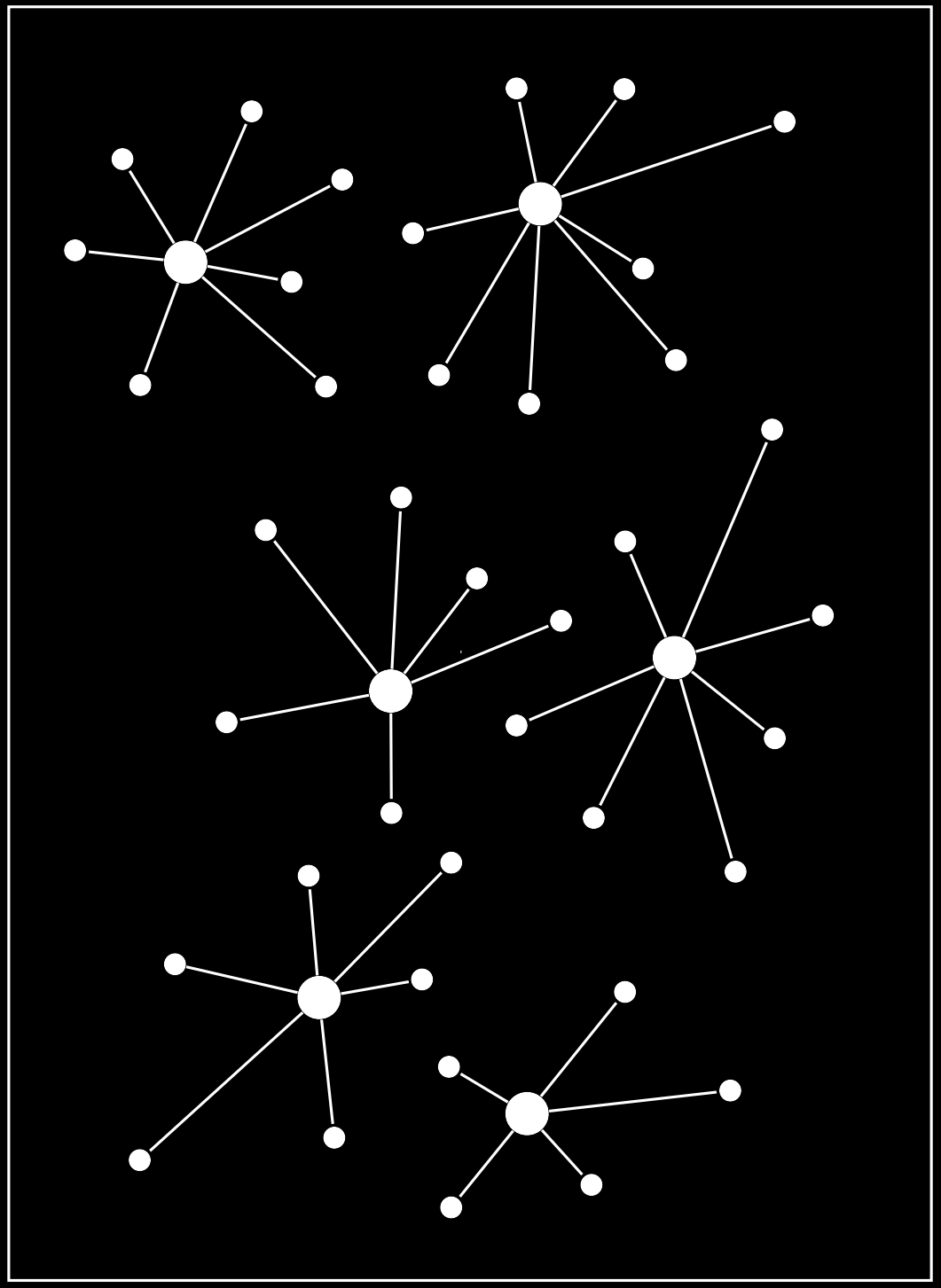
# Cryptoparty: Jabber, OTR, VPN und TOR

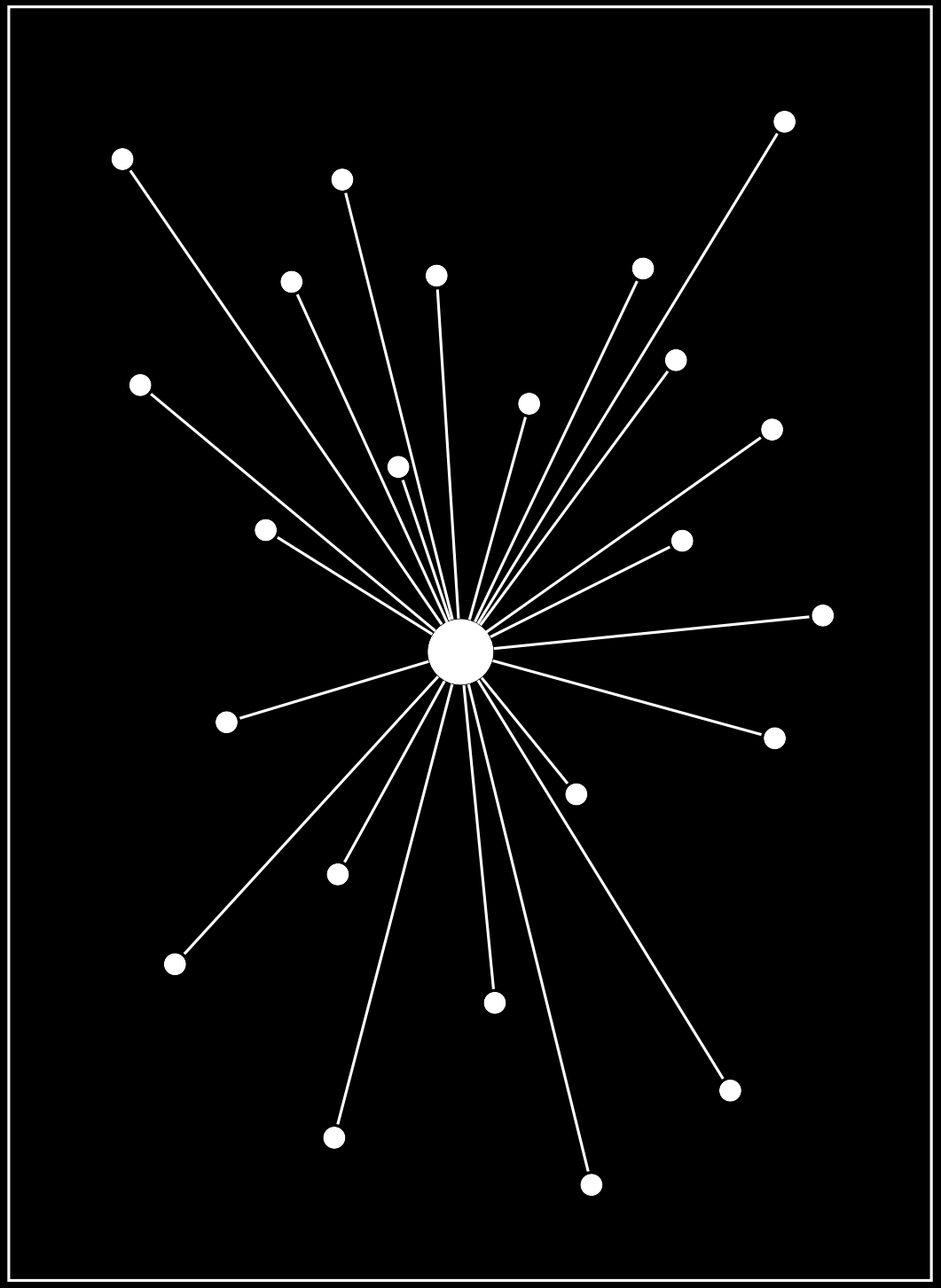
Digitale Selbstverteidigung

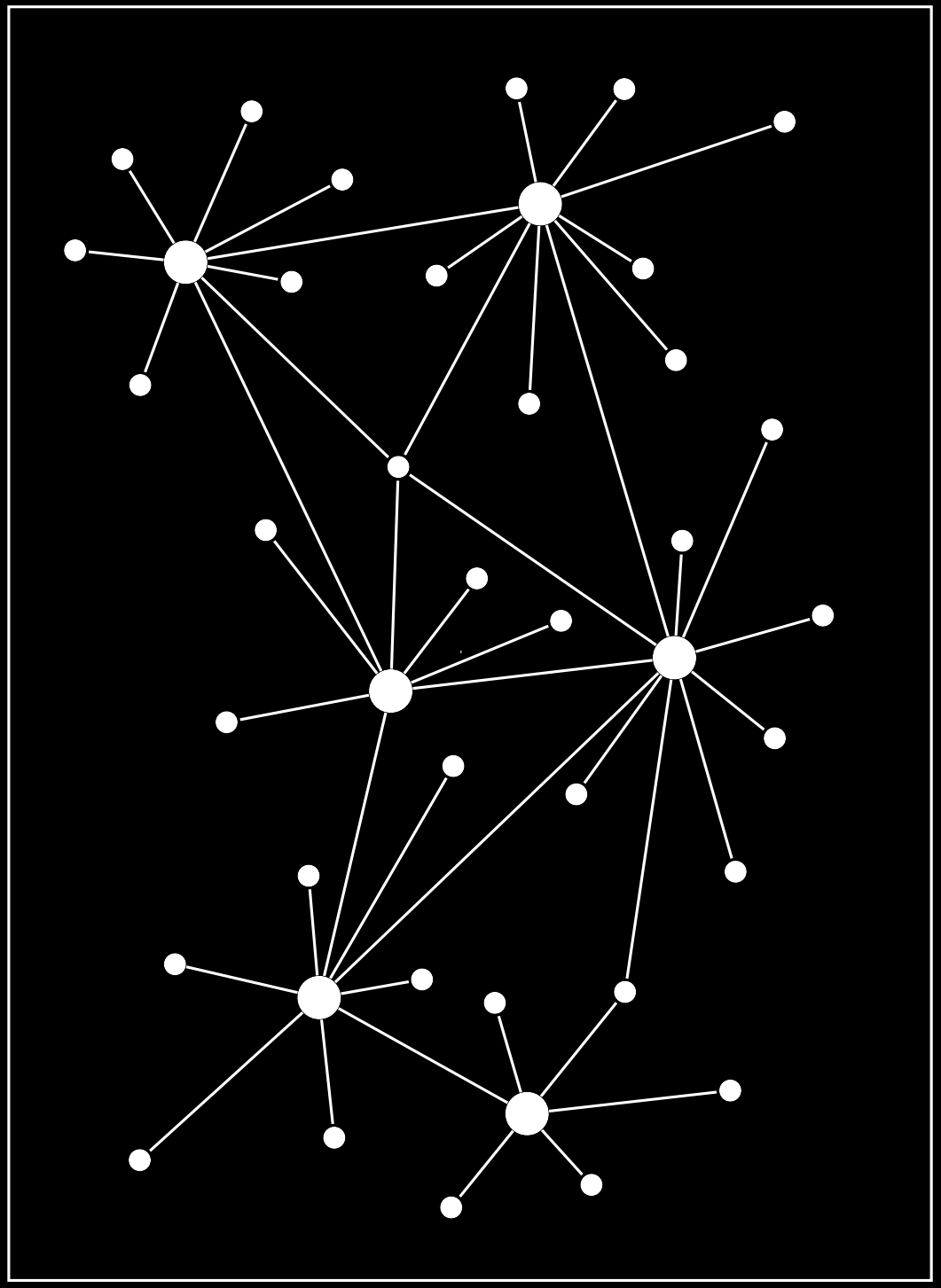
Torsten Grote
<t@grobox.de>
@t_grote

20.07.2013

# Jabber (XMPP)







# Chatprogramme

**GNU/Linux + Windows: Pidgin**

`http://pidgin.im/`

**MacOS: Adium**

`https://adium.im/`

# GNU/Linux Debian oder Ubuntu

```
