

Erstellen eines asymmetrischen Schlüsselpaars

1. Öffne das Programm GPA (GNU Privacy Assistant)¹.

Wenn du das Programm zum ersten Mal öffnest, erscheint das Fenster in Abbildung 1.

Klicke dort auf den Button *Jetzt Schlüssel erzeugen*.

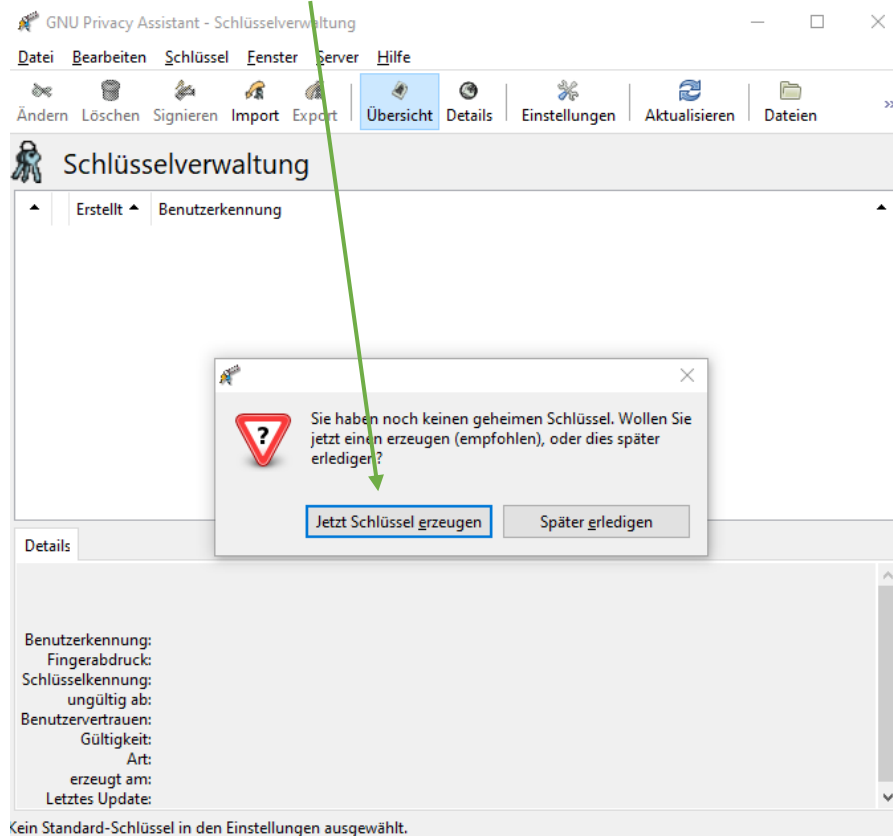


Abbildung 1: Startfenster GPA

Du kannst diese Option auch später jederzeit auswählen, indem du im Menü den Punkt *Schlüssel* → *Neuer Schlüssel...* anklickst (s. Abbildung 2).

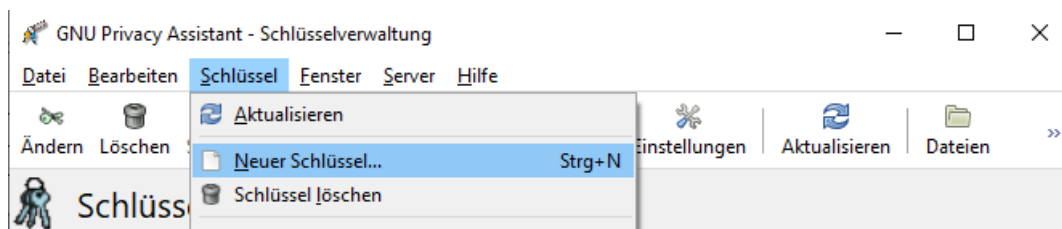


Abbildung 2: Auswahl der Option „Neuer Schlüssel“ über das Menü

¹ 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.
Gib hier bitte zuerst deinen Namen ein.
Klicke auf den Button *Vor*.
Gib nun deine Mailadresse ein. Die Mailadresse kann für die Übungen fiktiv sein. (Gib aber bitte deinen richtigen Namen ein, damit sich der Schlüssel leichter zuordnen lässt.)
Klicke 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 prompts the user to enter their name. It includes a cartoon illustration of a key and a person with a question mark. The text says: "Bitte geben Sie Ihren Namen an. Ihre Korrespondenzpartner können Ihren Schlüssel anhand Ihres Namens finden." The input field "Ihr Name:" contains the text "Bernhard Beispiel". The "Vor" button is highlighted.

