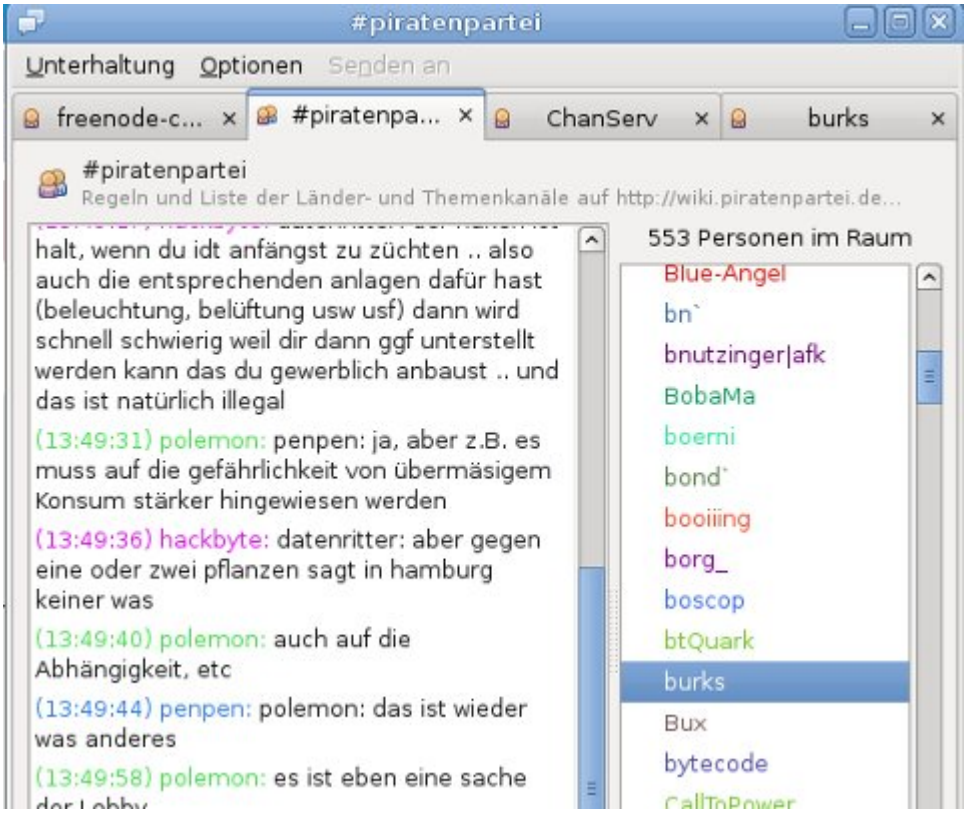
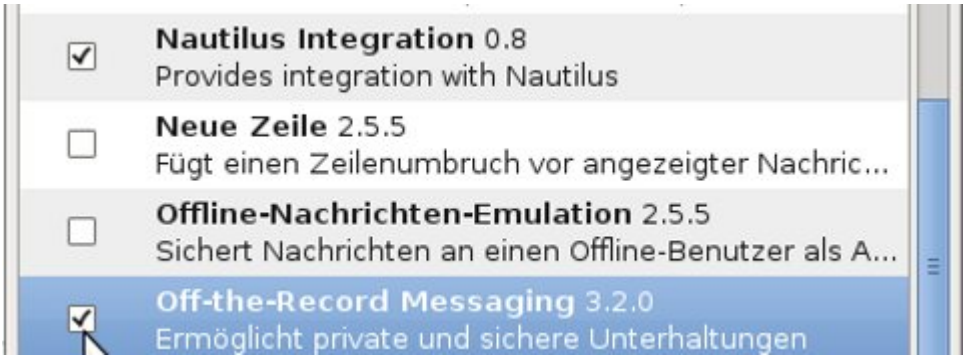
OTR (Off-the-Record Messaging)



Auf einer [Website der Piratenpartei] hat jemand [Off-the-Record Messaging] beschrieben. Das habe ich mir mal genauer angesehen.