apt-get install pidgin pidgin-otr
```

# Windows


Einfach
Erweitert
Proxy
Anmeldeoptionen
Protokoll:
XMPP
Benutzer:
beispiel1
Domain:
jabber.org
Ressource:
Passwort:
Passwort speichern
Benutzereinstellungen
Lokaler Alias:
Alexander
Benachrichtigung über neue Mails
Dieses Buddy-Icon für dieses Konto benutzen:
Entfernen
Dieses neue Konto auf dem Server anlegen
Abbrechen
Hinzufügen

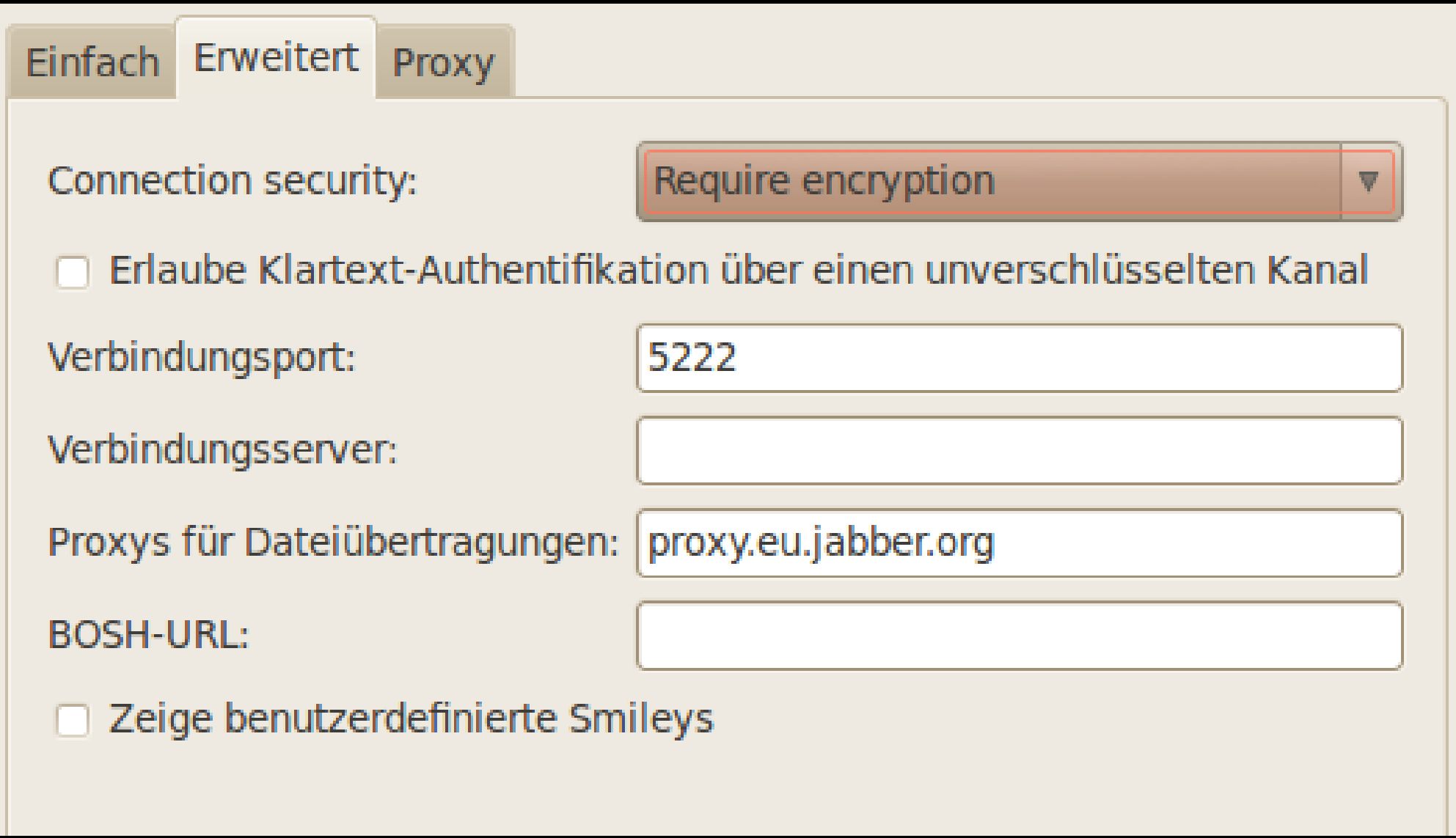
# Den passenden Server finden

https://list.jabber.at/

http://xmpp.net/

**oder einfach:**

jabber.piratenpartei.de


Einfach
Erweitert
Proxy
Connection security:
Require encryption
Erlaube Klartext-Authentifikation über einen unverschlüsselten Kanal
Verbindungsport:
5222
Verbindungsserver:
Proxys für Dateiübertragungen:
proxy.eu.jabber.org
BOSH-URL:
Zeige benutzerdefinierte Smileys

Einen Buddy hinzufügen.

