Katzen chat client user guide

This guide introduces the Katzen chat client. With Katzen you can securely share one-to-one and group messages with contacts. Katzen relies on Katzenpost, an advanced mixnet system designed for people who have something to say, but who also value their anonymity. Importantly, anonymity is not the same thing as encryption, which protects the *content* of communication over the Internet. Anonymity is about protecting *people*.

For technical information about how Katzenpost and mixnets in general work, see blah [sdsdsd]. To learn more about *why* Katzenpost works as it does, see Frequently asked questions [sdsdsd] .

Installing and starting Katzen

The Katzen client is available as a Docker image or as Python code available from GitHub. To run it, you need a computer that runs or emulates the Linux operating system. (We have tested Katzen on Debian [https://www.debian.org/] and Ubuntu [https://ubuntu.com/].) You can install Katzen by completing one of the following procedures.

Procedure 1. Docker procedure

To prepare to use the Docker image, first install Docker [https://www.docker.com] and Docker Compose [https://docs.docker.com/compose/] or, alternatively, the drop-in daemonless Docker-equivalents Podman [https://podman.io] and Podman Compose [https://docs.podman.io/en/latest/markdown/podman-compose.1.html]. We recommend using Podman because it runs by default without root privileges .

1. On Debian or Ubuntu, Podman can be installed with the following commands (running as superuser). **Apt** will pull in the needed dependencies.

   ```
   # apt update
   # apt install make podman podman-compose
   ```

2. Download the Katzen client from https://katzenpost.network/downloads to a convenient location on your computer.

3. In a terminal, navigate to the directory containing the package and unzip it.

4. In the xxx directory, start the client in a container using the provided Makefile.

   ```
   ~$ make
   ```

Procedure 2. Python code procedure

To prepare to use the Katzen client source code, you need Git and Python3 installed on your Debian or Ubuntu system. Our recommended method of building the application is to run it in a Python virtual environment using the Makefile included with the code.

1. Install the latest Git, Python3, and Make on your system.

   ```
   # apt update
   # apt install git python3 make
   ```

2. Clone the Katzen repository at https://github.com/katzenpost/katzenqt.

3. In the `katzenqt` directory, create a virtual environment, load additional required software, and start the client using the following commands.

   ```
   ~$ python3 -m venv myvenv
   ~$ source myvenv/bin/activate
   ~$ pip install --upgrade pip
   ```

```
~$ pip install 'git+https://github.com/katzenpost/thin_client@a5f87b9623eb34
~$ pip install -e .
~$ make
```

Communicating through the Katzen client

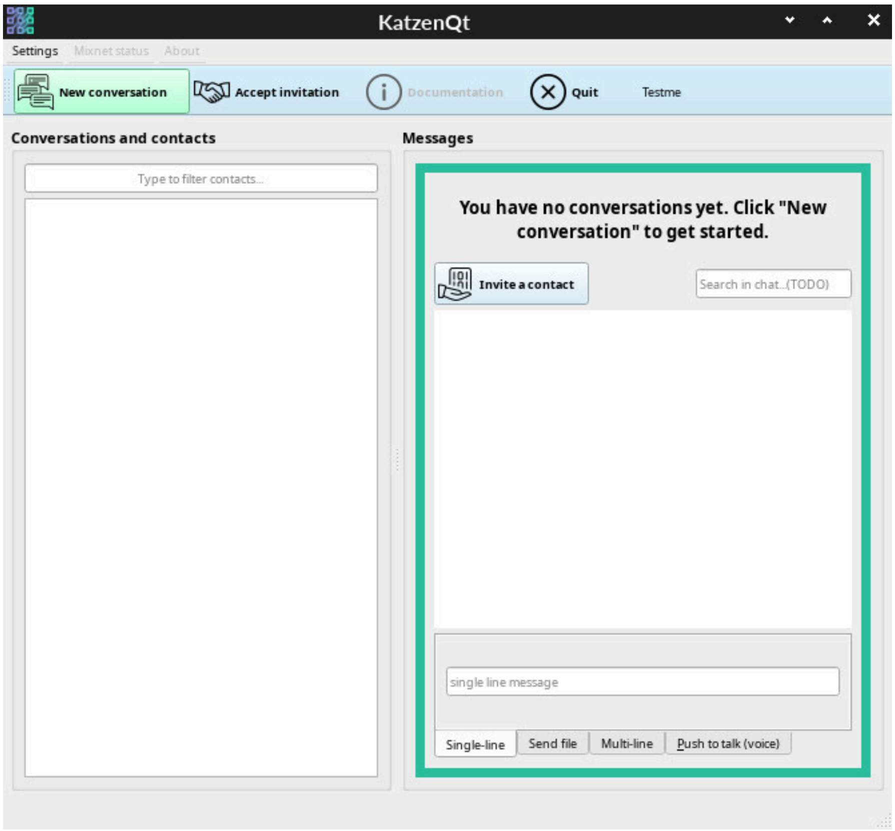
This section describes how to configure and use Katzen for secure, anonymous communication.

