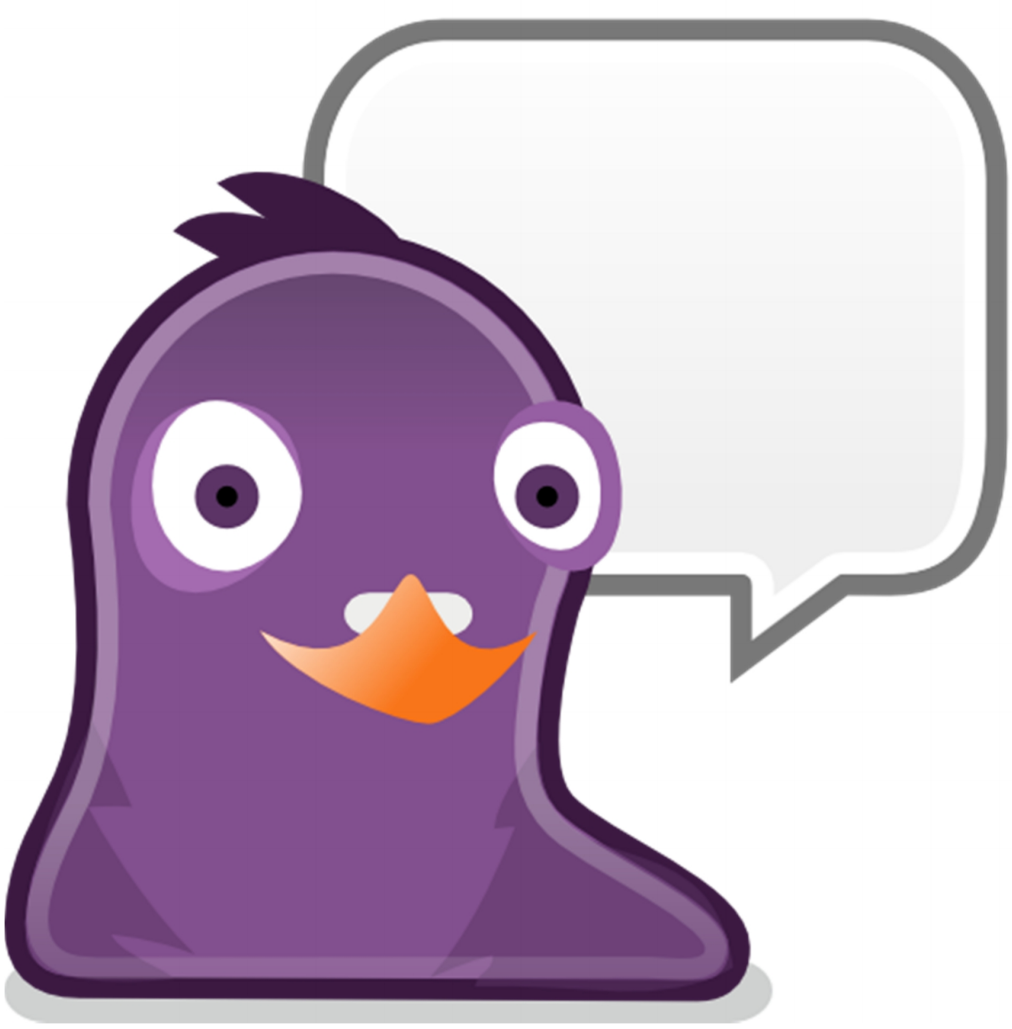
Anleitung – Sichere Kommunikation mit Pidgin, Jabber und OTR



1 Hinweis

Diese Anleitung wurde mit dem Betriebssystemen Windows 7 Home Premium (64 Bit) und Windows 8.1 (64 Bit) und Pidgin 2.10.11 mit OTR 4.0.1 getestet, bei anderen Betriebssystemen und Pidgin Versionen kann es ggf. zu Abweichungen kommen.

2 Einleitung

Viele von euch kennen sicherlich noch die alten Instant Messenger, wie ICQ oder MSN, heute werden diese nur noch selten genutzt. Die Chat Funktion von Facebook erfreut sich immer größerer Beliebtheit, darüber hinaus nutzen viele WhatsApp auf dem Smartphone. Warum also ein anderes Kommunikationsmittel nutzen?

Weder der Chat von Facebook und dessen Messenger auf dem Smartphone noch WhatsApp bieten eine (verifizierbar) sichere Kommunikation. Es ist möglich die Gespräche abzufangen und für Dritte lesbar zu machen. Pidgin ermöglicht mit dem Protokoll Jabber (XMPP – Extensible Messaging and Presence Protocol) und dem Plugin OTR (Off-the-Record) eine private und auch sichere Unterhaltung zu führen.

2.1 Was ist Pidgin?

Pidgin (früher Gaim) ist ein Instant Messenger Client. Diese Software bietet die Möglichkeit mehrere Dienste und Protokolle, wie auch ICQ oder MSN, aber eben auch Jabber, zu nutzen. Pidgin ist Open-Source-Software und kostenlos sowie werbefrei.

2.2 Was ist Jabber?

Jabber ist ein Dienst, der das XMPP-Protokoll nutzt. Mit Jabber hat man die Möglichkeit durch eine Freundesliste (Buddy-Liste) mit Freunden in Kontakt zu treten.

2.3 Welcher Jabber -Server?

Es gibt zahlreiche Jabber Server, empfehlenswert ist der Jabber-Server von systemli.org. Dieser Server wird von einem linken Tech-Kollektiv betreut und lässt nur verschlüsselte Verbindungen zu ihrem Server zu.

2.4 Off-the-Record Messaging (OTR)

Off-the-Record Messaging oder kurz OTR (deutsch: inoffizielle; vertrauliche, nicht für die Öffentlichkeit bestimmte Nachrichtenvermittlung) ist ein Verschlüsselungsprotokoll, welches als Plugin für Pidgin verfügbar ist. Mit diesem Plugin ist es möglich eine sichere und private Unterhaltung mit einem Buddy zu starten und dient als Erweiterung der bereits vorhanden Verschlüsselung zum Jabber-Server. Es werden keine Mitschnitte erstellt und es ist nicht möglich die Inhalte der Unterhaltung in irgendeiner Form sichtbar zu machen.

3 Download und Installation

3.1 Installationsvoraussetzungen

- Internetverbindung
- mind. Windows 2000
- 9,2 MB, installiert ca. 50 MB freier Speicher

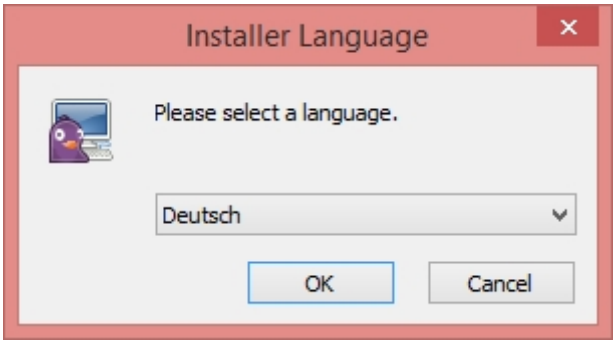
3.2 Download

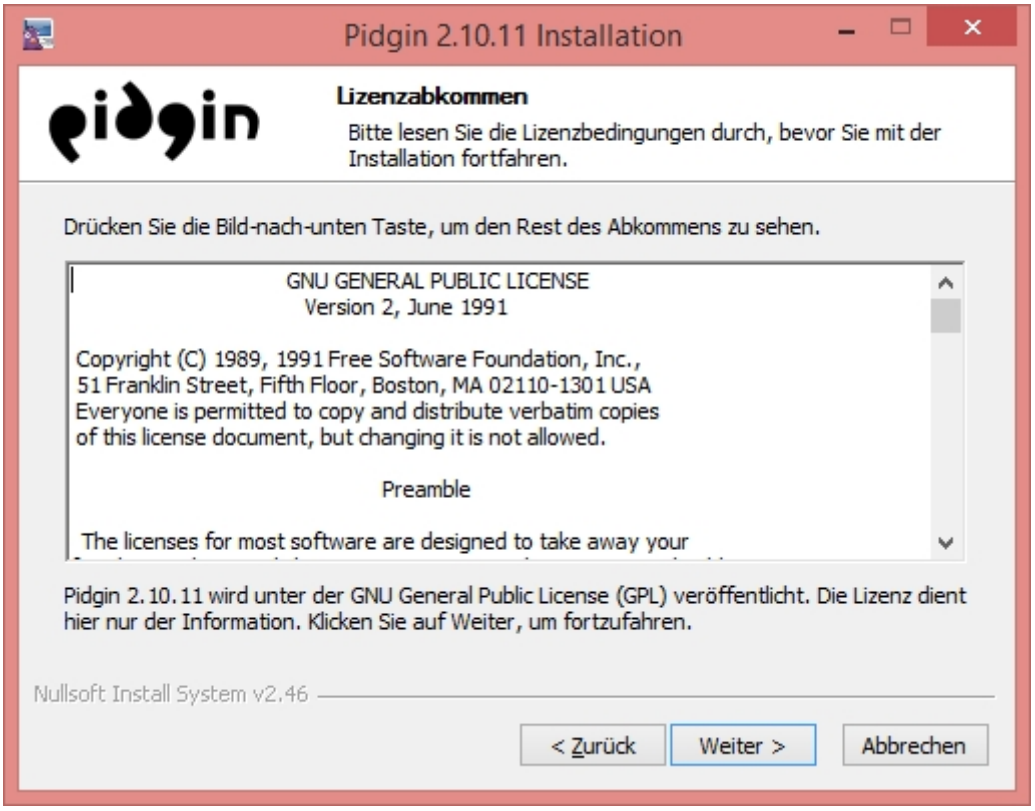
Download Pidgin Instant Messenger Client
https://www.pidgin.im/download/

