

## Erstellen eines asymmetrischen Schlüsselpaares

1. Öffnen Sie das Programm GPA (GNU Privacy Assistant)<sup>1</sup>.  
Wenn Sie das Programm zum ersten Mal öffnen, erscheint das Fenster in Abbildung 1.  
Klicken Sie dort auf den Button *Jetzt Schlüssel erzeugen*.

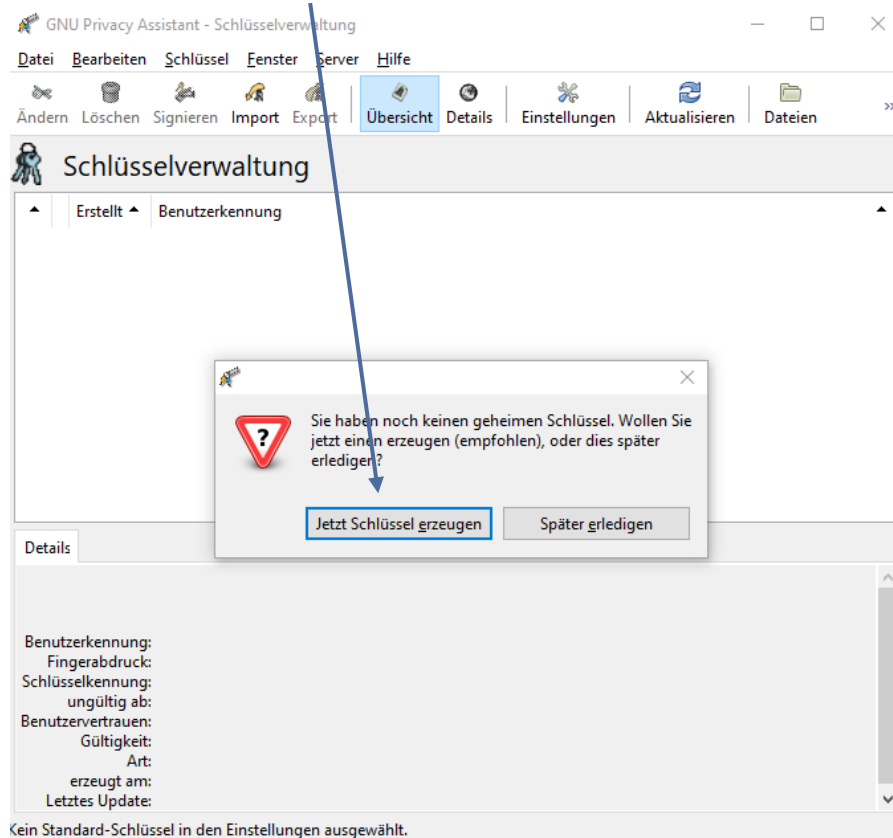


Abbildung 1: Startfenster GPA

Sie können diese Option auch später jederzeit auswählen, indem Sie im Menü den Punkt *Schlüssel* → *Neuer Schlüssel...* anklicken (s. Abbildung 2).

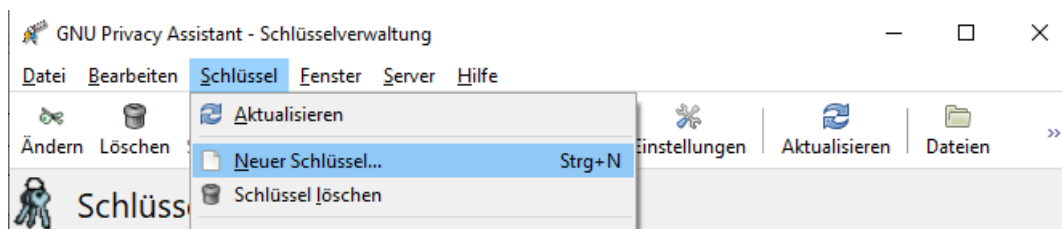


Abbildung 2: Auswahl der Option „Neuer Schlüssel“ über das Menü

<sup>1</sup> GPA ist Teil des Softwarepakets Gpg4win <https://www.gpg4win.org/> [Datum des Zugriffs: 12.02.2021]  
für diese Anleitung wurde die Version Gpg4win-3.1.15 verwendet

