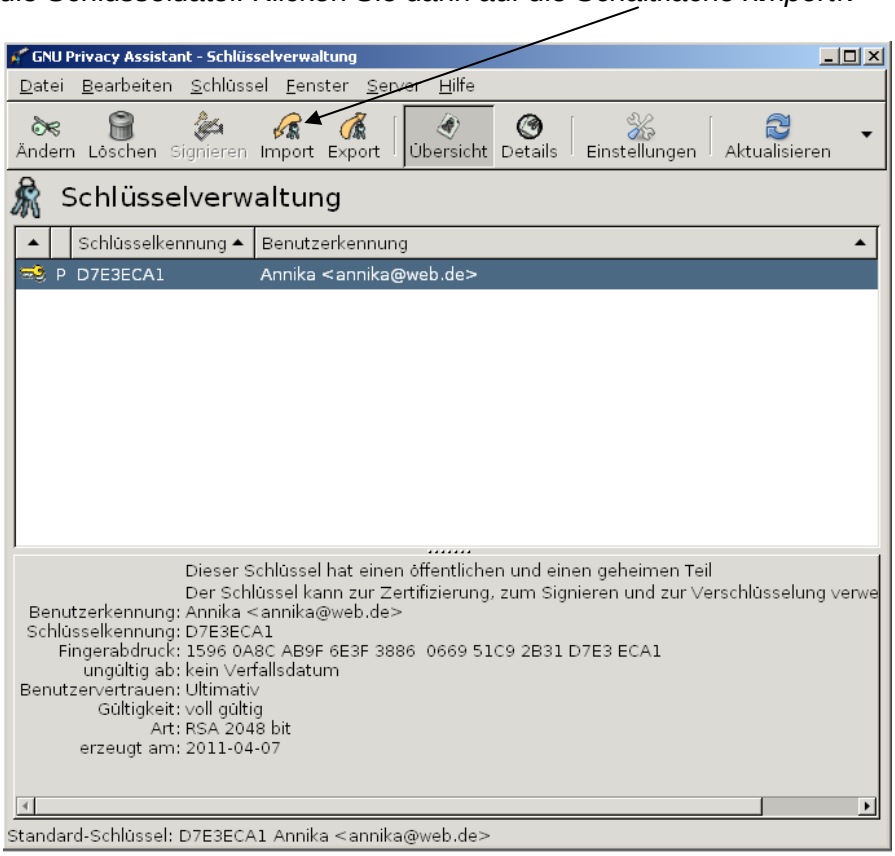


Wählen Sie als Namen Ihren Vor- oder Nachnamen, damit man erkennen kann, dass es sich um Ihren öffentlichen Schlüssel handelt. Nach dem Speichern können Sie die Datei, die Ihren exportierten öffentlichen Schlüssel enthält, z. B. per E-Mail versenden oder in einem öffentlichen Verzeichnis ablegen.