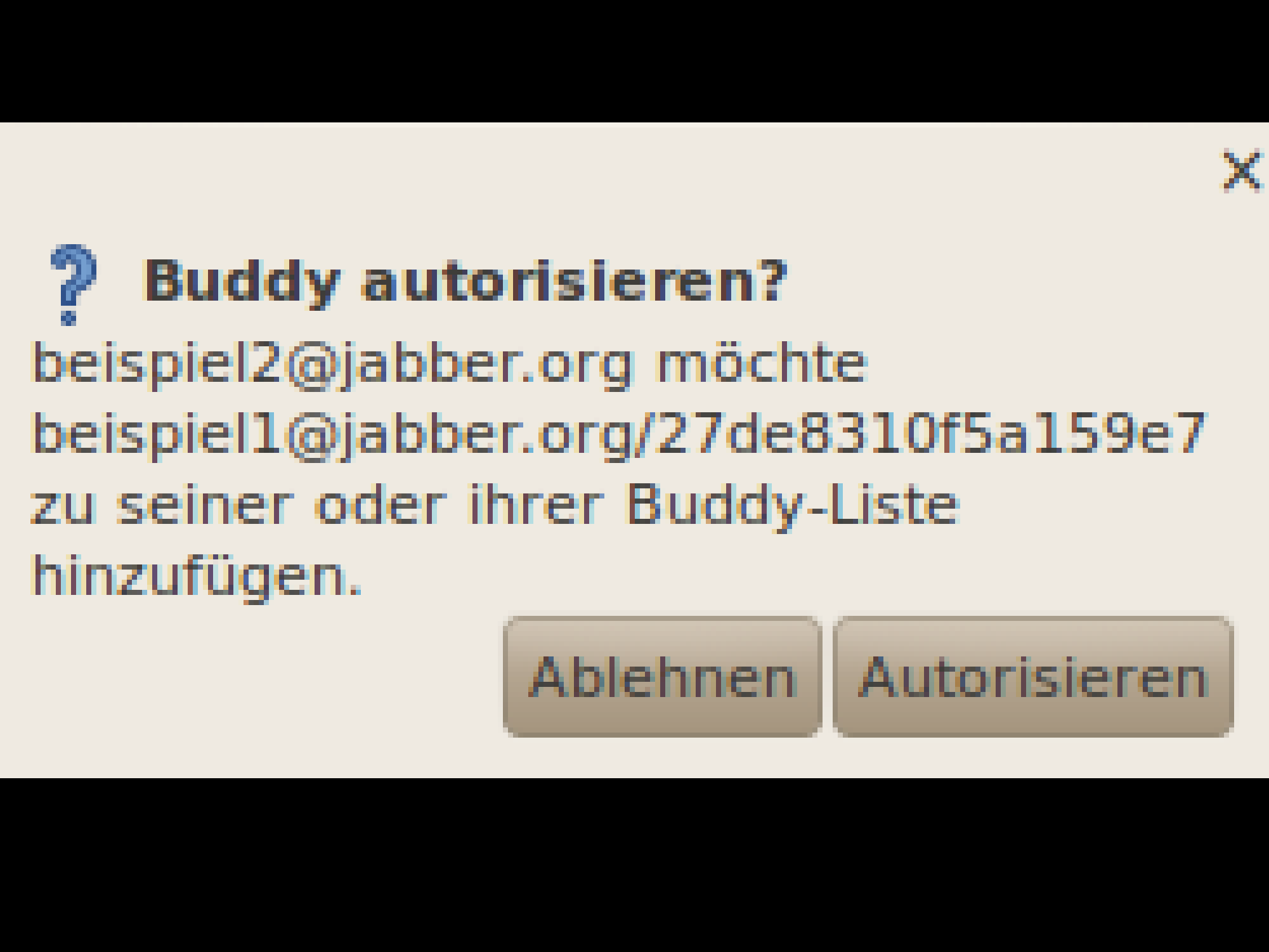
Konto: beispiel1@jabber.org/ (Alexander) (XMPP)