2. Es öffnet sich das Fenster in Abbildung 3.  
Geben Sie hier bitte zuerst Ihren Namen ein.  
Klicken Sie auf den Button *Vor*.  
Geben Sie nun Ihre Mailadresse ein. Die Mailadresse kann für die Übungen fiktiv sein. (Geben Sie aber bitte Ihren richtigen Namen ein, damit sich der Schlüssel leichter zuordnen lässt.)  
Klicken Sie noch einmal auf den Button *Vor*.

The image shows two sequential screenshots of the GNU Privacy Assistant window titled "Schlüssel erzeugen".

**Top Screenshot:** The window has a blue header with the title "Schlüssel erzeugen". On the left is a cartoon illustration of a yellow key with a question mark and exclamation mark inside its head. The main text area says: "Bitte geben Sie Ihren Namen an. Ihre Korrespondenzpartner können Ihren Schlüssel anhand Ihres Namens finden." Below this is a text input field labeled "Ihr Name:" containing the text "Bernhard Beispiel". At the bottom right are two buttons: "Vor" (highlighted with a blue border) and "Abbrechen".

**Bottom Screenshot:** The window is the same, but the text area now says: "Bitte geben Sie Ihre E-Mail-Adresse an. Ihre E-Mail-Adresse wird Teil des Schlüssels und erleichtert Ihren Korrespondenzpartner daher, Ihren Schlüssel zu identifizieren. Falls Sie mehrere E-Mail-Adressen haben, können Sie diese später hinzufügen." The text input field labeled "Ihre E-Mail-Adresse:" now contains "b.beispiel@meine-schule.edu". The buttons at the bottom are "Zurück", "Vor" (highlighted with a blue border), and "Abbrechen".

Abbildung 3: Eingabe von Name und Mailadresse.

3. Es erscheint das Fenster in Abbildung 4. Da Sie zunächst keine Sicherheitskopie des Schlüssels benötigen, wählen Sie hier die Option *Später erledigen*. Klicken Sie auf den Button *Vor*.



Abbildung 4: Optionales Erstellen einer Sicherheitskopie

4. Es erscheint die Meldung, dass das Erzeugen eines Schlüssels einige Zeit dauern kann. Außerdem werden Sie aufgefordert eine Passphrase einzugeben. Das ist ein Passwort, das Sie später eingeben müssen, bevor Sie den privaten Schlüssel verwenden können. Damit soll sichergestellt werden, dass nur Sie den privaten Schlüssel nutzen können. Dieses Passwort also bitte gut merken!  
Bestätigen Sie Ihr Passwort durch Klick auf den Button *OK*.

