RFID Chatroom Use Cases

Defining Actors

1. *Chatroom Client*: The actual user and device accessing the chat room. (Primary Actor)
2. *System Administrator*: The person who is responsible for developing, updating, and maintaining the system. (Supporting Actor)

Use Cases

1. *Use Case 1 (Fully Dressed): Access Chatroom*

Use Case Name:	*Access Chatroom*
Scope:	*RFID Chatroom*
Level:	*User goal*
Primary Actor:	*Chatroom Client*
Stakeholders and Interests:	- Chatroom Client: Wants to quickly and securely access system. - System Administrators: Wants to receive notification of system access request.
Preconditions:	- Chatroom Client has credentials within database. - Chatroom Client has RFID tag and passphrase. - Chatroom Client has a smart device with internet access and RFID reader.
Success Guarantee:	- Chatroom is shown and becomes available to send messages. - System access request is generated and sent to the System Administrator.
Main Success Scenario:	1. Chatroom Client wants to access chatroom with RFID tag. 2. Chatroom Client scans RFID tag with smart device. 3. RFID Tag prompts client to input passphrase to access Chatroom Log-In page. 4. Chatroom Client enters passphrase. 5. RFID Tag verifies passphrase and if valid, will populate the reader interface with a link. 6. Chatroom Client will click the link to display Chatroom Log-In page. 7. Chatroom Log-In page prompts client to enter password with the account while the username is automatically populated from the RFID Tag. 8. Chatroom Client enters password. 9. Chatroom Log-In page verifies account credentials and if valid, the server creates a thread for the client and opens the chatroom interface. 10. Chatroom Client can send and receive messages from other clients.
Extensions:	*a. At any time, System fails: 1. System shuts down server. 2. System disables link to access Log-In page.

	5a. RFID Tag detects incorrect passphrase. 1. Reader interface displays error. 2. Return to Step 3. 7a. Chatroom Log-In page does not detect username. 1. Reader interface displays error. 2. Generate error report and send it to the System Administrator. 3. Close Chatroom Log-In page. 4. Return to Step 1. 9a. Chatroom detects incorrect password. 1. Reader interface displays error. 2. If the number of incorrect password detections is more than 3. 2.1. Generate invalid user report and send it to the System Administrator. 2.2. Close Chatroom Log-In page. 2.3. Return to Step 1. 3. If the number of incorrect password detections is less than 3. 3.1. Return to Step 7.
Special Requirements:	- Text must be designed for touchscreen UI and standard desktop. - User verification must have a response within 10 seconds.
Technology and Data Variations List:	- Passphrase entered by touchscreen or keyboard. - Password entered by touchscreen or keyboard. - Time stamps will be in local device time.
Frequency of Occurrence:	Could be nearly continuous as it occurs every time anyone wants to access the system.
Open Issues:	What are the formats for error reports?

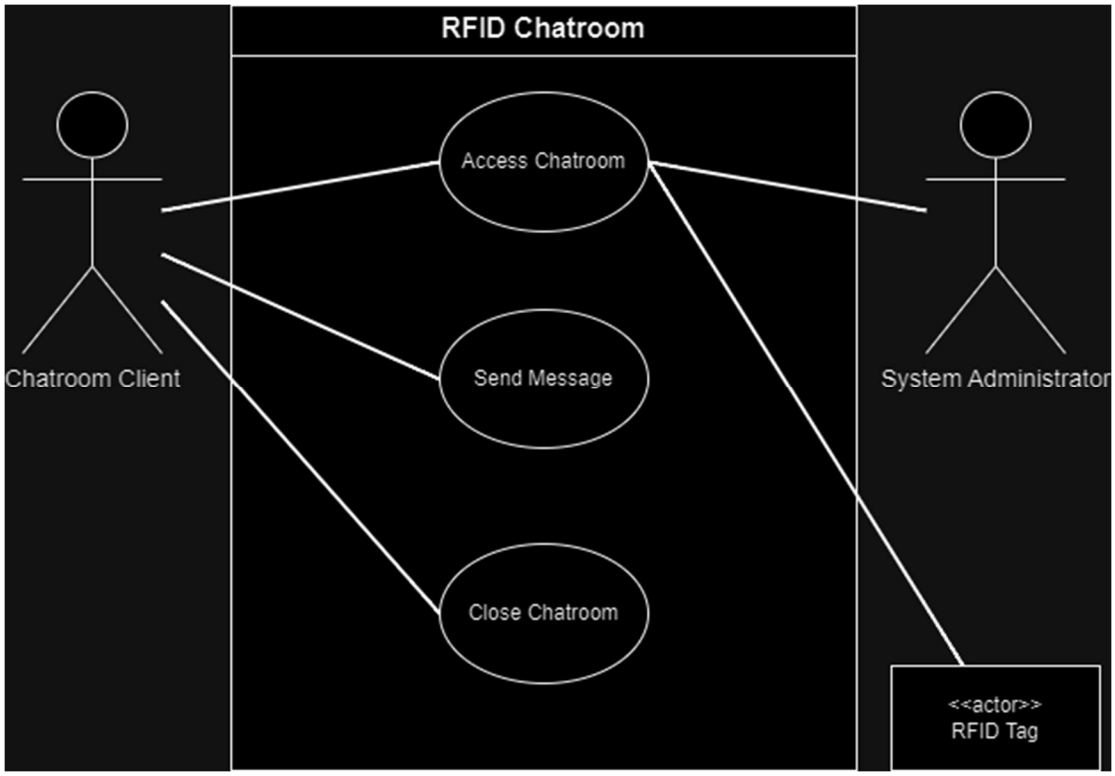
2. *Use Case 2 (Brief): Send Message*

The Chatroom Client sends a message using the Chatroom page, the server verifies the connection that the client is using, obtains username and current time, encrypts this message using the AES key, then the server sends this data to all other connected threads. The "Display Message" use case is a separate function. However, this use case is not able to be called unless the "Access Chatroom" use case has been successfully completed.

3. *Use Case 3 (Brief): Close Chatroom*

Chatroom Client presses the close window button within the Chatroom page, the server closes the connection for the client, displays exit message for all other threads, and closes the interface for the client. Like use case 2, this use case is not able to be called unless the “Access Chatroom” use case has been successfully completed.

Use Case Diagram



Sources:

[1] draw.io