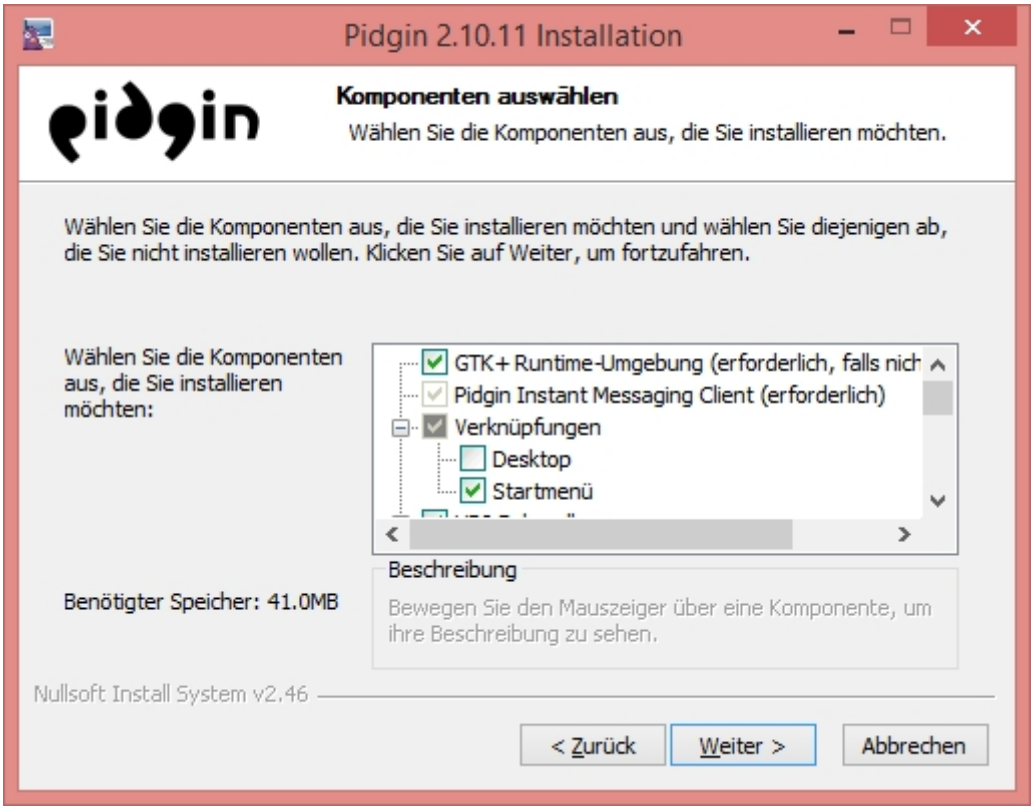
Download OTR - Off-the-Record Messaging
https://otr.cypherpunks.ca/binaries/windows/pidgin-otr-4.0.1.exe

3.3 Installation Pidgin 2.10.11

Einfach den Installationsanweisungen folgen.

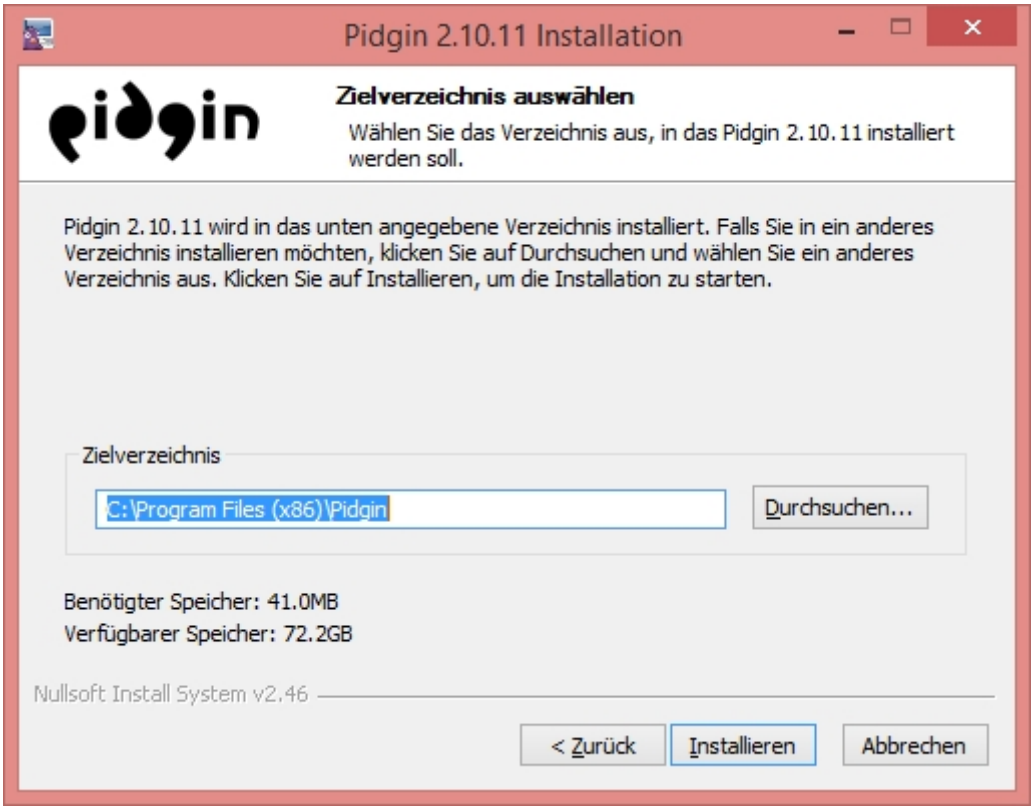


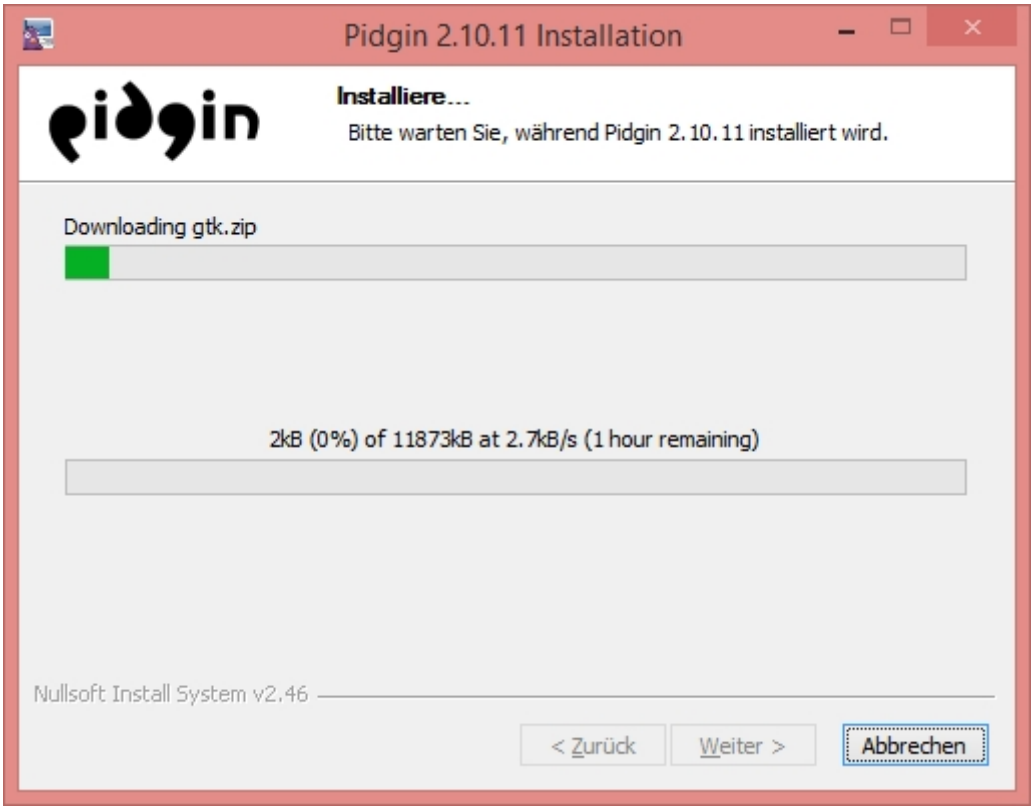


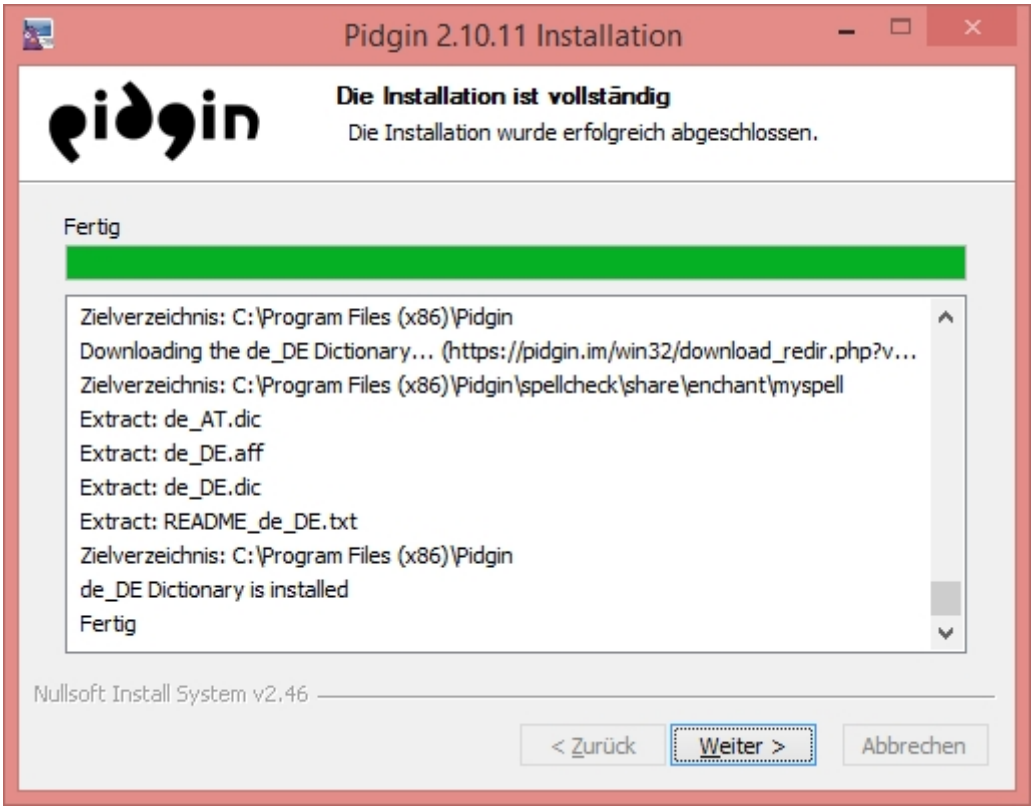


Einstellungen zur Installation:

