Vertrauliches Chatten

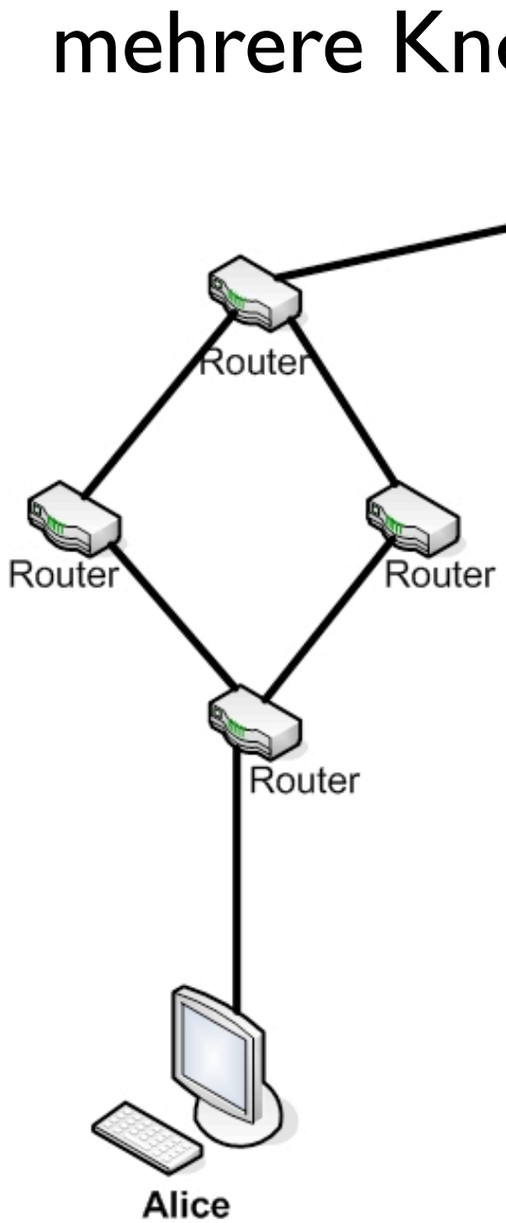
Unbefugtes Mitlesen verhindern

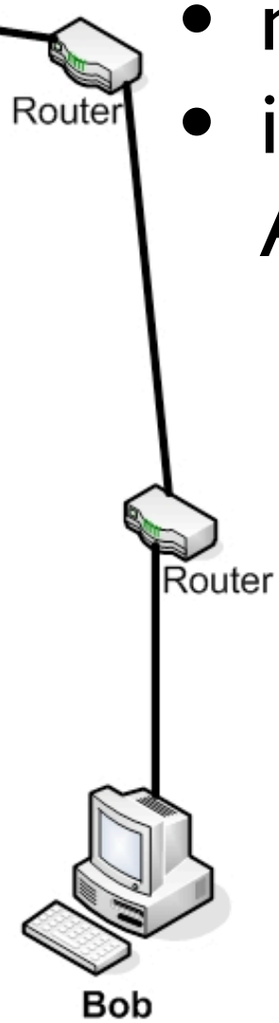
Inhalt

- Problematik beim Chatten
- Exkursion
  - AES, SHA
  - OTR
- Pidgin (allgemein)
- Pidgin mit OTR
- Live Demo

Problematik beim Chatten I

- Problem: Nachrichten passieren von Alice zu Bob mehrere Knoten





- mitlesbar
- manipulierbar
- ist Alice wirklich Alice?