Bottom Screenshot: The window prompts the user to enter their email address. It includes the same cartoon illustration. The text 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 input field "Ihre E-Mail-Adresse:" contains the text "b.beispiel@meine-schule.edu". The "Vor" button is highlighted.

Abbildung 3: Eingabe von Name und Mailadresse.

3. Es erscheint das Fenster in Abbildung 4. Da du zunächst keine Sicherheitskopie des Schlüssels benötigst, wähle hier die Option *Später erledigen*.
Klicke 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 wirst du aufgefordert eine Passphrase einzugeben. Das ist ein Passwort, das du später eingeben musst, bevor du den privaten Schlüssel verwenden kannst. Damit soll sichergestellt werden, dass nur du den privaten Schlüssel nutzen kannst. Dieses Passwort musst du dir also gut merken.
Bestätige dein Passwort durch Klick auf den Button *OK*.

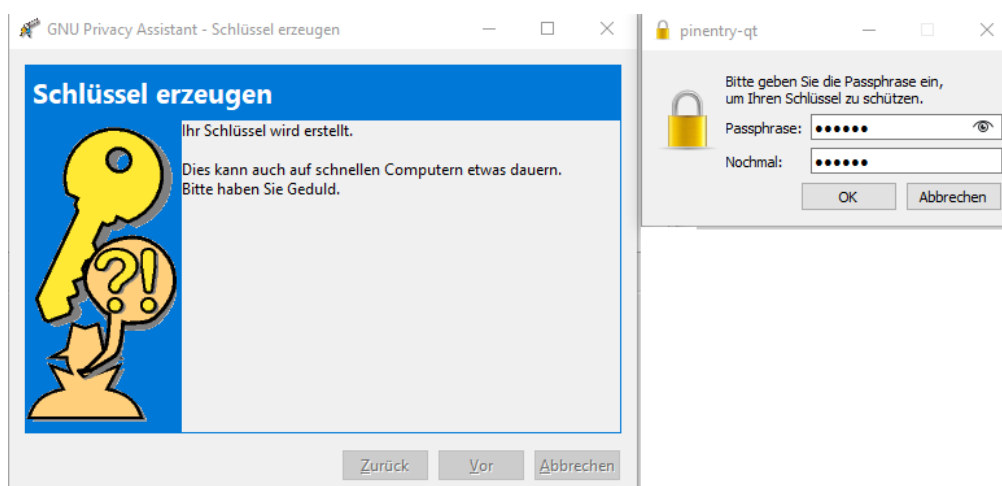


Abbildung 5: Auswahl einer Passphrase zum Schutz des privaten Schlüssels.