- ✓ GTK+ Runtime-Umgebung (erforderlich)
- ✓ Pidgin Instant Messaging Client (erforderlich)
- ✓ Verknüpfungen Desktop und Startmenü (manuell)
- ☐ URI-Behandlung (manuell) http://forum.pidgin-im.de/showthread.php?tid=701
- ✓ Unterstützung zur Rechtschreibkontrolle German (Germany)
- ☐ Debug-Symbole (zum Melden von Abstürzen)


Pidgin 2.10.11 Installation
pidgin
Zielverzeichnis auswählen
Wählen Sie das Verzeichnis aus, in das Pidgin 2.10.11 installiert werden soll.
Pidgin 2.10.11 wird in das unten angegebene Verzeichnis installiert. Falls Sie in ein anderes Verzeichnis installieren möchten, klicken Sie auf Durchsuchen und wählen Sie ein anderes Verzeichnis aus. Klicken Sie auf Installieren, um die Installation zu starten.
Zielverzeichnis
C:\Program Files (x86)\Pidgin
Durchsuchen...
Benötigter Speicher: 41.0MB
Verfügbarer Speicher: 72.2GB
Nullsoft Install System v2.46
< Zurück
Installieren
Abbrechen

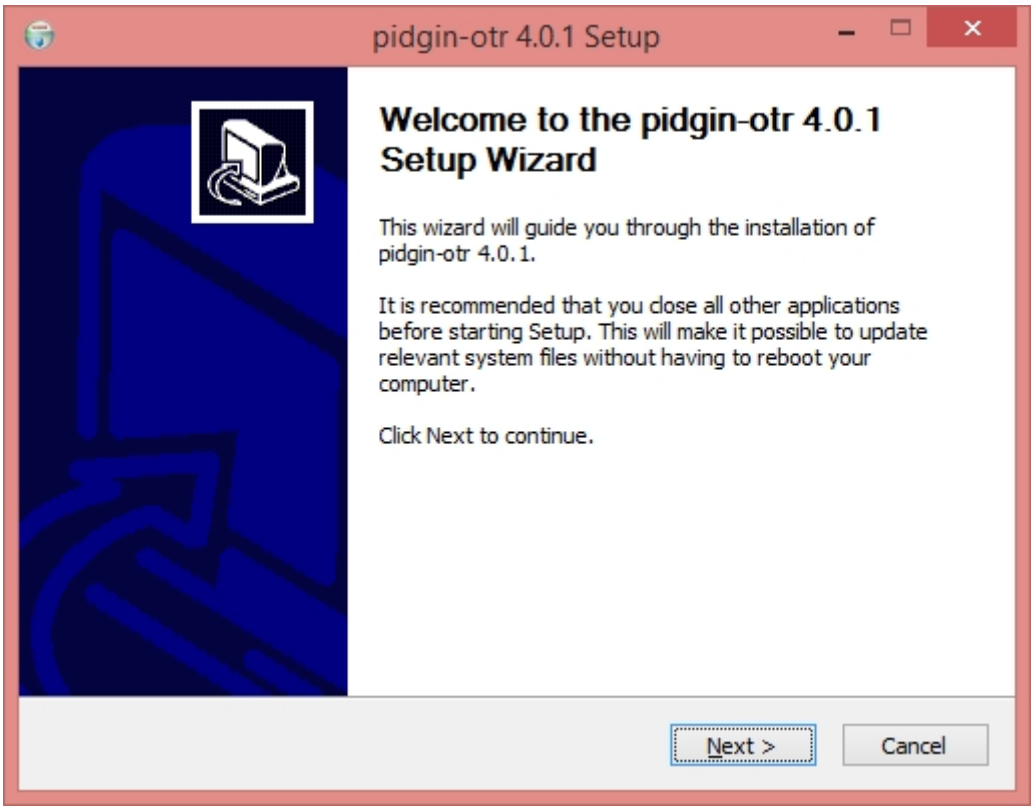

Pidgin 2.10.11 Installation
pidgin
Installiere...
Bitte warten Sie, während Pidgin 2.10.11 installiert wird.
Downloading gtk.zip
2kB (0%) of 11873kB at 2.7kB/s (1 hour remaining)
Nullsoft Install System v2.46
< Zurück
Weiter >
Abbrechen

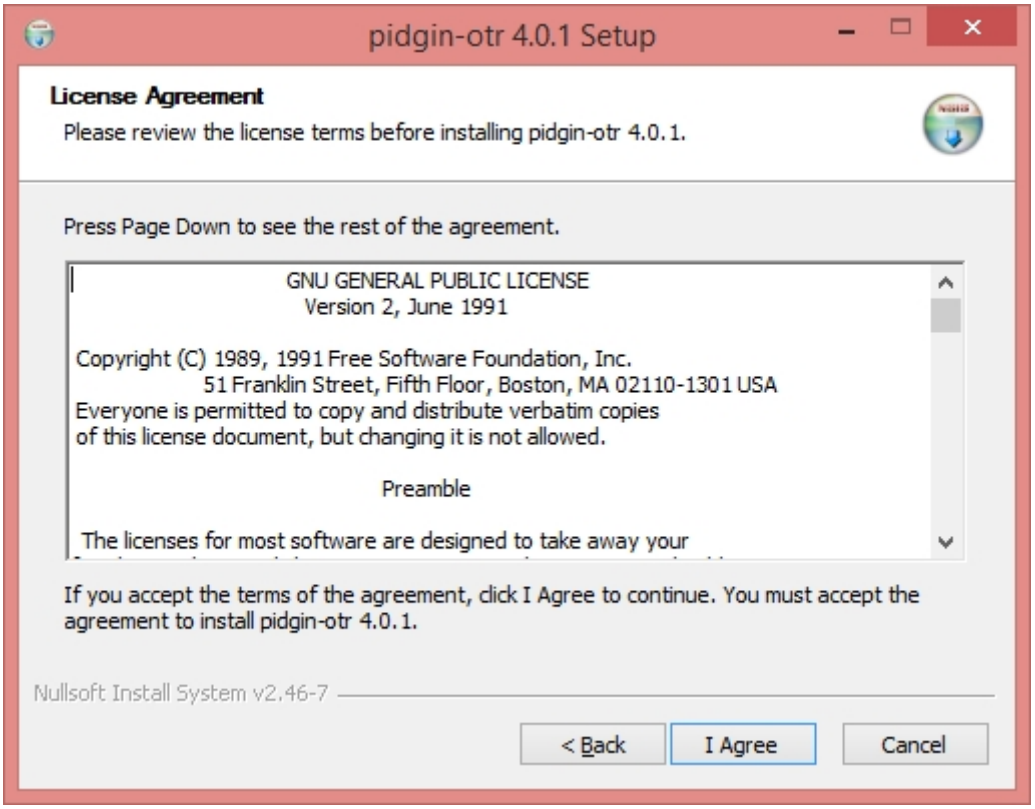

Pidgin 2.10.11 Installation
Die Installation ist vollständig
Die Installation wurde erfolgreich abgeschlossen.
Fertig
Zielverzeichnis: C:\Program Files (x86)\Pidgin
Downloading the de_DE Dictionary... (https://pidgin.im/win32/download_redir.php?v...
Zielverzeichnis: C:\Program Files (x86)\Pidgin\spellcheck\share\enchant\myspell
Extract: de_AT.dic
Extract: de_DE.aff
Extract: de_DE.dic
Extract: README_de_DE.txt
Zielverzeichnis: C:\Program Files (x86)\Pidgin
de_DE Dictionary is installed
Fertig
Nullsoft Install System v2.46
< Zurück
Weiter >
Abbrechen

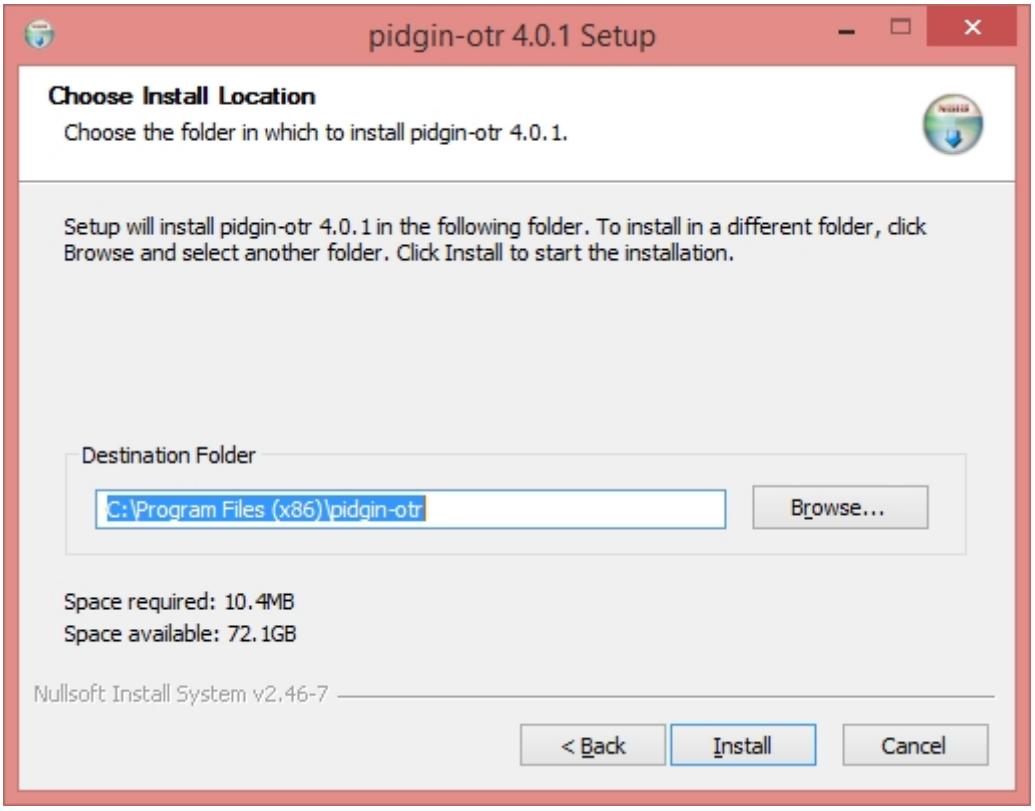

Pidgin 2.10.11 Installation
Die Installation von Pidgin 2.10.11 wird abgeschlossen
Pidgin 2.10.11 wurde auf Ihrem Computer installiert.
Klicken Sie auf Fertig stellen, um den Installations-Assistenten zu schließen.
Besuchen Sie die Pidgin-Webseite
< Zurück
Fertig stellen
Abbrechen

