

Šifrovano ćaskanje za Linuks

CRYPTOPARTY SERBIA

November 24, 2016

Contents

| | | |
|----------|--|-----------|
| 1 | Kratak uvod | 2 |
| 1.1 | Napomene | 2 |
| 2 | Preuzimanje i Instaliranje Pidgin-a | 3 |
| 3 | Podešavanje naloga | 4 |
| 4 | Generisanje OTR ključa | 7 |
| 5 | Dodavanje kontakta | 10 |
| 6 | Šifrovana konverzacija | 12 |

1 Kratak uvod

Ovo uputstvo će vam pomoći da instalirate **Pidgin**, program otvorenog koda (eng. open-source) na Linuks-u (Ubuntu) i pomoću njega šifrujete konverzaciju (eng. instant messaging) sa vašim kontaktima. Postoje i drugi programi otvorenog koda za ovu namenu poput Jitsi-ja i Gajim-a koi su kao i Pidgin multiplatformski.

Pidgin podržava preko petnaest protokola, ali mi ćemo pokazati podešavanja na primeru XMPP protokola. Za šifrovanje se koristi OTR dodatak (eng. plugin), koji šifruje tekstualne poruke između vas i vašeg sagovornika.

1.1 Napomene

OTR protokol ne podržava grupno šifrovano dopisivanje, kao ni šifrovanu razmenu fajlova, već samo tekstualne poruke. Međutim koristeći OTR možete se sa sagovornikom dogovoriti oko tajne šifre tokom dopisivanja, a zatim drugim programom šifrovati fajl dogovorenim šifrom pre slanja, i tek onda izvršiti slanje.

OTR protokol je nezavistan od protokola/servisa koji koristite za komunikaciju pa ćete tako moći da ga koristite za privatnu konverzaciju i preko IRC-a, Google Talk-a, Yahoo Messinger-a i drugih, dok god i vaš sagovornik koristi isti protokol, kao što se ne možete dopisivati ako koristiti Yahoo Messinger, a sagovornik IRC.

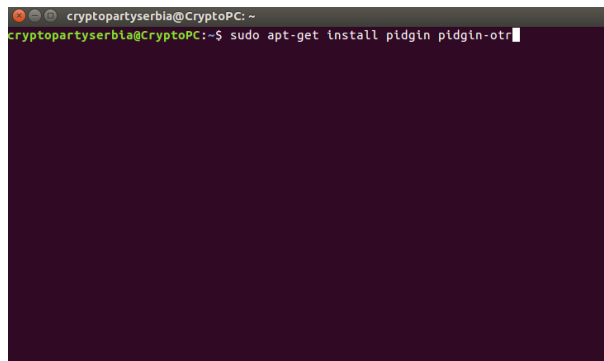
OTR funkcioniše samo ako ga koriste obe strane u komunikaciji.

2 Preuzimanje i Instaliranje Pidgin-a

Kako bi ste instalirali Pidgin na Ubuntu (i drugim distribucijama zasnovanim na Debian-u) izvršite sledeću komandu iz terminala:

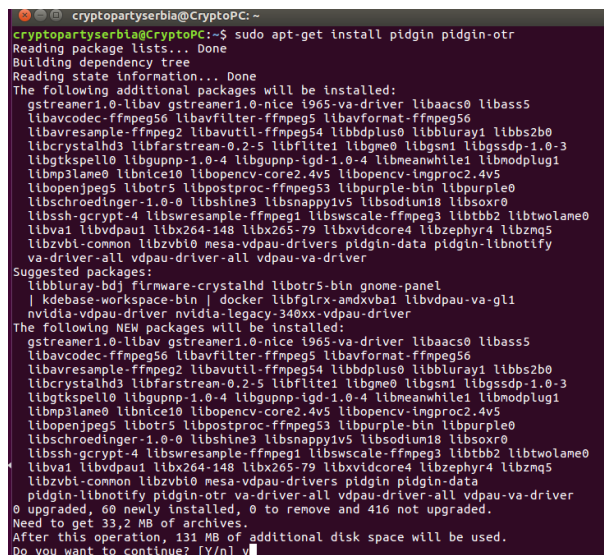
```
# apt-get install pidgin pidgin-otr
```

