Deliverable #1 Template : Software Requirement Specification (SRS)

SE 3A04: Software Design II – Large System Design

Tutorial Number: T03
Group Number: G8
Group Members:

- Kyle Jordan Ball McMaster
- Daniel David Franze-Da Silva
- Rosa Chen
- Aidan Edward Froggatt
- Edward Gao

1 Introduction

This SRS will outline the software requirements for an Android secure chat application. This document will outline the purpose, product description, use case diagram, functional, and non functional requirements.

1.1 Purpose

The purpose of this SRS is to describe the requirements for a secure chat application designed for an existing organization. The application allows users to send sensitive information over secure communication channels. The requirements cover the application's specifications, functions, use cases, and limitations. The intended audience for this SRS is the organization the application is associated with, to integrate it amongst all employee devices.

1.2 Scope

The secure chat application will allow users within an organization to send sensitive information to eachother without concerns of external threats. Secure communication between users will be established using keys with a Key Distribution Centre (KDC). The KDC establishes unique keys and sends them to communicating parties to begin a communication session.

In order to access the services within the secure chat application, users must register for an account. Registering for an account grants users permission to log in with their credentials. Once users have logged in, they will have the option to add a contact, view a conversation, or start a new chat session. When adding a new contact, users can search up employees within the organization to add them to their contacts list. Additionally, chat logs will be securely stored, so when users request to view a conversation the chat log will load onto the server. Lastly, upon loading a chat session, users will be given the option to send messages, remove contacts, and leave the chat.

A benefit of implementing this application is that there will be increased reliability when sending sensitive information and confidential documents. Users will not have to worry about malicious actors accessing personal information and chat history. This improves integrity, confidentiality, and decreases risk by investing in security and encryption services.

An objective of this application is to maximize security measures when communicating between users. Since a lot of high level professionals will be using this application, it is important that appropriate authentication protocols and symmetric-key crypto systems are incorporated.

A goal for this application is to emphasize user experience and ease of use. This will ensure seamless and easy integration within the organization. Since employees of all ages will be using this application, it is essential that users with all technical backgrounds are able to easily navigate and use the secure chat application.

1.3 Definitions, Acronyms, and Abbreviations

- **Key:** A string of randomized text that is used for cryptography purposes. It is often required to be decrypted to be used.
- **Key Distribution Center (KDC):** A centralized system responsible for generating unique keys to facilitate communication between two or more systems. A KDC is used to implement secure communication.
- **Software Requirements Specification (SRS):** A comprehensive document outlining how a software is expected to perform and how it will do.
- **Record Retention Date:** The date which important records must be accessible until for legal and auditing purposes. Each Record Retention Date is unique to the record it is associated with.

- **Accessbility for Ontarians with Disabilities Act (ADOA):** The law that outlines the accessibility standards that organizations in Ontario must adhere to.

1.4 References

1. R. Khedri, "Project Outline (SE3A04 2024)," Avenue to Learn, https://avenue.cllmcmaster.ca/d2l/le/content/557745/viewContent/4485984/View (accessed 2024).

2. R. Khedri, "SE3A04_D1_Template," Avenue to Learn, https://avenue.cllmcmaster.ca/d2l/le/content/557745/viewContent/4485974/View (accessed 2024).

3. R. Khedri, "SE3A04_D1_Template," Avenue to Learn, https://avenue.cllmcmaster.ca/d2l/le/content/557745/viewContent/4485973/View (accessed 2024).

4. M. B. Weingust, R. Liu, A. Gulia, and B. Ha, "3A04 D1," Avenue to Learn, https://avenue.cllmcmaster.ca/d2l/le/content/557745/viewContent/4558138/View (accessed 2024).

5. Government of Ontario, "Law document english view," Ontario.ca, https://www.ontario.ca/laws/statute/05a11 (accessed Feb. 14, 2024).

1.5 Overview

This document discusses a high-level overview of the requirements of the secure messaging application. In section 2, the context, functions, and expected users of the application are discussed. This section also discloses the constraints identified and assumptions made while developing this document. Section 3 contains a use case diagram for the messaging system. Section 4, outlines the key business events from each viewpoint. Finally, section 5 outlines the non-functional requirements for the application. A division of labour can be found in the appendix.