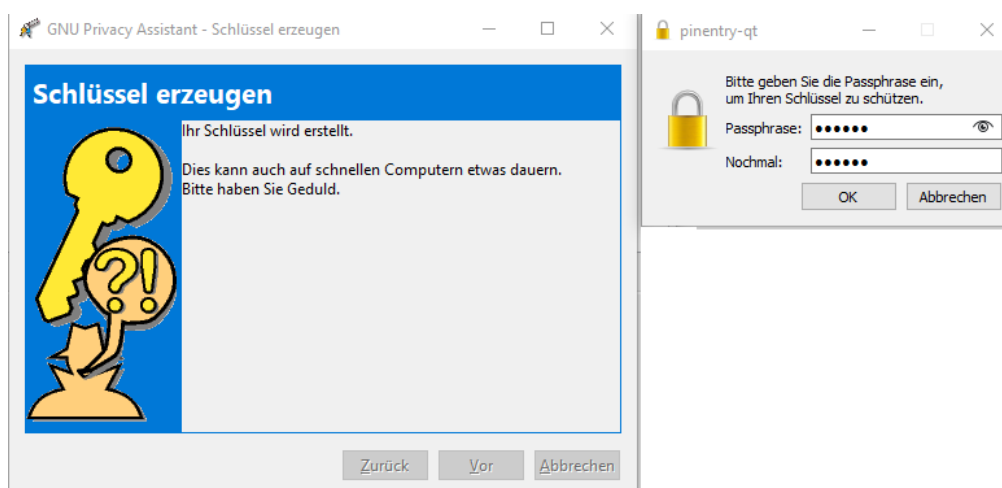


Abbildung 5: Auswahl einer Passphrase zum Schutz des privaten Schlüssels.

5. Der Schlüssel wird nun in der Übersicht angezeigt.

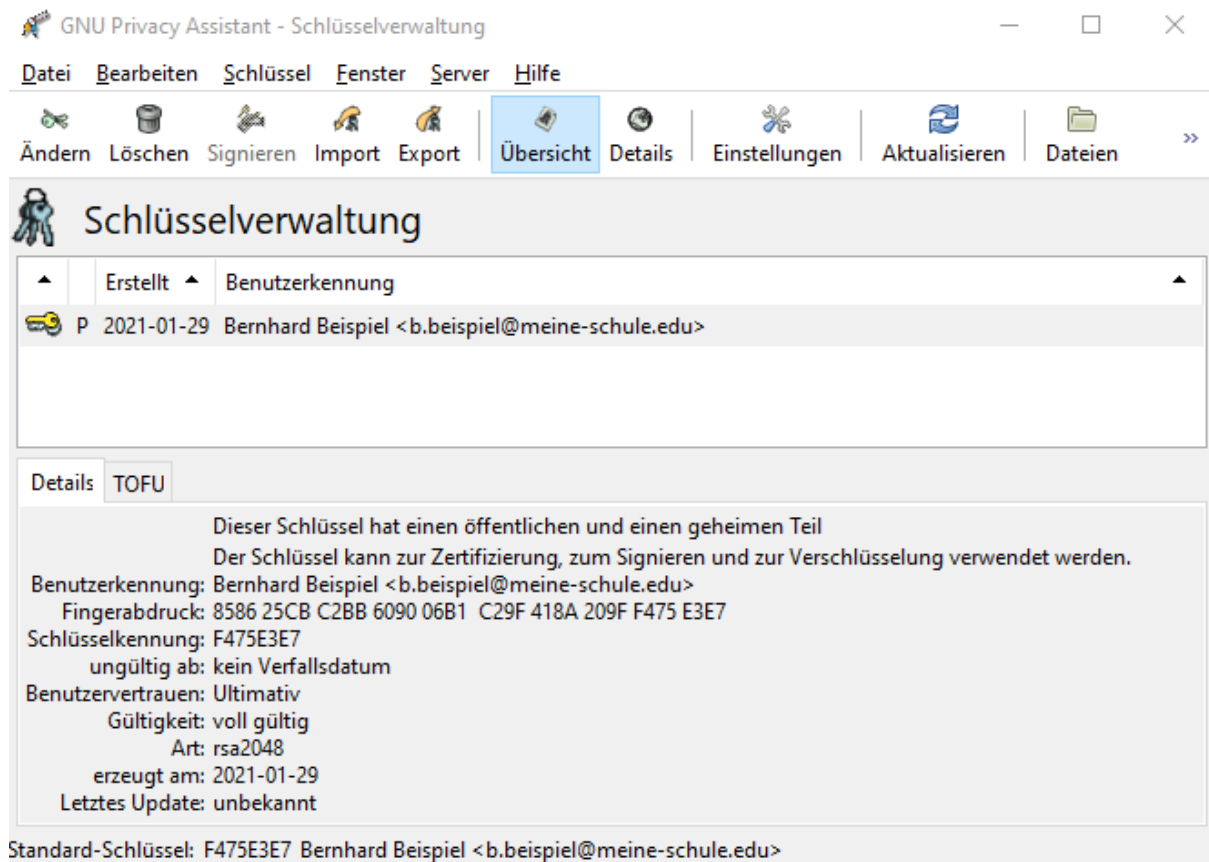


Abbildung 6: Anzeige des erstellten Schlüssels in der Übersicht.