Ova komanda će instalirati Pidgin i OTR dodatak za Pidgin za vas na vašem računaru.



```
cryptopartyserbia@CryptoPC: ~  
cryptopartyserbia@CryptoPC:~$ sudo apt-get install pidgin pidgin-otr
```

Figure 1: Instalirajte Pidgin i OTR dodatak za Pidgin.



```
cryptopartyserbia@CryptoPC: ~  
cryptopartyserbia@CryptoPC:~$ sudo apt-get install pidgin pidgin-otr  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  gstreamer1.0-libav gstreamer1.0-nice i965-va-driver libaacs0 libass5  
  libavcodec-ffmpeg56 libavfilter-ffmpeg5 libavformat-ffmpeg56  
  libavresample-ffmpeg2 libavutil-ffmpeg54 libbdplus0 libbluray1 libbs2b0  
  libcrystalhd3 libfarstream-0.2.5 libflite1 libgnue0 libgsml libgssdp-1.0-3  
  libgtkspell0 libgupnp-1.0-4 libgupnp-igd-1.0-4 libmeanwhile1 libmodplug1  
  libmp3lame0 libnice10 libopenvc-core2.4v5 libopenvc-lingproc2.4v5  
  libopenjpeg5 libotr5 libpostproc-ffmpeg53 libpurple-bin libpurple0  
  libschroedinger-1.0-0 libshlne3 libsnappy1v5 libsodium18 libsoxr0  
  libssh-gcrypt-4 libswresample-ffmpeg1 libswscale-ffmpeg3 libtbb2 libtwolame0  
  libva1 libvdpau1 libx264-148 libx265-79 libxvidcore4 libzephyr4 libzmq5  
  libzvt-common libzvt0 mesa-vdpau-drivers pidgin-data pidgin-libnotify  
  va-driver-all vdpau-driver-all vdpau-va-driver  
Suggested packages:  
  libbluray-bdj firmware-crystalhd libotr5-bin gnome-panel  
  | kdebase-workspace-bin | docker libglx-amdxbai libvdpau-va-gli  
  nvidia-vdpau-driver nvidia-legacy-340xx-vdpau-driver  
The following NEW packages will be installed:  
  gstreamer1.0-libav gstreamer1.0-nice i965-va-driver libaacs0 libass5  
  libavcodec-ffmpeg56 libavfilter-ffmpeg5 libavformat-ffmpeg56  
  libavresample-ffmpeg2 libavutil-ffmpeg54 libbdplus0 libbluray1 libbs2b0  
  libcrystalhd3 libfarstream-0.2.5 libflite1 libgnue0 libgsml libgssdp-1.0-3  
  libgtkspell0 libgupnp-1.0-4 libgupnp-igd-1.0-4 libmeanwhile1 libmodplug1  
  libmp3lame0 libnice10 libopenvc-core2.4v5 libopenvc-lingproc2.4v5  
  libopenjpeg5 libotr5 libpostproc-ffmpeg53 libpurple-bin libpurple0  
  libschroedinger-1.0-0 libshlne3 libsnappy1v5 libsodium18 libsoxr0  
  libssh-gcrypt-4 libswresample-ffmpeg1 libswscale-ffmpeg3 libtbb2 libtwolame0  
  libva1 libvdpau1 libx264-148 libx265-79 libxvidcore4 libzephyr4 libzmq5  
  libzvt-common libzvt0 mesa-vdpau-drivers pidgin-data pidgin-libnotify  
  va-driver-all vdpau-driver-all vdpau-va-driver  
0 upgraded, 60 newly installed, 0 to remove and 416 not upgraded.  
Need to get 33,2 MB of archives.  
After this operation, 131 MB of additional disk space will be used.  
Do you want to continue? [Y/n] y
```

Figure 2: Prihvatite instalaciju potrebnih biblioteka.