5. Der Schlüssel wird nun in der Übersicht angezeigt.

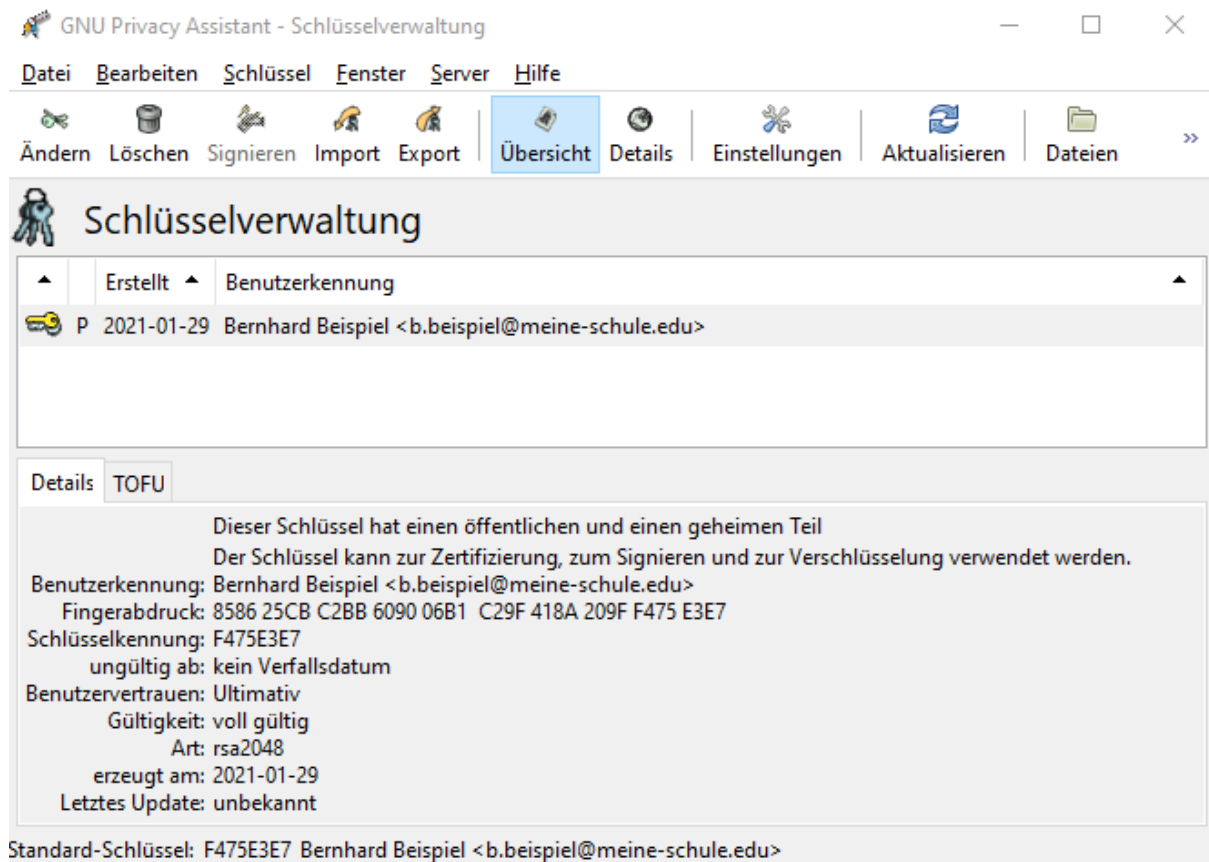


Abbildung 6: Anzeige des erstellten Schlüssels in der Übersicht.

Exportieren des öffentlichen Schlüssels

1. Markiere deinen Schlüssel in der Übersicht und wähle die Option *Export*.

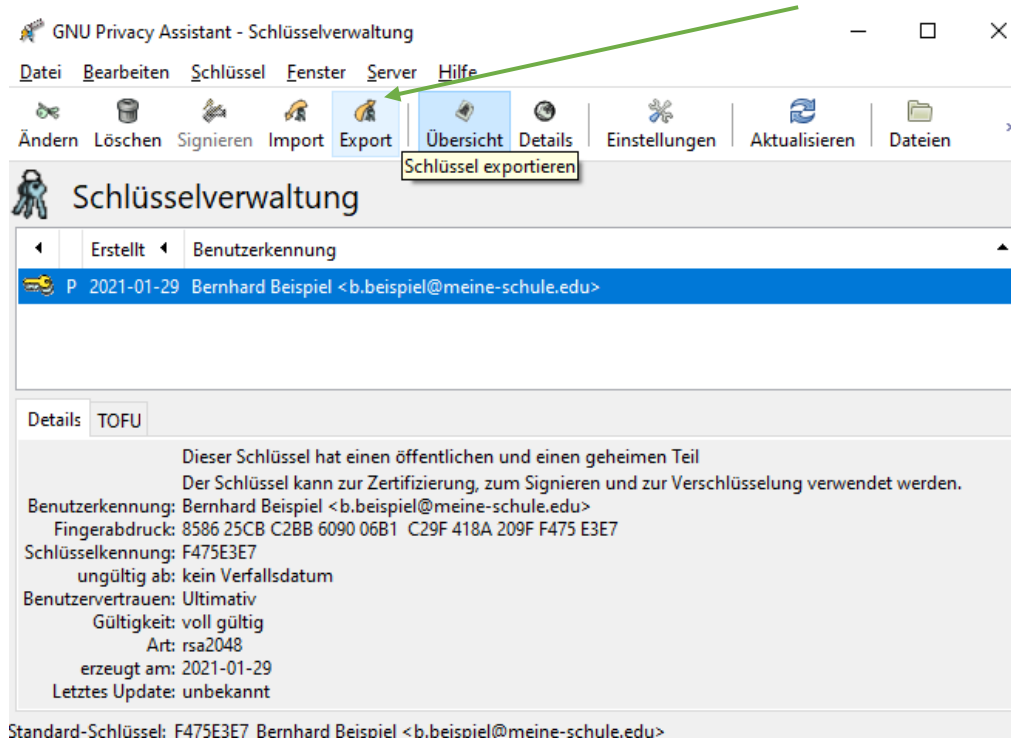


Abbildung 7: Exportieren des öffentlichen Schlüssels.