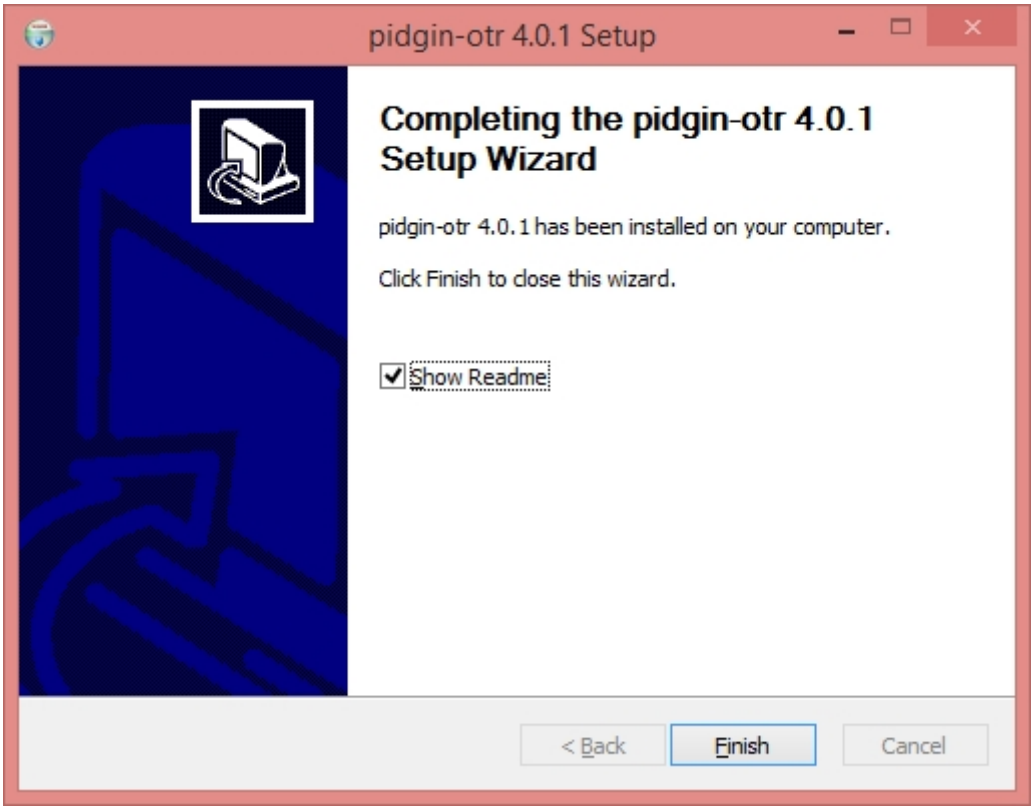
3.4 Installation OTR 4.0.1

Einfach den Installationsanweisungen folgen.






pidgin-otr 4.0.1 Setup
Choose Install Location
Choose the folder in which to install pidgin-otr 4.0.1.
Setup will install pidgin-otr 4.0.1 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files (x86)\pidgin-otr
Browse...
Space required: 10.4MB
Space available: 72.1GB
Nullsoft Install System v2.46-7
< Back
Install
Cancel


pidgin-otr 4.0.1 Setup
Completing the pidgin-otr 4.0.1 Setup Wizard
pidgin-otr 4.0.1 has been installed on your computer.
Click Finish to close this wizard.
Show Readme
< Back
Finish
Cancel

4 Konto erstellen (XMPP Account Registration)

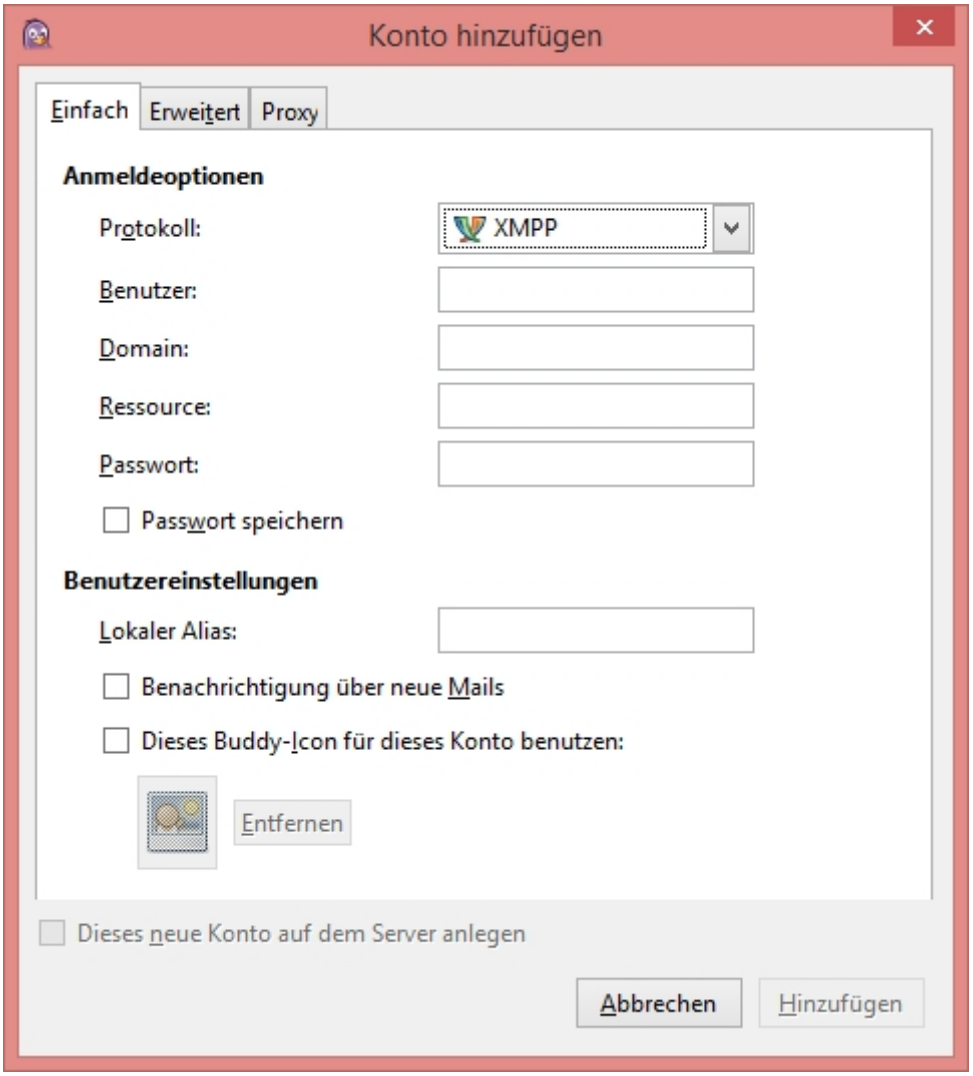
Auf folgender Internetseite kann ein neuer Jabber-Account angelegt werden.
https://www.systemli.org/service/xmpp.html
Der Username entspricht später dem Benutzername, dass Passwort sollte mind. 8 Zeichen haben, aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Sollte der Nutzername schon vorhanden sein, erhaltet ihr die Meldung „Username already taken“. Dann müsst ihr einen anderen Nutzername wählen.

Wie sicher dein Passwort ist, kannst du auf folgender Homepage testen.
http://www.wiesicheristmeinpasswort.de/

5 Pidgin Starten

Doppelklick auf das Desktop Symbol von Pidgin

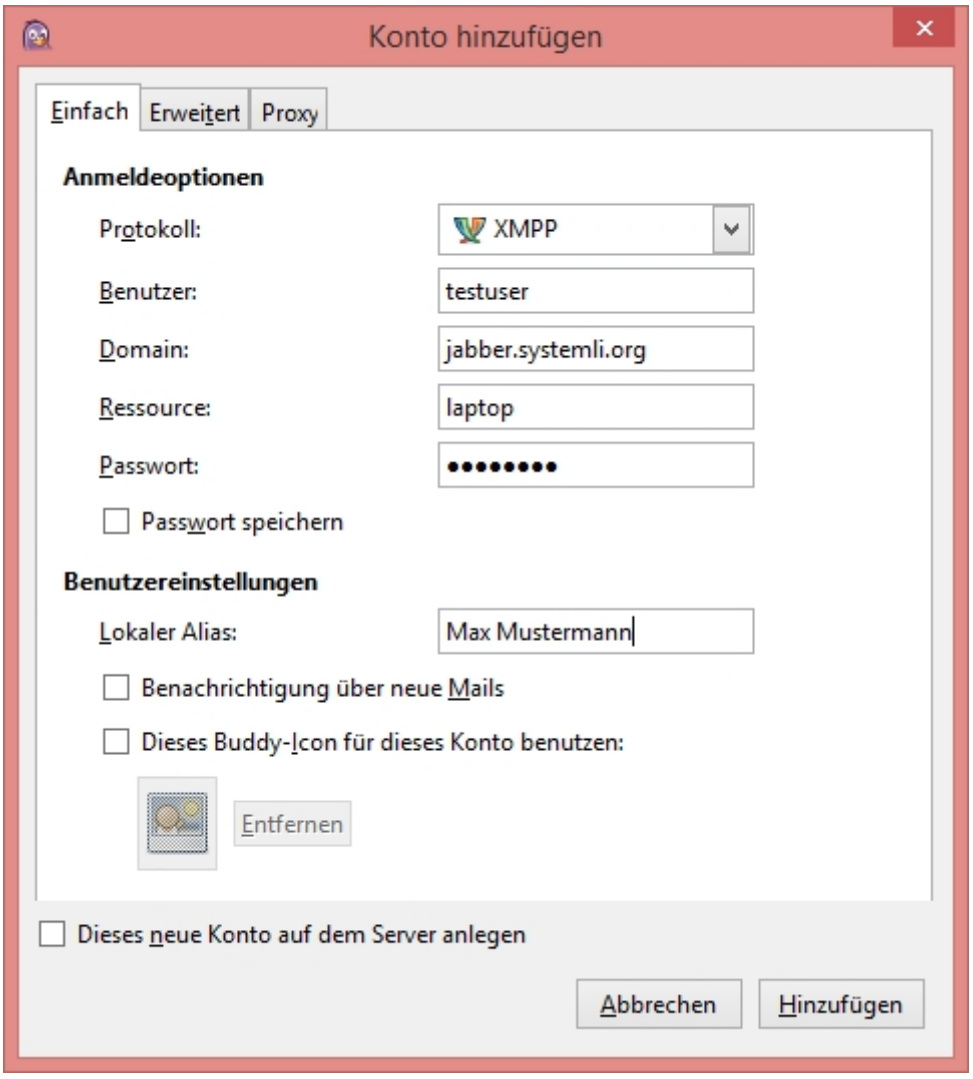
Unter Protokoll XMPP auswählen.