Like many other chat clients, Katzenexhibits two panes, one for contacts and one for messages, and a number of communication modes such as text chat, file transfer, and voice. The following illustration shows how Katzen looks when you first open it after installation.

Note

At present, only text chat works. Grayed out elements in the Katzen interface are not yet implemented.

Figure 1. Katzenclient on first use



You have no conversations yet. Click "New conversation" to get started.

Katzen consists of a menu bar, a toolbar, two panes, and a status bar (not visible). The Conversations and contacts displays existing conversations and the contacts specific to them. The Messages pane displays the title of the selected conversation (if any), its messgae log, an Invite a contact button for adding new members, and a text box near the bottom for typing new messages. Buttons in the toolbar include New conversation (opening a dialog to configure a conversation), Accept invitation (opening a dialog to accept or refuse an invitation from another user), Documentation (activating, once implemented, the internal help system), and Quit (which shuts down the client). The tabs at the bottom of the Messages pane allow selection of a communication mode, with only single-line message input currrently implemented.

Despite appearances, Katzen's emphasis on anonymity means that familiar concepts take on new meanings, particularly the idea of a "contact."

- Contact names are arbitrary. Contacts in one conversation are unconnected with contacts in other conversations.
- Katzen and Katzenpost operate with no information about the real-world identities behind contacts. There are no e-mail addresses, telephone numbers, postal addresses, or anything similar involved.
- Without phone numbers or email as anchors for identity, Katzen users require a real-world encounters to verify who they are and to share cryptographic secrets. This kind of contact bootstrapping occurs out-of-band (OOB), that is, without reliance on the primary communication channel. The concept is similar to the key-signing parties that PGP email users employ to build a web of trust [https://en.wikipedia.org/wiki/Web_of_trust], with the difference being that encrypted email provides little anonymity protection.

Consequently, *conversations* are the real organizing principle in Katzen.