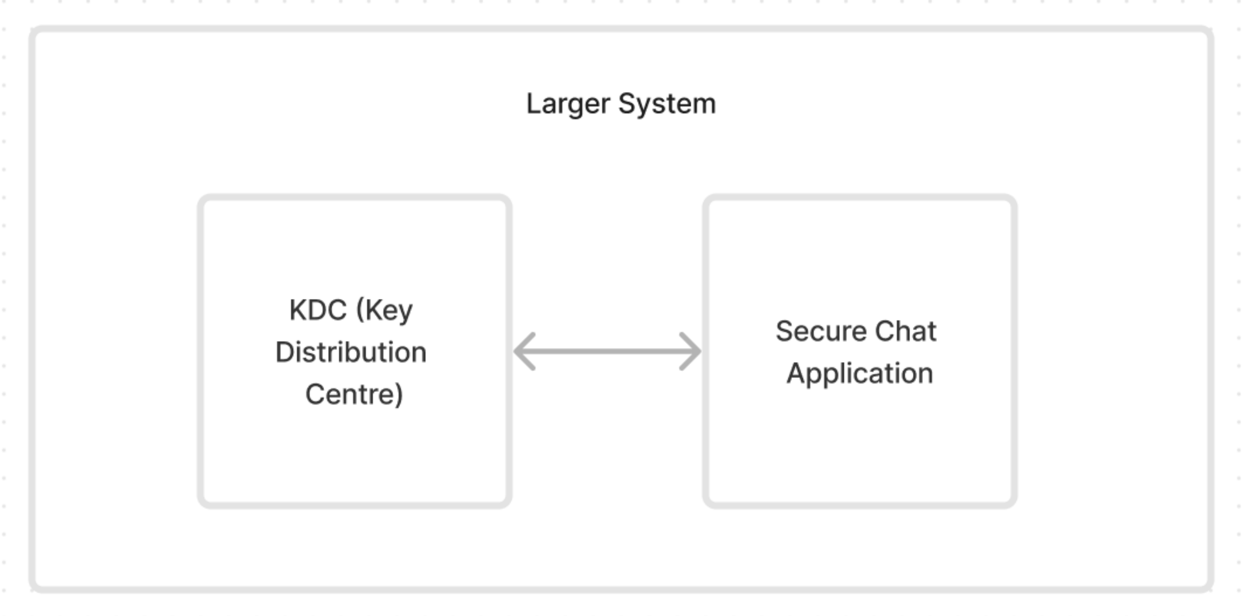
2 Overall Product Description

2.1 Product Perspective

The Secure Chat Android Application is part of the broader landscape of mobile applications designed for secure communication. It exists within the context of mobile operating systems, specifically targeting the Android platform. Similar products may include encrypted messaging apps like Signal, Telegram, or WhatsApp. However, the unique aspect of this application is its integration with a Key Distribution Centre (KDC) server, mediated authentication protocol, and a specific symmetric-key crypto-system, setting it apart in terms of security features tailored for an organization with sensitive information.

The Secure Chat Android Application is not entirely independent, as it relies on a company-issued Android device and requires communication with a centralized Key Distribution Centre (KDC) server. While it is self-contained on the Android device for individual usage, its functionality extends beyond the application itself to ensure secure communication channels through the KDC server.

The larger system, in this case, includes the organization's infrastructure for secure communication. The software, being a component of this larger system, interacts with a Key Distribution Centre (KDC) server. The KDC server is crucial for generating and distributing encryption keys for secure communication sessions. The application's role is to register with the KDC, receive fresh keys, and update the communicating agents about key changes. This integration is vital for maintaining the security of communication within the organization.



In this diagram, the Larger System encompasses both the KDC Server and the Secure Chat Application. The interaction involves the Secure Chat App communicating with the KDC server for key generation, distribution, and updates, emphasizing the interdependence of the components.

This product perspective outlines the relationship between the Secure Chat Android Application and the larger system, emphasizing its integration with the KDC server for secure communication within the organization.

2.2 Product Functions

Module	Functions	Source
Key Distribution Centre	• Generate Keys - Generates cryptographically secure keys • Refresh Keys - Update keys used by communicating agents • Distribute Keys - Distribute cryptographically secure keys to communicating agents	Min Reqs
Authentication Service	• Authenticate User - Authenticates new users to request keys • Add User - Add new user to secure environment • Remove User - Remove user from secure environment	Min Reqs
Encryption Service	• Encrypt Message - Encrypts outgoing messages using symmetric key crypto system • Decrypt Message - Decrypts incoming message using symmetric key crypto system	Min Reqs
	• Encrypt Audio - Encrypt outgoing audio message • Decrypt Audio - Decrypt incoming audio message	Addtl. Features
Client Application	• Display Message • Create an account - Allows a user to create an account to use the application - Displays a message to the users screen • Type a message - Allows a user to compose a message • Send a message - Allows a user to send a message they have composed	Min Reqs
	• Auto complete text - Allows a user to see recommended responses to a received message • Record audio - Record a 10 second audio message • Listen to audio - Allows a user to listen to an audio message	Addtl. Features
Message Service	• Deliver Message - Coordinates the transmission of a message to a client	Min Reqs
	• Create New Group - Allows user to create new chat with 2 or more users • Leave Chat - Allows a user to leave a chat • Add user to chat - Allows a user to add an additional user to the chat • Add contact - Allows a user to add a contact to their contacts list • Remove contact - Allows a user to remove a contact from their contacts list	Addtl. Features
Message Storage Service	• Save Messages - saves messages and metadata to the server • Load Messages - Allows a user to load chat log	Min Reqs
	• Generate Message report - Generate a log of messages for reporting purposes	Addtl. Features