3 Podašavanje naloga

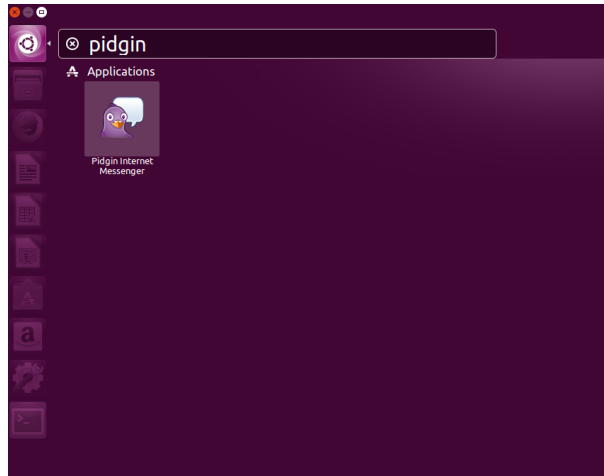


Figure 3: Kada ste instalirali Pidgin pokrenite ga.

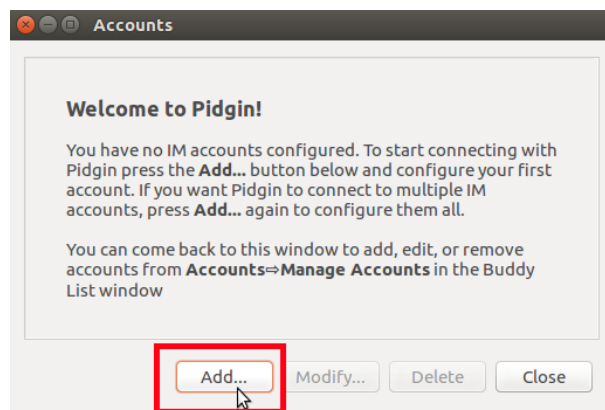


Figure 4: Otvoriće se prozor sa porukom dobrodošlice i ponuditi da dodate novi nalog. Kliknite "Add...".

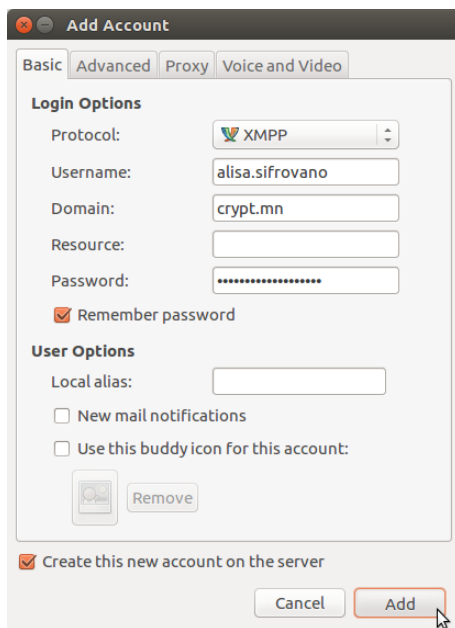


Figure 5: Izaberite XMPP protokol, vaše korisničko ime, server kao i šifru za postojeći ili željeni nalog i ukoliko tek kreirate novi nalog štiklirajte kvadratić "Create this new account on the server", a zatim pritisnite dugme "Add"

Ukoliko nemate već postojeći nalog, unesite željeno korisničko ime (mi koristimo ALISA.SIFROVANO korisničko ime) kao i server (mi koristimo crypt.mn server) i šifru koju želite i onda štiklirajte kvadratić "Create this new account on the server". Ukoliko već imate nalog, nemojte štiklirati kvadratić za kreiranje novog naloga. Ako ne znate koji XMPP server da koristite, listu javnih XMPP servera možete naći na list.jabber.at.

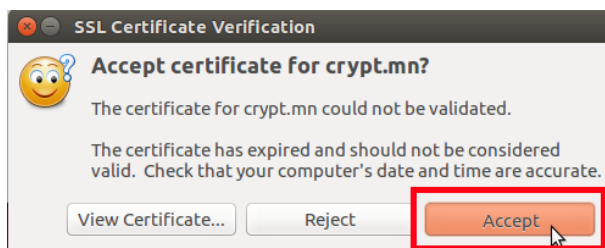


Figure 6: Prikazaće vam se novi prozor sa pitanjem da li želite da prihvatite sertifikat servera na kome imate ili kreirate nalog. To prihvatite. Pritisnite "Accept".

