Verschlüsselung von Jabber

Dieses HowTo beschreibt anhand des Instant Messaging Programms Pidgin die Konfiguration und Benutzung von Off-the-Record (OTR) Verschlüsselung.

OTR ermöglicht eine verschlüsselte Kommunikation zwischen Jabber-Programmen, als auch eine Überprüfung der Echtheit der Gesprächspartner.

Das Programm Pidgin wurde früher unter dem Namen „Gaim“ verteilt. Setzt man eine ältere GNU/Linux Distribution ein, in der Pidgin noch nicht enthalten ist, so sollte dieses HowTo dennoch anwendbar sein, wenn man Pidgin durch Gaim ersetzt.

Technische Voraussetzungen

Eigener Rechner

Auf dem eigenen Rechner muss neben Pidgin die OTR-Erweiterung (engl. "Plugin") für Pidgin installiert sein. Diese Erweiterung ist nicht Teil des Pidgin-Projektes, sondern wird in einem separatem Projekt entwickelt! Es ist deshalb i.d.R. notwendig ein separates Paket zu installieren. Beispielsweise ist in Debian GNU/Linux die Pidgin OTR-Erweiterung im Paket pidgin-otr enthalten und muss installiert sein.

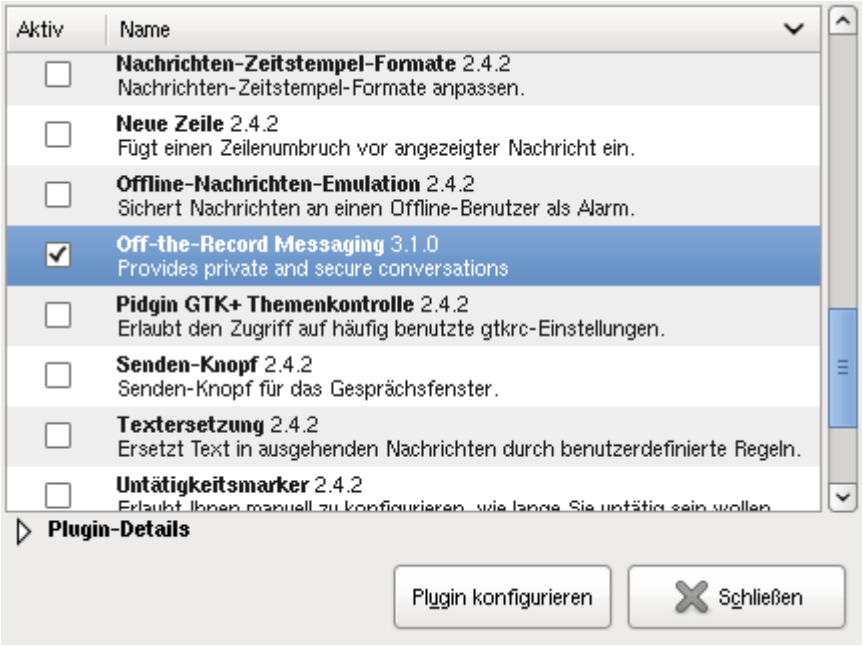
Rechner des Gesprächpartners

Das Jabber-Programm des Gesprächspartners muss ebenfalls OTR-Verschlüsselung unterstützen (s. OTR-fähige Jabber-Programme).