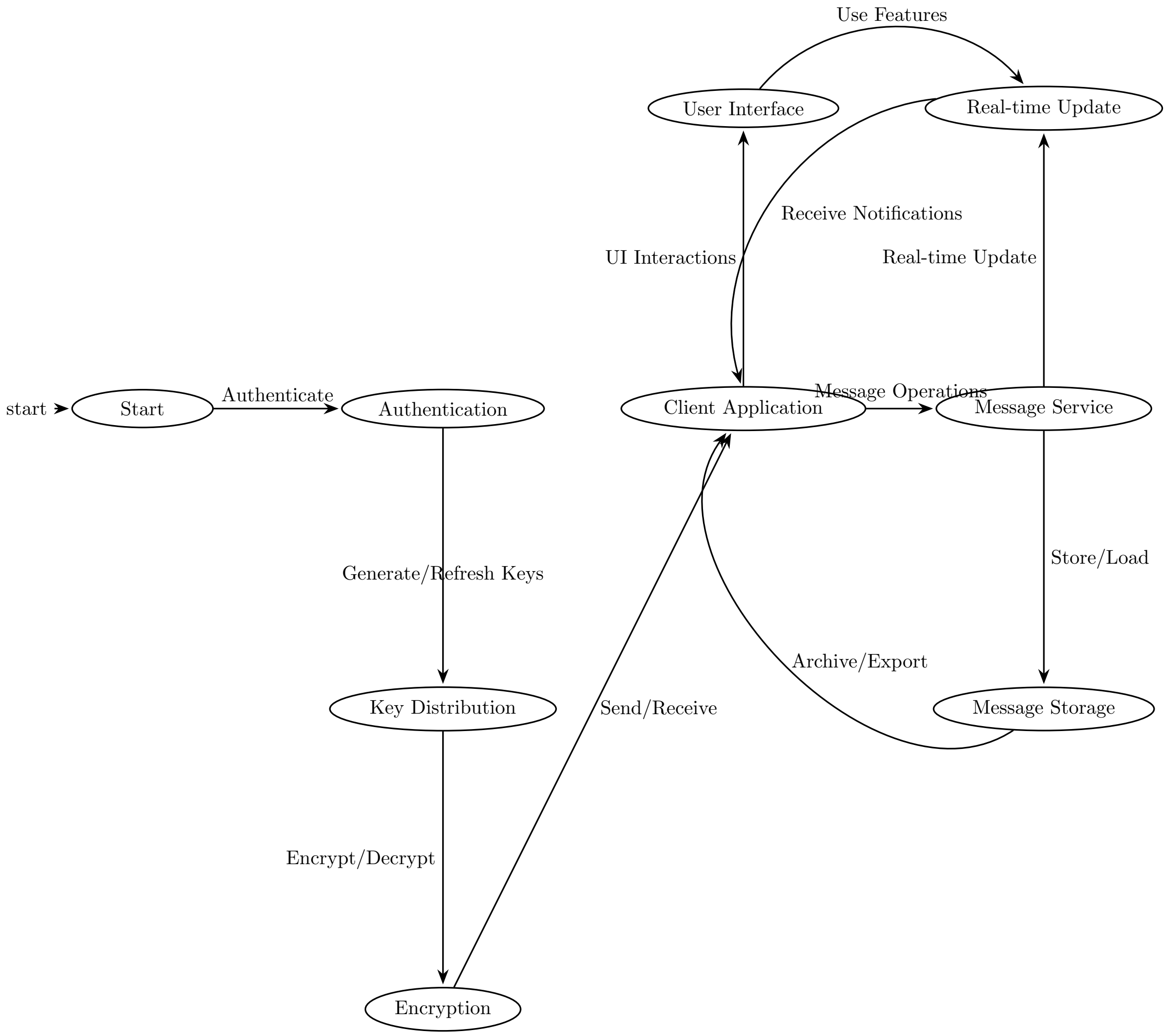


Figure 1: State Diagram

2.3 User Characteristics

The following are the minimum requirements that an employee must inhibit to properly utilize the app:

1. Education Level: High School Degree
   - Since this is a formal app that is intended for employees of the company, it is expected that messages are sent and handled in a formal manner with proper spelling and grammar.
2. Experience: Moderate Experience with the Company
   - This application is designed to facilitate secure messaging within trusted members of the company to prevent any corporate espionage. In order to participate in the secure messaging you must first be screened to ensure you have good experience and trust built with the company.
3. Technical Experience: Basic Knowledge of How Chat Applications Work
   - A person who is aware of how to send and receive messages from the typical chat application will have no trouble utilizing this app as the encoding and decoding is hidden from the user - all they need to worry about is the message they wish to send.

The following are the minimum requirements that a member of the Internal IT support team must inhibit to properly utilize the app:

1. Education Level: Bachelor's Degree in Computer Science, Software Engineering, or related fields
   - Members of the internal IT team require a strong knowledge in computing in order to maintain and handle any debugging, database management, or support with key distribution in order to fully service the users of the app.
2. Experience: Any
   - The messaging system is not intended for the use of the internal IT team. Their purpose is to facilitate the app's functionality and maintenance, therefore they do not require any experience with chat applications.
3. Technical Experience: High Level of Experience with the Encryption and Decryption Process
   - In order to emphasize the security of message passing between employees it is important that the internal IT team is able to maintain the app's security protocols to prevent any leaks of sensitive information.

2.4 Constraints

- **Technical:** The secure chat application must be compatible with the Android operating system (Android 10 or later). This is the only mobile operating system that will be supported by the devices within the organization.
- **Regulatory:** The application must abide to the Google Play Store policies. Compliance is essential in order to properly deploy the application for use.
- **Time Constraint:** This project will have a timeline of 4 months to be completed. This includes the requirements document and the physical implementation