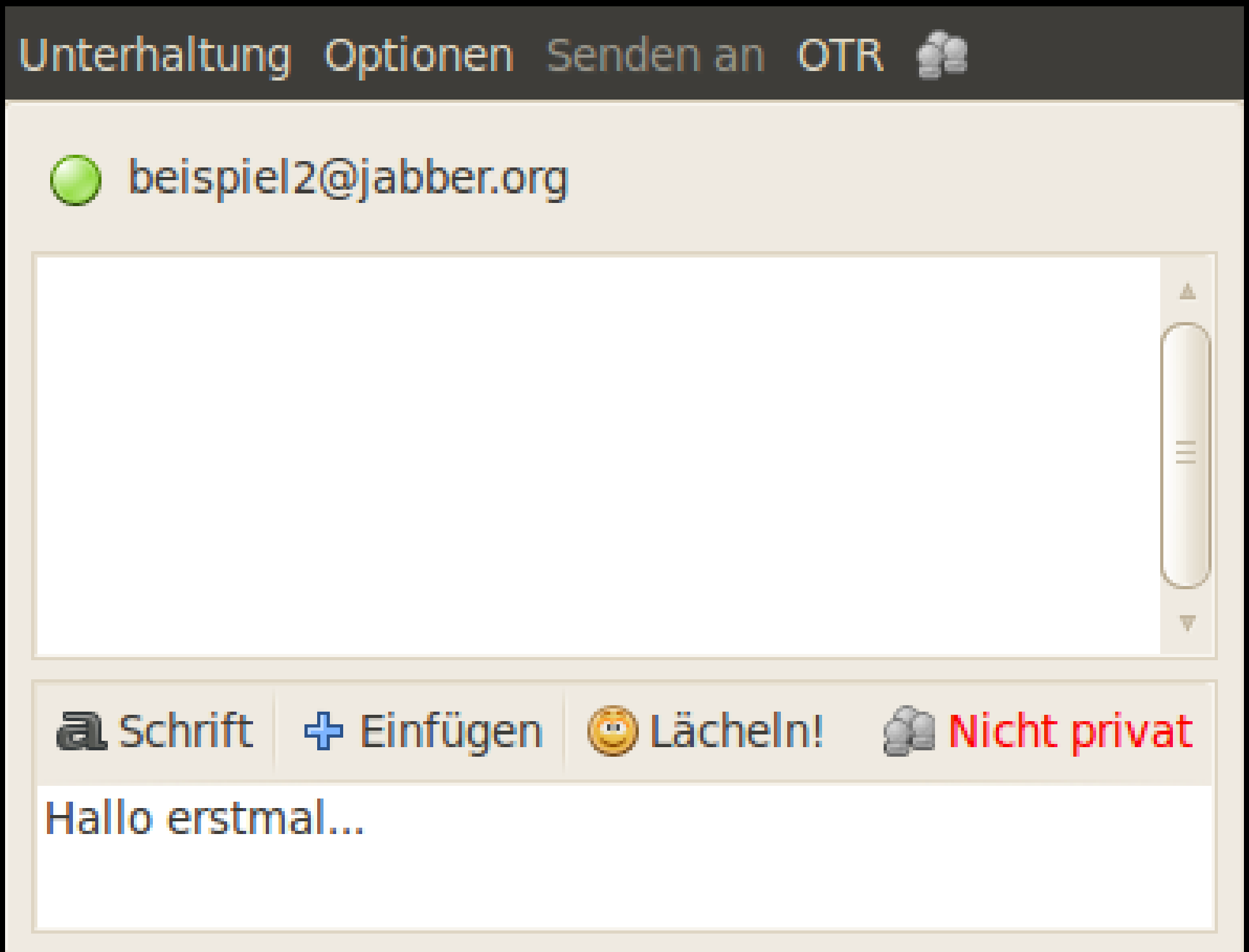
Benutzername des Buddys: beispiel2@jabber.org

(Optionaler) Alias:

Buddy zu folgender Gruppe hinzufügen:

Abbrechen | Hinzufügen


Buddy autorisieren?
beispiel2@jabber.org möchte beispiel1@jabber.org/27de8310f5a159e7 zu seiner oder ihrer Buddy-Liste hinzufügen.
Ablehnen
Autorisieren


Unterhaltung Optionen Senden an OTR
beispiel2@jabber.org
Schrift
Einfügen
Lächeln!
Nicht privat
Hallo erstmal...

# Off-the-Record Messaging

http://www.cypherpunks.ca/otr/

- **Verschlüsselung (Encryption)**
- **Beglaubigung (Authentication)**
- **Abstreitbarkeit (Deniability)**
- **Folgenlosigkeit (Perfect forward secrecy)**

# Off-the-Record Messaging

News | Downloads | Mailing Lists | Documentation | FAQ | Press | Software | People

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

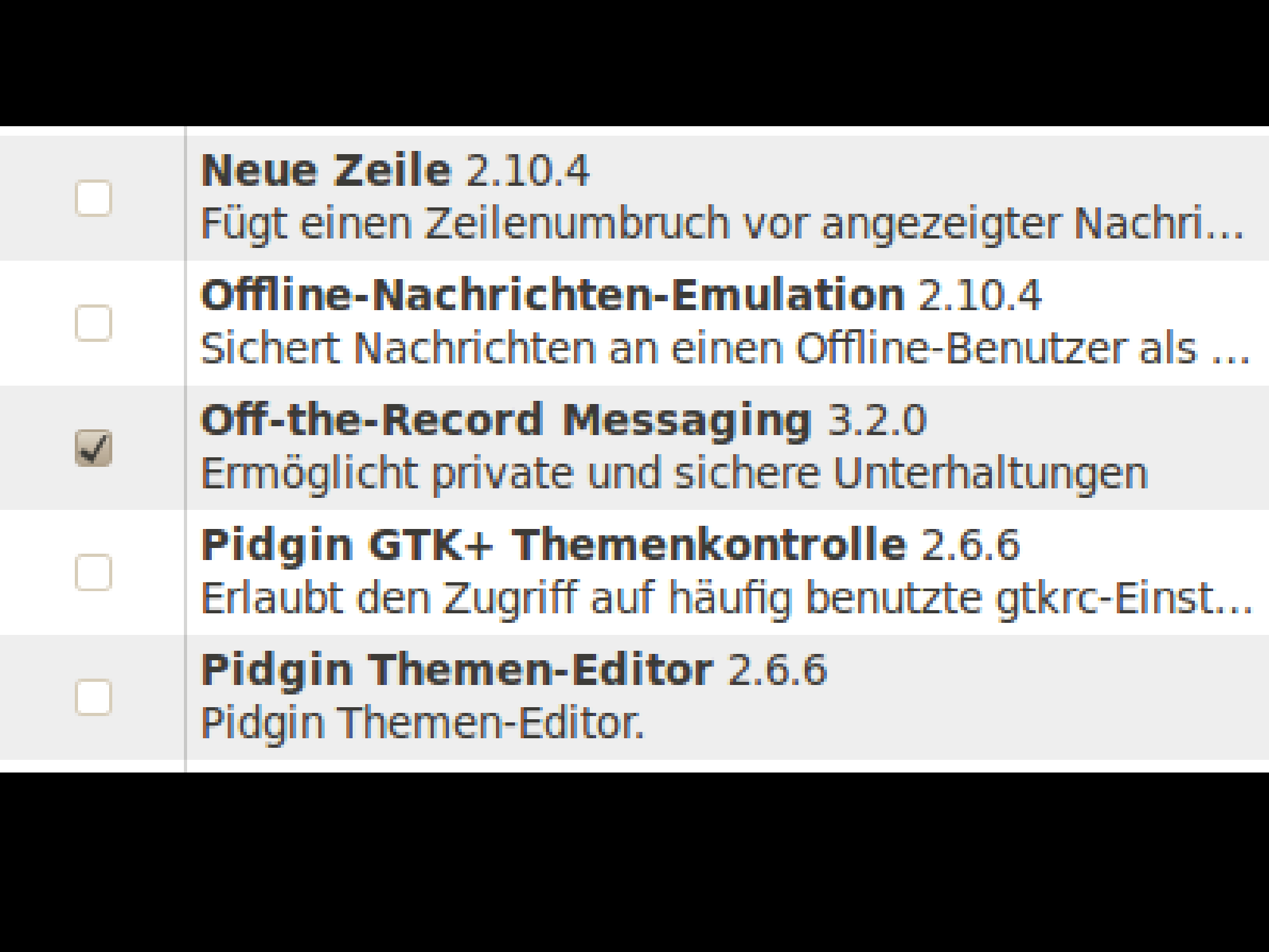
- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, *during* a conversation, your correspondent is assured the messages he sees are authentic and unmodified.