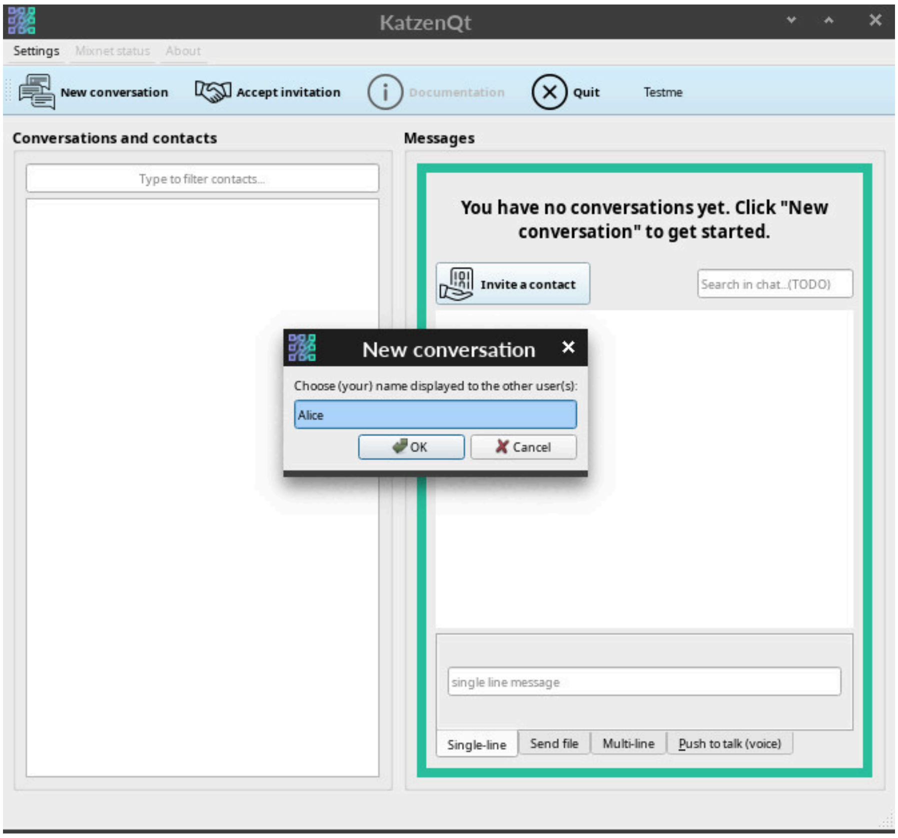
Creating conversations

Communication in Katzen takes place in the context of conversations. A conversation may contain just two particpants, or it may involve a large group. The first thing that a new user of Katzen must do is create a conversation. Each participating contact also creates a conversation.

To create a conversation

1. Open Katzen.
2. In the toolbar, click the New conversation button.
3. In the New conversation window, type a name in the Choose conversation name field. This name is how you identify the conversation in your own Katzen client. It may differ from what your contacts call their corresponding conversations. Click OK when finished.

4. **Figure 2. Creating a conversation – conversation name**



You have no conversations yet. Click "New conversation" to get started.

New conversation

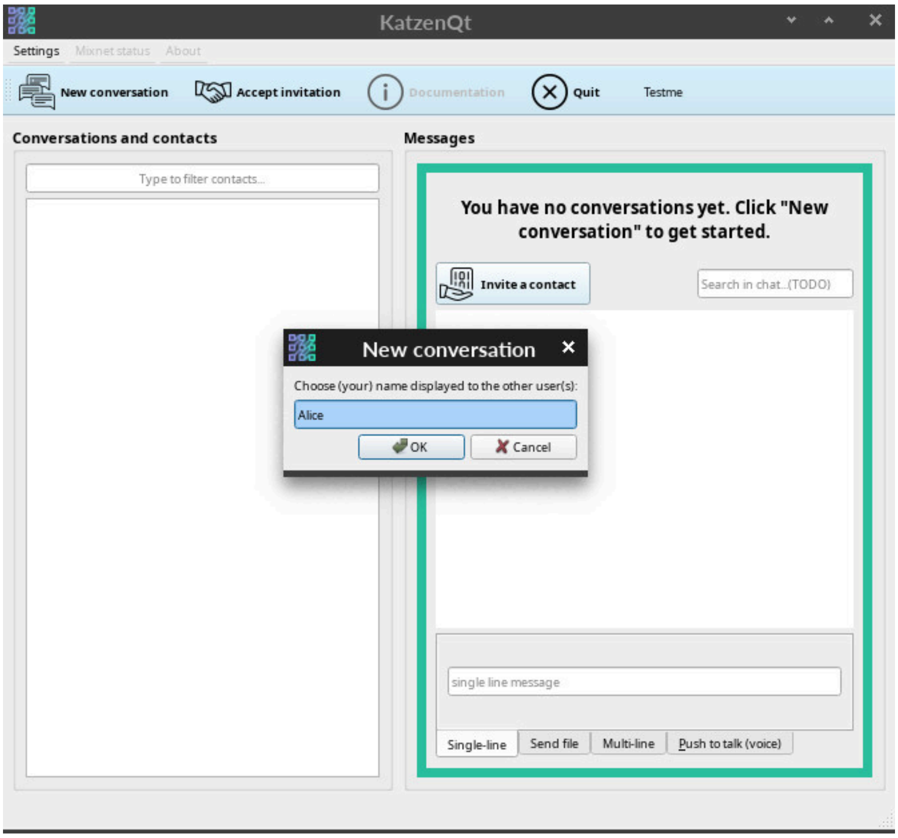
Choose (your) name displayed to the other user(s): Alice

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

5. Type a name for yourself in the field labeled Choose (your) name displayed to the other user(s). Click OK when finished. Your contacts will see this name when the accept your invitation, although they may assign some other name to you[1].

[1] dwrob: Is this actually supported?

Figure 3. Creating a conversation – display name



You have no conversations yet. Click "New conversation" to get started.