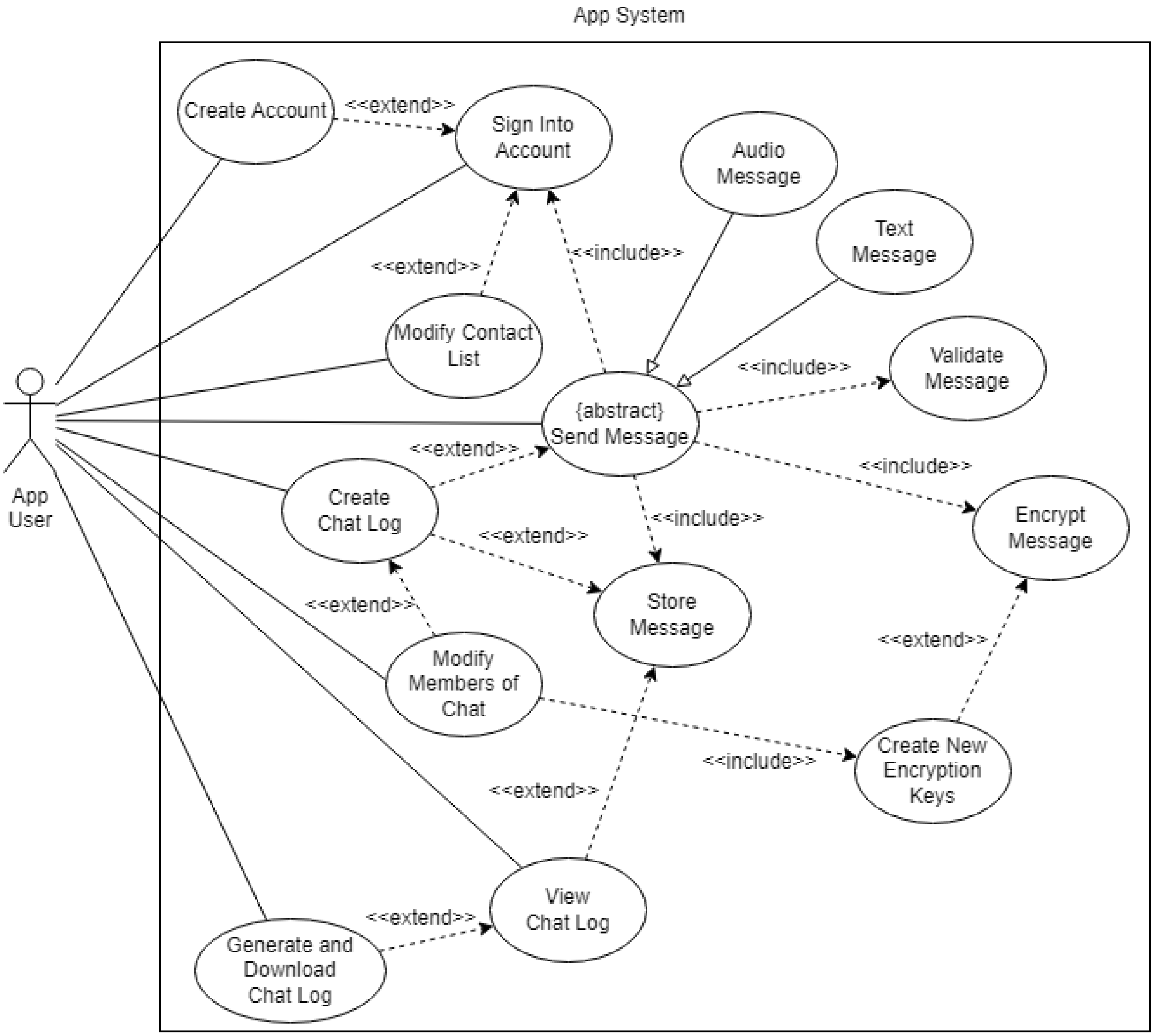
2.5 Assumptions and Dependencies

- It is assumed that English will be the only supported language within the application.
- The time zone in which inidviduals will use the application will be set to Eastern Standard Time (EST). All chat logs will be recorded within this time zone as well.
- The application is assumed to be used by a singular organization. Thus, the requirements are tailored towards the organization as a stakeholder.
- Messaging functions will be operational during typical work hours. A typical work day is assumed to be from 7am to 7pm.
- It is assumed that the company will grow by 5 percent a year to support scalability and growth.
- The application is assumed to undergo weekly maintenance updates to enhance security.

2.6 Apportioning of Requirements

N/A

3 Use Case Diagram



For this use case diagram the sole actor ”App User” represents a generalization of all the stakeholders, since each stakeholder will be required to access the app in a similar manner. All stakeholders will be given an account with which to access the app by, and each stakeholder will be able to utilize the chat messaging features in order to address and validate the app’s capabilities through their own viewpoints.

4 Highlights of Functional Requirements

Our main business events:

- BE1 User Creates an Account
- BE2 User Sign's into Account
- BE3 User Sends a Message
- BE4 User Views a Conversation
- BE5 User Creates a Chat
- BE6 User Leaves a Chat
- BE7 User Generates Chat Log
- BE8 User Adds a Contact

The viewpoints we considered:

- VP1 Common Employee
- VP2 Upper Management
- VP3 Legal
- VP4 Security Team
- VP5 Human Resources
- VP6 Finance
- VP7 Internal IT Team

BE1. User Creates an Account
Precondition: User has access to the app and does not have an existing account.

VP1.1 Common Employee

Main Success Scenario

- S_1**:** System displays a dialogue box for a new username.
- E_1**:** User enters a new username into the dialogue box.
- S_2**:** System validates the username and displays a dialogue box for a new password.
- E_2**:** User enters a new password into the dialogue box.
- S_3**:** System validates the password and creates a new account with the provided credentials.

Secondary Scenario

- $E_{2.1}$**:** An account with the provided credentials already exists.
  - $S_{2.1}$**:** System prompts user to enter a new username.
  - $E_{3.1}$**:** Return to E_1 (User enters a new username).

VP1.2 Upper Management
N/A

VP1.3 Legal

Main Success Scenario

- S_1**:** System displays company policies, terms and agreements for app utilization.
- E_1**:** User reads and selects the "I accept" button to acknowledge they understand and have reviewed the terms and agreements.
- S_2**:** System creates a new account with the provided credentials.

Secondary Scenario

- $E_{1.1}$**:** User attempts to select the "I accept" button without fully reading the company policies, terms and agreements.
  - $S_{2.1}$**:** System does not process the button selection since the company policies, terms and agreements has not been fully scrolled through.

VP1.4 Security Team

Main Success Scenario

- S_1**:** System requests verification details from employee.
- E_1**:** User provides proof of employment with the company.
- S_2**:** System validates that the user is an employee and authenticates them to continue.
- E_2**:** User enters credentials.
- S_3**:** System accesses and validates the strength of the password.

Secondary Scenario

- $E_{1.1}$**:** User does not provide sufficient proof of employment.
  - $S_{2.1}$**:** System denies access and reports a potential breach of security.
- $E_{2.1}$**:** User does not enter a strong enough password.
  - $S_{3.1}$**:** System identifies weak password and prompts user to enter a new stronger password (i.e. with more characters, inclusion of diverse characters, etc.). Return to E_3 (User enters a new password).