## Exportieren des öffentlichen Schlüssels

1. Markieren Sie Ihren Schlüssel in der Übersicht und wählen Sie die Option *Export*.

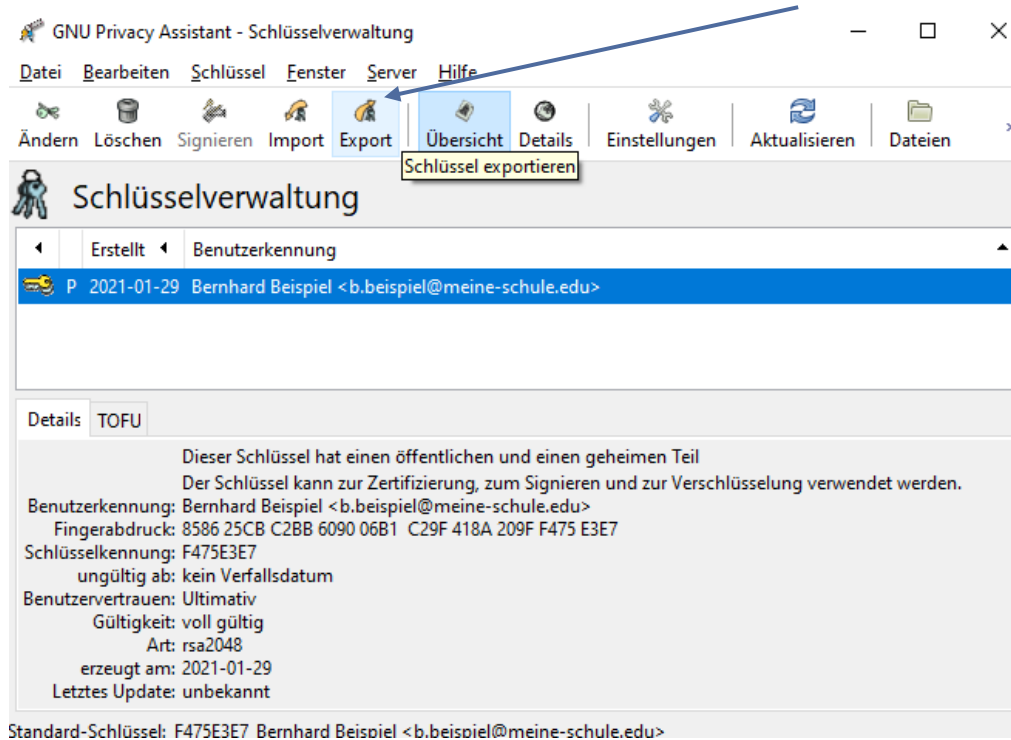


Abbildung 7: Exportieren des öffentlichen Schlüssels.

Sollten die Schaltfläche nicht wie in Abbildung 7 angezeigt werden, können Sie die Option auch über das Menü *Schlüssel* → *Schlüssel exportieren* auswählen.

2. Es öffnet sich das Fenster in Abbildung 8.

Geben Sie zunächst einen Dateinamen ein. Der Dateiname sollte Ihren Namen enthalten, damit sich der Schlüssel leichter zuordnen lässt.

Wählen Sie anschließend aus, wo Sie die Datei mit Ihrem öffentlichen Schlüssel speichern möchten. Diese Datei können Sie anschließend an alle weitergeben, die Ihnen eine verschlüsselte Nachricht schicken möchten. Falls Sie einen gemeinsamen Austauschordner für Ihre Lerngruppe besitzen, können Sie diesen direkt als Speicherort auswählen. Sie können diese Datei aber z. B. auch als Anhang einer Mail verschicken.

