User Manual

Welcome! This guide will demonstrate how to use our messaging application, from the perspective of a user.

Disclaimer On Features

- This chat application is a proof-of-concept prototype, so many UX features such as displaying group members, deleting messages from chat history is missing, these kind of features are expected to exist if a full production version of the software is made. But due to time constraints, these UX features are not implemented here.
- The current system will still properly protect the software even if these features are added back in later. Missing features should not have an impact on the security of the system.
  - e.g. The message deletion request will still be encrypted and sent as a special message to the RS, such it is still encrypted with the session key like any other messages.

Running the Application

This application is based in the console. To launch the messaging client, just use the launch script `main.bash`

To run this script, run `bash main.bash`

Using the Application

Before logging in, you should use the Update Auth Server IP option (#1) to enter in the IP and port of the Auth Server. Then, user will be prompted to either 1. Login or 2. Register an account if they dont have one.

Upon either logging in or registering a new account, the user will be given 8 options.

- Get Token Sign into the RS: This option will generate the token, sign it, and log you into the RS.
- Make Group Chat: Create a new group chat
- Delete Person from Group Chat (Admin only): If admin of a Group Chat, allows the user to remove a person from the chat
- Add person to Group Chat (Admin only): If admin of a Group Chat, allows the user to add a person to the chat
- Delete account: Allows a user to delete their account (unrecoverable).
- List Groups: Allows a user to view the groups they are a part of.
- Delete Group Chat: Allows an admin of a group chat to delete that specific group chat (unrecoverable).
- Leave AS: Will return the user to the AS Screen IP/Port selection screen they are presented with at startup.

There are more details below about the specifics of each command.

Connect to Resource Server

If the user chooses to login (option 1) Get Token and sign into RS, they will then be prompted for the resource server IP and port #. From here, the user is prompted whether they want to private message or message in a group. After that, they will be prompted whether or not they want to re-encrypt messages on the resource server. `yes` should only be entered after removing a member from a group. After entering yes the auth server will send the client a list of keys needed for the operation.

After connecting to the resource server. If the user types "exit" in this prompt, they will disconnect from the resource server. If they type "back" at the 'Choose Resource Server' stage (where you enter the IP and port #), they will return to the application's main menu.

Private Message

If the user selects private message, they shall be queried on which user they would like to message. Users may only message users currently connected to the same resource server; a list of the currently connected users shall be displayed to the user. Upon selecting a user, the console will display the last 20 messages (if applicable) between the two users.

To type a message, they can simply type in the console and click enter. New messages from the other user will likewise appear in the console.

To go back, the user may type "~back" at any time, which will bring them back to the prompt asking which user they want to private message. If they type "back" again from this menu, they will be brought back to the prompt found in "Connect to Resource Server" asking if they want to private message or message in a group.

Group Chat

If the user selects to enter a group chat, they will be shown a list of the groups they are in on this resource server. When they select a group to enter, the console will display the last 20 messages (if applicable) in the group.

The 20 message count is due to the prototype nature of the application, we do not want to spam the user's screen full of messages, so the max number of message saved is capped. In a realistic scenario, there would be some display methods that handles the number of messages shown, and the limit of 20 messages stored will be removed.

To type a message, they can simply type in the console and click enter. New messages from the other user will likewise appear in the console.

To go back, the user may type "~back" at any time, which will bring them back to the prompt asking which group they want to enter. If they type "~back" again from this menu, they will be brought back to the prompt found in "Connect to Resource Server."

Auth Server Commands

This section will provide a more in-depth description of the authentication server commands.

Update Auth Server IP and Port

If the user selects Update Auth Server IP and Port, they will be prompted on what server IP and port they would like to connect to. Localhost is the default for the IP, however the user can manually input wherever the AS is currently being hosted.

Login

If the user selects login, they will be prompted to enter their username and password. Upong entering this information the AS will verify the username and password match and will either validate the credentials and the user will be redirected to the AS where they will be given a list of 8 options.

Register Account

This option allows for users to register a new account by entering a username and password. This will work without fail, as long as the username is not currently in use.

Get Token and Sign into RS

If the user selects the 'Get token and sign into RS' command, a token will be generated for the user with a timestamp of when it is generated, it will be signed and sent over to the client where they will be able to enter the IP of the resource server they would like to join and then the port number.

Upon selecting this option, the user will be prompted for the IP address of the inteded Resource Server they intend on joining.

Make Group Chat

If the user selects 'Make Group Chat' they will be prompted to create a group chat. They must enter a unique group_id between 0 and 9999, and will receive warnings if they enter any invalid input. Then, they must enter the users they want to join the group (not including themselves). A group must have at least 2 users, so entering nobody at this stage will also fail to create the group.

Delete Person from Group Chat (Admin only)

If the user selects 'Delete Person from Group Chat', this will allow them to remove someone from a group chat they are the admin of. They will be prompted for the group_id and the username of the person to remove; this will only work if they are the admin of the group, and the user in question exists.

Add Person from Group Chat (Admin only)

This option is the reverse of the above; the user wil be prompted for the same information (group_id and username), but this will instead give permission to that user to access this group chat.

Delete Account

This option allows for users to delete their account. This makes the account unrecoverable, removing all permissions associated with the account and preventing login.

List Groups

The 'List Groups' option simply allows users to view all groups they are currently in.

Delete Group Chat (Admin only)

Delete Group Chat is reserved for admins of a specific group to delete that specific group. This is unrecoverable, removing all of the message history and permissions the users have.

Leave AS

The last option that the user is presented with on the AS is Leave AS. Selecting this option will return the user back to the screen where they can either update the authentication server IP/Port, or they can return to the AS by selecting option 2 in which they will be prompted to login or create a new account.