VP1.5 Human Resources

N/A

VP1.6 Finance

N/A

VP1.7 Internal IT Team

Main Success Scenario

- S_1**:** System displays a dialogue box for a new username, with a list of permitted characters.
- E_1**:** User enters a new username into the dialogue box.
- S_2**:** System validates the username.

Secondary Scenario

- $S_{1.1}$**:** User includes invalid character(s) into their username.
  - $S_{2.1}$**:** Return to E_1 (User enters a new username).

Global Scenario of ***User Creates an Account*****:**

Precondition: User has access to the app and does not have an existing account.

Main Success Scenario

- S_1**:** System requests verification details from employee.
- E_1**:** User provides proof of employment with the company.
- S_2**:** System validates that the user is an employee and authenticates them to continue.
- S_3**:** System displays a dialogue box for a new username, with a list of permitted characters.
- E_3**:** User enters a new username into the dialogue box.
- S_4**:** System validates the username and displays a dialogue box for a new password.
- E_4**:** User enters a new password into the dialogue box.
- S_5**:** System validates the password.
- S_6**:** System displays company policies, terms and agreements for app utilization.
- E_6**:** User reads and selects the ”I accept” button to acknowledge they understand and have reviewed the terms and agreements.
- S_7**:** System creates a new account with the provided credentials.

Secondary Scenario

- $E_{1.1}$**:** User does not provide sufficient proof of employment.
  - $S_{2.1}$**:** System denies access and reports a potential breach of security.
- $E_{3.1}$**:** An account with the provided credentials already exists.
  - $S_{4.1}$**:** System prompts user to enter a new username.
  - $E_{4.1}$**:** Return to E_1 (User enters a new username).
- $S_{3.2}$**:** User includes invalid character(s) into their username.
  - $S_{4.2}$**:** Return to E_1 (User enters a new username).
- $E_{4.1}$**:** User does not enter a strong enough password.
  - bf $S_{5.1}$: System identifies weak password and prompts user to enter a new stronger password (i.e. with more characters, inclusion of diverse characters, etc.). Return to E_3 (User enters a new password).
- $E_{6.1}$**:** User attempts to select the ”I accept” button without fully reading the company policies, terms and agreements.
  - $S_{7.1}$**:** System does not process the button selection since the company policies, terms and agreements has not been fully scrolled through.

BE2. User Sign's Into Account

Precondition: User has access to the app and has a pre-existing account.

VP2.1 Common Employee

Main Success Scenario

- S_1**:** System displays a dialogue box for the user to enter a username.
- E_1**:** User enters username into the dialogue box.
- S_2**:** System validates the username and displays a dialogue box for a password.
- E_2**:** User enters password into the dialogue box.
- S_3**:** System validates the password and the user is authenticated to use the app.

Secondary Scenario

- $E_{1.1}$**:** User enters invalid username.
  - $S_{2.1}$**:** System does not recognize username. Sign-in fails.
- $E_{2.1}$**:** User enters invalid password.
  - $S_{3.1}$**:** System cannot match the password to the given username. Sign-in fails.

VP2.2 Upper Management

N/A

VP2.3 Legal

N/A

VP2.4 Security Team

Main Success Scenario

- S_1**:** System prompts user to enter credentials.
- E_1**:** User enters username and password into the dialogue boxes.
- S_2**:** System validates the credentials and the user is authenticated to use the app.

Secondary Scenario

- $E_{1.1}$**:** User reaches limit for incorrect sign-in attempts.
  - $S_{2.1}$**:** System reports potential security breach. Sign-in fails and blocks user from signing in from that device for 1 hour.

VP2.5 Human Resources

N/A

VP2.6 Finance

N/A

VP2.7 Internal IT Team

N/A

Global Scenario of ***User Signs Into Account*****:**

Precondition: User has access to the app and has a pre-existing account.

Main Success Scenario

- S_1**:** System displays a dialogue box for the user to enter a username.
- E_1**:** User enters username into the dialogue box.
- S_2**:** System validates the username and displays a dialogue box for a password.
- E_2**:** User enters password into the dialogue box.
- S_3**:** System validates the password and the user is authenticated to use the app.

Secondary Scenario

- $E_{1.1}$**:** User enters invalid username.
  - $S_{2.1}$**:** System does not recognize username. Sign-in fails.
- $E_{2.1}$**:** User enters invalid password.
  - $S_{3.1}$**:** System cannot match the password to the given username. Sign-in fails.
- $E_{2.2}$**:** User reaches limit for incorrect sign-in attempts.
  - $S_{3.2}$**:** System reports potential security breach. Sign-in fails and blocks user from signing in from that device for 1 hour.

BE3. User Sends a Message

VP3.1 Common Employee

Precondition: User opens a chat log with the intended recipient

Main Success Scenario

- S_1**:** System displays a dialogue box to enter message
- E_1**:** User composes a message
- S_2**:** System prompts user with recommended responses to auto complete message
- E_2**:** User clicks "Send"
- S_3**:** System verifies that message is valid
- S_4**:** System sends message

Secondary Scenario

- $E_{1.1}$**:** User exceeds the word count limit while composing the message
  - $S_{2.1}$**:** System notifies user that the message is invalid
- $E_{1.2}$**:** User records an audio clip
  - $S_{2.2}$**:** System allows user to listen to audio message
  - $E_{2.2}$**:** Return to E_2
- $E_{1.2}$**:** User sends a message with an incompatible symbol or file type
  - $S_{2.2}$**:** System notifies user that the message is invalid
- $E_{2.1}$**:** User sends message to a recipient who is not in their contact list
  - $S_{3.1}$**:** System deems message invalid and does not deliver the request
- $S_{3.1}$**:** System verifies that message is invalid
  - $S_{3.2}$**:** System notifies the user that the message is invalid and does not send the message