Klicken Sie auf den Button *Speichern*.

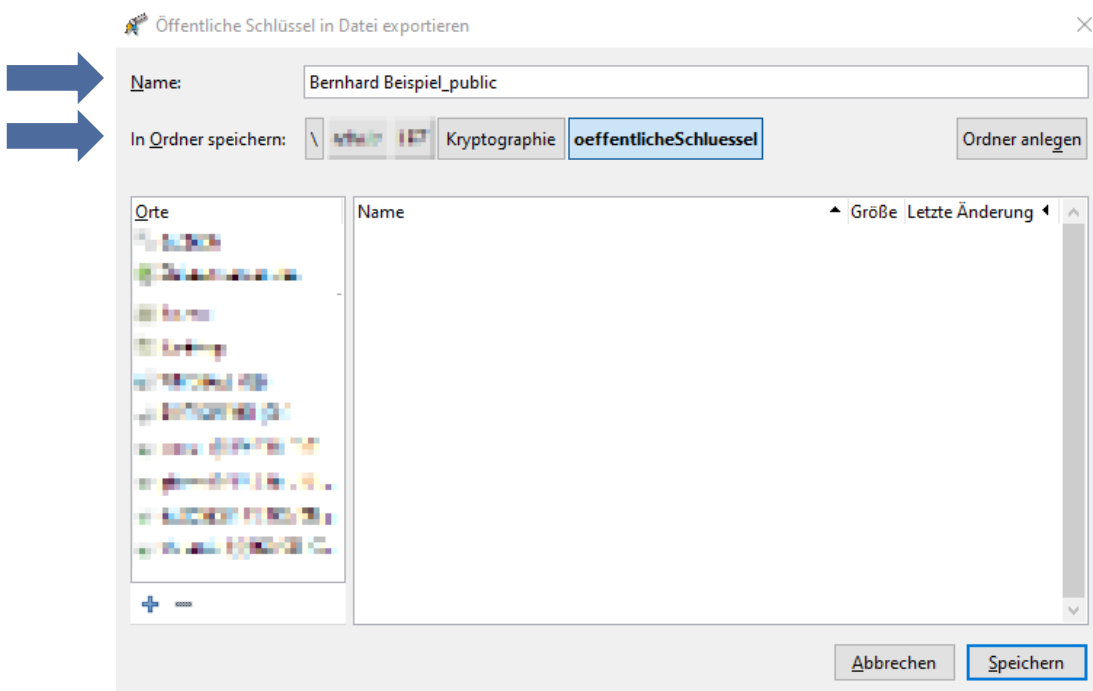


Abbildung 8: Speichern des öffentlichen Schlüssels zur Weitergabe

3. Es erscheint eine Bestätigung wie in Abbildung 9. Klicken Sie auf den Button *Schließen*.

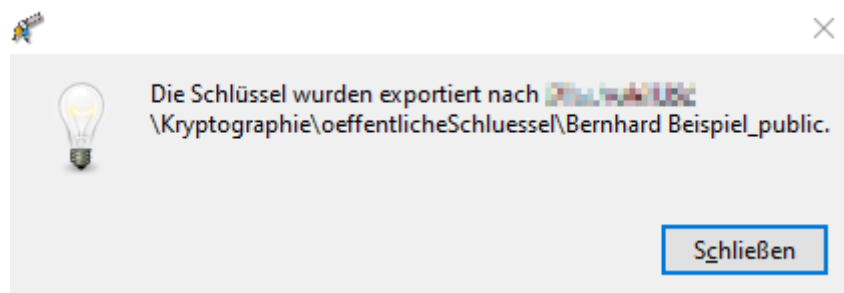


Abbildung 9: Bestätigung des erfolgreichen Exportierens

## Importieren öffentlicher Schlüssel

1. Um die öffentlichen Schlüssel Ihrer Mitschülerinnen und Mitschüler zu importieren, wählen Sie die Option *Importieren*.