Einrichten der OTR-Erweiterung

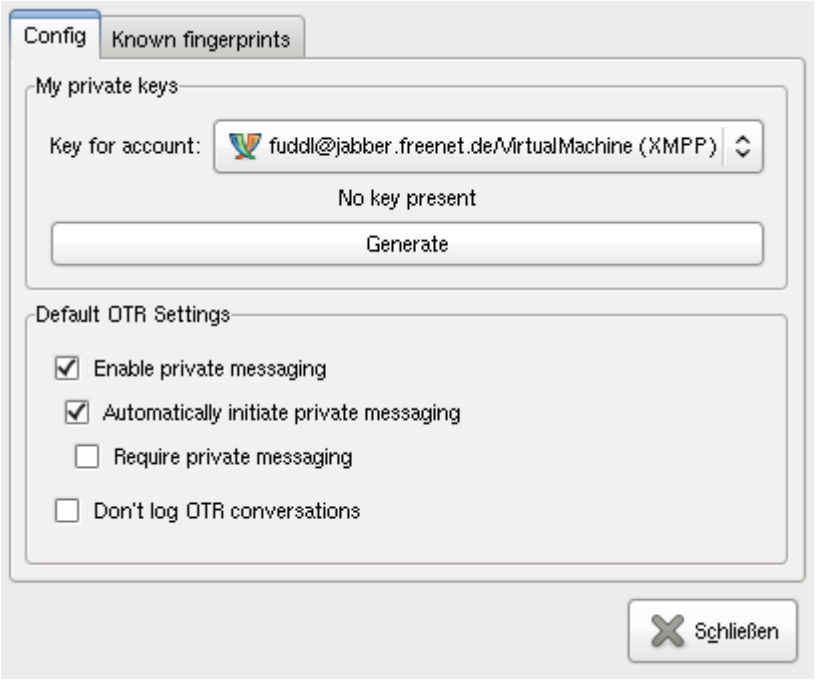
Zunächst muss Pidgin dazu gebracht werden, die OTR-Erweiterung zu laden.

Im Menü Werkzeuge → Plugins wählen, Häkchen bei „Off-the-Record Messaging“ setzen:



OTR benötigt einen einmalig generierten Schlüssel.

Im Plugin-Dialog Off-the-Record Messaging wählen und „Plugin konfigurieren“ klicken. Im anschließend erscheinendem Fenster unter Config → My private keys → Key for account: das entsprechende Jabber-Konto wählen und auf „Generate“ klicken:



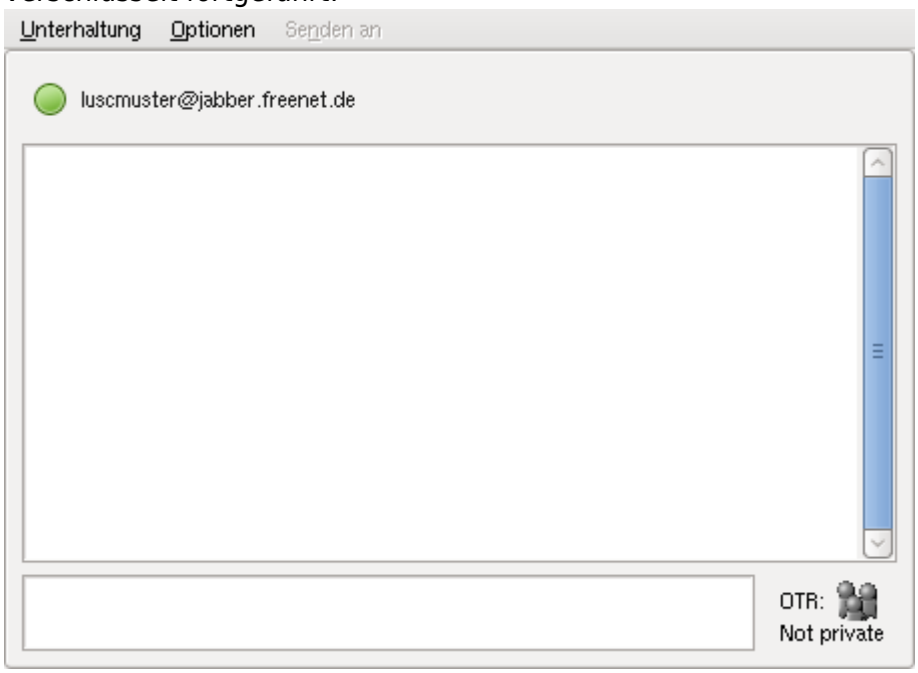
Das generieren des Schlüssels kann etwas dauern. Dieses Fenster erscheint, wenn der Schlüssel generiert ist:

Pidgin ist nun vorbereitet für die Arbeit mit OTR-Verschlüsselung!