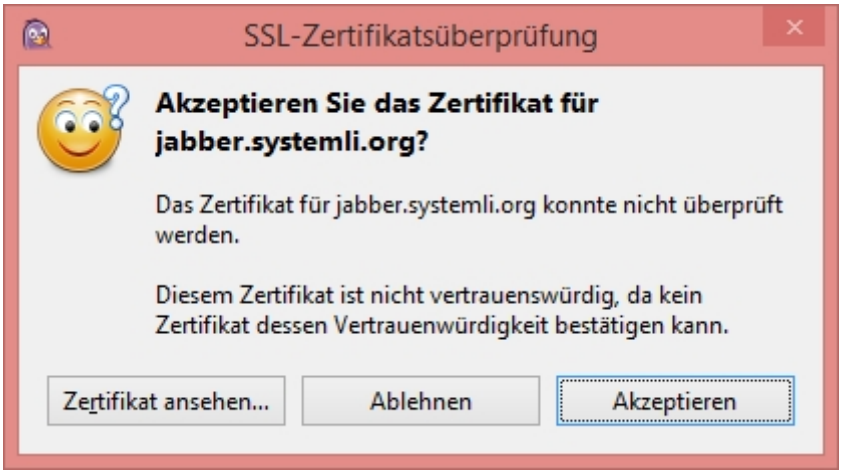
Einstellungen Reiter Einfach:
Benutzer: Username wählen, der bei der Registrierung verwendet worden ist
Domain: jabber.systemli.org
Ressource: Gerätename oder frei lassen
Passwort: vergebenes Passwort bei der Registrierung

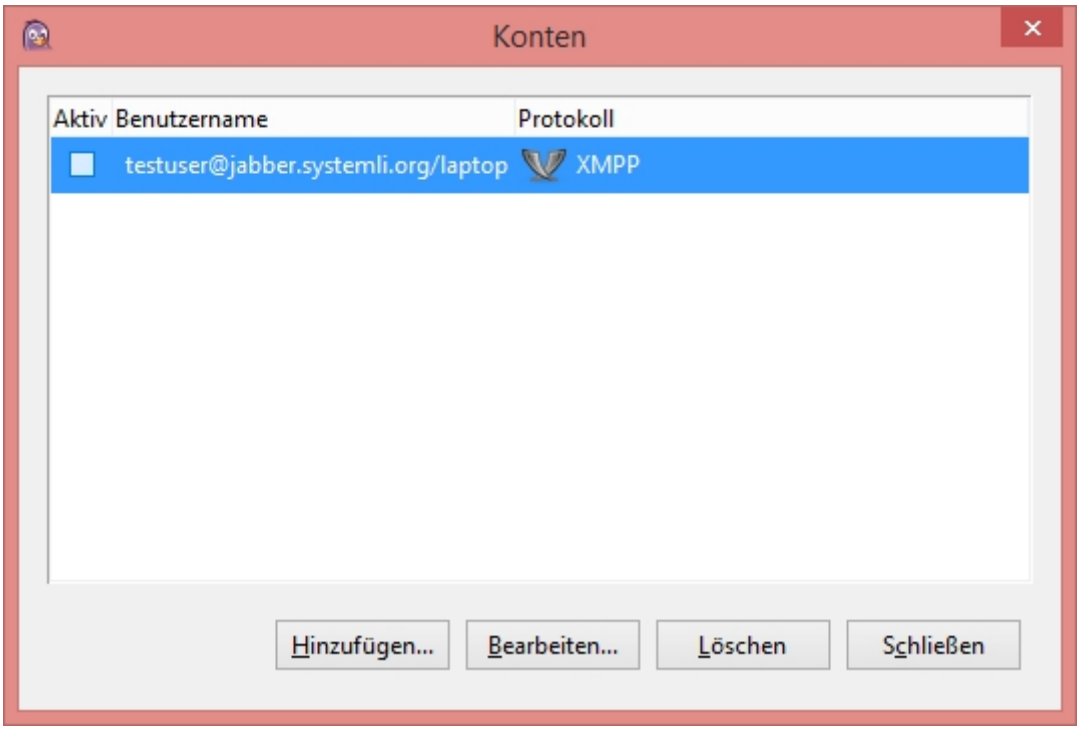
Passwort speichern: nein
Benachrichtigung über neue Mails: nein
Lokaler Alias: Nickname, der in der Buddy-Liste angezeigt werden soll
Buddy-Icon: Avatar bzw. Profilbild, wird ebenfalls in der Buddy-Liste angezeigt

Kein Haken bei „Dieses neue Konto auf dem Server anlegen“ setzen und auf „Hinzufügen“ klicken.

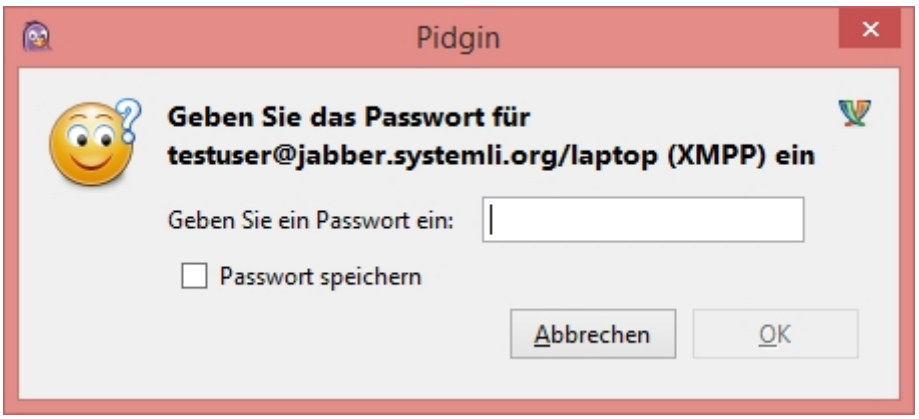


Folgendes Fenster mit Akzeptieren bestätigen.