Sollte dir die Schaltfläche nicht wie in Abbildung 7 angezeigt werden, kannst du die Option auch über das Menü *Schlüssel* → *Schlüssel exportieren* auswählen.

2. Es öffnet sich das Fenster in Abbildung 8.

Gib zunächst einen Dateinamen ein. Der Dateiname sollte deinen Namen enthalten, damit sich der Schlüssel leichter zuordnen lässt.

Wähle anschließend aus, wo du die Datei mit deinem öffentlichen Schlüssel speichern möchtest. Diese Datei kannst du anschließend an alle weitergeben, die dir eine verschlüsselte Nachricht schicken möchten. Falls ihr einen gemeinsamen Austauschordner für eure Klasse besitzt, kannst du diesen direkt als Speicherort auswählen. Du kannst diese Datei aber z. B. auch als Anhang einer Mail verschicken.

Klicke auf den Button *Speichern*.

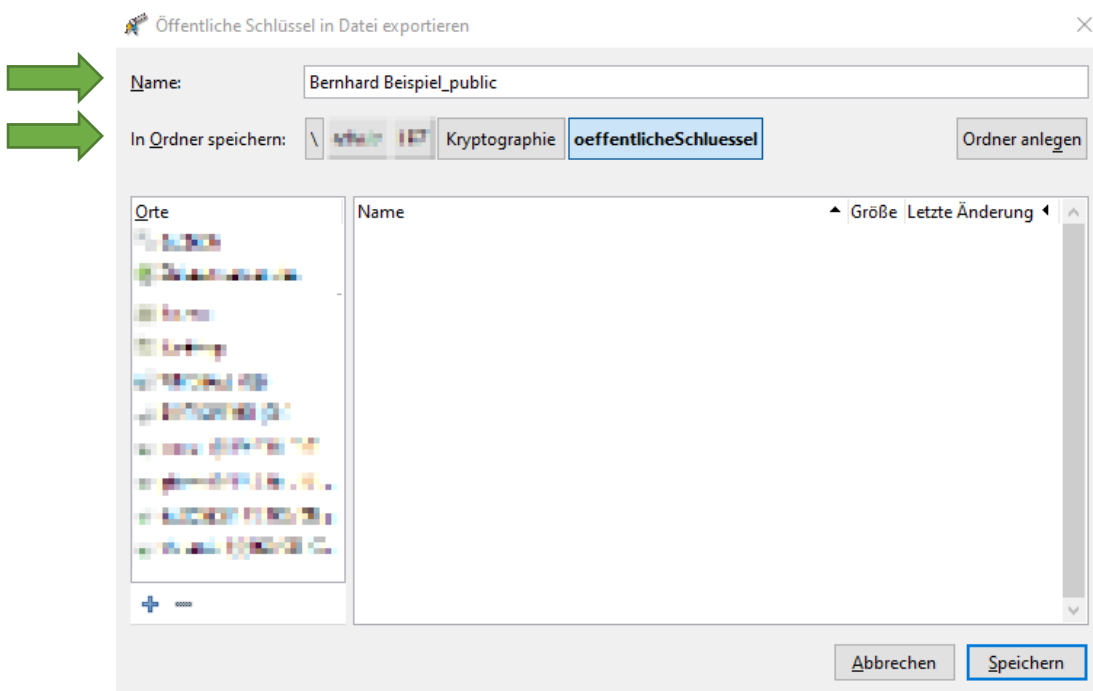