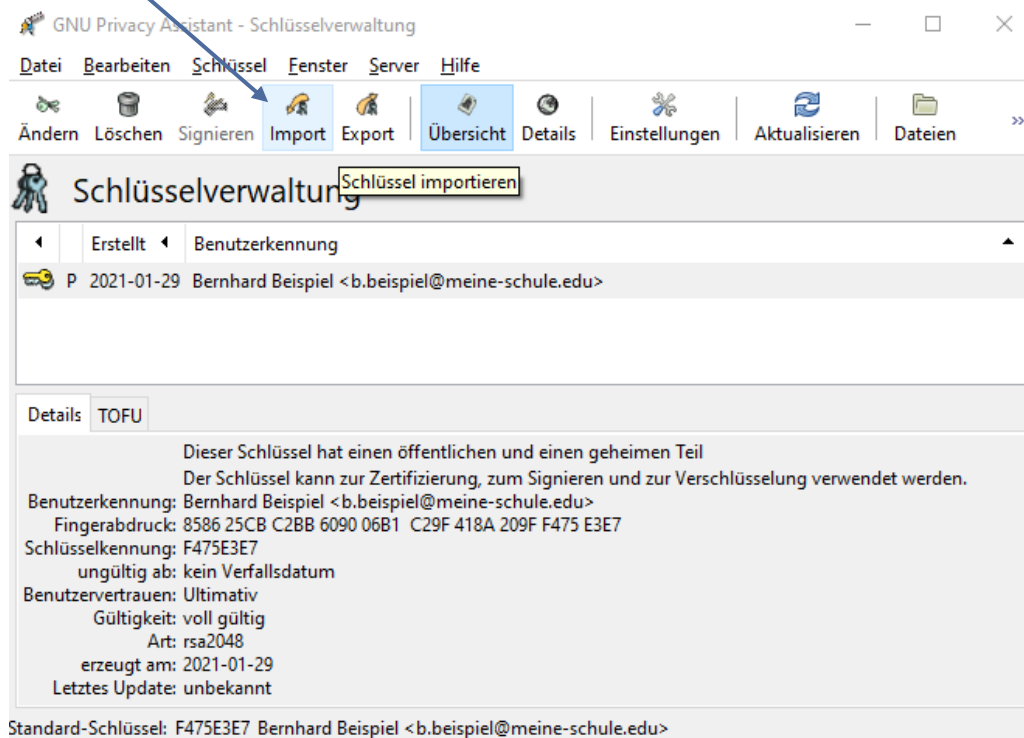


Abbildung 10: Importieren öffentlicher Schlüssel

Sollte Ihnen die Schaltfläche nicht wie in Abbildung 10 angezeigt werden, können Sie die Option auch über das Menü *Schlüssel* → *Schlüssel importieren* auswählen.

2. Es öffnet sich das Fenster in Abbildung 11.  
Wählen Sie hier zunächst den Ordner aus, in dem die öffentlichen Schlüssel gespeichert sind.  
Markieren Sie anschließend den öffentlichen Schlüssel, den Sie importieren möchten.  
Klicken Sie auf *Öffnen*.