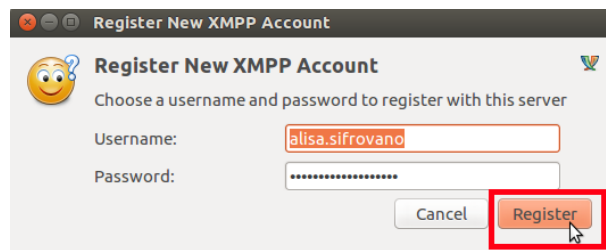


Figure 7: Ipotvrdite vaše korisničko ime i šifru za taj nalog.

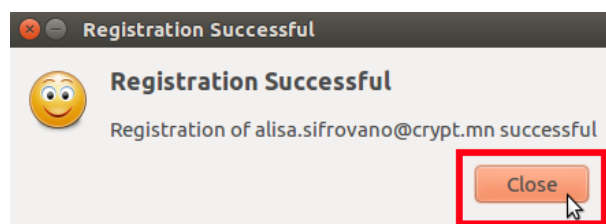


Figure 8: Ako sve prođe kako treba obavestiće vas o uspešno registrovanom nalogu. Pritisnite "Close".

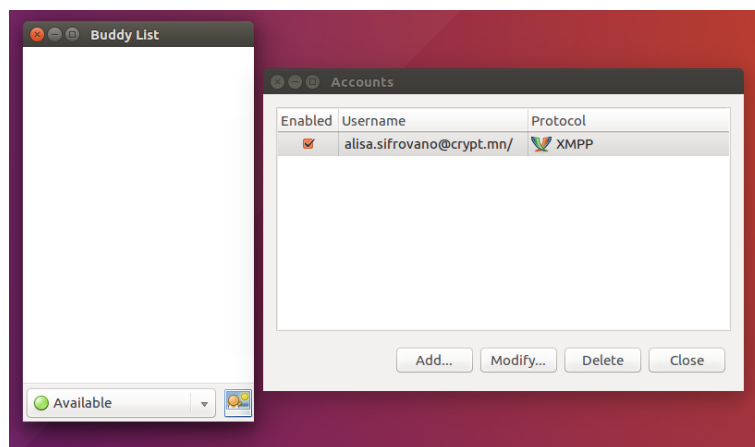


Figure 9: Sada bi trebalo da ste povezani i na vaz (eng. Online). I da pidgin izgleda otprilike ovako.

4 Generisanje OTR ključa

Kada ste podesili vaš nalog potrebno je da generišete vaš jedinstveni OTR ključ kako bi kasnije mogli da privatno časkate razmenjujući šifrovane poruke.

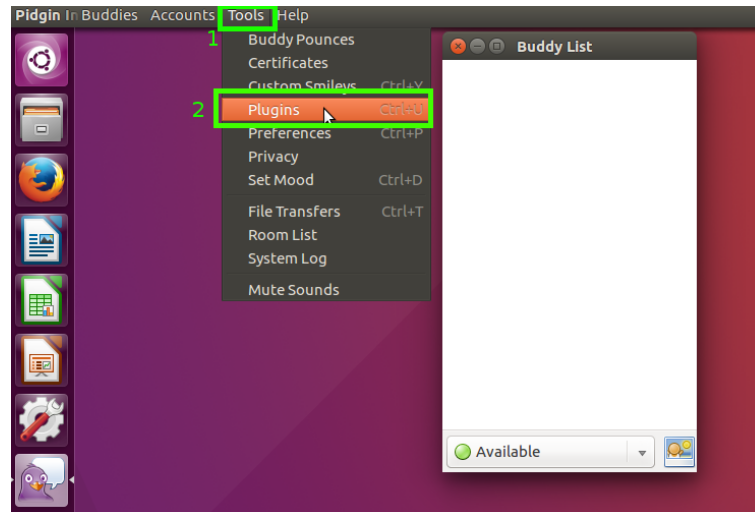


Figure 10: Idite na "Tools" pa "Plugins".