Abbildung 8: Speichern des öffentlichen Schlüssels zur Weitergabe

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

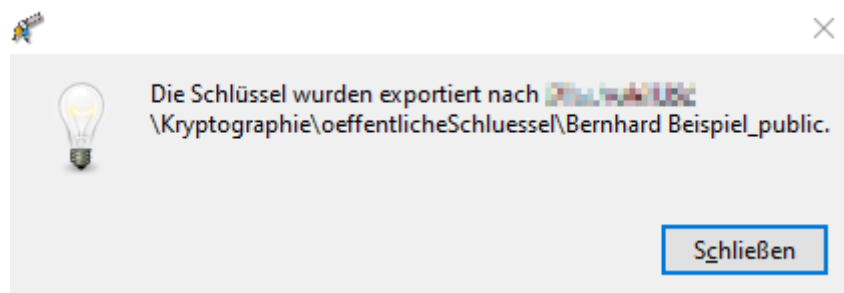


Abbildung 9: Bestätigung des erfolgreichen Exportierens

Importieren öffentlicher Schlüssel

1. Um die öffentlichen Schlüssel deiner Mitschülerinnen und Mitschüler zu importieren, wähle die Option *Importieren*.

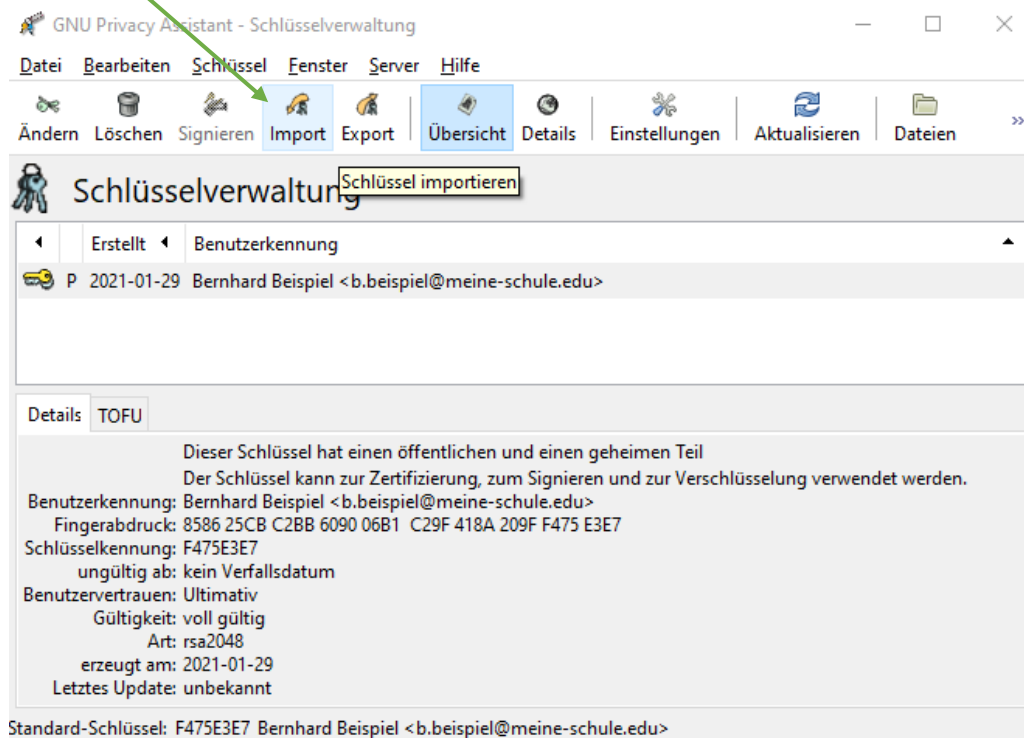


Abbildung 10: Importieren öffentlicher Schlüssel

Sollte dir die Schaltfläche nicht wie in Abbildung 10 angezeigt werden, kannst du die Option auch über das Menü *Schlüssel* → *Schlüssel importieren* auswählen.

2. Es öffnet sich das Fenster in Abbildung 11.
Wähle hier zunächst den Ordner aus, in dem die öffentlichen Schlüssel gespeichert sind.
Markiere anschließend den öffentlichen Schlüssel, den du importieren möchtest.
Klicke auf *Öffnen*.

