XMPP-OTR-Einrichtung (Pidgin/Windows)

Version 1.8, 11.03.2015

Kurzfassung

1. Pidgin installieren, dann Pidgin-OTR (beides mit Administratorrechten)
2. ggf. Account bei z.B. www.jabber.de einrichten
3. eigenen Account in Pidgin konfigurieren
4. Support-Chatraum hinzufügen, möglichst daraus den Support-Account hinzufügen
5. Die anderen Teilnehmer hinzufügen (idealerweise aus dem Chatraum) und in OTR verifizieren

(WP:) XMPP (Extensible Messaging and Presence Protocol), auch bekannt unter dem Namen *Jabber*, ist ein offenes Protokoll für Chat (Instant Messaging). (WP:) OTR (Off the Record) ist eine Verschlüsselungstechnik für Chatsysteme, die nicht an ein bestimmtes Protokoll gebunden ist. Man kann OTR also nicht nur mit XMPP verwenden, sondern auch mit ICQ, MSN, Yahoo usw. Da XMPP ein offenes Protokoll ist, gibt es eine Menge (WP:) Chatprogramme (und auch Open-Source-Server), mit denen man es nutzen kann.

Installation

Unter Windows und Linux verwenden wir den verbreiteten Client Pidgin (www.pidgin.im), der OTR über ein gesondertes Plugin (otr.cypherpunks.ca) nachrüsten muss. Für MacOS wird Adium (adium.im) verwendet, das OTR bereits integriert hat. Auch für Smartphones gibt es XMPP-Clients ((WP:) reine XMPP-Clients und (WP:) Multi-Protokoll-Clients). Die sind aber nicht Bestandteil dieser Schulung.

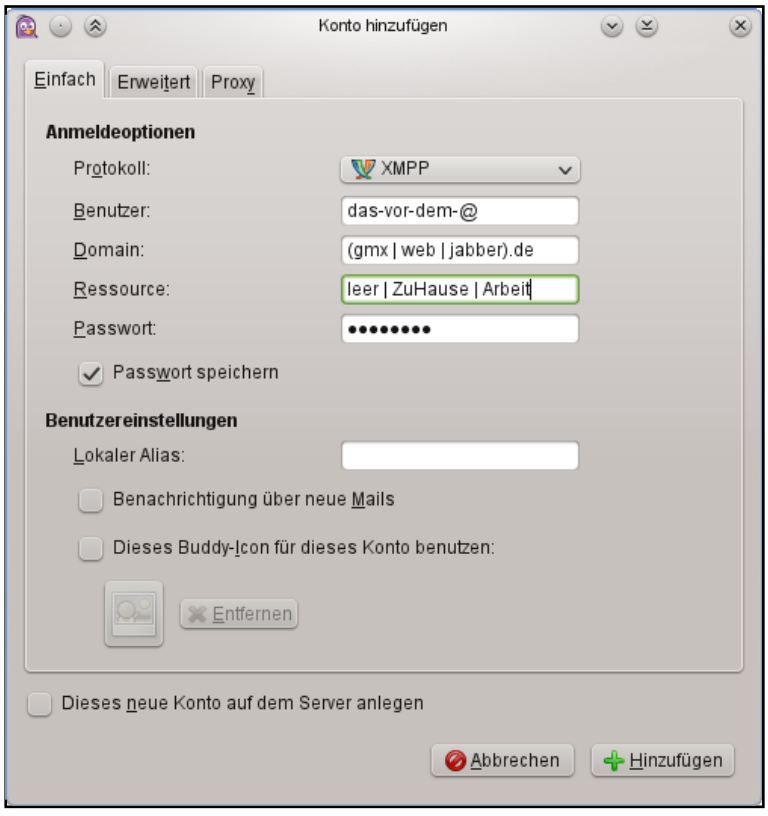
Pidgin (*pidgin-2.*.*-offline.exe*) muss vor OTR (*pidgin-otr-4.*.*-*.exe*) installiert werden. Beides muss mit Administratorrechten installiert werden.

Konfiguration

XMPP-Account

Die Teilnehmer können sich aussuchen, welchen XMPP-Server sie nutzen. Manche Mailprovider bieten XMPP automatisch mit an (z.B. mailbox.org); Wer dort eine E-Mail-Adresse hat, kann für XMPP einfach seine E-Mail-Adresse und sein zugehöriges Passwort verwenden. Ansonsten kommt z.B. jabber.de in Frage; dort muss man den Account über das Webinterface anlegen. Auf `xmpp.net/directory.php` gibt es eine Übersicht kostenlos nutzbarer XMPP-Server.

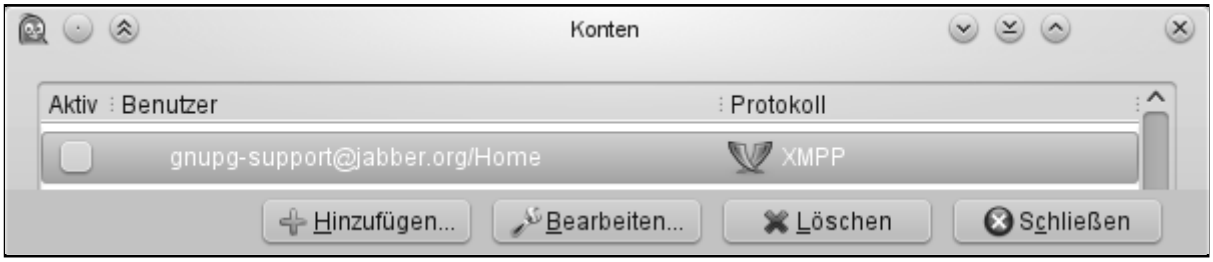
Pidgin



Im ersten Schritt fragt das Chatprogramm nach dem Protokoll, für das der Zugang eingerichtet werden soll. Da ist XMPP bzw. Jabber auszuwählen. Dann kommt man in Pidgin zu einer Seite, die aussieht wie links dargestellt.