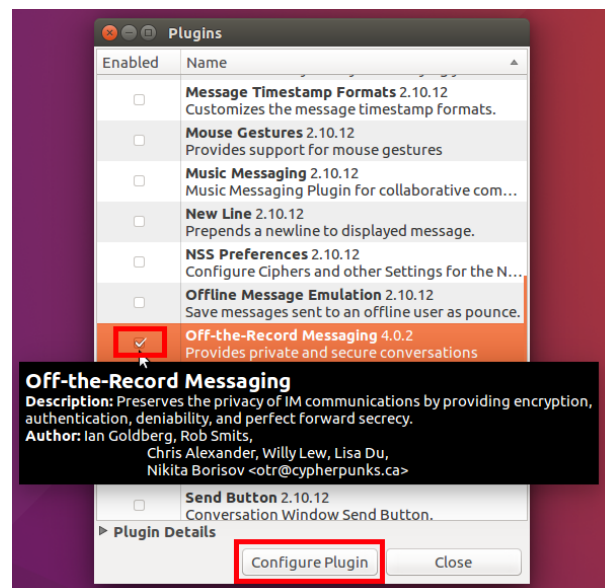


Figure 11: Štiklirajte kvadratić ispred dodatka "Off-The-Reccord Messaging", a zatim pritisnite "Configure".

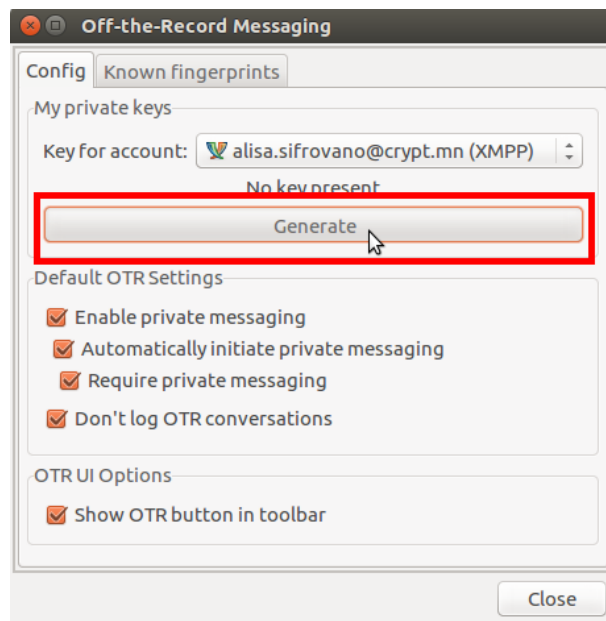


Figure 12: Otvoriće se novi prozoru kome treba da pritisnete dugme Generate da bi ste generisali svoj novi i jedinstveni OTR ključ. Takođe trebalo bi da štiklirate sve kvadratiće u tom istom prozoru kako bi olakšavaju kasnije šifrovanje konverzacija, ne bi čuvali logove, i automatski zahtevali šifrovanu konverzaciju sa sagovornikom.

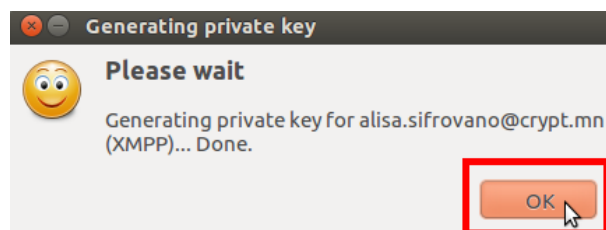


Figure 13: Morate malo sačekati da se OTR ključ generiše.