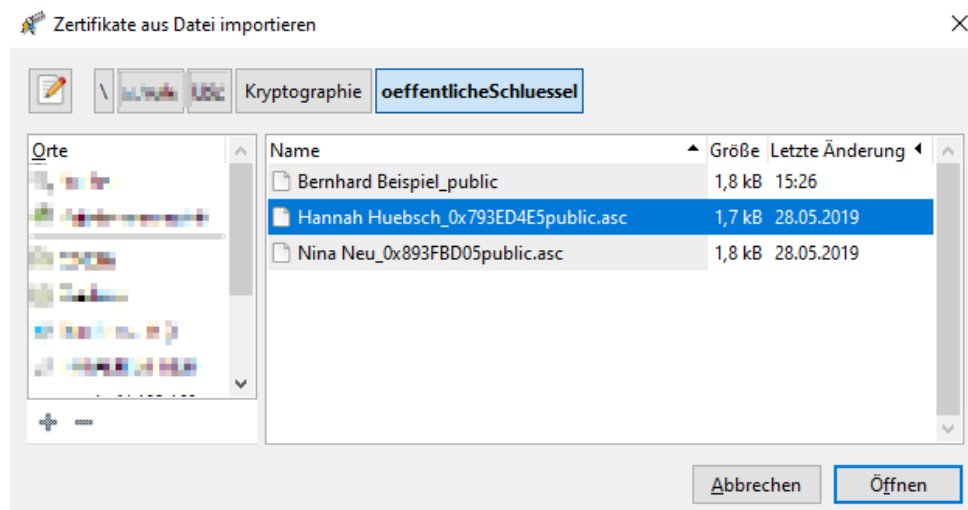


Abbildung 11: Auswählen der öffentlichen Schlüssel

3. Du erhältst eine Statusmeldung, wie viele Schlüssel importiert wurden. Klicke auf *Schließen*. Die importierten öffentlichen Schlüssel werden nur in deiner Übersicht angezeigt.

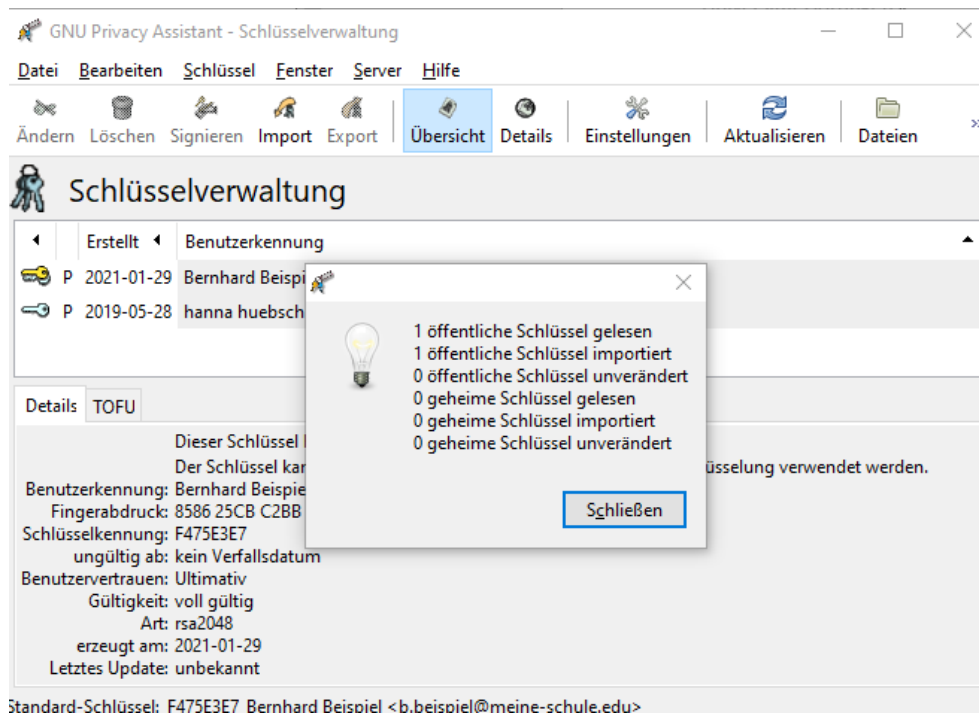


Abbildung 12: Bestätigung des Importierens

Anhand der Schlüsselsymbole erkennst du, dass es sich bei dem importierten Schlüssel nur um einen öffentlichen Schlüssel handelt (Symbol: nur ein blauer Schlüssel). Bei deinem eigenen Schlüssel handelt es sich hingegen um ein Schlüsselpaar (Symbol: blauer und gelber Schlüssel).

4. Wenn du weitere Schlüssel importieren möchtest, wiederhole 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.