- **Perfect forward secrecy**

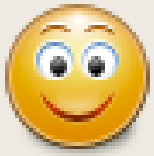
  If you lose control of your private keys, no previous conversation is compromised.

## Primary download: Win32 installer for pidgin-otr 3.2.1 [other downloads]


Neue Zeile 2.10.4
Fügt einen Zeilenumbruch vor angezeigter Nachri...
Offline-Nachrichten-Emulation 2.10.4
Sichert Nachrichten an einen Offline-Benutzer als ...
Off-the-Record Messaging 3.2.0
Ermöglicht private und sichere Unterhaltungen
Pidgin GTK+ Themenkontrolle 2.6.6
Erlaubt den Zugriff auf häufig benutzte gtkrc-Einst...
Pidgin Themen-Editor 2.6.6
Pidgin Themen-Editor.


Konfiguration
Bekannte Fingerprints
Meine privaten Schlüssel
Schlüssel für Konto:
beispiel1@jabber.org/ (Alexander) (XMPP)
Kein Schlüssel vorhanden
Generieren
Standard OTR-Einstellungen
Privaten Nachrichtenversand aktivieren
Privaten Nachrichtenversand automatisch aktivieren
Privaten Nachrichtenversand erzwingen
OTR-Unterhaltungen nicht speichern
OTR-Erscheinungsbild
OTR-Button in Symbolleiste anzeigen


beispiel2@jabber.org
Unterhaltung Optionen Senden an OTR
Private Unterhaltung aktualisieren
Private Unterhaltung beenden
Buddy authentifizieren
beispiel2@jabber.org/816b50086f00cef6 (beispiel1@jabber.org/)
Unverifiziert
Was ist das?
beispiel2@jabber.org
(15:33:24) Alexander: Hallo erstm
(15:33:26) beispiel2@jabber.org
nicht authentifiziert. Sie sollte
Buddy authentifizieren.
(15:33:26) Nicht verifizierte U
mit beispiel2@jabber.org/816b
begonnen.
Schrift
Einfügen
Lächeln!
Unverifiziert



## beispiel2@jabber.org authentifizieren

Einen Buddy zu authentifizieren hilft sicherzustellen, dass die Person, mit der Sie sprechen die ist, die sie zu sein behauptet.

Wie möchten Sie Ihren Buddy authentifizieren?

Manueller Fingerprint-Vergleich

Fingerprint für Sie, beispiel1@jabber.org/ (XMPP):
6E28051F 7A4AD831 DFA010F4 A651ADB2 185BB7B9

Angegebener Fingerprint für beispiel2@jabber.org:
9BFA30BC AD5C4BE5 11718859 04CE3B8F 72C9C49B

Ich habe überprüft, dass dies tatsächlich der richtige Fingerprint für beispiel2@jabber.org ist.