Verschlüsseln von Gesprächen

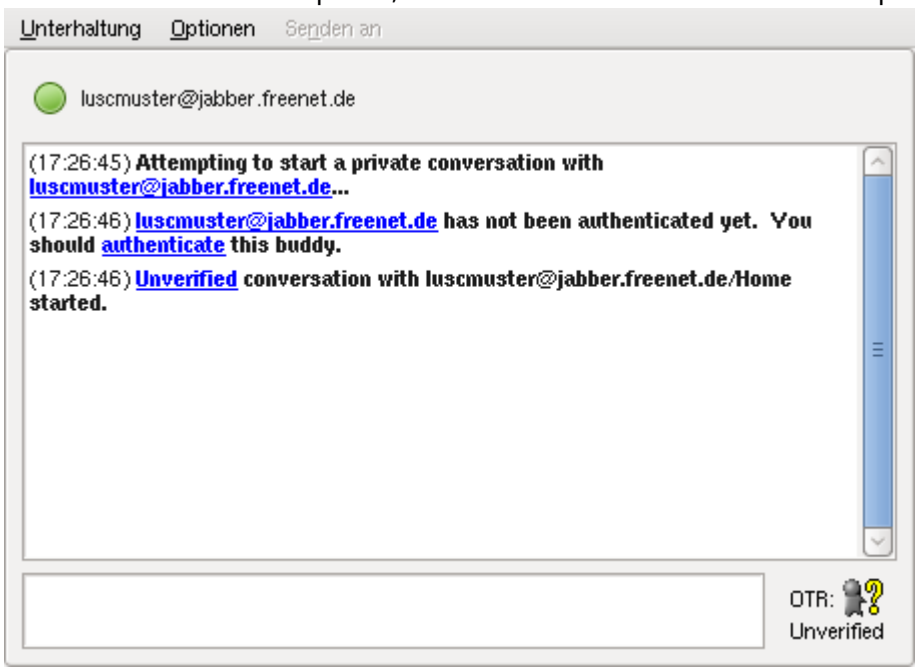
Sobald die OTR-Erweiterung von Pidgin geladen wird, erscheint in jedem Gesprächsfenster in der unteren rechten Ecke ein Knopf um OTR-spezifische Einstellungen vorzunehmen.

Ein anfangs unverschlüsseltes Gespräch wird durch anklicken des Knopfes „OTR: Not private“ verschlüsselt fortgeführt:



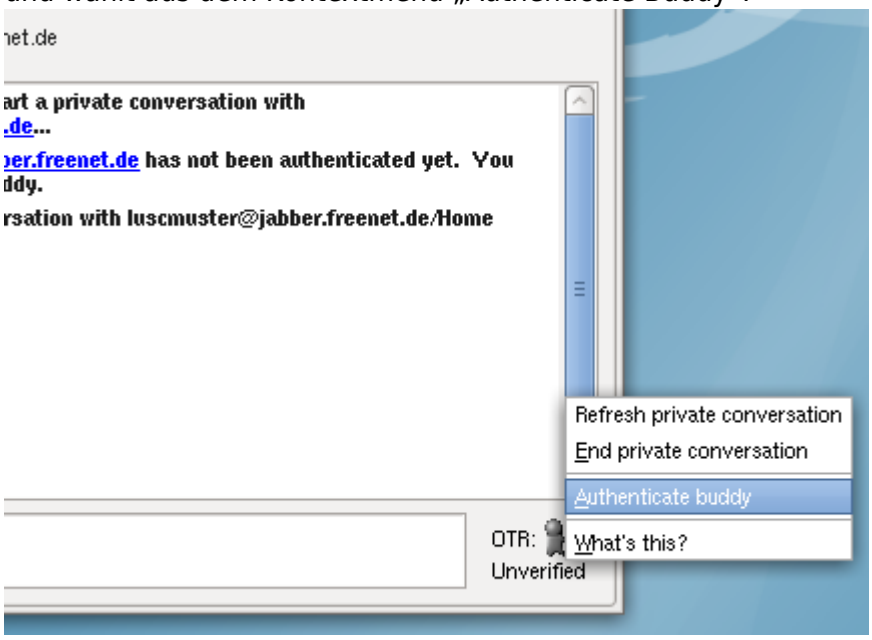
Wird die OTR-Verschlüsselung für ein Gespräch aktiviert, so ändert sich die Beschriftung des Knopfes zu „OTR: unverified“. In diesem Zustand hat man sich jedoch noch nicht von der Identität des Gesprächpartners überzeugt!