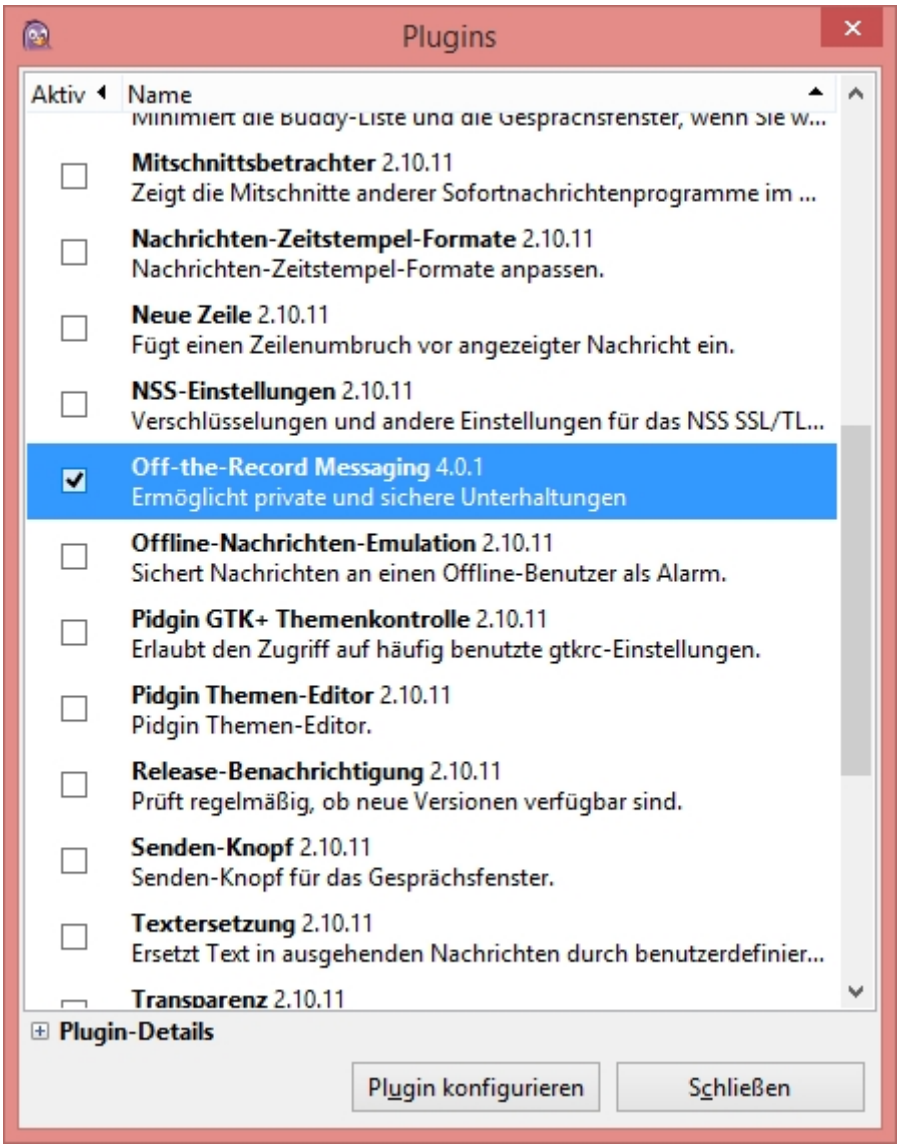


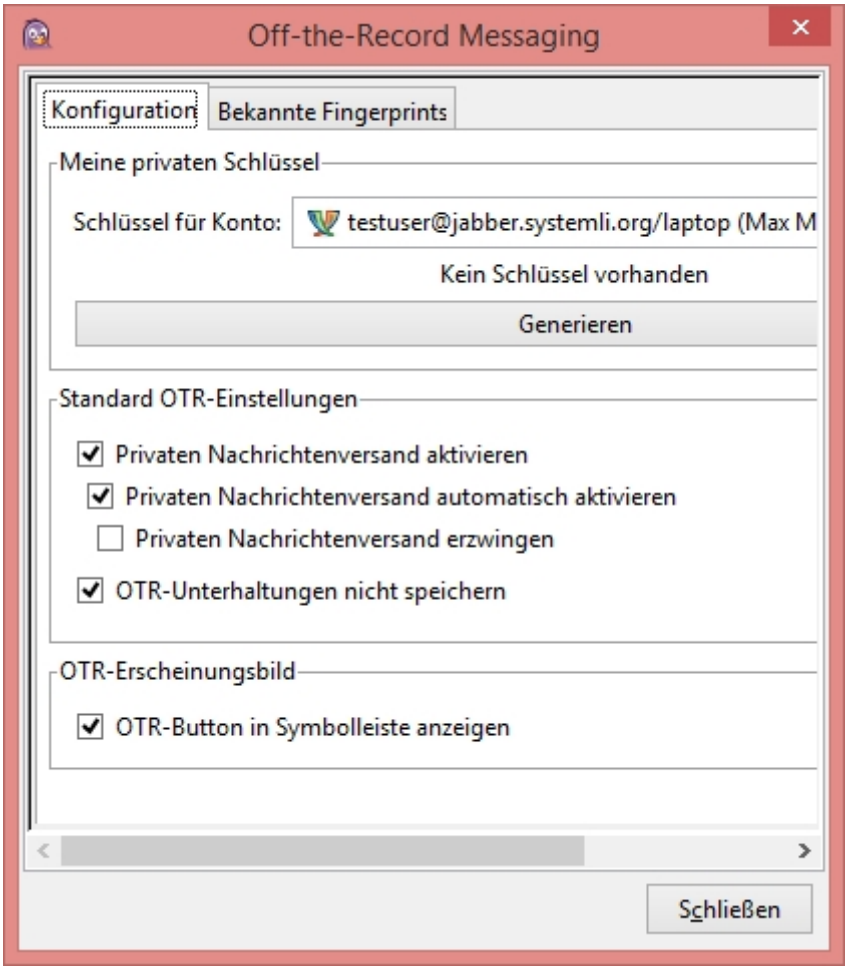
Nun einen Haken beim Jabber-Account setzen und es öffnet sich folgendes Fenster, hier euer Passwort eingeben und auf OK klicken.



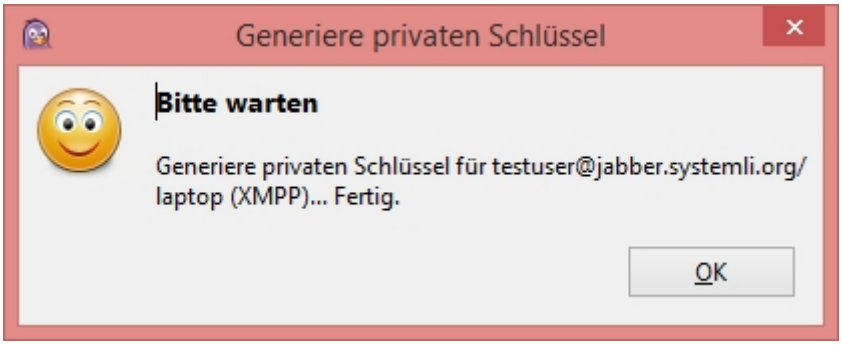
6 Einstellungen

Nun ist dein Account eingerichtet und du bist das erste Mal bei Jabber angemeldet. Jetzt sind noch ein paar Einstellungen vorzunehmen, bevor du deine Freunde in deine Liste hinzufügst. Als erstes aktivieren wir OTR. Unter Werkzeuge -> Plugins (alternativ Strg+U) einen Haken bei „Off-the-Record Messaging“ setzen und unten auf „Plugin konfigurieren“ klicken.





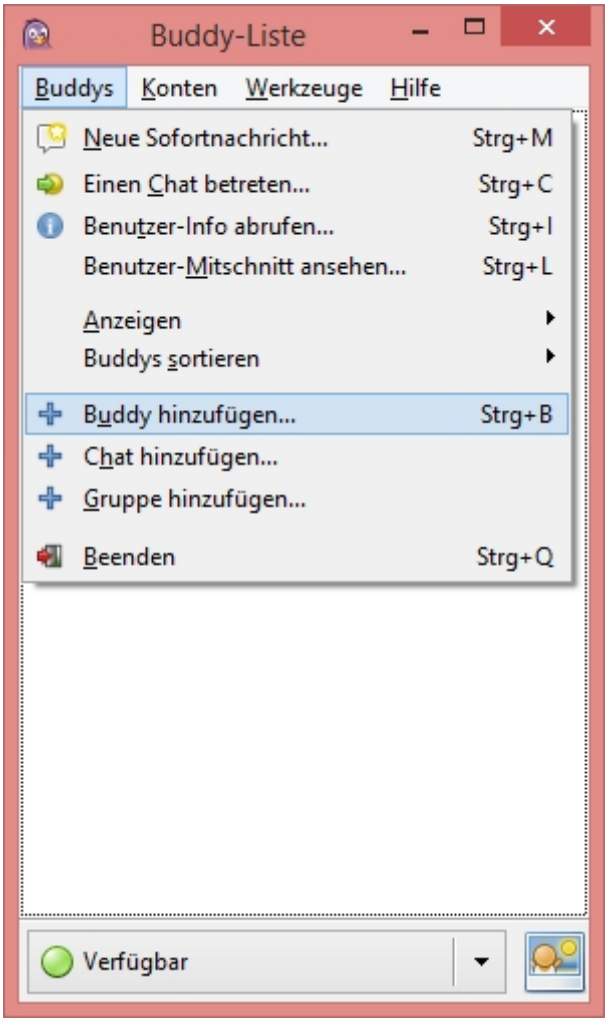
Unter „Meine privaten Schlüssel“ auf Generieren klicken, dort erhaltet ihr dann einen privaten Schlüssel (Fingerprint), danach das Fenster einfach mit OK bestätigen und die OTR-Einstellungen schließen.

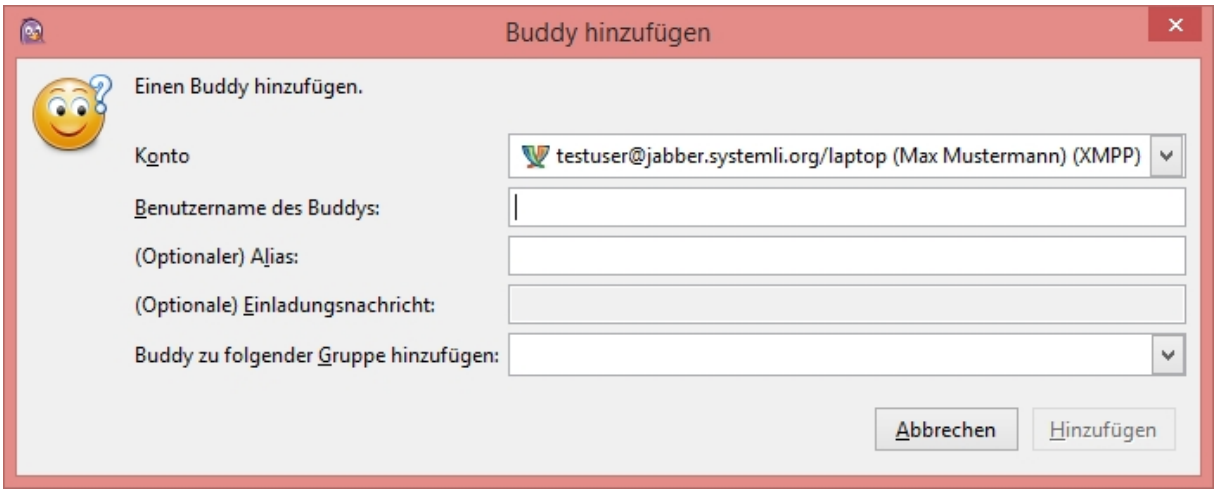


7 Buddys (Freunde)

7.1 Buddys hinzufügen

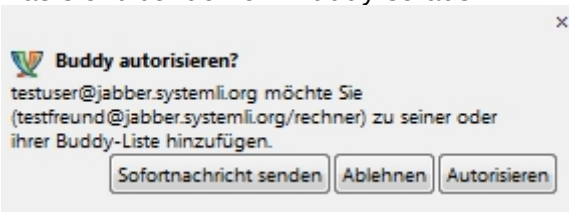
In der Buddy-Liste unter Buddys - Buddy hinzufügen… (alternativ Strg+B) habt ihr nun die Möglichkeit, Freunde hinzuzufügen.



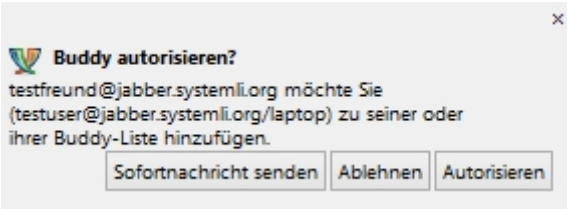


Unter Benutzername des Buddys ist der Jabber-Account einzutragen, also beispielsweise testfreund@jabber.systemli.org. Dein Buddy erhält dann eine sogenannte Freundschaftsanfrage und muss dich „Autorisieren“.