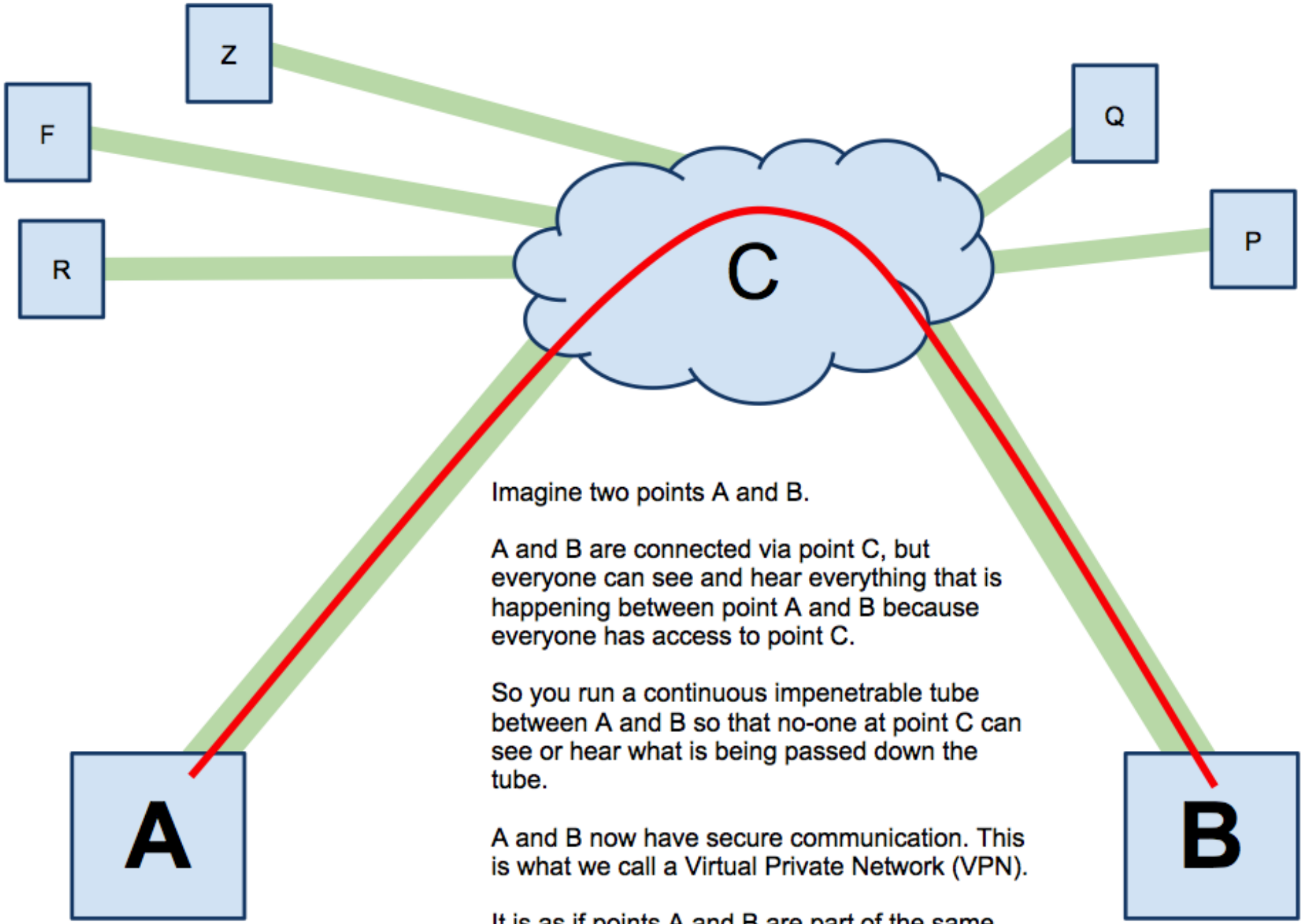
Hilfe | Abbrechen | Authentifizieren

 (15:38:59) **Der Status der aktuellen Unterhaltung ist jetzt: Privat**

Schrift | Einfügen | Lächeln! | Privat

Nun können wir reden.. ;)

http://www.digitales-grundwissen.de/pidgin-installieren/




Imagine two points A and B.

A and B are connected via point C, but everyone can see and hear everything that is happening between point A and B because everyone has access to point C.

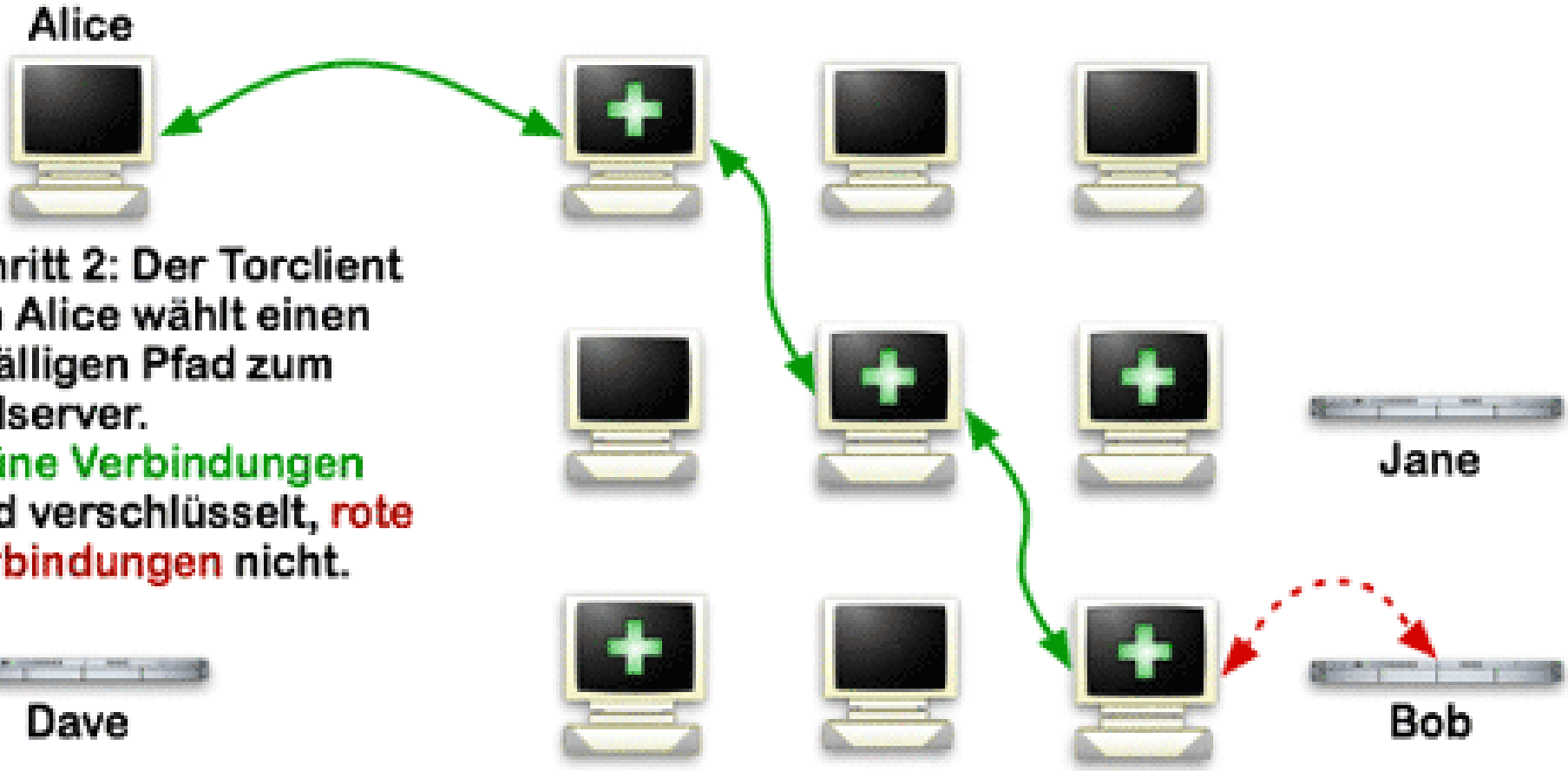
So you run a continuous impenetrable tube between A and B so that no-one at point C can see or hear what is being passed down the tube.