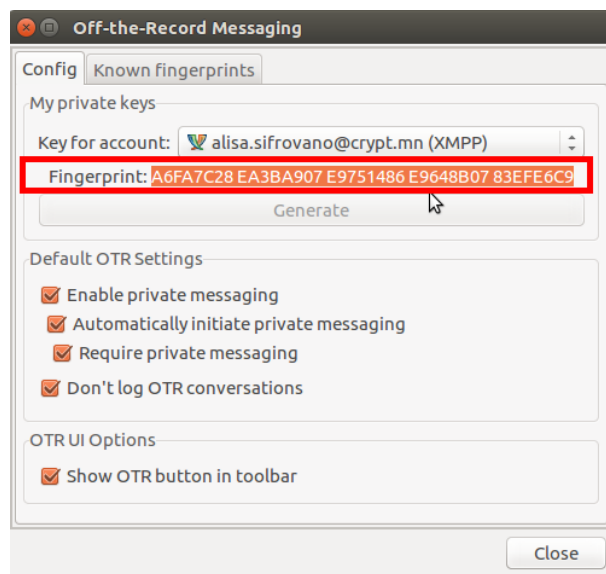


Figure 14: Kada se ključ generiše prikazaćevam se OTR otisak (eng. OTR fingerprint) dužine 40 heksadekadnih karaktera. To je vaš javniotisak koga možete objaviti, a svakako ga moraju znati osobe koje žele da sa vama šifrovano komuniciraju koristeći OTR.

5 Dodavanje kontakta

Kada imate namešten XMPP nalog i OTR ključ samo vam fali još kontakt sa kojim možete šifrovano da razmenjujete poruke. Ono što treba naglasiti je da i kontakt osoba mora koristiti isti protokol kako bi ste komunicirali sa njom, i da mora imati svoj OTR ključ. Međutim kontakt osoba ne mora imati nalog na istom serveru na kome imate i vi, samo je važno da ima nalog na nekom XMPP serveru kao i vi.

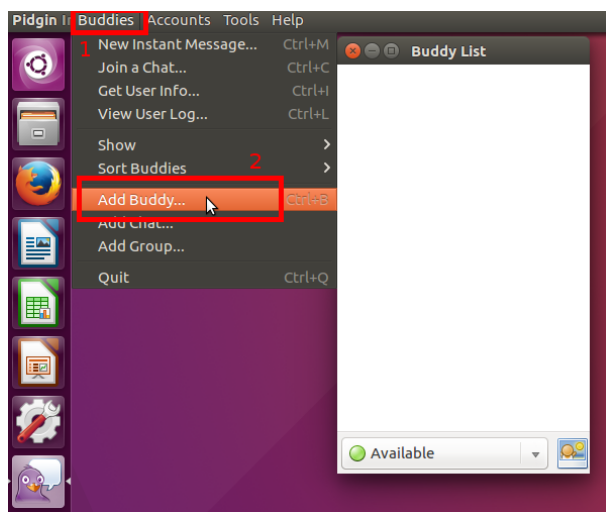


Figure 15: Izaberite "Buddies" -> "Add buddy..."

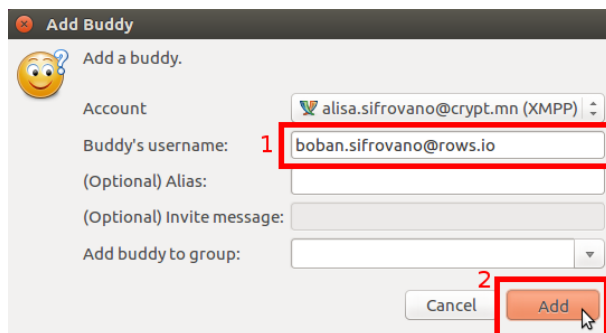


Figure 16: U novootvorenom prozoru unesite puni ID vašeg kontakta (u našem slučaju to je BOBAN.SIFROVANO@ROWS.IO) i eventualno ime tog kontakta.

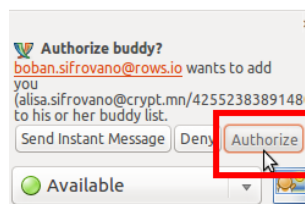
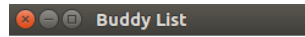


Figure 17: Kada dodate novog kontakta, njemu će stići obaveštenje da ste ga dodali i da želite da stupite u kontakt sa njime. Ovo obaveštenje može stići i vama ukoliko vas neko doda za svog kontakta. Ukoliko vaš zahtev prihvati, ili vi njegov, oboje nakon toga možete stupiti u dalju konverzaciju.