VP3.2 Upper Management
N/A

VP3.3 Legal
N/A

VP3.4 Security Team

Precondition: User opens a chat log with the intended recipient

Main Success Scenario

- S_3**:** System encrypts message before sending it to the recipient

VP3.5 Human Resources
N/A

VP3.6 Finance
N/A

VP3.7 Internal IT Team
N/A

Global Scenario of *User Sends a Message***:**

Precondition: User logs in

Main Success Scenario

- S_1**:** System displays a dialogue box to enter message
- E_1**:** User composes a message
- S_2**:** System prompts user with recommended responses to auto complete message
- E_2**:** User clicks ”Send”
- S_3**:** System verifies that the message is valid
- S_4**:** System encrypts message
- S_5**:** System sends message

Secondary Scenario

- $E_{1.1}$**:** User exceeds the word count limit while composing the message
  - $S_{2.1}$**:** System notifies user that the message is invalid
- $E_{1.2}$**:** User records an audio clip
  - $S_{2.2}$**:** System allows user to listen to audio message
  - $E_{2.2}$**:** Return to E_2
- $E_{1.2}$**:** User sends a message with an incompatible symbol or file type
  - $S_{2.2}$**:** System notifies user that the message is invalid
- $E_{2.1}$**:** User sends message to a recipient who is not in their contact list
  - $S_{3.1}$**:** System securely sends the message to the recipient’s message invitation inbox
- $S_{3.1}$**:** System verifies that message is invalid
  - $S_{3.2}$**:** System notifies the user that the message is invalid and does not send the message

BE4. User Views A Conversation

VP4.1 Common Employee

Precondition: User logs in

Main Success Scenario

- S_1**:** System displays a list of past open conversations
- E_1**:** User selects a past conversation they want to view
- S_2**:** System retrieves the chat log stored on the server
- E_2**:** User views conversation

Secondary Scenario

- $E_{1.1}$**:** User selects a conversation with a deactivated user account
  - $S_{2.1}$**:** System notifies user that the account is deactivated

VP4.2 Upper Management
N/A

VP4.3 Legal
N/A

VP4.4 Security Team

Precondition: User logs in

Main Success Scenario

- S_2**:** System verfies that security requirements are met
- E_2**:** User meets security requirements
- S_3**:** System displays conversation

VP4.5 Human Resources
N/A

VP4.6 Finance
N/A

VP4.7 Internal IT Team

Precondition: User logs in

Secondary Scenario

- $E_{1.1}$**:** System does not display conversation and aborts
  - $S_{2.1}$**:** System notifies the IT Team of the bug through diagnostic and troubleshooting tools

Global Scenario of *User Views a Conversation***:**

Precondition: User logs in

Main Success Scenario

- S_1**:** System displays a list of past open conversations
- E_1**:** User selects a past conversation they want to view
- S_2**:** System retrieves the chat log stored on the server
  subtabitem $S_{2.1}$**:** System verfies that security requirements are met
- S_3**:** System displays conversation

Secondary Scenario

- $E_{1.1}$**:** User selects a conversation with a deactivated user account
  - $S_{2.1}$**:** System notifies user that the account is deactivated
- $E_{3.1}$**:** System does not display conversation and aborts
  - $S_{2.1}$**:** System notifies the IT Team of the bug through diagnostic and troubleshooting tools

BE5. User Creates a Chat

VP5.1 Common Employee

Precondition: User is authenticated in the app

Main Success Scenario

- S_1**:** System displays dialogue to create new chat
- E_1**:** User selects additional users to add to the chat
- S_2**:** Chat is created.

Secondary Scenario

- $E_{1.1}$**:** User does not select additional users to add to the chat
  - $S_{2.1}$**:** System aborts chat creation

VP5.2 Upper Management
N/A

VP5.3 Legal
N/A

VP5.4 Security Team

Precondition: User is authenticated in the app

Main Success Scenario

- S_1**:** System displays dialogue to create new chat.
- E_1**:** User selects additional users to add to the chat.
- S_2**:** System verifies that selected users meet security requirements.
- E_2**:** Users meet security requirements.
- S_3**:** Chat is created.

Secondary Scenario

- $E_{2.1}$**:** Users do not meet security requirements.
  - $S_{2.1}$**:** Chat creation is aborted. User is notified of error.

VP5.5 Human Resources
N/A

VP5.6 Finance
N/A

VP5.7 Internal IT Team

Precondition: User is authenticated in the app

Main Success Scenario

- S_1**:** System displays dialogue to create new chat.
- E_1**:** User selects additional users to add to the chat.
- S_2**:** System registers the chat with the message storing system.
- E_2**:** Registration is successful.
- S_3**:** Chat is created.

Secondary Scenario

- $E_{2.1}$**:** No space is available.
  - $S_{3.1}$**:** System aborts chat creation. IT Team is notified of error.

Global Scenario of *User Creates a Chat***:**

Precondition: User is authenticated in the app

Main Success Scenario

- S_1**:** System displays dialogue to create new chat.
- E_1**:** User selects additional users to add to the chat.
- S_2**:** System verifies that selected users meet security requirements.
- E_2**:** Users meet security requirements.
- S_3**:** System registers the chat with the message storing system.
- E_3**:** Registration is successful.
- S_4**:** Chat is created.