A and B now have secure communication. This is what we call a Virtual Private Network (VPN).

It is as if points A and B are part of the same location.

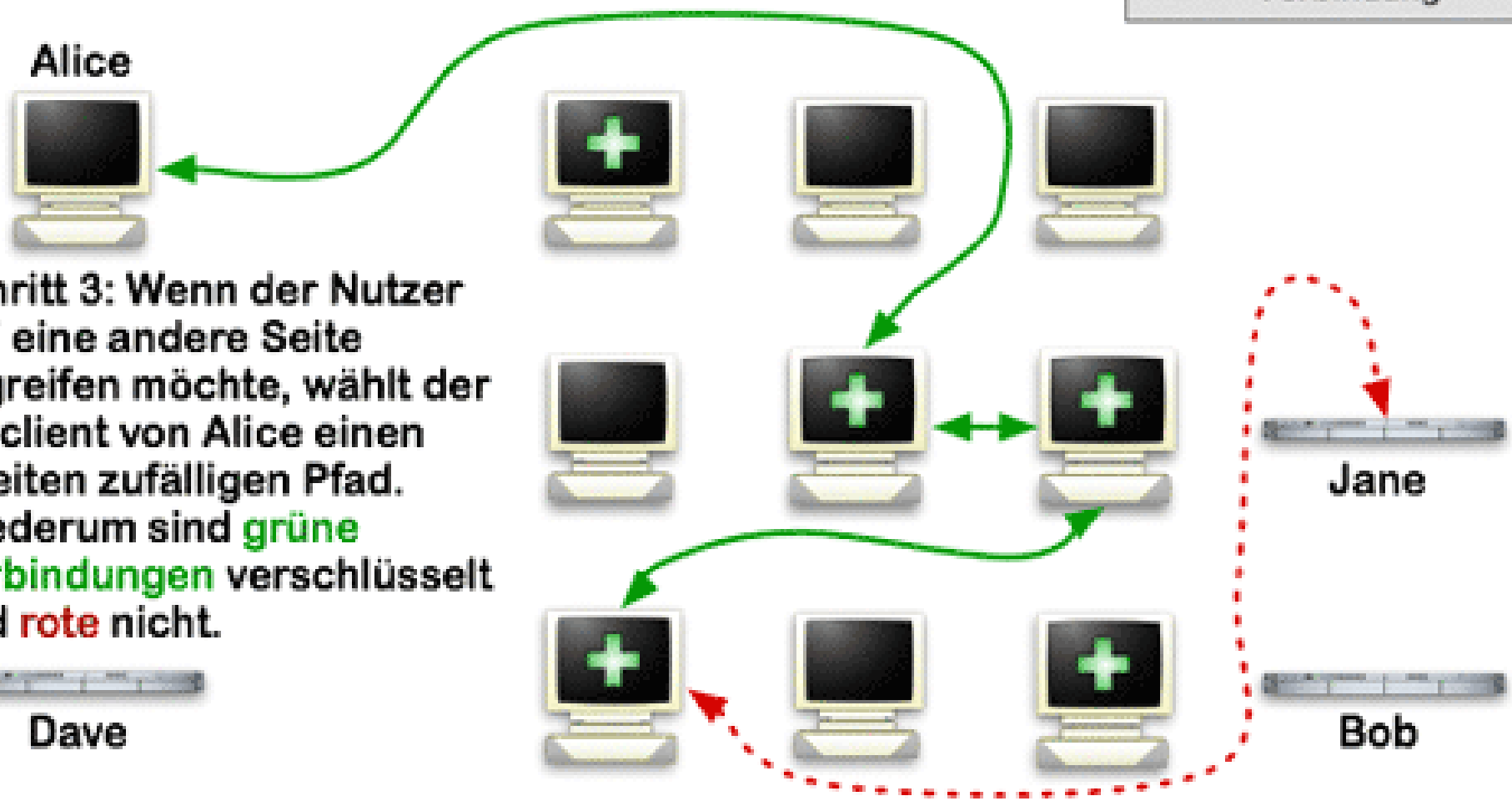
# Wie Tor funktioniert: 1


# Wie Tor funktioniert: 2


Schritt 2: Der Torclient von Alice wählt einen zufälligen Pfad zum Zielserver.
Grüne Verbindungen sind verschlüsselt, rote Verbindungen nicht.

# Wie Tor funktioniert: 3


Schritt 3: Wenn der Nutzer auf eine andere Seite zugreifen möchte, wählt der Torclient von Alice einen zweiten zufälligen Pfad. Wiederum sind grüne Verbindungen verschlüsselt und rote nicht.