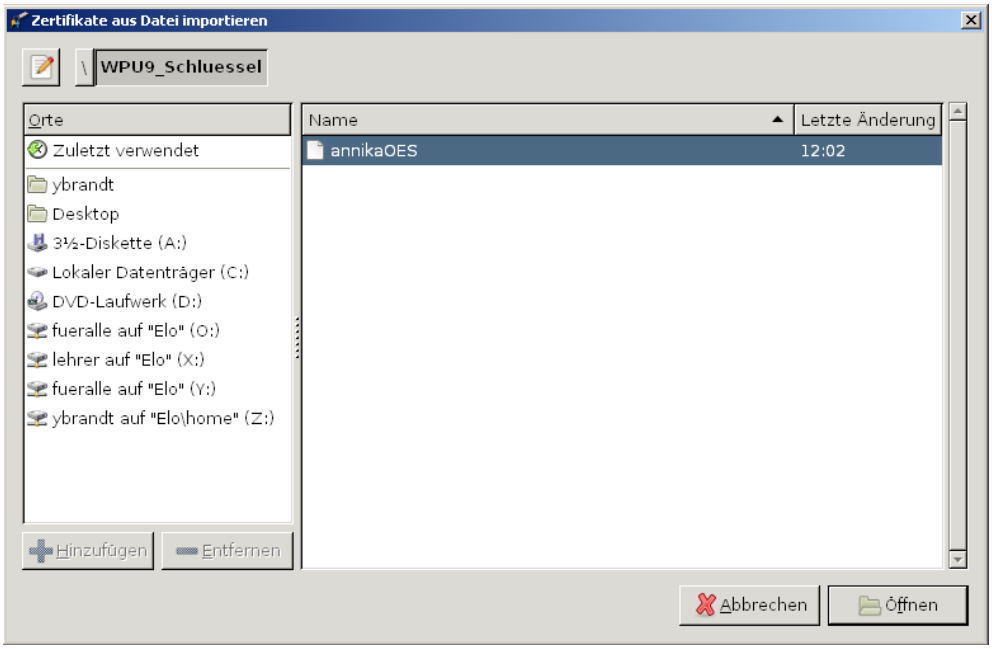


3. Schlüssel importieren

Um anderen eine geheime Nachricht zu schicken, benötigen Sie deren öffentlichen Schlüssel. Besorgen Sie sich von den Teilnehmern, denen Sie eine Nachricht schicken möchten, die Schlüsseldatei. Klicken Sie dann auf die Schaltfläche *Ämportñ*



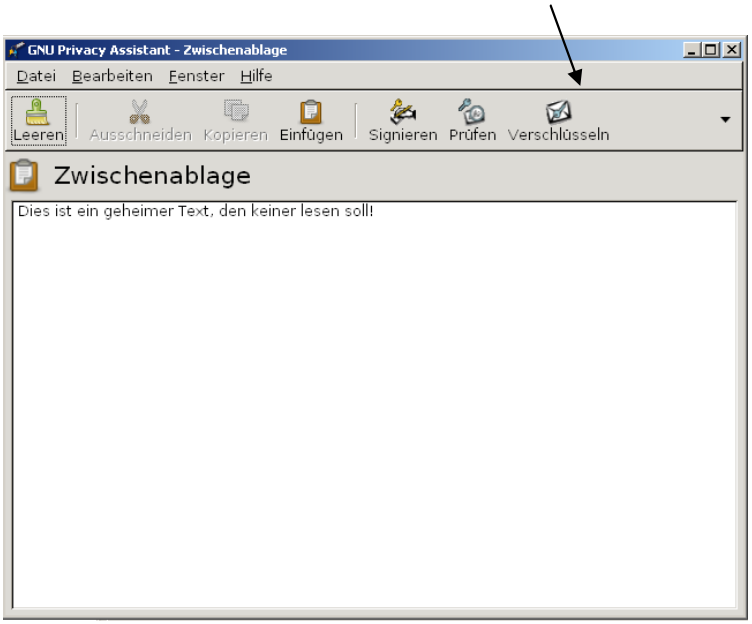
Wählen Sie die Datei mit dem Schlüssel aus, den Sie importieren möchten und klicken Sie dann auf *Öffnenñ*



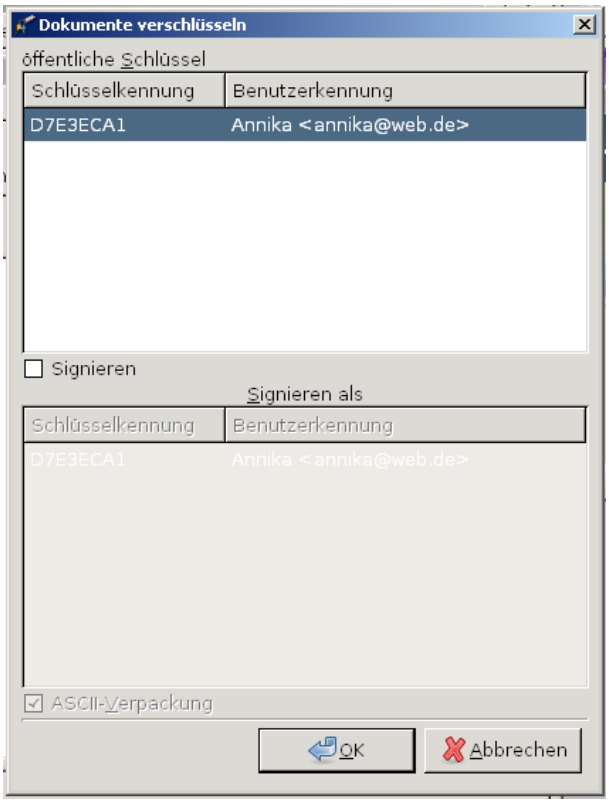
4. Verschlüsseln einer Nachricht

Um einen Text zu Verschlüsseln, öffnen Sie zunächst die *Zwischenablage* bzw. das *Clipboard* über ÄFenster → *Zwischenablage*ñ Den zu verschlüsselnden Text können Sie hier direkt eingeben oder hinein kopieren.