Secondary Scenario

- $E_{2.1}$**:** Users do not meet security requirements.
  - $S_{2.1}$**:** Chat creation is aborted. User is notified of error.
- $E_{3.1}$**:** No space is available.
  - $S_{4.1}$**:** System aborts chat creation. IT Team is notified of error.

BE6. User Leaves a Chat

VP6.1 Common Employee

Precondition: User is authenticated in the app. User is a member of the chat

Main Success Scenario

- S_1**:** System displays dialogue to leave chat.
- E_1**:** User confirms request to leave chat.
- S_2**:** System removes chat from user display.

Secondary Scenario

- $E_{1.1}$**:** Users does not confirm intention to leave chat.
  - $S_{2.1}$**:** Chat removal is aborted.

VP6.2 Upper Management

N/A

VP6.3 Legal

Precondition: User is authenticated in the app. User is a member of the chat

Main Success Scenario

- S_1**:** System checks if user is last member of chat
- E_1**:** User is last member of chat.
- S_2**:** System calculates record retention date using company policy. Chat log is stored on message storing service until this date.

Secondary Scenario

- $E_{1.1}$**:** User is not last member of chat
  - $S_{2.1}$**:** Log is not considered an archived record. No retention calculation is necessary.

VP6.4 Security Team

Precondition: User is authenticated in the app. User is a member of the chat

Main Success Scenario

- S_1**:** System displays dialogue to leave chat.
- E_1**:** User confirms request to leave chat.
- S_2**:** System changes encryption keys for chat. Remaining users of chat are notified.

Secondary Scenario

- $E_{1.1}$**:** Users does not confirm intention to leave chat.
  - $S_{2.1}$**:** Chat removal is aborted.

VP6.5 Human Resources

N/A

VP6.6 Finance

N/A

VP6.7 Internal IT Team

Precondition: User is authenticated in the app. User is a member of the chat

Main Success Scenario

- S_1**:** System displays dialogue to leave chat.
- E_1**:** User confirms request to leave chat.
- S_2**:** System updates message log to track when user left chat.

Secondary Scenario

- $E_{1.1}$**:** Users does not confirm intention to leave chat.
  - $S_{2.1}$**:** Chat removal is aborted.

Global Scenario of *User Leaves a chat*:

Precondition: User is authenticated in the app. User is a member of the chat

Main Success Scenario

- S_1**:** System displays dialogue to leave chat.
- E_1**:** User confirms request to leave chat.
- S_2**:** System removes chat from user display.
- S_3**:** System changes encryption keys for chat. Remaining users of chat are notified.
- S_4**:** System updates message log to track when user left chat.
- S_5**:** System checks if user is last member of chat
- E_2**:** User is last member of chat.
- S_6**:** System calculates record retention date using company policy. Chat log is stored on message storing service until this date.

Secondary Scenario

- $E_{1.1}$**:** Users does not confirm intention to leave chat.
  - $S_{2.1}$**:** Chat removal is aborted.
- $E_{2.1}$**:** User is not last member of chat
  - $S_{6.1}$**:** Log is not considered an archived record. No retention calculation is necessary.

BE7. User Generates Chat Log
Precondition: A chat history pre-exists to be generated.

VP7.1 Common Employee

Main Success Scenario

- S_1**:** The system displays the option to generate chat log reports.
- E_1**:** The employee selects their user identifier.
- S_2**:** The system processes the request and retrieves the chat history associated with the selected user identifier.
- E_2**:** The system presents the chat log report to the employee for personal reference.
- S_3**:** The system confirms the successful generation of the chat log report.
- E_3**:** The employee reviews the report and may choose to download or further interact with it.

Secondary Scenario

N/A

VP7.2 Upper Management

Main Success Scenario

- S_1**:** The system provides access to the chat log report feature upon login.
- E_1**:** Upper management selects the desired time frame for the summarized reports.
- S_2**:** The system aggregates chat logs within the specified time frame.
- E_2**:** Upper management receives the summarized reports for strategic decision-making.
- S_3**:** The system logs the access and generation of reports for auditing purposes.
- E_3**:** Upper management may request further analysis or additional reports based on the provided summaries.

Secondary Scenario

N/A

VP7.3 Legal

Main Success Scenario

- S_1**:** The legal team accesses the system and navigates to the chat log report generation feature.
- E_1**:** The legal team selects the criteria for the chat log reports, such as date range or specific users.
- S_2**:** The system retrieves and compiles chat logs meeting the specified criteria.
- E_2**:** The legal team reviews the compiled chat log reports for compliance and legal purposes.
- S_3**:** The system archives the generated reports according to regulatory requirements.
- E_3**:** The legal team may take further actions based on the contents of the reports, such as initiating legal proceedings or issuing warnings.

Secondary Scenario

N/A

VP7.4 Security Team

Main Success Scenario

- S_1**:** The security team accesses the system and enters the chat log report feature.
- E_1**:** The security team sets parameters to filter for suspicious activity or security breaches.
- S_2**:** The system scans the chat logs based on the specified parameters.
- E_2**:** The security team identifies any anomalies or potential security threats within the chat logs.
- S_3**:** The system provides tools for further investigation or response to the identified threats.
- E_3**:** The security team takes appropriate actions to mitigate risks and secure the system.

Secondary Scenario

N/A

VP7.5 Human Resources

Main Success Scenario

- S_1**:** HR personnel log into the system and navigate to the chat log report feature.
- E_1**:** HR specifies the criteria for generating chat log reports, such as employee names or keywords related to incidents.
- S_2**:** The system retrieves and organizes chat logs relevant to the specified criteria.
- E_2**:** HR reviews the chat log reports to support employee-related investigations or conflict resolution efforts.
- S_3**:** The system logs the access and generation of reports for HR records and compliance purposes.
- E_3**:** HR may use the information from the reports to take appropriate actions, such as disciplinary measures or conflict mediation.