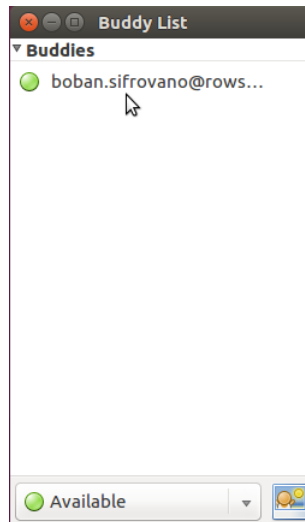


Figure 18: Nakon čega bi vaš glavni Pidgin prozor trebalo da izgleda ovako.

6 Šifrovana konverzacija

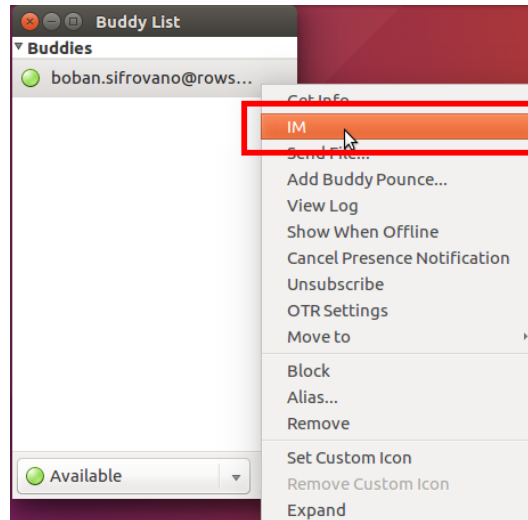


Figure 19: Kada imate kontakta, možete započeti konverzaciju. Desni klik na kontakta, pa "IM".

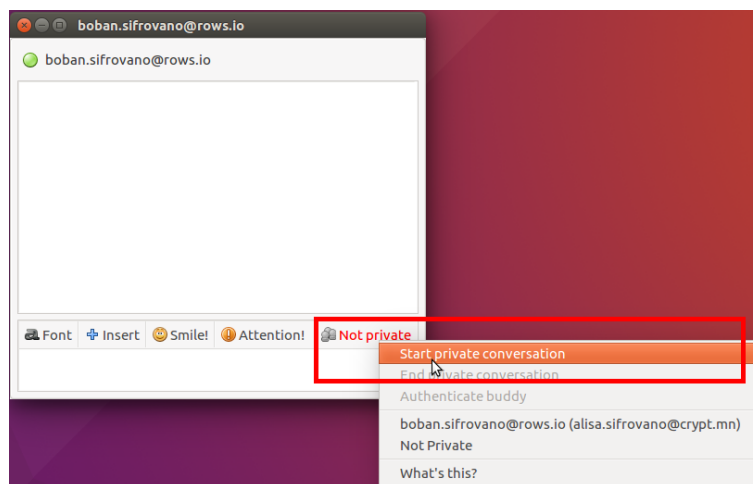


Figure 20: Sada kada imate i kontakta možete započeti konverzaciju. Samo što ona neće biti šifrovana dok to sami ne omogućite. Pritisnite crveno dugme "Not Private" u donjem desnom uglu prozora započete konverzacije, pa "Start private conversation" kako bi ste započeli šifrovanu konverzaciju.