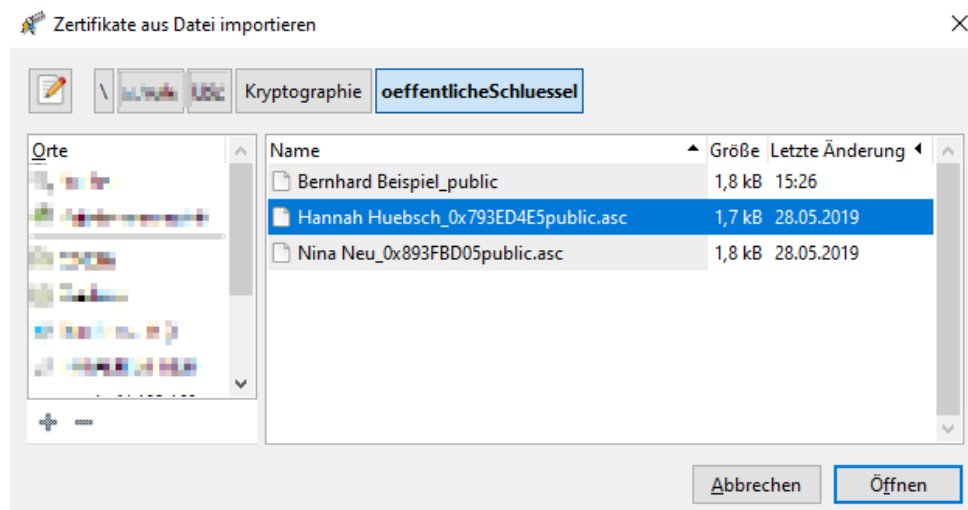


Abbildung 11: Auswählen der öffentlichen Schlüssel

3. Sie erhalten eine Statusmeldung, wie viele Schlüssel importiert wurden. Klicken Sie auf *Schließen*. Die importierten öffentlichen Schlüssel werden nur in Ihrer Übersicht angezeigt.

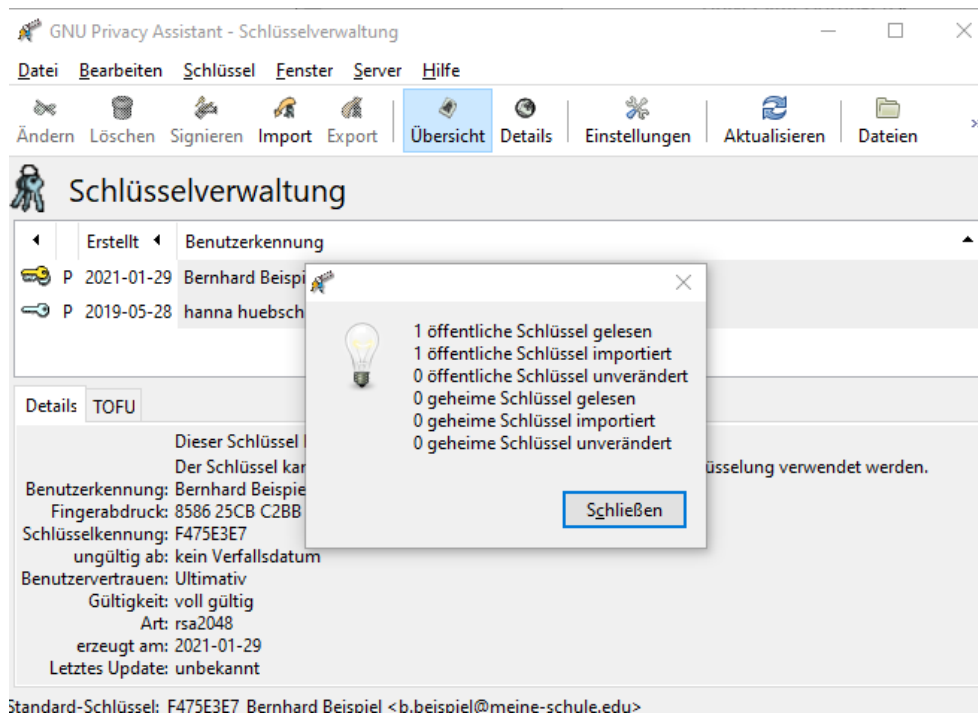


Abbildung 12: Bestätigung des Importierens

- Anhand der Schlüsselsymbole erkennen Sie, dass es sich bei dem importierten Schlüssel nur um einen öffentlichen Schlüssel handelt (Symbol: nur ein blauer Schlüssel). Bei Ihrem eigenen Schlüssel handelt es sich hingegen um ein Schlüsselpaar (Symbol: blauer und gelber Schlüssel).
4. Wenn Sie weitere Schlüssel importieren möchten, wiederholen Sie die Schritte 1 bis 3.

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#). Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.