Kurzanleitung XMPP-OTR / OpenPGP

Version 1.1, 31.05.2015

XMPP

- *normale Kontakte hinzufügen*

  Wenn man mit einem vernetzten (*XMPP federation*) Server verbunden ist (im Gegensatz zu z.B. Facebook), kann man mit den Nutzern der anderen vernetzten Server kommunizieren. Neue Kontakte werden einem als offline angezeigt, solange die Gegenseite einen nicht für Statusupdates autorisiert hat. Oftmals werden Offline-Kontakte (inklusive nicht-autorisierte) standardmäßig gar nicht angezeigt.

  - **Pidgin:** [Buddy-Liste] *Buddys* → *Buddy hinzufügen*

    [aus einem Gespräch heraus] *Unterhaltung* → *hinzufügen*

    Man kann seine Kontakte in Gruppen sortieren (denselben Kontakt auch in mehreren Gruppen haben). Der *Alias* ist eine beliebige (optonale) Bezeichnung, die statt der Adresse angezeigt wird.

    Kontakte lassen sich aus einem Chatraum heraus indirekt hinzufügen.
  - **Adium:** [Menü] Kontakt → Kontakt hinzufügen → bei Dienst *XMPP* auswählen

    Hier kann der Kontakt auch in Gruppen einsortiert werden und ein Alias vergeben werden.

- *Passwort ändern*
  - **Pidgin:** [Buddy-Liste] *Konten* → [Konto auswählen → Untermenü] → *Passwort ändern*
  - **Adium:** [Menü] Adium → Einstellungen → Konten → [Konto auswählen] → mit der rechten Maustaste klicken (bzw. Str/Ctrl beim Klicken drücken) →> Passwort ändern

OTR

Die Standardeinstellung sollte sein, dass das Chatprogramm automatisch erkennt, dass die Gegenstelle OTR unterstützt. Dabei geht allerdings die erste Nachricht unverschlüsselt raus, wenn man nicht vorher selber Verschlüsselung für das jeweilige Gespräch aktiviert.

- *verschlüsselte Verbindung aufbauen*
  - **Pidgin:** [Chatfenster] Schaltfläche unten rechts zeigt: `nicht privat`
    Klick auf die Schaltfläche, Aktion *Private Unterhaltung starten* auswählen.
  - **Adium:** [Chatfenster] Das Vorhängeschloss oben links ist geöffnet.
    Klick darauf, *Verschlüsselte OTR-Unterhaltung einleiten* auswählen.
- *Schlüssel verifizieren*
  - **Pidgin:** [Chatfenster] Schaltfläche unten rechts zeigt: `unverifiziert`

    1. Klick auf die Schaltfläche, Aktion *Buddy authentifizieren* auswählen.
    2. Authentifizierungsmethode auswählen: *manueller Fingerprint-Vergleich*
    3. Fingerprint vergleichen (nur bei einem Kommunikationspartner erforderlich)
    4. auf *ich habe überprüft* umschalten
    5. auf *Authentifizieren* klicken

    Ein Fingerprint kann auch außerhalb einer OTR-Session bestätigt werden, und zwar über die Konfiguration des OTR-Plugins.
  - **Adium:** Adium: [Chatfenster] Wenn eine OTR-Session mit einem nicht verifizierten Kontakt beginnt, erscheint ein Hinweis: *“[Kontakt] hat Ihnen ([Deine Adresse]) einen unbekannten Fingerabdruck geschickt. […] Wollen Sie diesen Fingerabruck akzeptieren?”*

    Mögliche Auswahl ist zwischen *Später überprüfen* und *Akzeptieren*.

    In beiden Fällen beginnt anschließend die OTR-Session. Der Fingerabdruck kann jederzeit bestätigt oder abgelehnt werden: Im Chatfenster Klick auf das Vorhängeschloss, dann *Überprüfen* auswählen.

OpenPGP (Enigmail 1.8.x)

- *neue Kontakte / Zertifikate hinzufügen*
  1. *importieren*
     - *von Keyserver importieren*
       - [Menüleiste] *Enigmail* → *Schlüssel verwalten*
         [Menüleiste Schlüsselverwaltung] *Schlüsselserver* → *Schlüssel suchen*
         Name, E-Mail-Adresse oder Key-ID (0x12345678) eingeben.
     - *aus einer Datei importieren*
       - [Menüleiste] *Enigmail* → *Schlüssel verwalten*
         [Menüleiste Schlüsselverwaltung] *Datei* → *importieren*
         (Import möglich aus ASCII- (**.asc*) und Binärdateien (**.gpg*).
     - *aus einem Mailanhang importieren*
       - [Rechtsklick auf die Zertifikatsdatei] → *OpenPGP-Schlüssel importieren*
  2. *signieren (zertifizieren)*
     [Menüleiste] *Enigmail* → *Schlüssel verwalten*
     [Rechtsklick auf das zu signierende Zertifikat] → *unterschreiben*
     - Fingerprint prüfen (**Vergleichswert aus sicherer Quelle!**)
     - falls mehrere vorhanden: den privaten Schlüssel auswählen, der signieren soll
     - sinnvolle Auswahl des Zertifizierungslevels
     - Option *lokal unterschreiben* auswählen (solange man es nicht besser weiß)
- *Passphrase ändern*
  - [Mailfenster] [Rechtsklick auf den Schlüssel oder Schlüssel mit Linksklick markieren und dann im Menü *Bearbeiten*] → *Passphrase ändern*
- *verschlüsselte Mail an unsignierten Schlüssel schicken*
  - [Mailfenster Menüleiste] *Enigmail* → *Temporär den Schlüsseln aller Empfänger vertrauen*
    Wenn man das vergisst, gibt es eine wenig hilfreiche Fehlermeldung.
  - Warnung (bis mindestens Enigmail 1.8.1): Das Häkchen bleibt bei weiteren neuen Mails gesetzt, bis es manuell gelöscht wird. Das gilt absurderweise getrennt für die beiden Gruppen neue Mails und Antworten (inklusive Weiterleitungen).
    Es empfiehlt sich daher, nach dem Versenden oder Beantworten / Weiterleiten einer Mail diese Einstellung sofort zurückzunehmen, damit man später nicht vergisst nachzusehen.