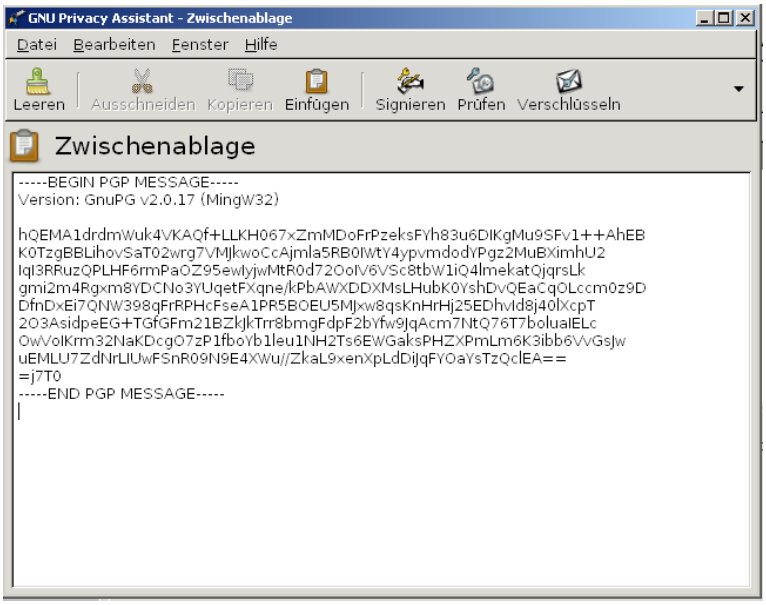
Klicken Sie anschließend auf die Schaltfläche Ä*Verschlüsseln*ñ

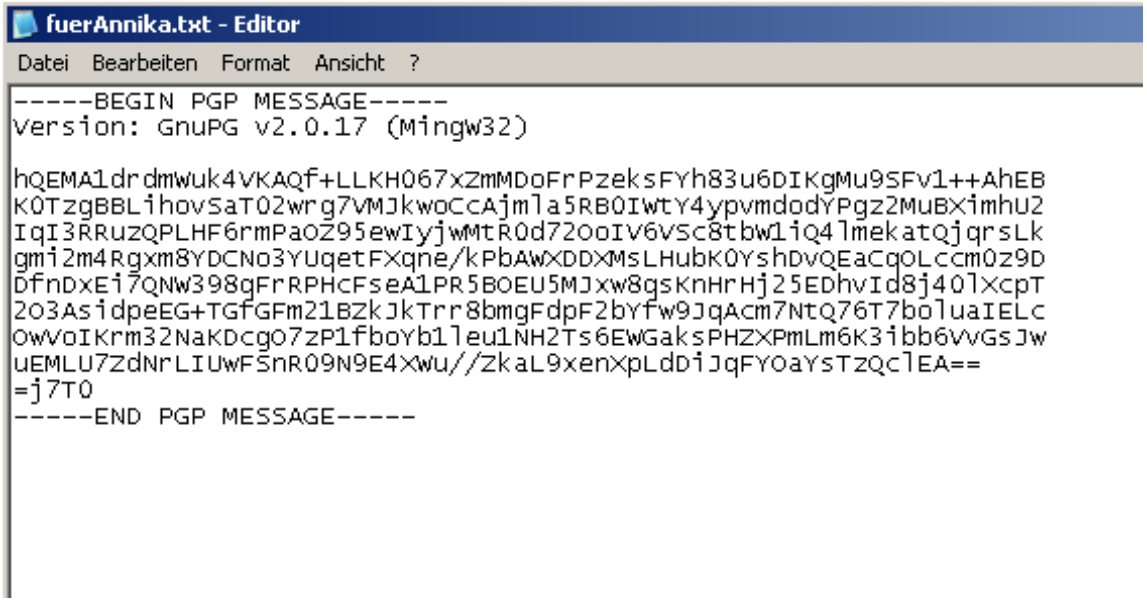


Es öffnet sich ein Fenster, in dem ausgewählt werden kann, für wen die Nachricht verschlüsselt werden soll. Wenn Annikas Freund Ben hier z.B. den öffentlichen Schlüssel von Annika auswählt, dann kann nur Annika diese Nachricht wieder entschlüsseln. Klicken Sie den Schlüssel an, mit dem verschlüsselt werden soll, und klicken Sie anschließend auf ok.