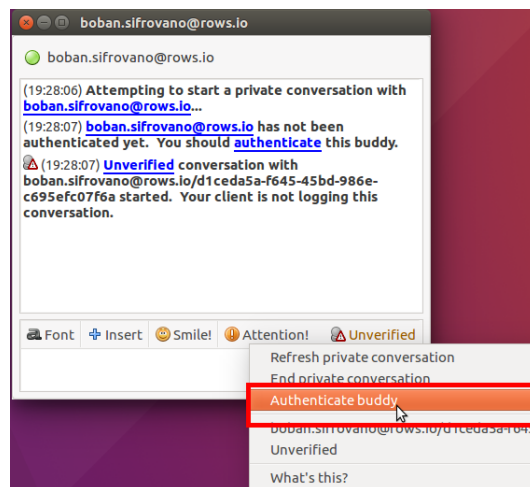


Figure 21: Posle čega je potrebno da verifikujete sagovornika iako je dalja konverzacija šifrovana kako bi bili sigurni da neki napadač izmedju vas i vašeg kontakta ne pokušava da vas prevari i predstavi se kao vaš kontakt (tzv. MiTM napad). Pritisnite "Unverified" pa "Authenticate buddy".

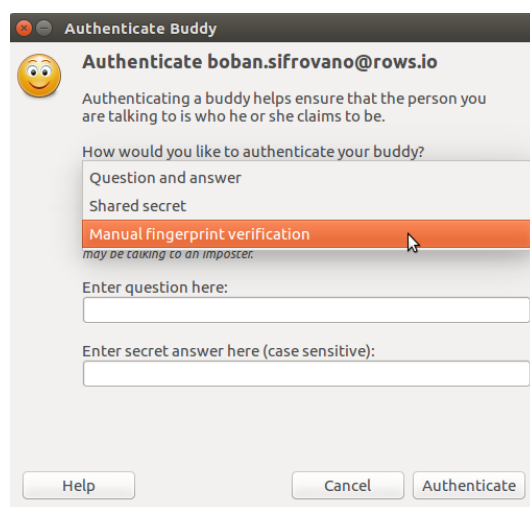


Figure 22: Nakon toga otvoriće sa novi prozor za verifikaciju kontakta. Izaberite metod verifikacije (preko pitanja i odgovora, zajedničke tajne, ili jednostavno uporedite OTR otiske).

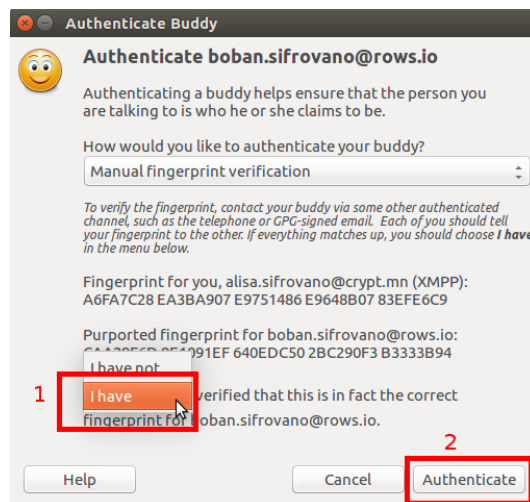


Figure 23: Mi bira mo upoređivanje OTR otisaka jer je naš sagovornik u istoj prostoriji pa možemo se uveriti da je to baš njegov OTR otisak. Izaberite "I have" i onda "Authenticate". Možete odabrati i druge načine verifikacije putem deljenja tajne (ukoliko ste ste oko tajne predhodnodogovorili) ili pitanja-i-odgovora ako poznajete kontakta (ukoliko lično poznajete kontakta i zante pitanje na koje samo on može odgovoriti).

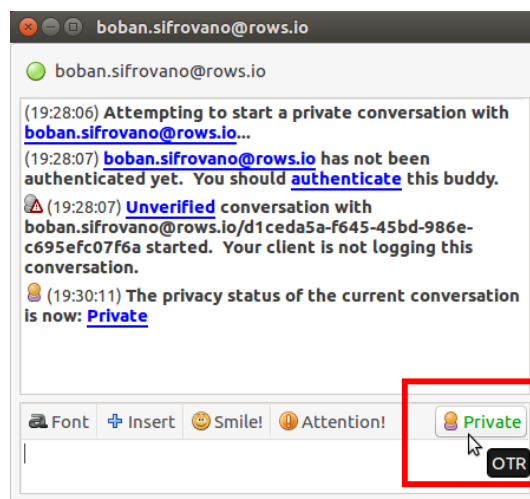


Figure 24: Nakon toga sva dalja konverzacija je šifrovana End-To-End.