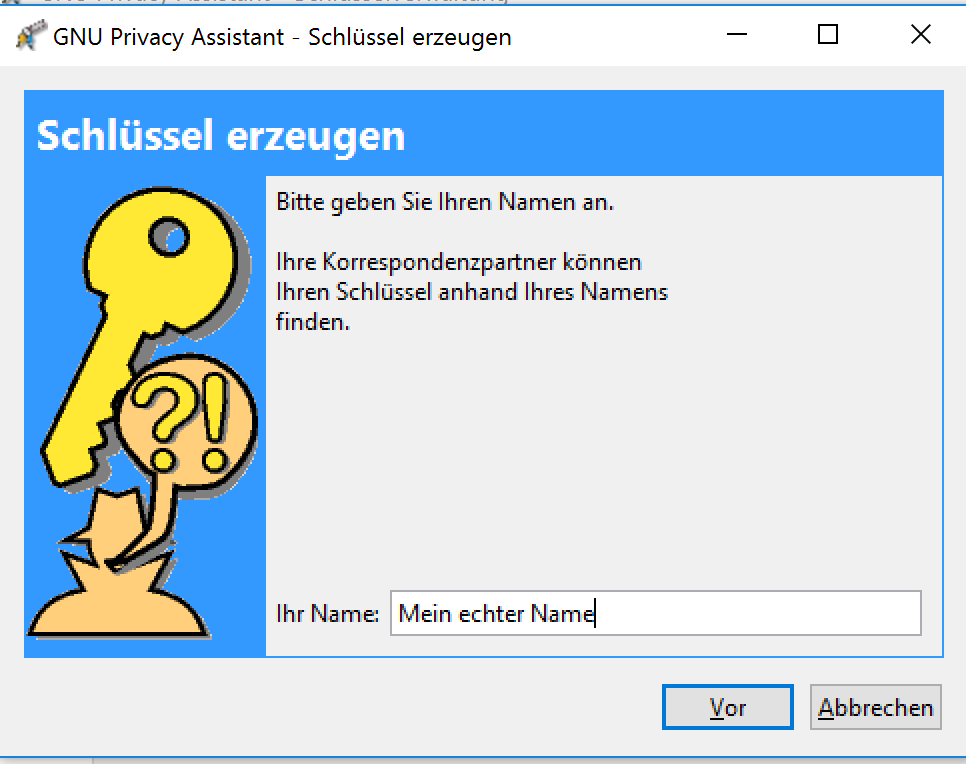
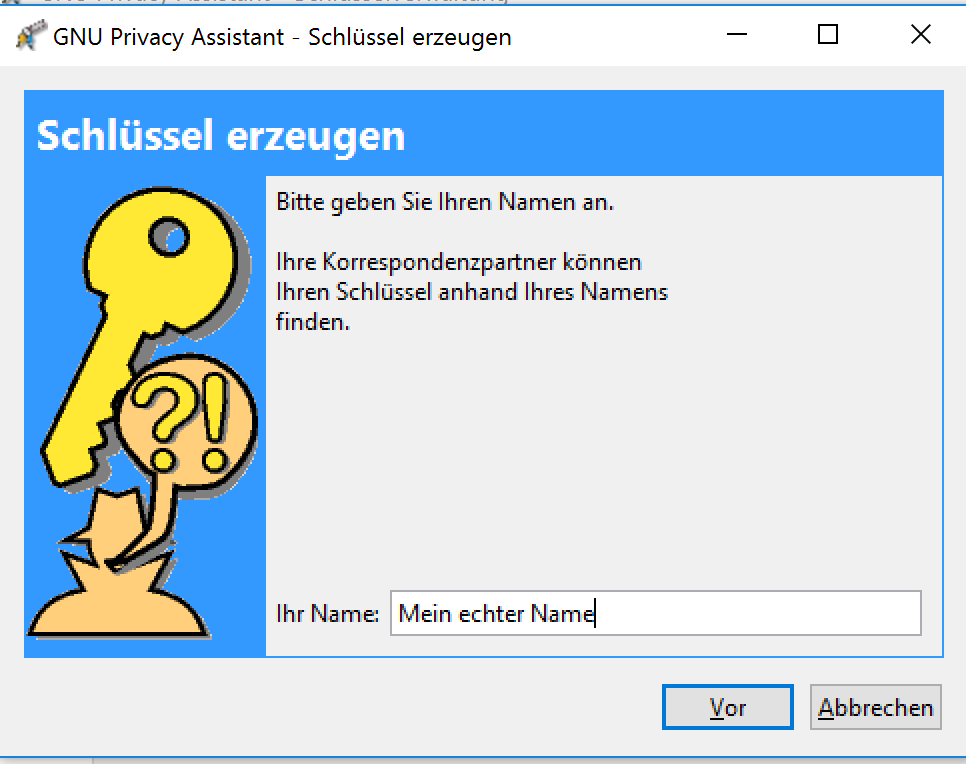