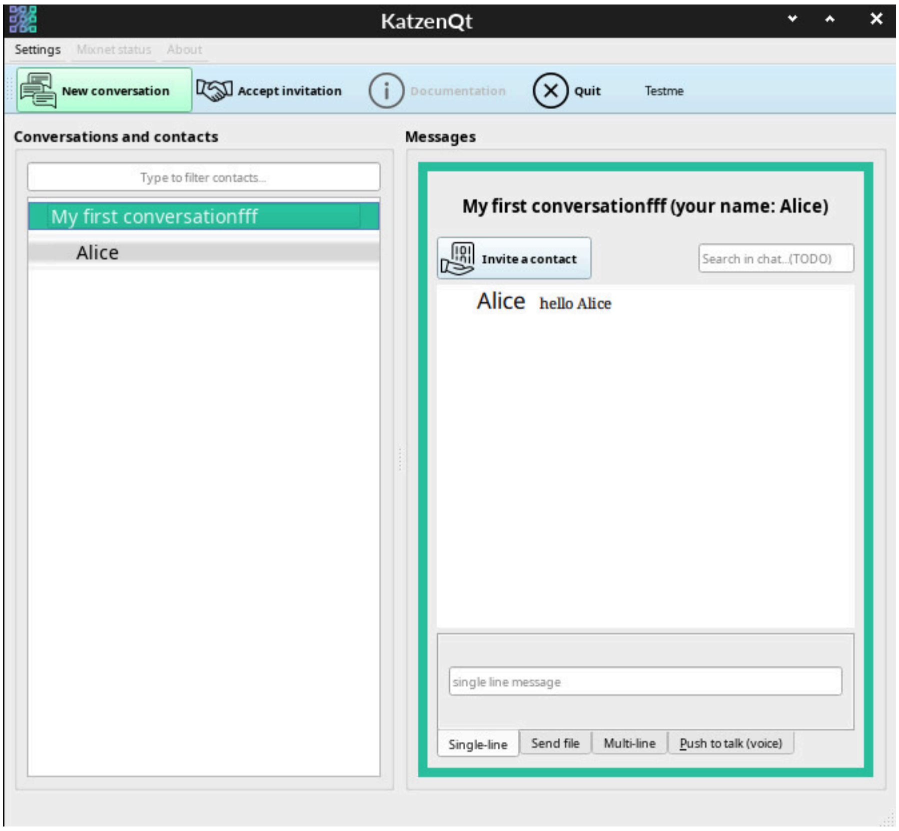
Choose (your) name displayed to the other user(s): Alice

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

In the left pane of the client, labeled Conversations and contacts, the name of your new conversation is displayed along with your own name as the first contact. In the right pane, labeled Messages, Katzen prints a greeting message[2].

[2] dwrob: This should look more like a stage direction than like a regular message.

Figure 4. Creating a conversation – completed



My first conversationfff (your name: Alice)

Alice hello Alice

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

You can create any number[3] of conversations, each completely separate from the others.

Adding contacts to a conversation

Once you have a created a conversation, you can begin adding contacts to it. This requires issuing an invitation that you pass OOB to one or more Katzen users. An invitation is a Base64-encoded string that designates a conversation and offers a display name to represent you there. An Katzen user who receives your invitation accepts it by returning a message, in Katzen, that grants read access to members of your conversation, and also offers a display name. When the process is complete, the new contact's display name will appear in the list of contacts for each participant in the conversation.

Important

We recommend saving the encoded invitation string to a USB drive or to paper, and presenting this physically to the person whom you are inviting. The storage medium should be guarded carefully and either destroyed or securely erased after use.

Warning

It is possible to simply send the invitation to your contact through an existing electronic channel. However, doing this degrades the Katzenpost anonymity protections to the level of anonymity

[3] dwrob: Is there in fact a limitation, other than all available RAM?

offered by the channel you use. *Never do this.* When encryption breaks, the damage, with up-to-date forward secrecy, may be limited in scope. When anonymity breaks, the damage is total.