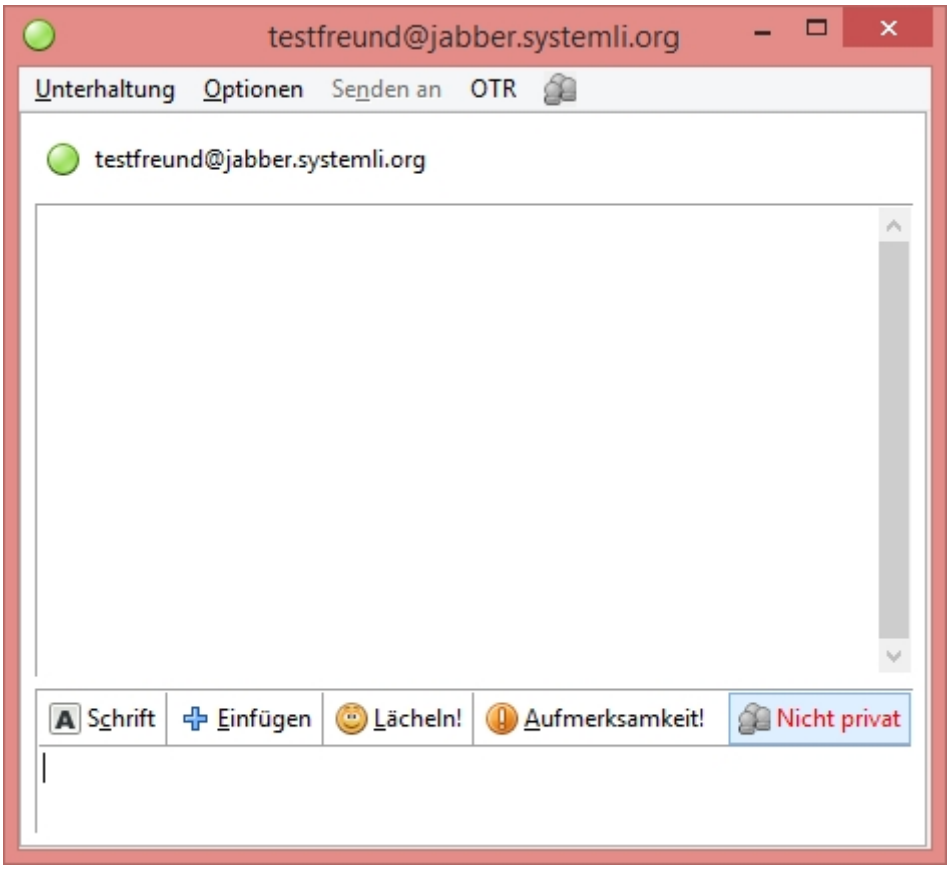
Das sieht bei deinem Buddy so aus:



Sollte dein Buddy dich autorisiert haben, erhältst du ebenfalls solch eine Anfrage. Diese ebenfalls durch Klick auf „Autorisieren“ bestätigen.

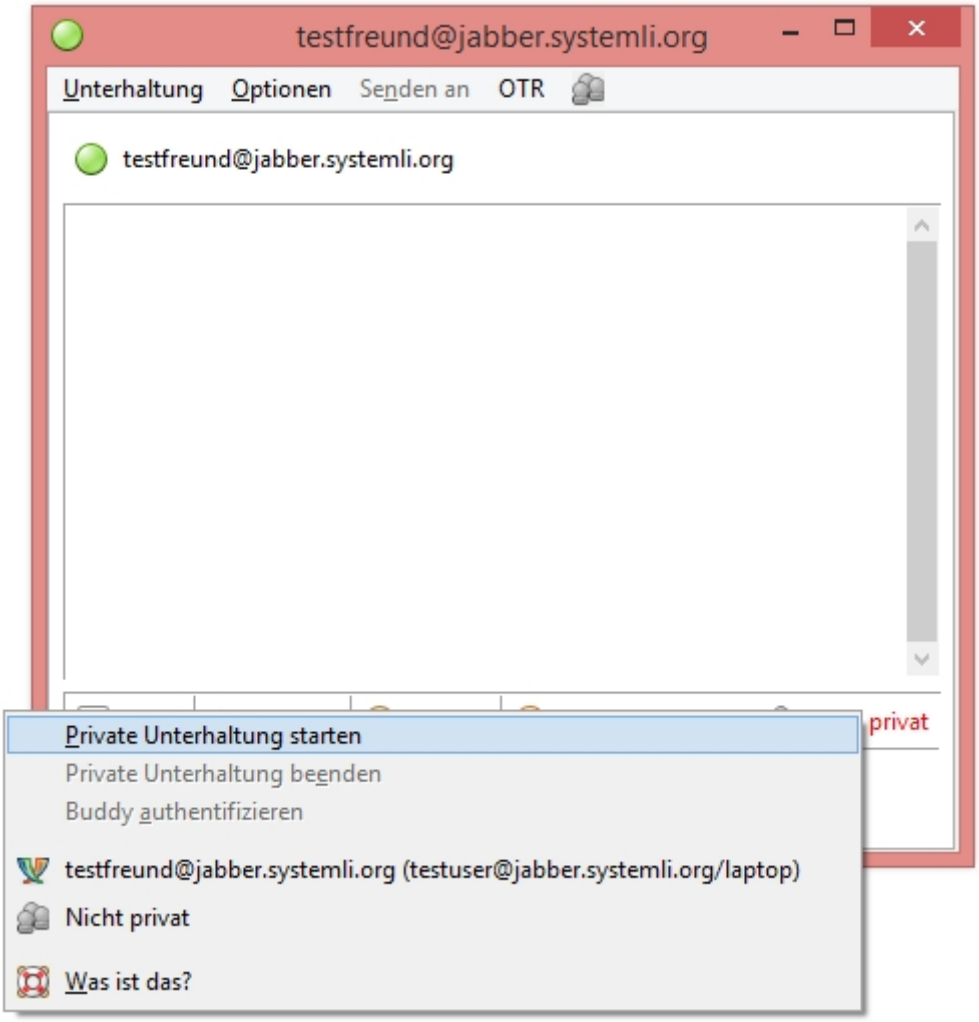


Jetzt erscheint dein Buddy in der Buddy-Liste. Durch Doppelklick auf seinen Namen öffnet sich das eigentliche Chatfenster.

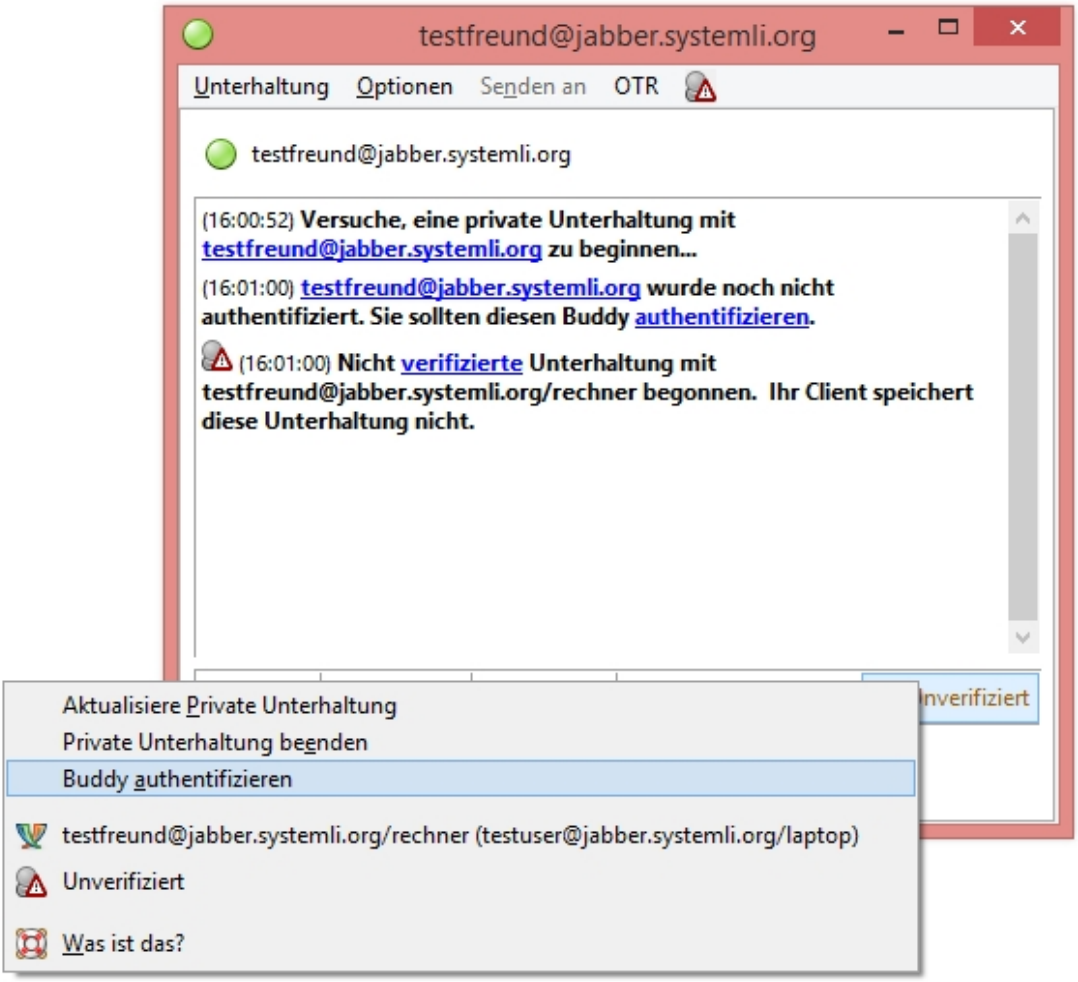


7.2 Private Unterhaltung starten

Nun ist es noch notwendig eine private Unterhaltung zu starten und deinen Buddy zu authentifizieren. Dafür gibt es drei verschiedene Möglichkeiten.