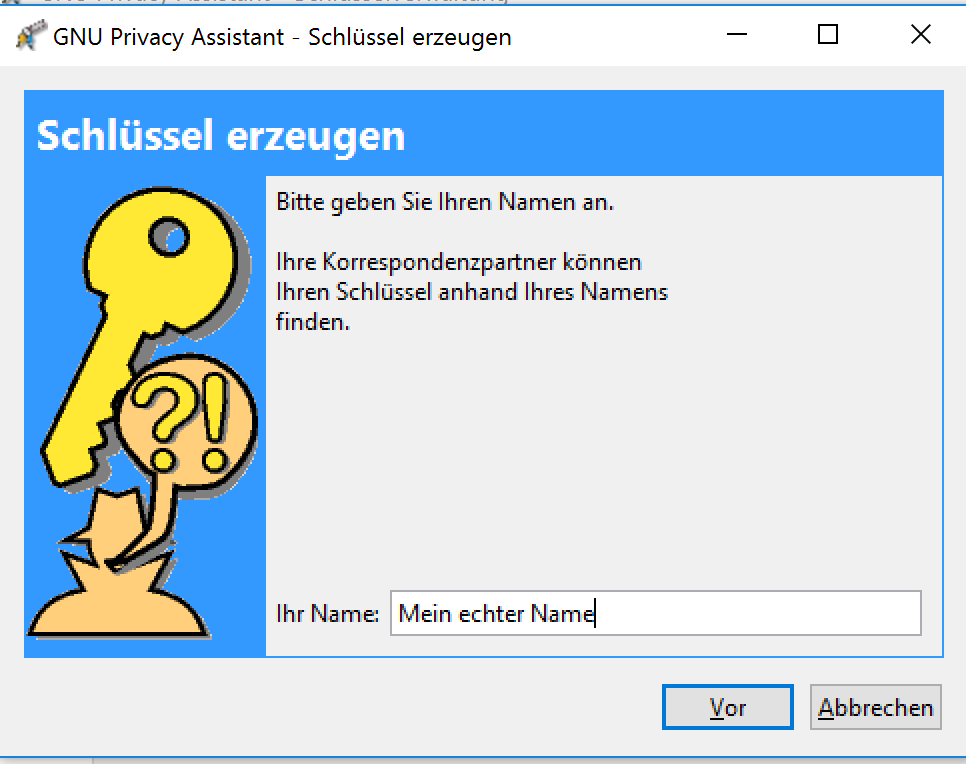
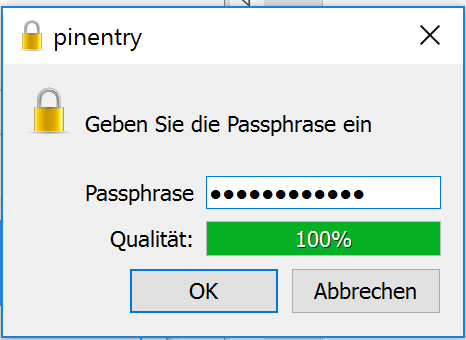
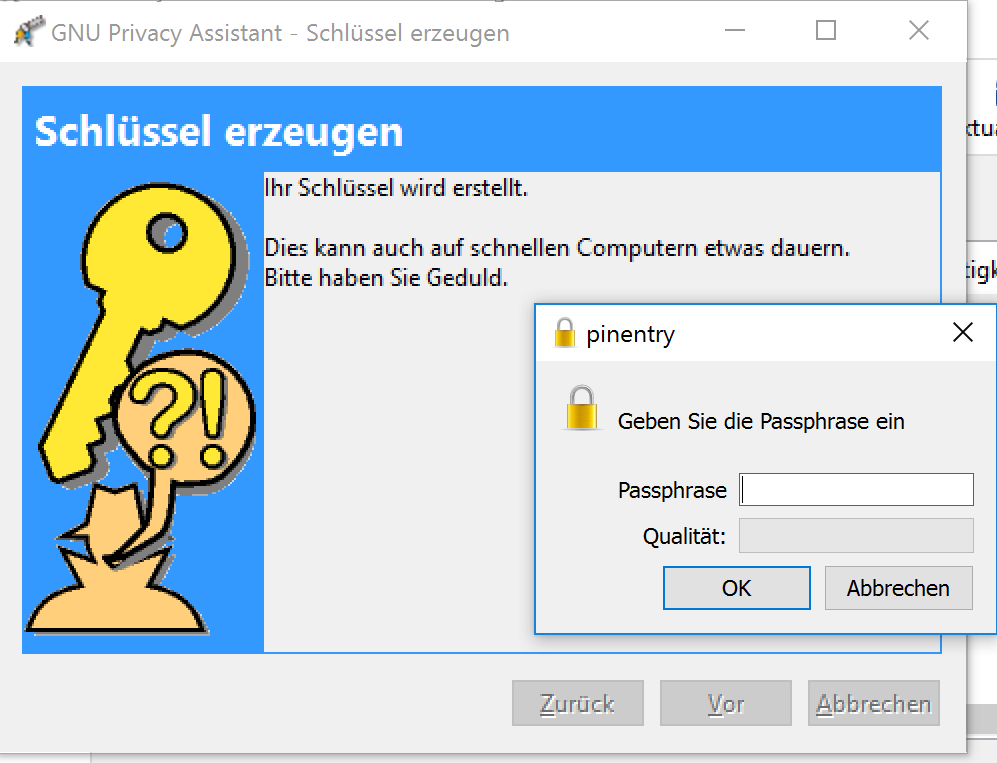
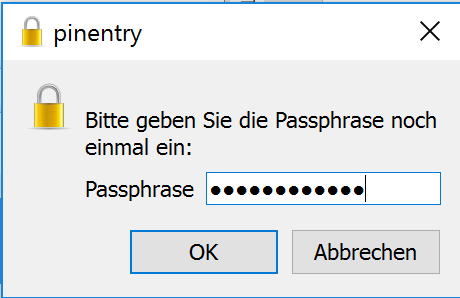
# 12 Verschlüsselungsprogramm verwenden