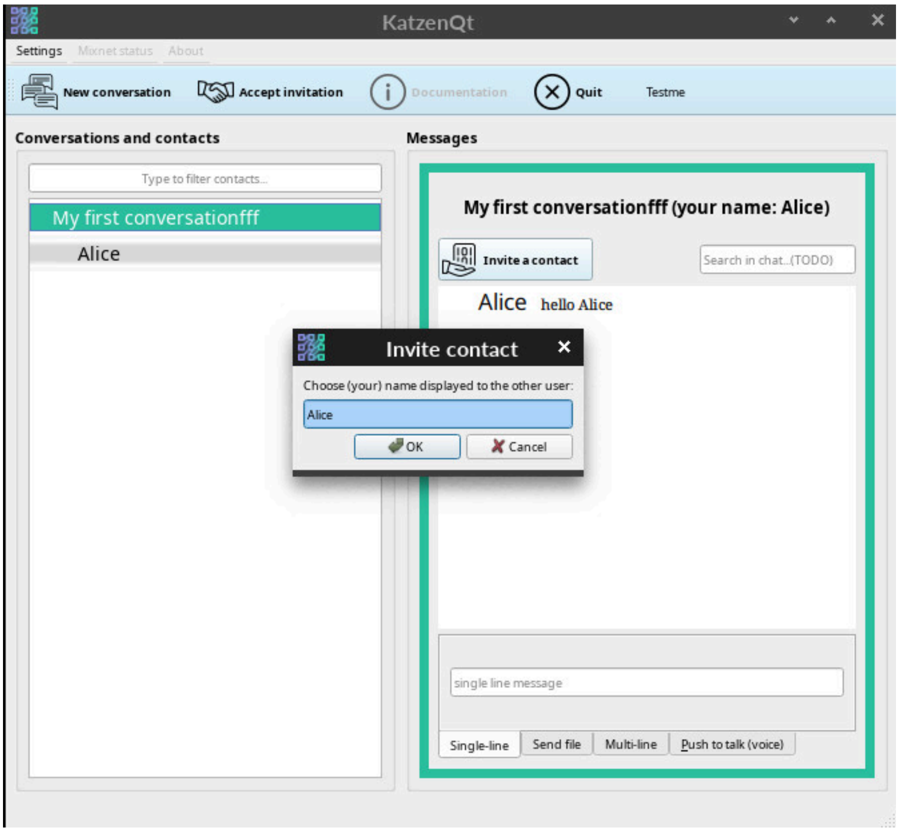
To invite a new contact to a conversation

1. Open Katzen.

2. With the desired conversation selected, in the Messages pane on the right, click Invite a contact.

3. In the Invite contact window, type your desired display name in the field labeled Choose (your) name displayed to the other user, then click OK.

Figure 5. Inviting a contact



My first conversationfff (your name: Alice)

Alice hello Alice

Invite contact

Choose (your) name displayed to the other user: Alice

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

4. STEP MISSING PENDING IMPLEMENTION

5. Provide the invitation string to your intended contact OOB.

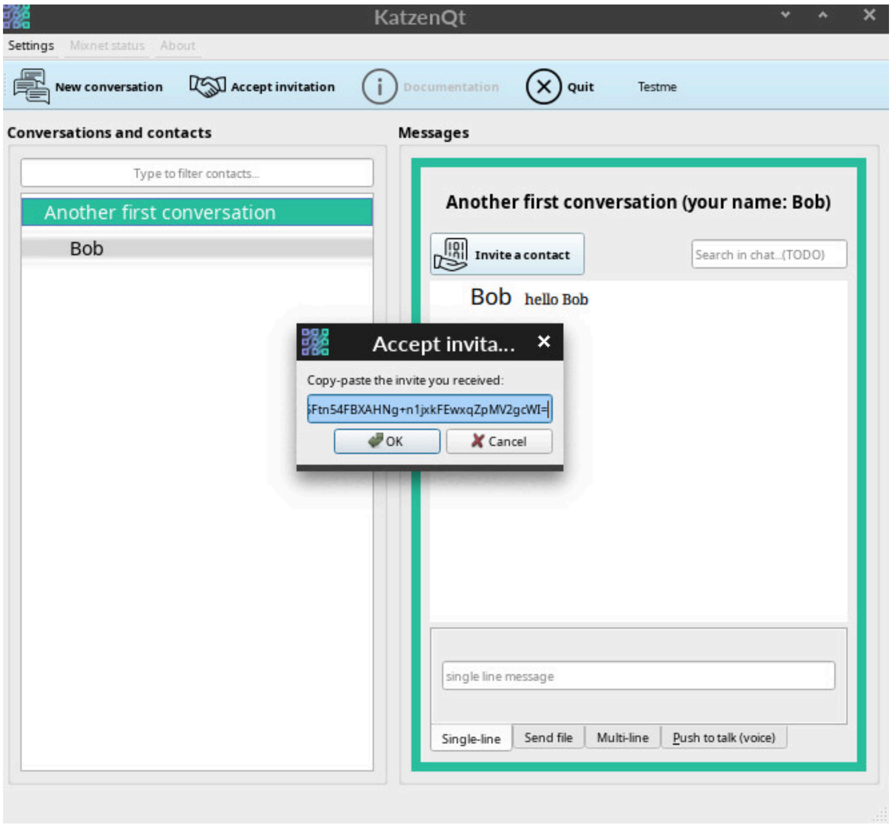
To accept an invitation that you have received

