How To Encrypt Chat And VoIP With Jitsi and XMPP

 pillowfortress.wordpress.com/2013/08/01/how-to-encrypt-chat-and-voip-with-jitsi-and-xmpp/

Posted: 1 August 2013 | **Author:** Building20 | **Filed under:** | **Tags:** , , , , , , , , |

- Secure alternative to: Skype, Google Talk/Chat

This guide will show how to set up encrypted off-the-record (OTR) chat and VoIP using ZRTP encryption in the following three sections:

- Section 1 will show how to **register with an XMPP service**, here **dukgo.com**.
- Section 2 will show how to **set up XMPP with Jitsi**.
- Section 3 will show how to find friends and initiate chat using **end-to-end OTR encryption** and **secure VoIP calls using ZRTP**, so no one but you and the receiver can read your messages or hear your conversations (and not a government or private company).

Note that in my experience chat works great, whereas VoIP calls are inconsistent in terms of voice and video quality.

Section 1: Register with dukgo.com

- **Step 1**: Register with an XMPP client (once called “Jabber”), in this example dukgo.com at https://dukgo.com/my/register. (There are many XMPP clients, not just dukgo.com; see the additional notes at the end for more information.)
- **Step 2**: Register an account (see Figure 1). Save your username and unique and long password somewhere safe (perhaps using KeePassX, for example).

Figure 1: Registering at dukgo.com

Section 2: Set up Jitsi

- **Step 1**: Download a stable release of Jitsi for your operating system: https://jitsi.org/Main/. (Gnu/Linux, Mac, and Windows are all supported, with Android coming soon.)
- **Step 2**: If opening Jitsi for the first time, skip the initial set up! Once the program is open, go to “File” and select “Add New Account.”
- **Step 3**: Under “select network,” scroll down to XMPP (see Figure 2).

Figure 2: Select XMPP in Jitsi

- **Step 4**: See Figure 3. Select “Existing XMPP account.” Under XMPP username, put your username like so: username@dukgo.com. Type your password. Click add. You should now appear online in Jitsi.

Figure 3: Set up XMPP with Jitsi

- Optional Step 5: Note that if you select “Remember password” you can set a master password to require a password to launch Jitsi. This is found under Preferences > Security > Passwords > Use a

master password.

Section 3: Set up encryption

You can already use chat and encrypted VoIP. Just add

your friends (see Step 1 below) and chat/call away. Note, however, that your chat is not encrypted and can easily be picked up by 3rd parties. Steps 3–5 assist in setting up encryption for chat.

Find Friends

- **Step 1**: To contact your friends, in the main Jitsi window put their address (e.g., username@dukgo.com) in the "Enter name or number" text box (see Figure 4). After typing their username, add them to your contact list by clicking "Add Contact." They will have to accept your contact request.

Figure 4: Add friends in Jitsi

Encrypted VoIP

- **Step 2**: Encrypted ZRTP VoIP calls should work right away. Just call your contact and click the red-colored ZRTP lock symbol. Once the connection is secured, it will turn green. Note that you may not hear the contact until after a secure connection is established. Once it is green, your call is now encrypted.

Encrypted Chat

- **Step 3:** For chat, a few extra steps are necessary for encryption. In Jitsi, go to Preferences > Security > Chat. Here you will need to generate a fingerprint to allow OTR chat. Select account and click generate. Now next to "Fingerprint" you should see a long combination of numbers and letters.

- **Step 4**: Your unique "fingerprint" will need to be verified by your contacts. This is done by starting a chat with your contact and clicking on the lock symbol (Figure 5).

Figure 5: Initiating OTR encryption in chat

- **Step 5:** Now, verify your contact's fingerprint by clicking on "Verify [contact]," which will appear in the chat window after clicking the lock symbol in Figure 5. A window called "Verifying Buddy" will pop up and you will see both your and your contact's fingerprint there. You should exchange fingerprints with your contact (i.e., you send yours and they sends theirs) using a secure method of communication, preferably an email signed with PGP or a phone call. Once you have it, type their fingerprint into the appropriate text box to verify it.

This step can be frustrating at first and initially may result in some errors, but will get easier the more familiar you are with the process. Note that the 0 symbol in the fingerprint is the number and not the letter, in my experience.

- **Done!** After this, when initiating a chat click the lock symbol in the top right corner of the chat window (again, see Figure 5). If both people have verified fingerprints, the lock symbol will close and you should see a message indicating that your chat is now secure ("Private conversation with X started.").

If the fingerprint of the contact has not been verified, the lock symbol in Figure 5 should have a yellow triangle with an exclamation mark in it, and you may receive notification in a pop-up window that you need

to verify the contact's fingerprint.

Some Additional Notes

I have shown how to register with dukgo.com, the XMPP server of duckduckgo.com. Note that there are many XMPP servers, all of which can communicate with each other given the open protocol of the XMPP service, similar to how different email services communicate with each other regardless of which service you use.

A list of public XMPP servers can be found here: http://xmpp.net/. Make sure to inform yourself of the privacy policy of whatever service you use. For information about dukgo.com's privacy policy, look here:

- https://duckduckgo.com/privacy
- https://duck.co/topic/privacy-questions-regarding-xmpp-server-of-ddg

Note that dukgo.com is hosted in the USA, as far as I know.

A lot of other software supports chat with encrypted OTR (but not necessarily VoIP, unfortunately). I like Jitsi for its cross-platform ease of use as well as its support for encrypted voice and video calls.

Other software that supports OTR chat is as follows. Note that all software in this list is free and open source (FOSS). There are many benefits to using FOSS software—relevant here is that given open access to the source code it is much harder to create hidden backdoor access to 3rd parties, making FOSS software much more secure by design. You can never know for sure what closed, proprietary software is doing since you cannot get access to the source code that makes the program run.

Gnu/Linux

- Pidgin (install pidgin-otr)
- Kopete
- Psi+
- Gajim (OTR?)

Mac OS X

- Adium
- Psi+

Windows

- Pidgin (with plugin for OTR)
- Miranda IM (with plugin for OTR)
- Gajim (OTR?)
- Psi+

Android

- Gibberbot
- Xabber

iPhone

- ChatSecure