|  |  |
| --- | --- |
| **erwünschtes Ergebnis** | Sie können ein Verschlüsselungsprogramm verwenden. |
| **Zeitaufwand** | 60 min. |
| **Ausgangslage** | Installieren Sie die Software GNUPG von der Webseite <http://www.gpg4win.org/index-de.html> auf Ihrem Windows Computer.  Alternativ: Enigmail für Thunderbird oder GPGTools für Mac.  Führen Sie die komplette Installation durch. |
| **Aufgabe** | Gehen Sie gemäss den nachfolgenden Aufgaben vor. |
| **Unterlagen** | Lehrmittel Kapitel 11, Internet |
| **Ergebnis** | Sie können eine privaten Schlüssel generieren, öffentliche Schlüssel importieren, eine Nachricht verschlüsseln und signieren. |

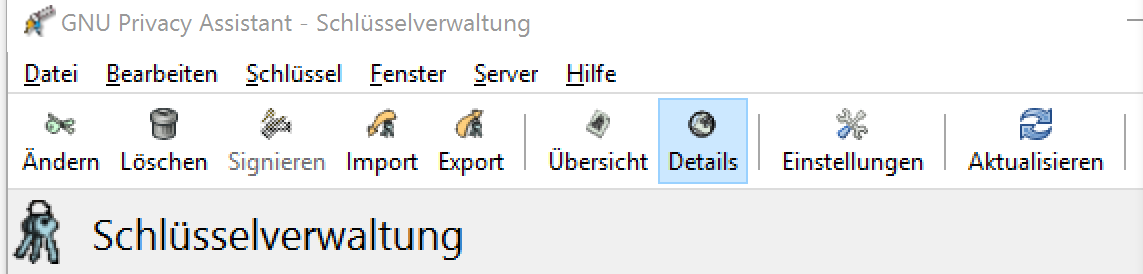
## Privaten Schlüssel erstellen

Nach der erfolgreichen Installation der Anwendung starten Sie die Anwendung GP4Win und führen sie die folgenden Schritte aus.

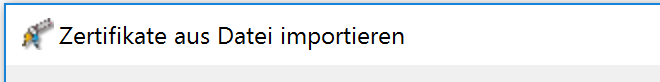
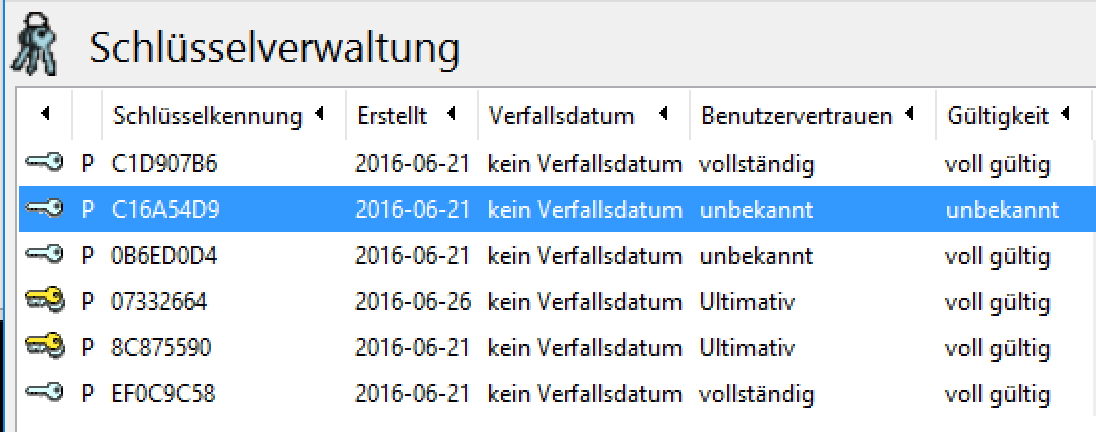
1. Auf Fenster 🡪 Schlüsselverwaltung klicken
2. Im Menü «Schlüssel» den Punkt «neuer Schlüssel» auswählen
3. Ihren Namen eingeben
4. Geben Sie Ihre gültige E-Mail-Adresse ein
5. Lassen Sie nach dem Erstellen des Schlüssels eine Sicherheitskopie anlegen.
6. Für die Nutzung des privaten Schlüssels ist ein Passwort Schutz notwendig. Geben Sie ein sicheres Kennwort ein und bestätigen Sie es.