1. Open Katzen.

2. In the toolbar, click Accept invitation.

3. In the Accept invitation window, type or paste the invitation string into the field labeled Copy-paste the invite you received, then click OK.

Figure 6. Accepting an invitation – string entered



Another first conversation (your name: Bob)

Bob hello Bob

Copy-paste the invite you received:

;Ftn54FBXAHNg+n1jxkFEwxqZpMV2gcWI=

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

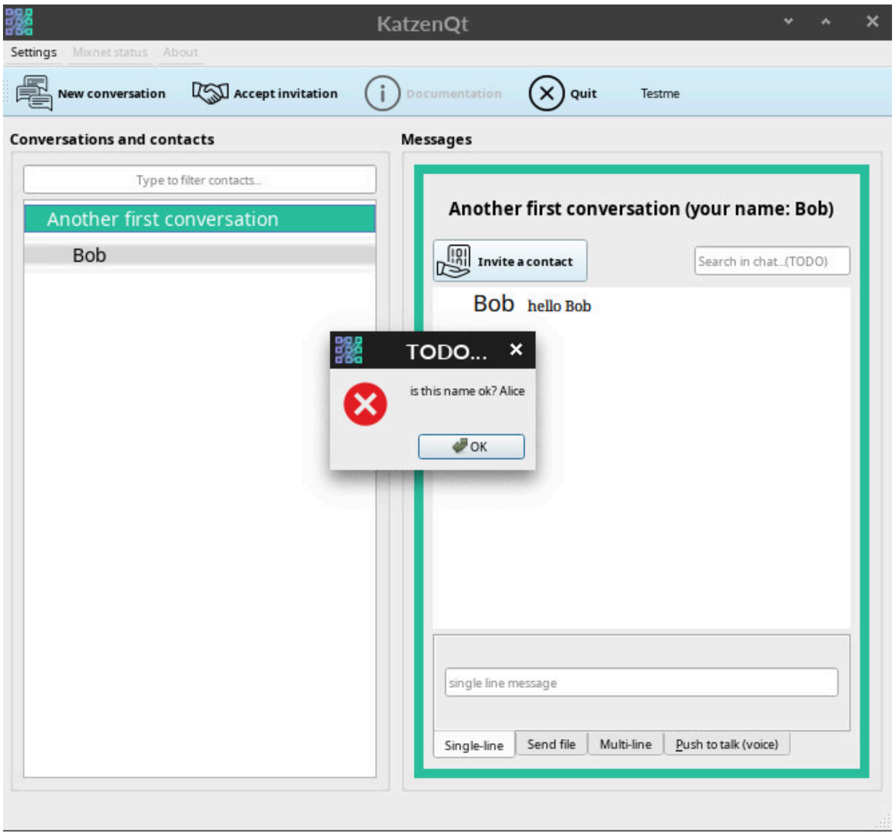
[4]

4. In TODO window, click OK if you accept the offered display name.[5]

[4] dwrob: Edit the strings

[5] dwrob: But there is no alternative as yet, so more TODO. Also edit the string.

Figure 7. Accepting an invitation – inviter's display name



Another first conversation (your name: Bob)