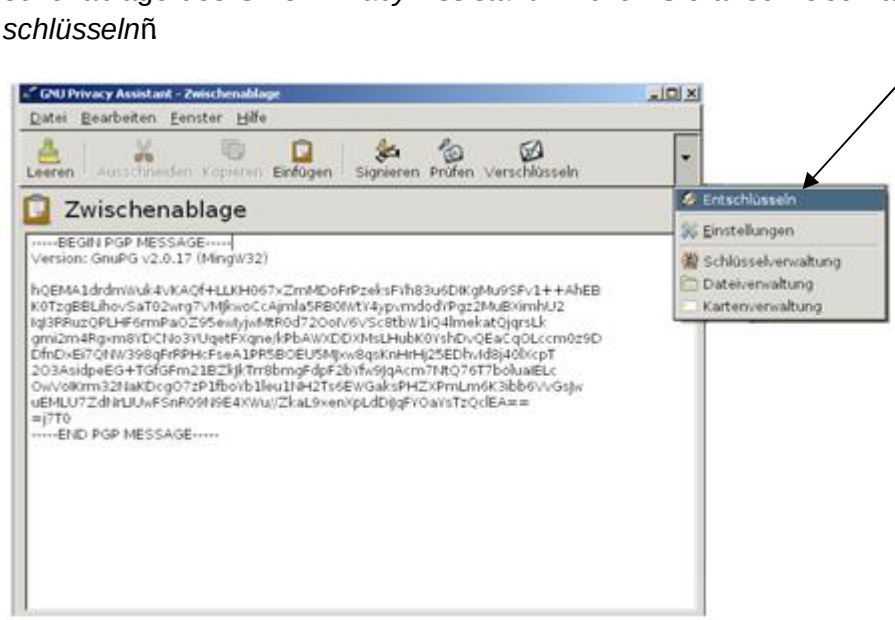
In der Zwischenablage wird nun der verschlüsselte Text angezeigt. Der gesamte Text kann nun z. B. in eine E-Mail kopiert werden oder in einen Editor, um Sie als Textdatei abzuspeichern. Wichtig ist, den gesamten Text zu kopieren. Die Textdatei könnte z. B. auch wieder in ein öffentliches Verzeichnis kopiert werden. Denn lesen kann ihn nur, wer den passenden privaten Schlüssel besitzt.



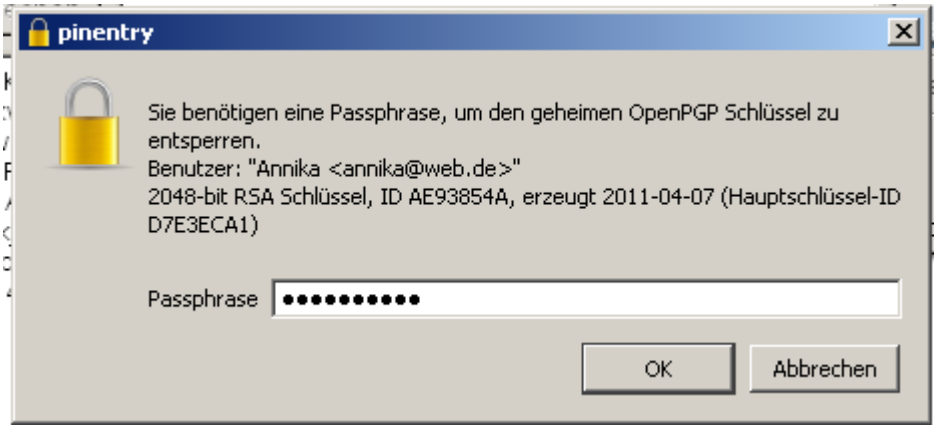


5. Texte entschlüsseln

Kopieren Sie den verschlüsselten Text aus dem Texteditor oder einer E-Mail in die Zwischenablage des *GNU Privacy Assistant*. Klicken Sie anschließen auf die Schaltfläche Ä*Entschlüsseln*ñ