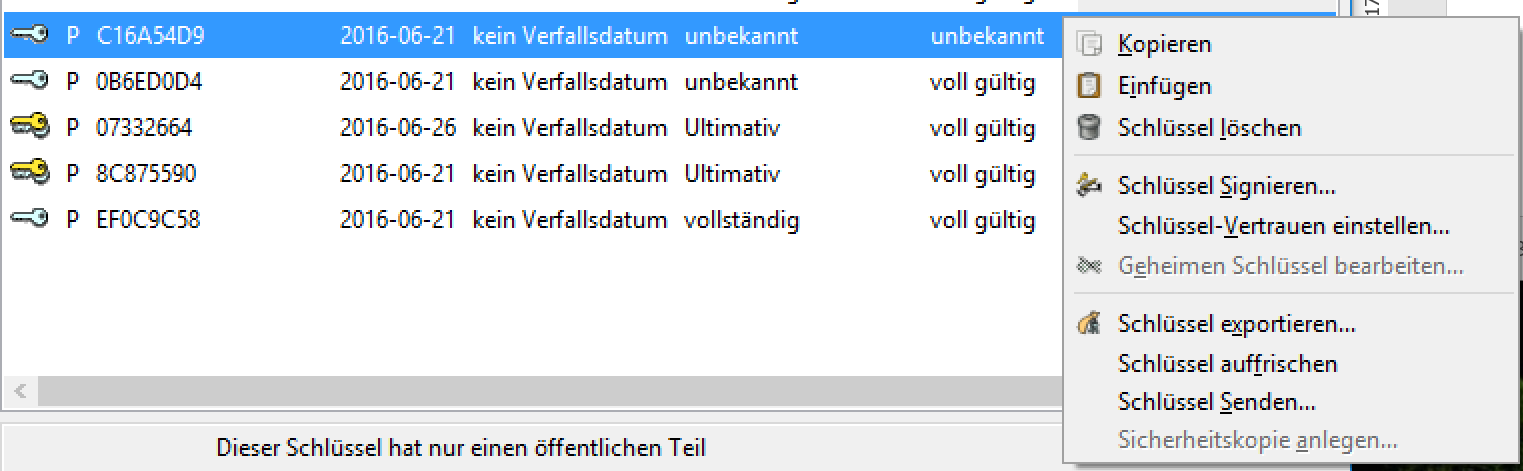


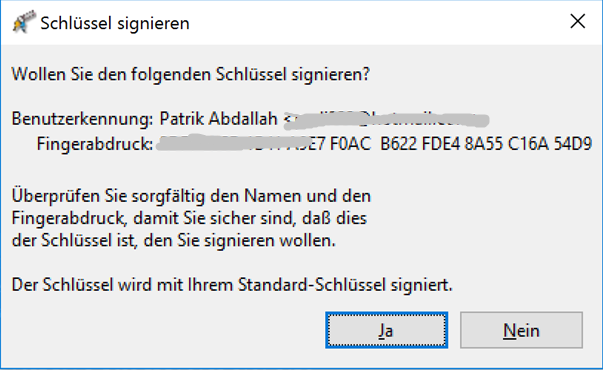
1. Erstellen Sie die Sicherheitskopie Ihres Schlüssels. Bewahren Sie diesen gut und SICHER auf.



## Importieren eines öffentlichen Schlüssels

1. Importieren Sie einen öffentlichen Schlüssel mit «Import»
2. Wählen Sie den Schlüssel aus (bei Gpg4win mit dem Programm «Kleopatra», welches automatisch installiert wurde).
3. Damit Sie den öffentlichen Schlüssel verwenden können, müssen Sie ihn beglaubigen:



1. Bestätigen Sie den Schlüssel, in dem Sie den Fingerprint verifizieren.
2. Mit der Eingabe ihres Kennwortes für den privaten Schlüssel, bestätigen Sie die Echtheit des öffentlichen Schlüssels und können ihn für die Übungen verwenden.
3. Erstellen Sie nun eine Nachricht und verschlüsseln und signieren Sie diese.

## Ablaufskizze

Zeichnen Sie den Ablauf der Verschlüsselung vom Sender zum Empfänger auf.



5

3

4

2

1