Problematik beim Chatten II

Probleme	Lösungen
Mitlesbarkeit	Verschlüsselung
Manipulierbarkeit	Signierte Nachrichten
Authentizität	“Fingerabdruck” des Gegenübers

- **OTR kann diese Probleme lösen**

Exkursion I
AES

- AES (*Advanced Encryption Standard*)
- Symmetrisches Verschlüsselungsverfahren
  - ein gemeinsamer Schlüssel
- auch bekannt als "*Rijndael-Algorithmus*"

  (Joan Daemen, Vincent Rijmen)
- Standard seit 2000

Exkursion II
SHA

- SHA (*Secure Hash Algorithm*)
- Idee:
  - kurzer Prüfwert über einen längeren Text
  - Einwegfunktion, d.h. aus Prüfwert ist es nicht möglich den entsprechenden Text zu bestimmen
  - keine zwei Nachrichten mit gleichem Prüfwert

Exkursion II
SHA

- Beispiel:

$$h(x) = x \bmod 12$$

$$h(1) = 1$$

$$h(23) = 11$$

$$h(125) = 5$$

OTR I
Grundsätze

- OTR = **O**ff-**T**he-**R**ecord Messaging

  (deutsch: *inoffiziell; vertraulich, nicht für die Öffentlichkeit bestimmt*)

- Entwickelt von Ian Goldberg, Chris Alexander und Nikita Borisov

- Prinzip der
  - Verschlüsselung
  - Beglaubigung
  - Abstreitbarkeit
  - Folgenlosigkeit

OTR II
Das Protokoll

- Mit einem mathematischen Verfahren wird sicher ein Schlüssel ausgetauscht
- Nachrichten werden mit diesem Schlüssel verschlüsselt (*AES*) (→Verschlüsselung)
- Teilnehmer haben eine eindeutige Signatur (SHA) (→Beglaubigung)
- Nachrichten enthalten keine Signatur

  Beide Teilnehmer erhalten die alten, nicht mehr gültigen, geheimen Schlüssel (→Abstreitbarkeit)
- Schlüssel werden für jede Sitzung neu erzeugt und ausgetauscht (→Folgenlosigkeit)

OTR III

Die 3 Zustände von OTR

1. Unverschlüsselt:

2. Verschlüsselt, aber <u>nicht</u> verifiziert:

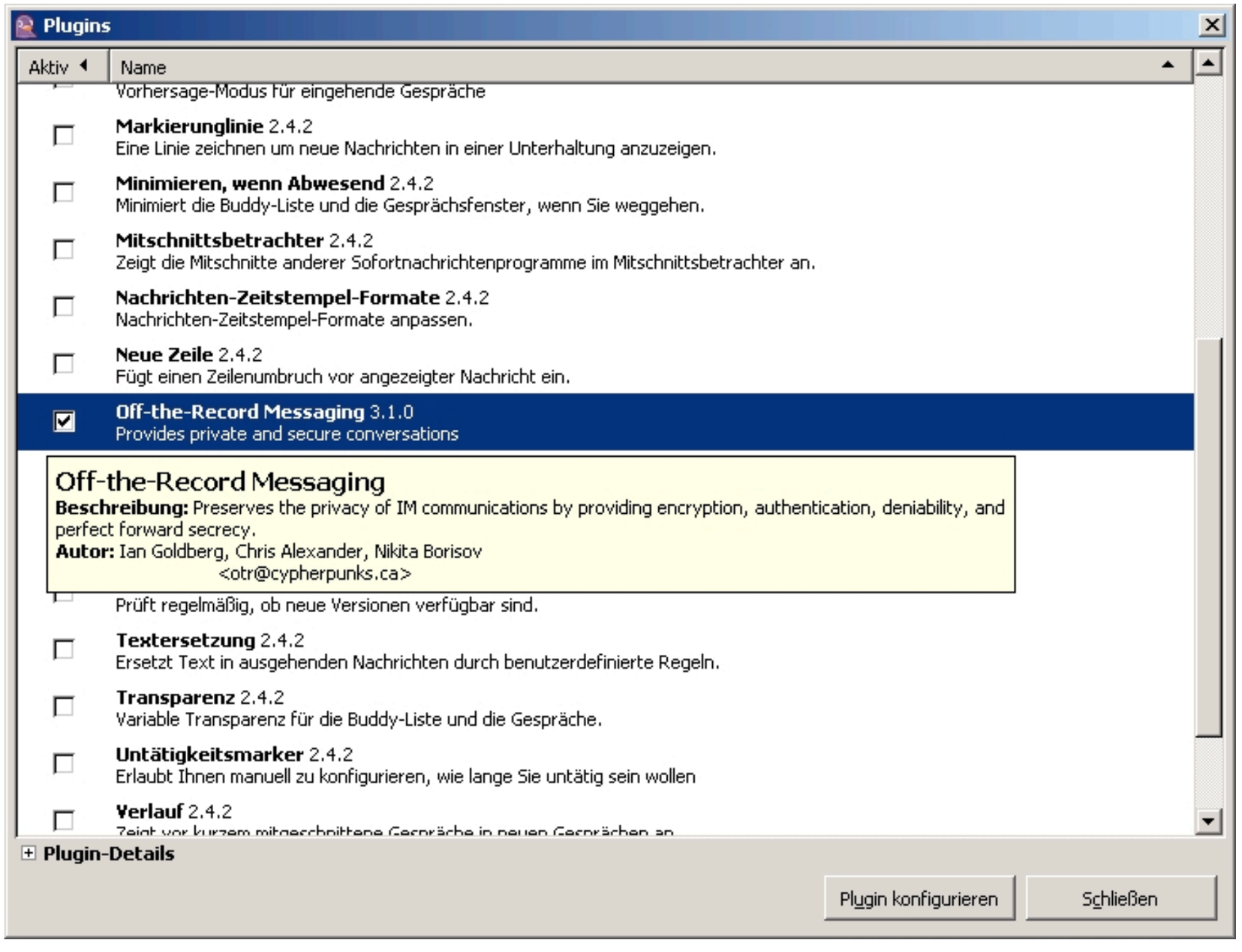
3. Verschlüsselt und verifiziert:

(*http://www.cypherpunks.ca/otr/help/buttonhelp.php*)

pidgin

- Multi-Protokoll-Client (ICQ, AIM, Jabber, Yahoo, MSN, ...)
- Open-Source (GPL)
- 2005 - 2007 unter dem Namen Gaim entwickelt
- Nach einem Streit mit AOL folgte Umbenennung in Pidgin
- Erhältlich für Windows, Linux, *BSD

- OTR als Plugin installierbar

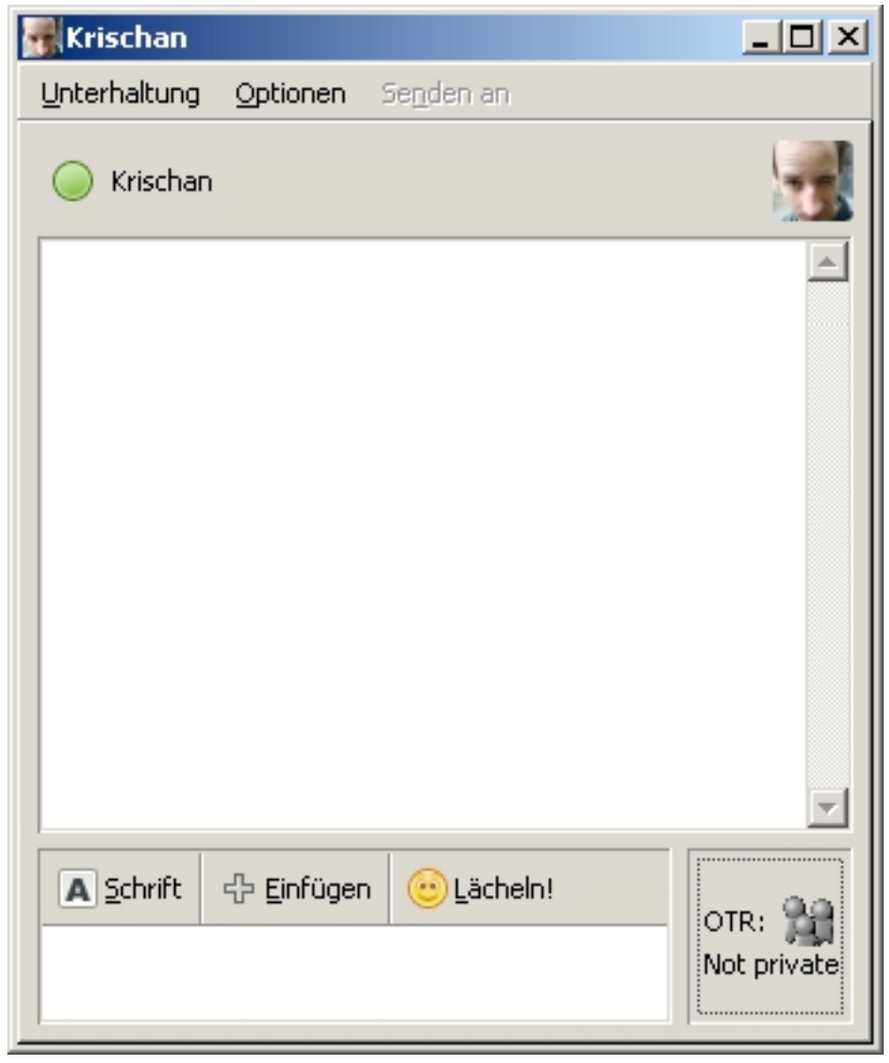


Pidgin mit OTR I

- Unverschlüsselt:

- Schlüssel werden erzeugt:

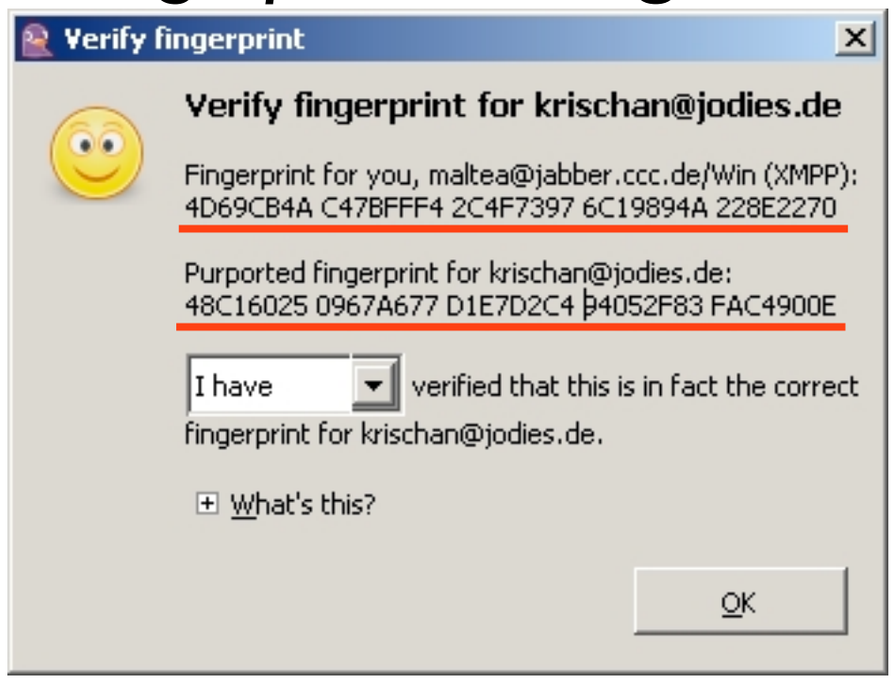
- Das Chatfenster:



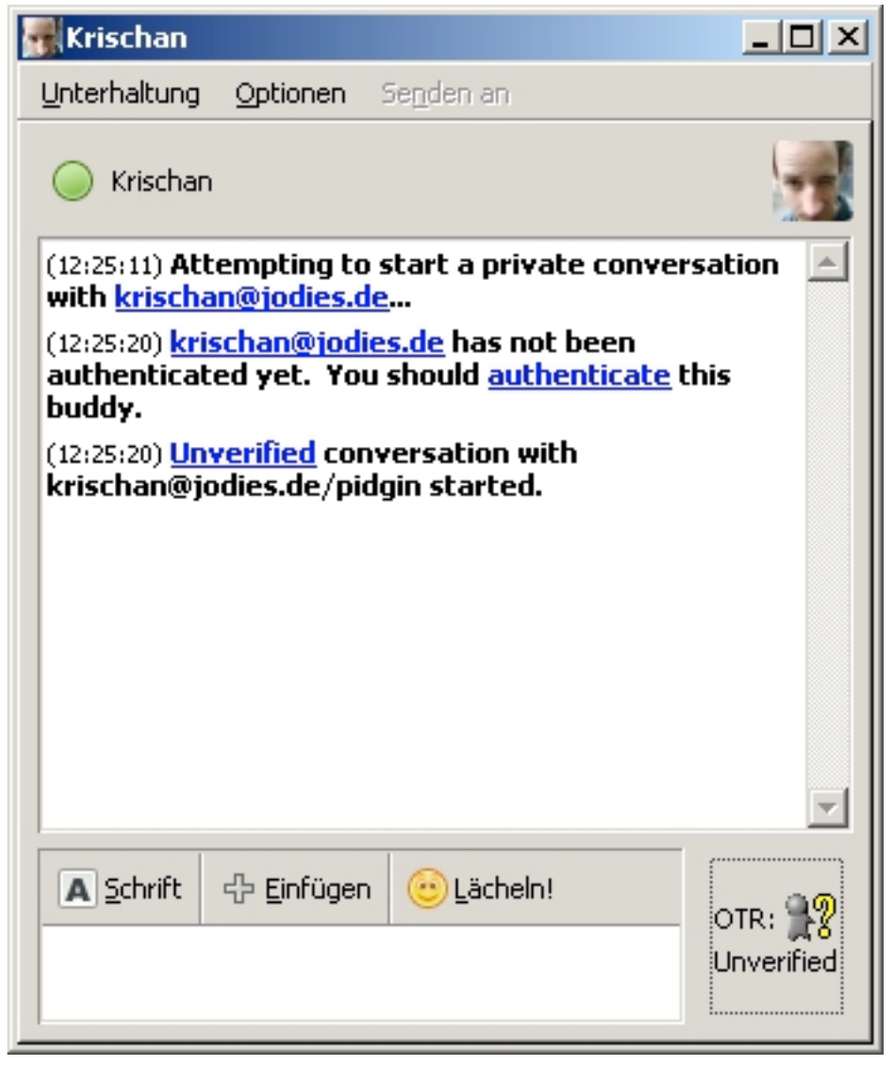
Pidgin mit OTR II

- Verschlüsselt (***nicht*** *verifiziert*):

- "*Fingerprints*" vergleichen:

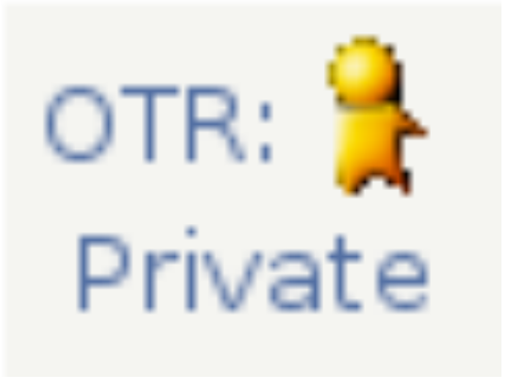


- Das Chatfenster:

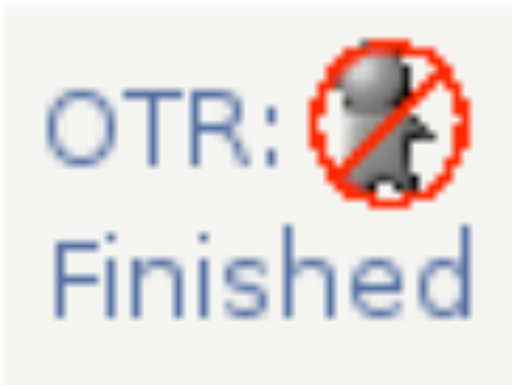


Pidgin mit OTR III

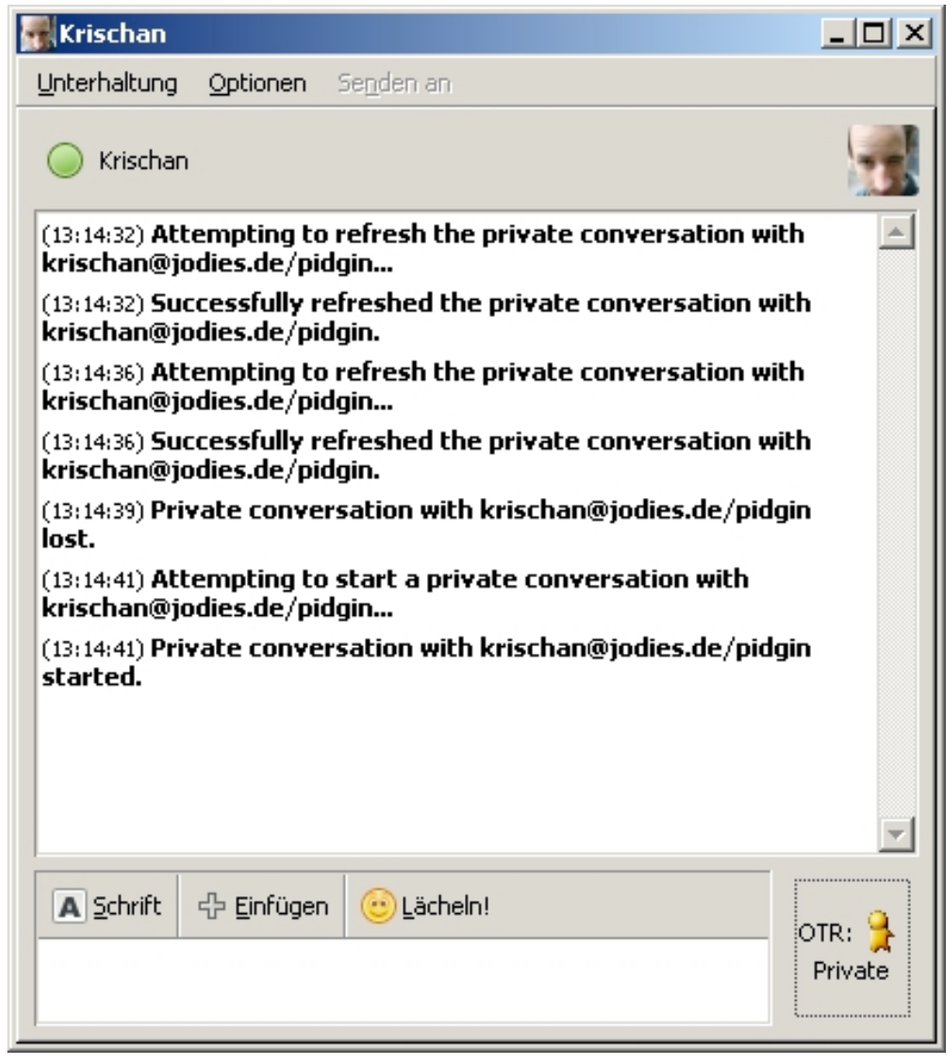
- Verschlüsselt (*verifiziert*):



- Verschlüsselten Chat beendet:



- Das Chatfenster:



Live Demo

- Instant Messenger Pidgin (*www.pidgin.im*)
- OTR Plugin für Pidgin (*www.cypherpunks.ca/otr*)

Alternative Multi-Protokoll-Clients

- Pidgin (Window, Linux) (*www.pidgin.im*)
- Miranda (Windows) (*www.miranda-im.org*)
- Adium (Mac OS X) (*www.adiumx.com*)

Vielen Dank