Ein verschlüsseltes Gespräch, ohne sich von der Identität des Gesprächpartners überzeugt zu haben:



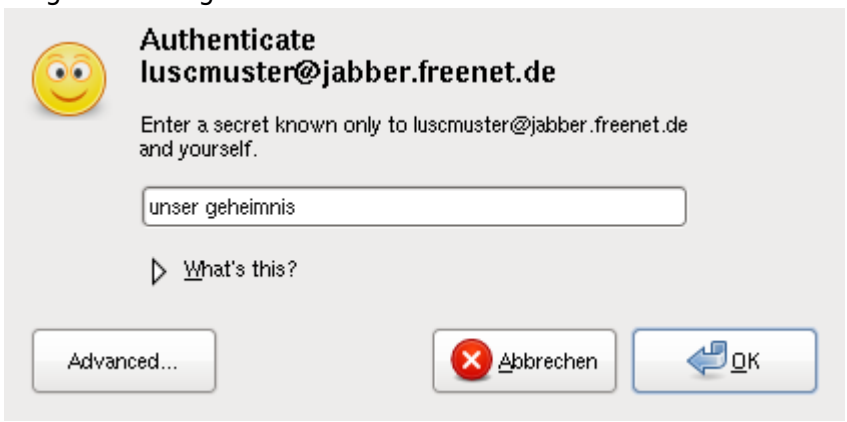
Um sich von der Identität des Gesprächpartners zu überzeugen bietet OTR die Möglichkeit, dass beide Gesprächspartner ein gemeinsames Geheimnis eingeben können.

Um die Identität der Gesprächpartner zu prüfen klickt man rechts auf den Knopf „OTR: unverified“ und wählt aus dem Kontextmenü „Authenticate Buddy“:



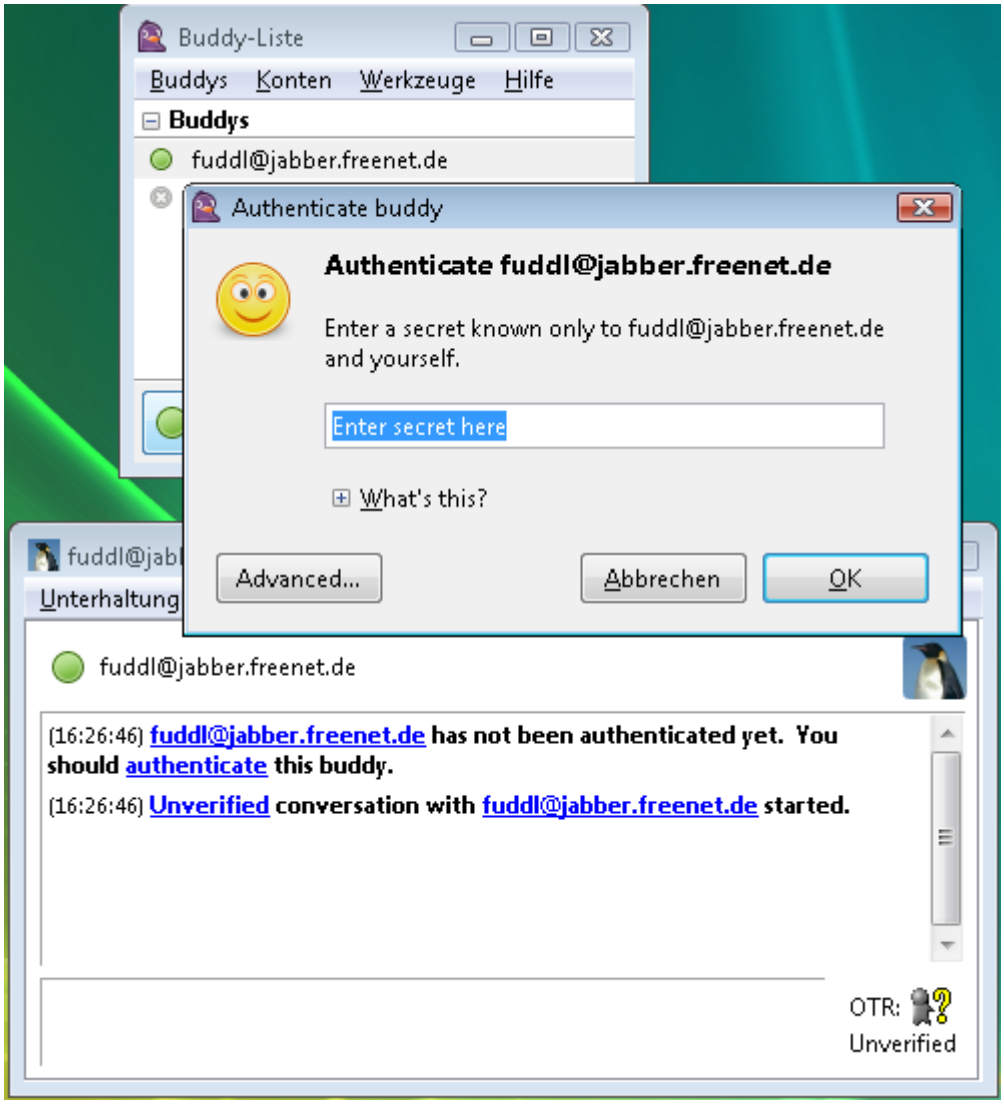
Im anschließend erscheinendem Fenster muss man nun ein gemeinsames Geheimnis eingeben. Erfahrungsgemäß eignen sich Insider-Witze besonders gut ;)

Eingabe eines gemeinsamen Geheimnisses:



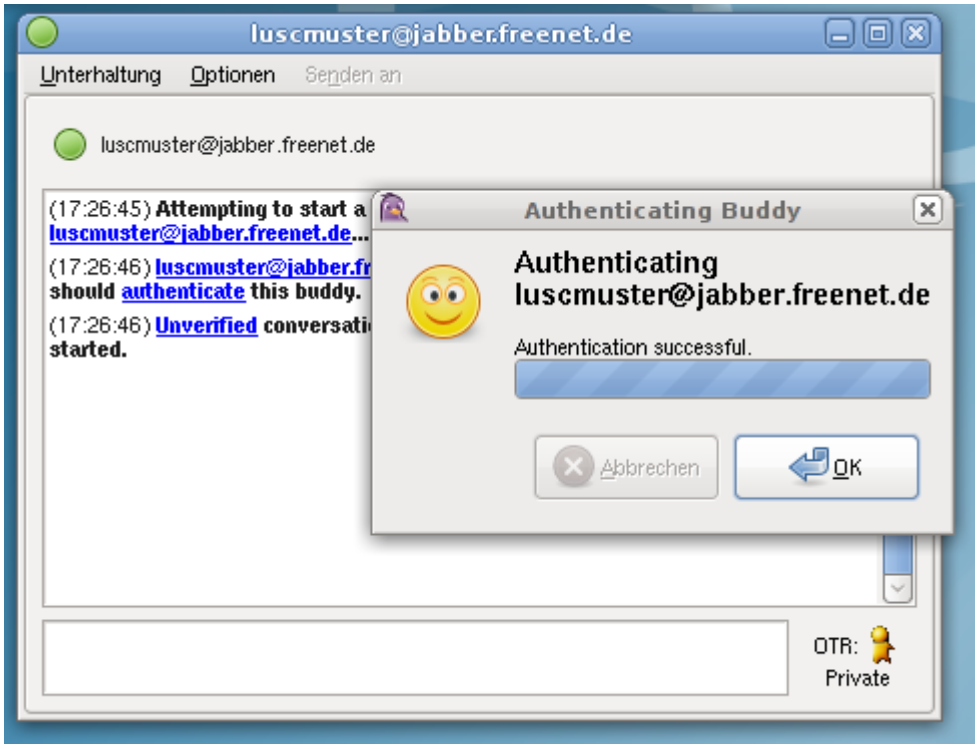
Hat man das Geheimnis eingegeben, wartet Pidgin auf die Eingabe des Geheimnisses beim Gesprächspartner:

Sobald man das Geheimnis eingegeben hat, erscheint beim **Gesprächspartner** ein Fenster, das zur Eingabe des gemeinsames Geheimnisses auffordert:

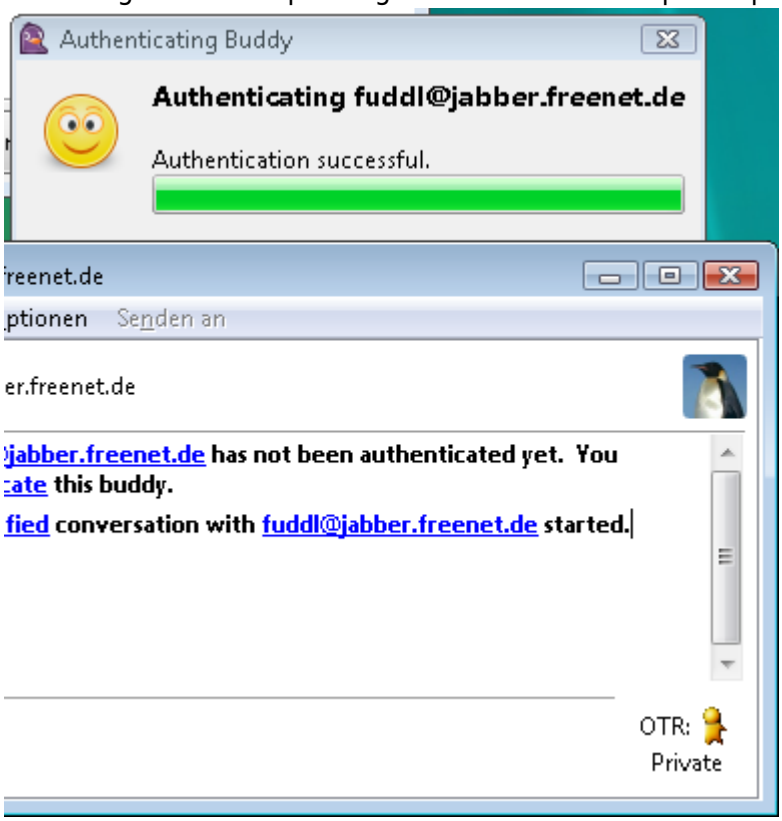


Hat der Gesprächspartner das gleiche geheime Wort/den gleichen geheimen Satz eingegeben, so findet das Gespräch nun verschlüsselt statt und beide Teilnehmer können sich über die Identität des Gesprächpartners sicher sein. Diesen Zustand zeigt Pidgin im Gesprächsfenster an, indem die Beschriftung des OTR-Symbols zu „OTR: private“ wechselt.

Erfolgreiche Überprüfung der Identität der Gesprächspartner:



Die Erfolgreiche Überprüfung wird auch beim Gesprächspartner angezeigt:



OTR-fähige Jabber-Programme

Linux

- Pidgin (GTK2)
- Kopete (KDE/Qt)

- mcabber (Textbasiert)

Mac OS X

- Adium X (Aqua)
- mcabber (Textbasiert)

Windows

- Pidgin (GTK2)
- Miranda (Windows)
- mcabber (Textbasiert)