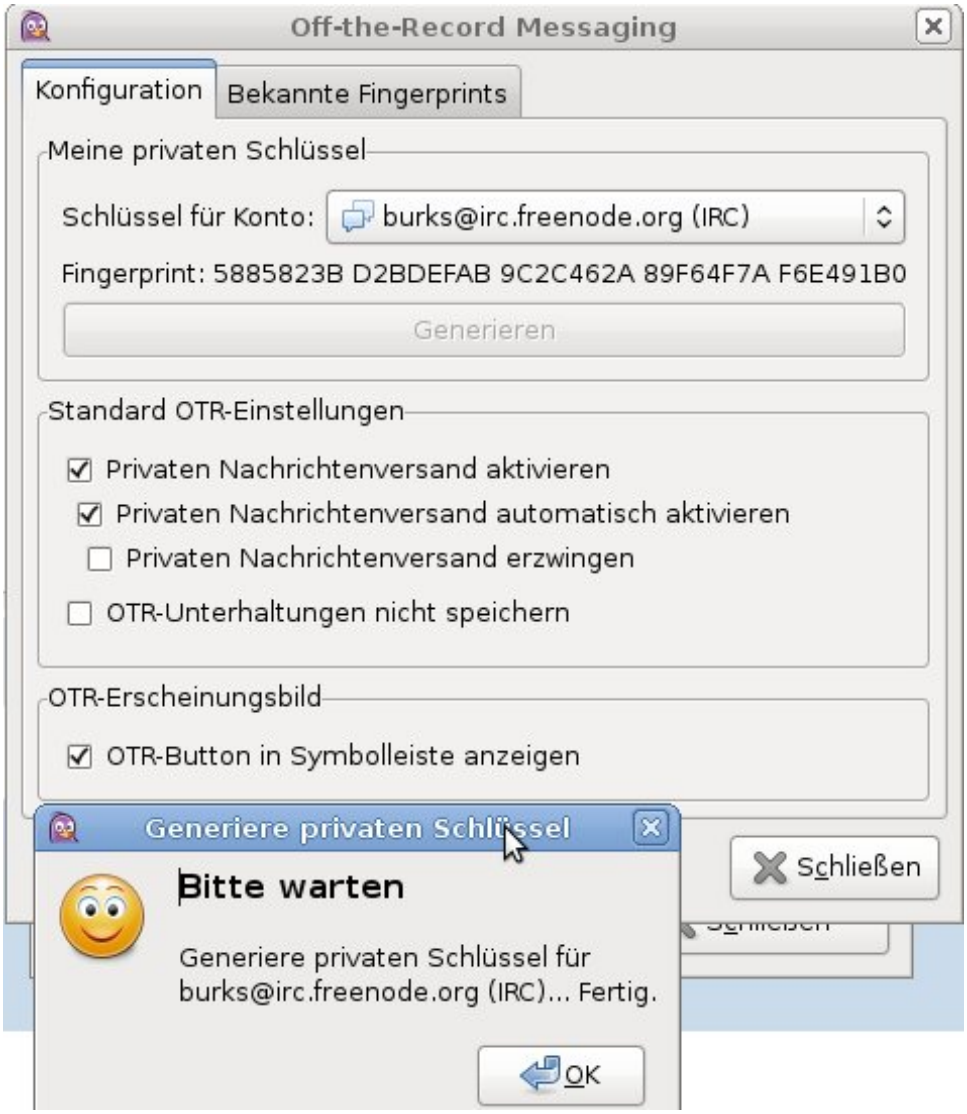
Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:
Encryption: No one else can read your instant messages.
Authentication: You are assured the correspondent is who you think it is.
Deniability: The messages you send do not have digital signatures 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.



Das habe ich sofort ausprobiert. Im Forum der German Privacy Foundation schrieb jemand: „OTR ist für Instant-Messaging das, was OpenPGP für E-Mails ist. Unter Ubuntu (was für Dich interessant sein dürfte) installiert man das Pidgin-OTR-PlugIn, ist bereits alles vorhanden. (Man kann auch OpenPGP für Instant-Messaging nutzen, aber OTR ist wahrscheinlich weiter verbreitet.)“

Und: „Auch das OTR-PlugIn ist schon unter Ubuntu mit dabei. Wenn Pidgin gestartet ist, findest Du es bei Werkzeuge/Plugins. Auf den OTR-PlugIn-Eintrag den Haken setzen und dann „Plugin konfigurieren“ wählen. Jetzt nur noch für das entsprechenden Netzwerk den Schlüssel „Generieren“. Mit seinen Chattpartner, welcher natürlich ebenfalls OTR nutzt, sollte man sich jedoch noch die Schlüssel gegenseitig beglaubigen.“ (Der Link zum FreheIT-Bblog „Verschlüsseltes Instant Messaging- Teil 2: Pidgin“, Anleitung für Windows) Funktioniert wunderbar.


Off-the-Record Messaging
Konfiguration
Bekannte Fingerprints
Meine privaten Schlüssel
Schlüssel für Konto:
burks@irc.freenode.org (IRC)
Fingerprint: 5885823B D2BDEFAB 9C2C462A 89F64F7A F6E491B0
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
Schließen
Generiere privaten Schlüssel
Bitte warten
Generiere privaten Schlüssel für
burks@irc.freenode.org (IRC)... Fertig.
OK