Bob hello Bob

is this name ok? Alice

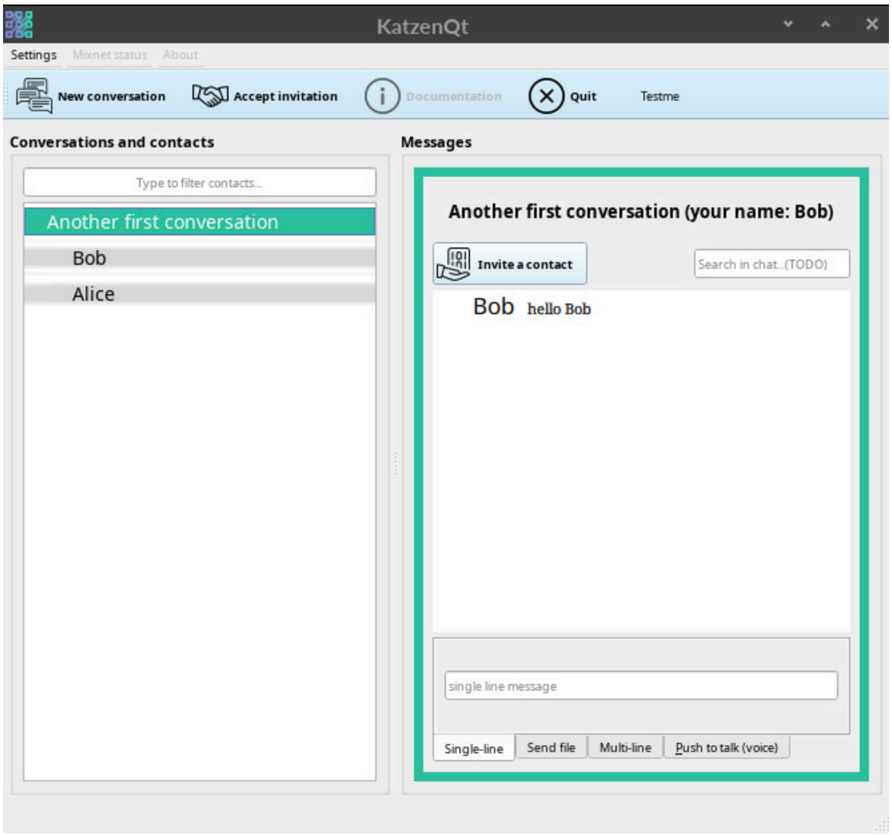
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

5. MORE?[6]

Members of the conversation should see each other in their lists of contact, and can begin exchanging messages.

[6] dwrob: The client currently lets me add myself on both sides of the chat.

Figure 8. Accepting an invitation – completed



Bob hello Bob

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Exchanging messages in a conversation

TODO

Figure 9. Exchanging messages

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Frequently asked questions – TODO

Users of conventional encrypted chat tools (Meta WhatsApp, Meta Messenger, Apple iMessage, Signal, etc.) may wonder, "Why should I care about that?" Many people may not care. However, businesses, governments, and criminals care very much about your identity and all of the information linked to it.

- Internet businesses routinely harvest and sell sensitive identity data to profit from invasively personalized ads and other sources.

- Governments, especially law enforcement and spy agencies, collect and store any data about identity, movements, employment, and political views that they can get their hands on, sacrificing the privacy of millions of innocent people to catch a tiny number of suspected criminals.

- Actual criminals make daily use of the data they steal from these same businesses and governments, enabling identity theft, credit-card fraud, and blackmail.

Consequently, Katzenpost users are likely to be drawn from the following demographics.

- People and groups who are likely to be under surveillance by government entities, including corrupt police forces and intelligence agencies.
- People facing business or government censorship.
- Businesses aware of the dangers of leaking internal information to their local and global competitors or to their own or other governments.
- Non-profit organizations engaging in advocacy that earns them enemies in high places with powerful surveillance capabilities.katzen
- People worried about the utter insecurity of personal data stored in both cloud and on-premises databases that are accessible from the Internet.
- People who want to use the Internet for communication, but who viscerally detest being the raw material that feeds surveillance capitalism [https://en.wikipedia.org/wiki/Surveillance_capitalism].

  Hiding who is talking to whom

And what about crime?

The Namenlos network

Threat model and security guarantees.

- Global passive adversaries (timing/correlation attacks)

  Second-party anonymity – why it matters …GPA can take advantage of the additional metadata contacts have about other contacts.

  aim for neutrality

- Encryption vs. anonymity
- Social graphs
- Dishonest service providers.
- Collection of metadata – All metadata collected will eventually be seized, whether by hackers, police, domestic intelligence, foreign intelligence, or criminals. The only way protect data is not to possess it.

Trade-offs

- No live video.
- Live audio still in development.
- Keeping track of identities.

https://papersplease.org/wp/2025/10/01/ice-is-buying-location-data-from-smartphone-apps-etc/

For technical information about the invitation process, see Katzenpost Group Chat Design [https://katzenpost.network/docs/specs/group_chat.html].