Meist ist es sinnvoll, das Passwort speichern zu lassen (das ist standardmäßig nicht aktiviert). Die Einstellungen auf den anderen Seiten kann man so lassen. Über *"Hinzufügen"* kommt man dann zum Registrierungsdialog, den man einfach bestätigt.

Treten dabei keine Fehler auf, landet man anschließend bei der Kontenübersicht, die typischerweise nur den einen Eintrag hat. Dort muss man dann ggf. noch das Häkchen setzen, damit der Zugang aktiviert wird:



Es empfiehlt sich, in der Buddy-Liste unter *Buddys → Anzeigen* die Offline-Kontakte zu aktivieren.

OTR

Bevor OTR genutzt werden kann, muss es aktiviert werden. In der Buddy-Liste: *Werkzeuge → Plugins*; dort das Plugin *Off-the-Record Messaging* über die Checkbox links aktivieren und über den Button unten rechts konfigurieren. Die Einstellung *OTR-Unterhaltungen nicht speichern* sollte deaktiviert werden. Man kann dann auch gleich den Schlüssel generieren (das passiert aber sonst später automatisch).

Support-Adressen

Zu dieser Schulung gehören die XMPP-Support-Adresse des Dozenten und ein Support-Chatraum (*Buddys → Chat betreten* (temporär) oder (dauerhaften Eintrag in der Buddy-Liste) *Buddys → Chat hinzufügen*):

Chatraum: openpgp-schulung-berlin – Server: conference.jabber.org – Passwort: openpgp

gnupg-support@jabber.org – Fingerprint: 3162B7FC 56390CBA 69CB5086 97F1A3C0 E17E939B

Es bietet sich an, zuerst den Chatraum hinzuzufügen (sinnvollerweise mit Angabe des eigenen Namens als *Kürzel*), weil der Support-Account dort online ist und von da aus einfacher hinzugefügt werden kann (wie auch die Accounts der anderen Schulungsteilnehmer).

Wenn der Account *gnupg-support@jabber.org* online ist (obwohl er zunächst als offline angezeigt wird), angeschrieben wird und OTR aktiviert ist, dann wird der öffentliche Schlüssel automatisch übertragen. Über die Schaltfläche *unauthentifiziert* und den Menüpunkt *Buddy authentifizieren* kann der Fingerprint geprüft (also mit obigem verglichen) werden.

Facebook

Facebook hat seit mehreren Jahren ein XMPP-Gateway für seinen Chat. Das heißt, man kann bei Facebook online sein (für die anderen sichtbar online) und Nachrichten empfangen sowie verschicken, ohne über die Webseite eingeloggt zu sein. Es ist mit deutlich weniger Ressourcenaufwand verbunden, XMPP zu nutzen (auch wenn ab und zu Nachrichten nicht ankommen...).

Wenn ein Facebook-Nutzer Gefallen daran findet, Facebook über XMPP zu nutzen, wird Pidgin (o.Ä.) deswegen öfter laufen. Und dadurch sind auch die anderen XMPP-Accounts öfter online.

Pidgin hat einen eigenen Protokolleintrag für Facebook (das ist effektiv XMPP mit voreingestellter Domain). Es gibt auch eine Anleitung auf der Facebook-Seite für mehrere Clients (facebook.com/sitetour/chat.php); auf dieser Seite werden die für den konkreten Account nötigen Zugangsdaten angezeigt. Eventuell muss man sich vorher einen Nutzernamen zulegen: https://de-de.facebook.com/username

Und warum das alles?

Im Rahmen der OpenPGP-Schulung wird den Teilnehmern XMPP-OTR aus mehreren Gründen installiert, obwohl viele bisher kein Chatprogramm nutzen:

- Das ist einfach, geht schnell, verwendet mehrere Aspekte von OpenPGP, und die Teilnehmer haben schnell ein Erfolgserlebnis.
- Nicht immer sind am Ende der Schulung alle Probleme gelöst (auch wenn es so scheint). XMPP bietet gute Support-Möglichkeiten.
- Chatsysteme werden immer wichtiger – die Jugend nutzt E-Mail kaum noch. Die massenhaft genutzten Dienste sind allerdings nicht flexibel und standardisiert nutzbar (wie E-Mail), sondern jeweils in der Hand eines einzelnen Unternehmens. Deshalb ist es wichtig, den Leuten eine Alternative zu zeigen und deren Verbreitung zu fördern. Jeder kann XMPP nicht nur als Client nutzen (auch mit einer eigenen Domain), sondern – quasi kostenlos – zu Hause, in der Firma, im Verein u.Ä. einen Open-source-Chatserver einrichten und der Öffentlichkeit oder nur einem bestimmten Nutzerkreis zur Verfügung stellen.