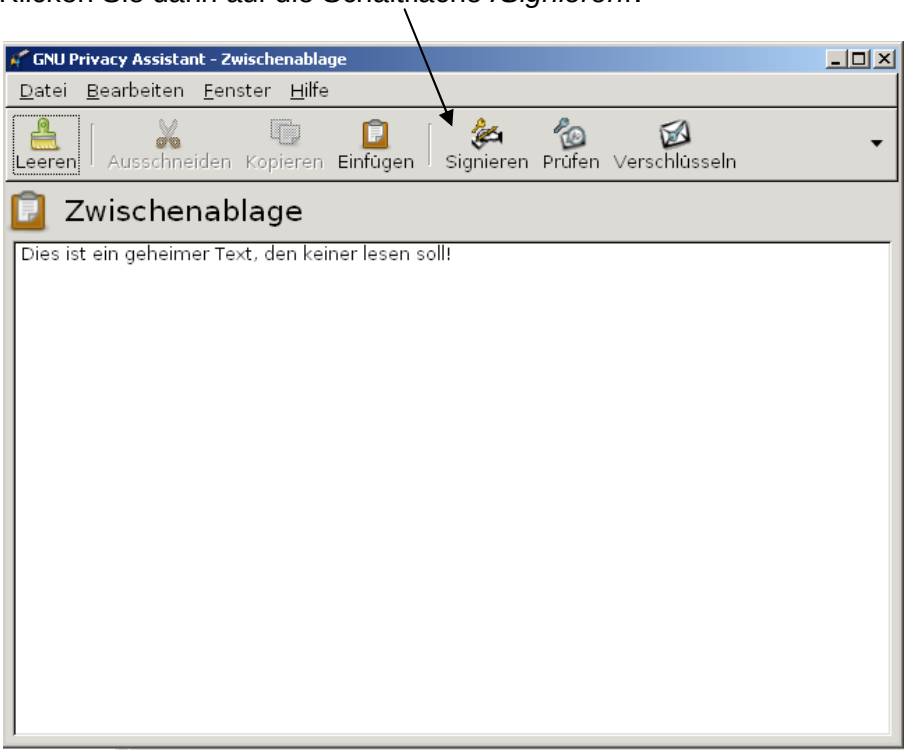


Um die Nachricht zu entschlüsseln, müssen Sie nun das Passwort für Ihren privaten Schlüssel eingeben, um sich als Eigentümer des privaten Schlüssels auszuweisen. Klicken Sie anschließend auf ok.