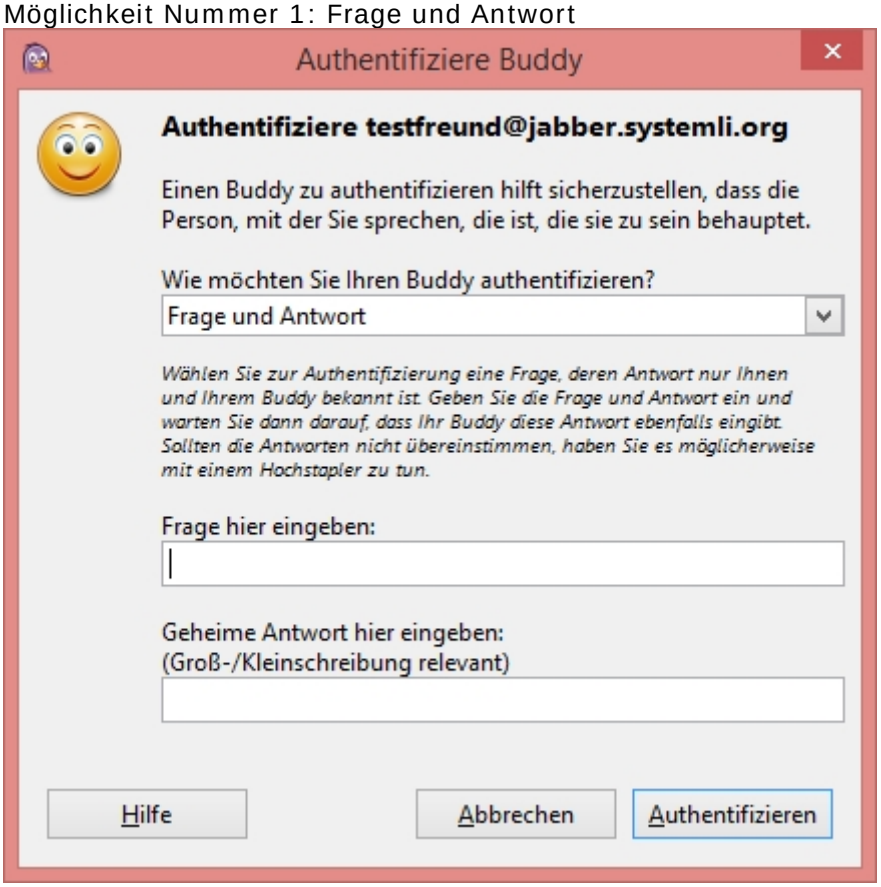


7.3 Authentifizierung

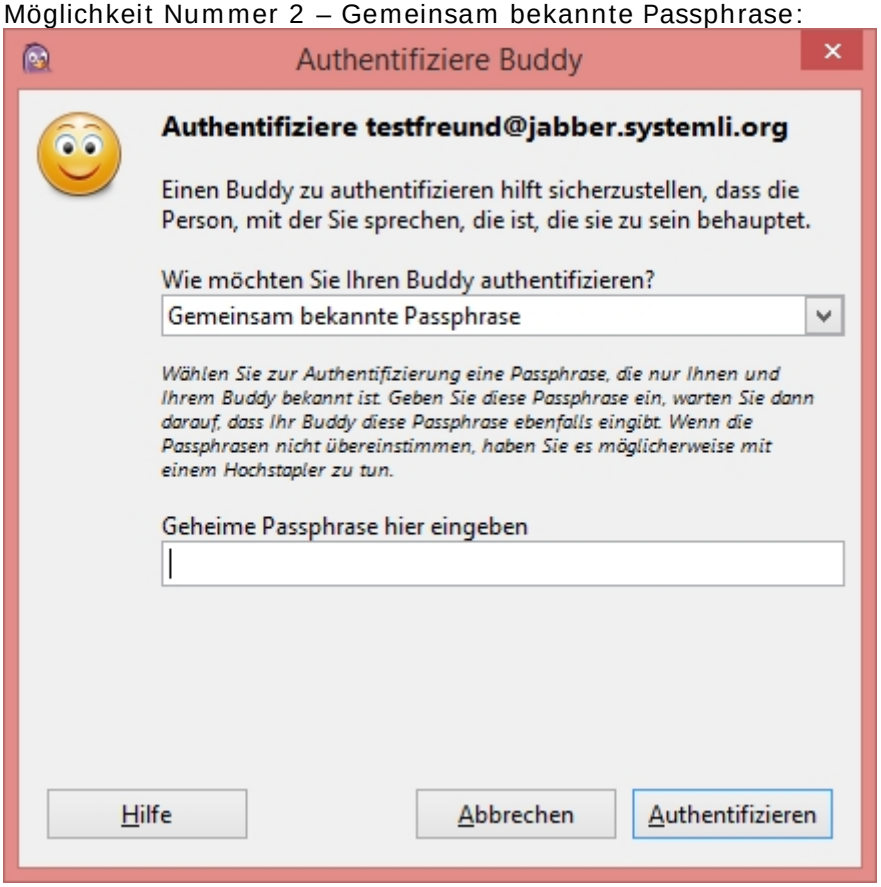


Durch Klick auf „Unverifiziert“ im Chatfenster und im anschließenden Auswahlmenü auf „Buddy authentifizieren“, ist jetzt noch die Authentifizierung deines Buddys notwendig. Welche Authentifizierungsart ihr wählt, ist völlig egal.

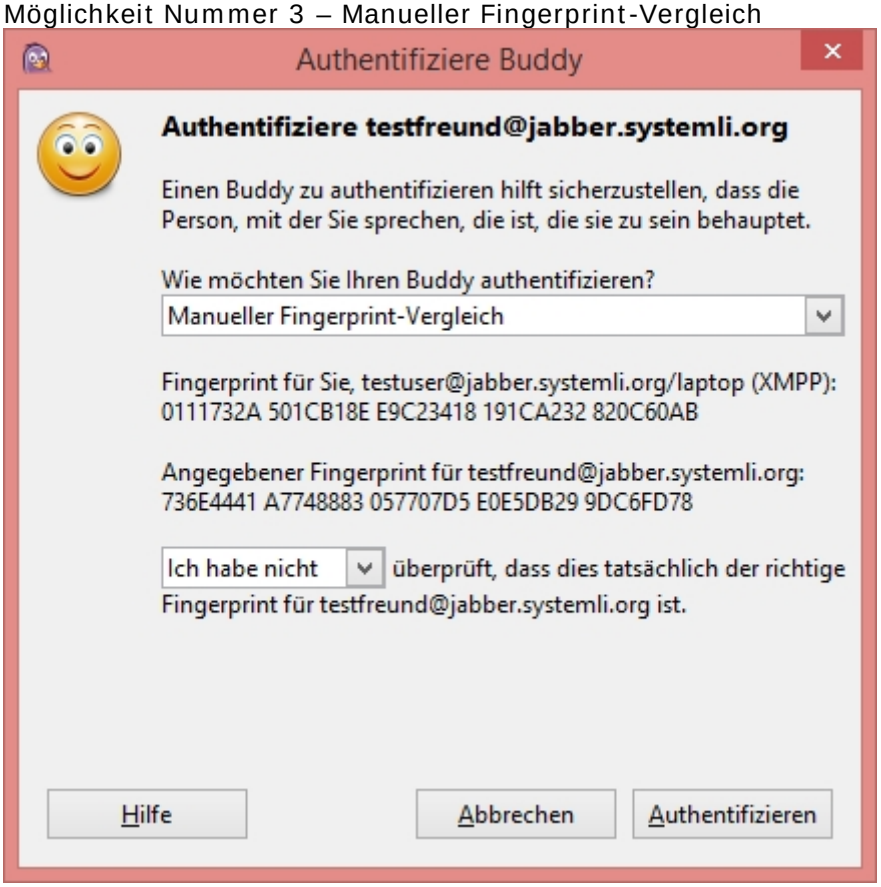
Möglichkeit Nummer 1: Frage und Antwort

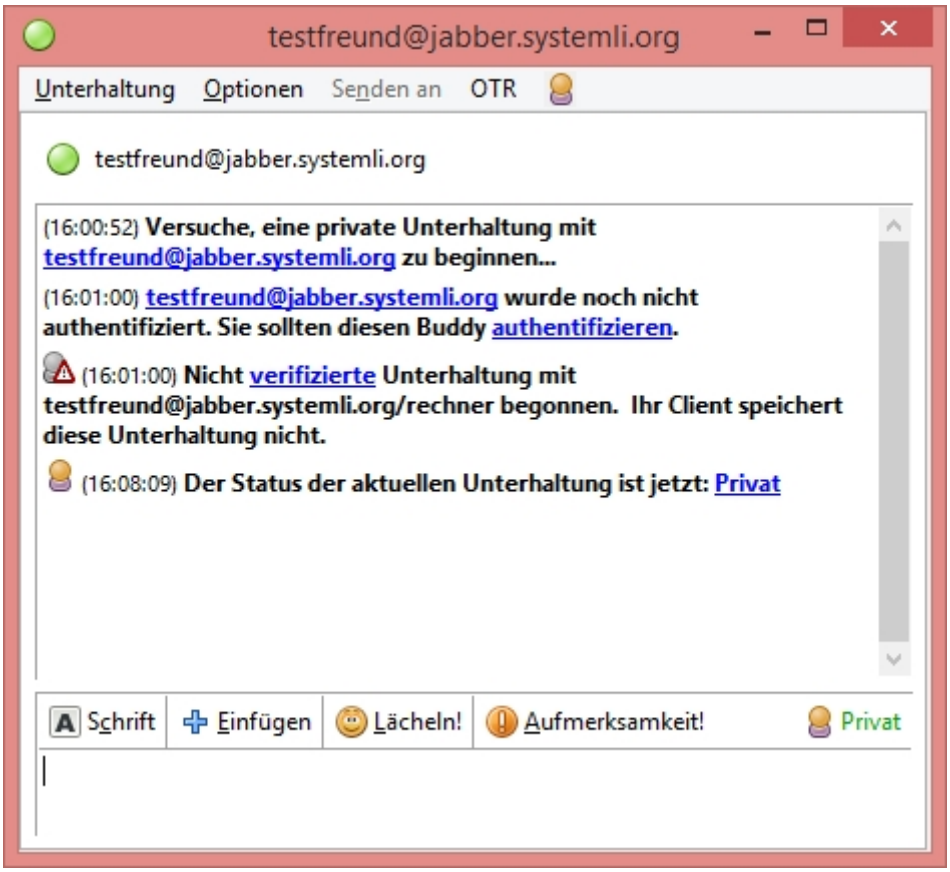


Möglichkeit Nummer 2 – Gemeinsam bekannte Passphrase:



Möglichkeit Nummer 3 – Manueller Fingerprint-Vergleich





7.4 Weitere Tipps:

- Private Unterhaltungen immer beenden, bevor du Pidgin schließt.
- Stelle sicher, dass niemand Zugriff auf deinen Computer hat, solange du eingeloggt bist.
- Halte dein Betriebssystem & deine Sicherheitssoftware auf dem aktuellen Stand.
- Offline Buddys lassen sich in der Buddy-Liste unter „Buddys - Anzeigen - Offline Buddys“ anzeigen
- für Smartphone-Nutzer mit Android oder iOS ist die App „ChatSecure“ empfehlenswert
- Pidgin Portable bietet die Möglichkeit jederzeit von einem USB-Stick gestartet zu werden http://portableapps.com/de/apps/internet/pidgin_portable

8 Kontakt und Links

Bei Fragen, Anregungen und Kritik könnt Ihr euch gerne per E-Mail an antifa-sth@riseup.net melden.

Um sicher mit uns in Kontakt zu treten, verschlüsselt eure Mails mit unserem PGP-Schlüssel.

Fingerabdruck: FEEB AF58 73D8 DABE 06C6 E470 A103 D34E FB4B E829

Weitere Infos erhaltet ihr unter:
http://www.afaction.info/
https://wiki.systemli.org/howto/jabber
https://www.systemli.org/service/xmpp.html

Stand 11.02.2015