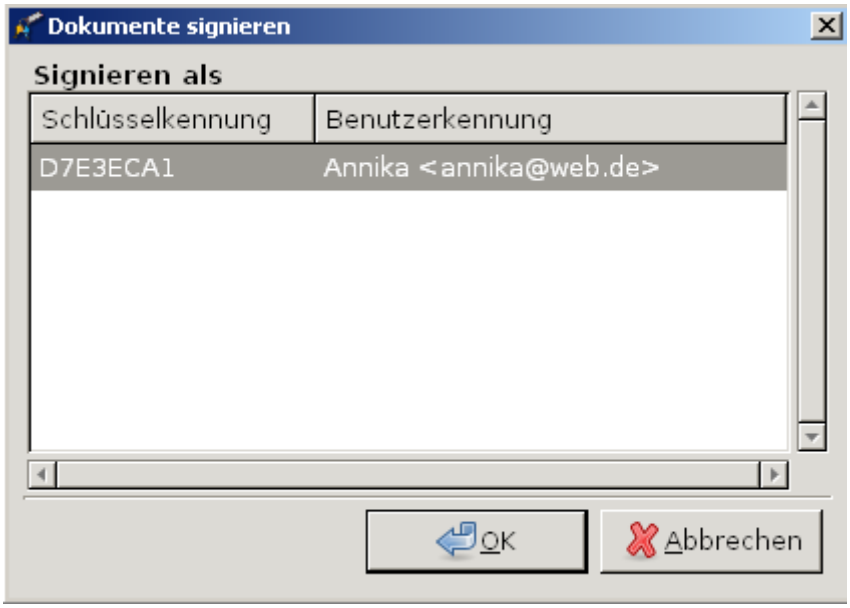


6. Texte signieren

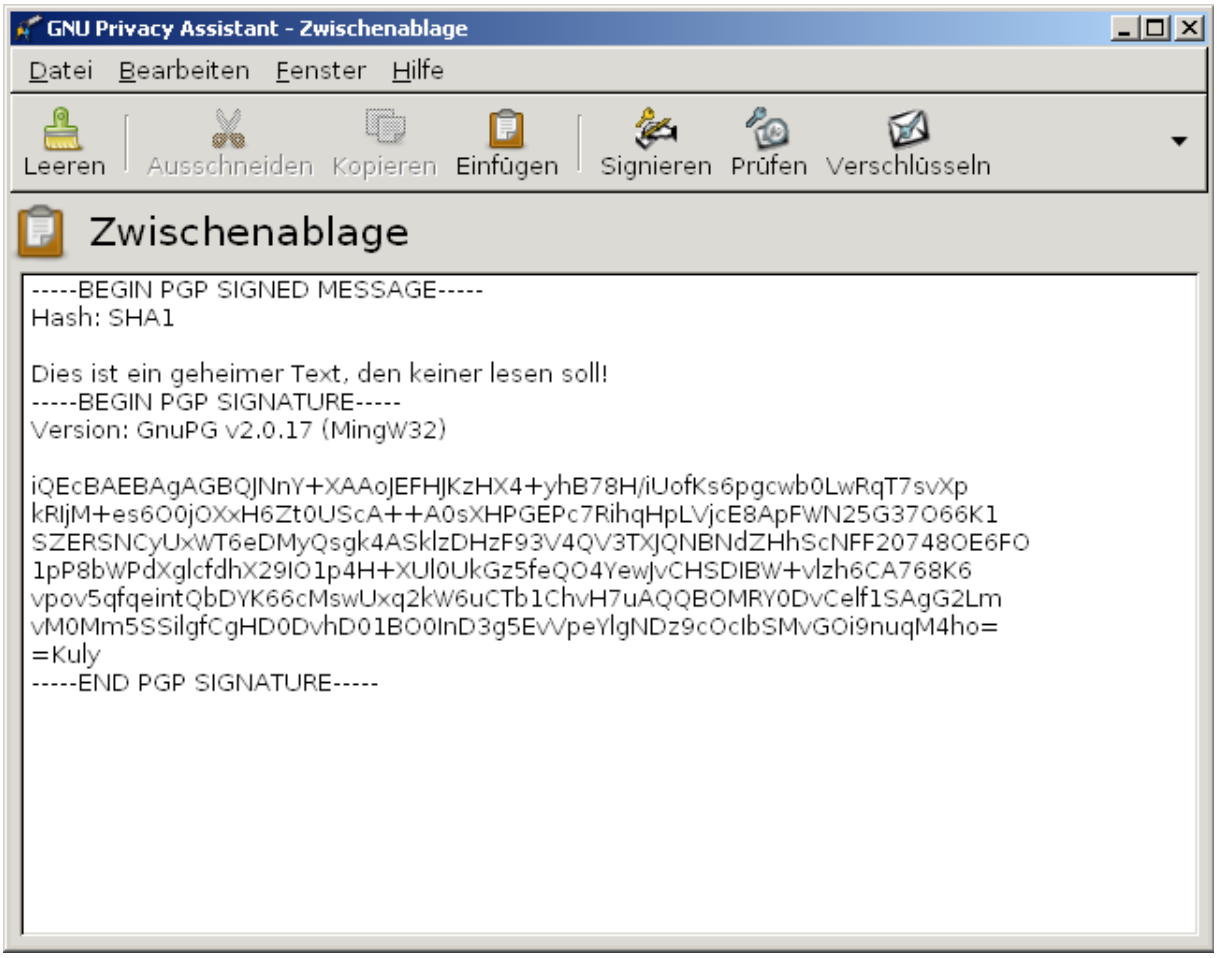
Einen Text zu signieren, bedeutet einen Text zu unterscheiben, um zu bezeugen, dass der Text tatsächlich von einem selbst stammt. Dazu muss der Text, der signiert werden soll, wieder in die Zwischenablage des *GNU Privacy Assistant* geschrieben oder kopiert werden. Klicken Sie dann auf die Schaltfläche ĂSignierenñ



Das Unterschreiben erfolgt mithilfe des privaten Schlüssels. Es öffnet sich ein Fenster in dem der Schlüssel mit dem signiert werden soll, ausgewählt werden kann. In diesem Fall würde Annika einen Text mit ihrem privaten Schlüssel signieren. Wählen Sie Ihren privaten Schlüssel aus und klicken Sie auf ok.

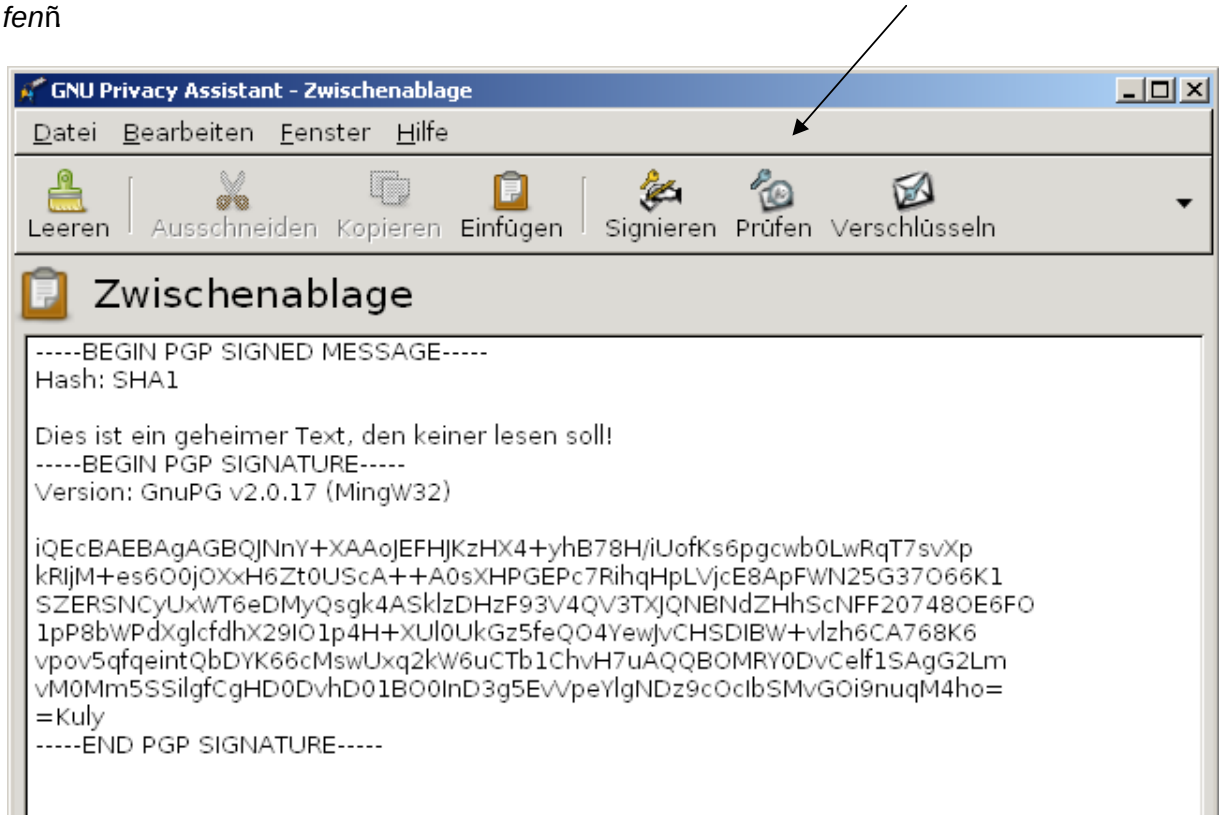


In der Zwischenablage erscheint nun der signierte Text. Dieser Text kann nun wieder als E-Mail versendet oder als Text abgespeichert werden.



7. Signatur überprüfen

Um eine Signatur zu überprüfen, also um zu schauen, ob der Absender tatsächlich derjenige ist, der unterschrieben hat, muss die unterschriebene Nachricht wieder in die Zwischenablage des *GNU Privacy Assistant* kopiert werden. Klicken Sie dann auf die Schaltfläche *ÄPrüfenñ*



Der *GNU Privacy Assistant* überprüft nun, zu welchem öffentlichen Schlüssel die Signatur der Nachricht passt. Ich kann also nur Unterschriften von Leuten erkennen, deren öffentlichen Schlüssel ich vorher importiert habe. Wenn die Signatur korrekt ist, muss der Eigentümer des öffentlichen Schlüssels mit dem vermeintlichen Absender der Nachricht identisch sein. Das Ergebnis wird in einem kleinen Fenster angezeigt. In diesem Fall zeigt der Status *ÄGültigñ*an, dass die Nachricht von Annika stammt.