Secondary Scenario

N/A

VP7.6 Finance

Main Success Scenario

- S_1**:** The financial team accesses the system and locates the chat log report feature.
- E_1**:** The financial team defines parameters for generating reports, focusing on financial transactions or discussions.
- S_2**:** The system retrieves chat logs related to financial activities based on the specified parameters.
- E_2**:** The financial team analyzes the chat log reports to support auditing or financial analysis processes.
- S_3**:** The system securely stores the generated reports in compliance with financial regulations.
- E_3**:** The financial team may use insights from the reports to inform financial decision-making or identify areas for improvement.

Secondary Scenario

N/A

VP7.7 Internal IT Team

Main Success Scenario

- S_1**:** IT operators log into the system and access the chat log report feature.
- E_1**:** IT specifies criteria to generate reports, focusing on system maintenance or issue resolution.
- S_2**:** The system retrieves relevant chat logs based on the specified criteria.
- E_2**:** IT reviews the chat log reports to troubleshoot technical issues or perform system maintenance tasks.
- S_3**:** The system logs the access and activities performed by IT personnel for security and accountability.
- E_3**:** IT takes necessary actions

Secondary Scenario

N/A

Global Scenario of *User Generates Chat Log***:**

Precondition: A chat history pre-exists to be generated.

Main Success Scenario

- S_1**:** Users from different departments interact with the system to access the chat log report feature.
- E_1**:** System provides a unified interface for generating chat log reports.
- S_2**:** Users specify their requirements for the chat log reports (e.g., time frame, user identifiers).
- E_2**:** System retrieves and presents the requested chat log reports tailored to each user's needs.
- S_3**:** Users review, analyze, or download the generated chat log reports for various purposes, including compliance, personal reference, decision-making, security monitoring, employee investigations, financial analysis, and system maintenance.
- E_3**:** Users utilize the information obtained from the chat log reports to fulfill their respective roles and responsibilities within their departments, contributing to the overall effectiveness and efficiency of organizational operations.

Secondary Scenario

N/A

BE8. User Adds a Contact

VP8.1 Common Employee

Precondition:

- User is registered and authenticated in the app.
- User has the contact's identifier (username, phone number, or email).

Main Success Scenario:

- S_1**:** System validates if the requested contact exists. If so, the system sends a connection request to the contact.
- E_1**:** The contact receives request and accepts it.
- S_2**:** System adds the contact to the user's contact list and opens a communication channel between user and contact.
- E_2**:** User is notified and can now begin a conversation with their contact.

Secondary Scenario:

- $E_{1.1}$**:** The requested contact is not found.
- $S_{2.1}$**:** The app displays an error, and user is promped to re-enter the contact's identifier.
- $E_{1.2}$**:** System relays declined request to user.
- $S_{2.2}$**:** User is notified of declined contact request.

VP8.2 Upper Management
N/A

VP8.3 Legal
N/A

VP8.4 Security Team
N/A

VP8.5 Human Resources
N/A

VP8.6 Finance
N/A

VP8.7 Internal IT Team

Precondition:

- Security user is registered and authenticated in the app with admin privileges.

Main Success Scenario:

- S_1**:** Add contact event modifies the communications permission handler.
- E_1**:** Security team wishes to view or make changes to permissions through an interface.
- S_2**:** System provides user permissions, and updates them accordingly.
- E_2**:** Users' contacts and communication channels are changed according to their new permissions.

Secondary Scenario: N/A

Global Scenario of Adding a Contact:

Preconditions:

- User is registered and authenticated in the app.
- User has the contact's identifier (username, phone number, or email).
- Special roles (Security Team, HR) have additional privileges.

Main Success Scenario:

- S_1**:** System validates if the requested contact exists. If so, sends a connection request.
- E_1**:** Contact receives request and accepts.
- S_2**:** System adds the contact to the user's contact list and opens a communication channel.
- E_2**:** User is notified and can now begin a conversation with their contact.
- S_3**:** Add contact event modifies communication permission handler and updates user permissions accordingly.

Secondary Scenario:

- $E_{1.1}$**:** The requested contact is not found.
- $S_{2.1}$**:** The app displays an error, and user is promped to re-enter the contact's identifier.
- $E_{1.2}$**:** System relays declined request to user.
- $S_{2.2}$**:** User is notified of declined contact request.

BE9. Removing a Contact

VP9.1 Common Employee

Precondition:

- User is registered and authenticated in the app.
- User has the contact in their contact list.

Main Success Scenario:

- S_1**:** System validates if the contact to be removed exists in the user's contact list.
- E_1**:** User selects the contact they wish to remove and confirms removal.
- S_2**:** System removes the contact from the user's contact list and closes any open communication channels with that contact.
- E_2**:** User is notified that the contact has been successfully removed.

Secondary Scenario:

- $E_{1.1}$**:** Contact is not in the user's list.
- $S_{2.1}$**:** The app displays an error, and user is prompted to check the contact's identifier.

VP9.2 Upper Management
N/A

VP9.3 Legal
N/A

VP9.4 Security Team
N/A

VP9.5 Human Resources
N/A

VP9.6 Finance
N/A

VP9.7 Internal IT Team
N/A

Global Scenario of Removing a Contact:

Preconditions:

- User is registered and authenticated in the app.
- User has the contact in their contact list.

Main Success Scenario:

- S_1**:** System checks for the existence of the contact in the user's list.
- E_1**:** User selects and confirms the removal of the contact.
- S_2**:** System removes the contact from the user's list and updates communication permissions if necessary.
- E_2**:** User receives confirmation of the contact's removal.

Secondary Scenario:

- $E_{1.1}$**:** Contact is not in the user's list.
- $S_{2.1}$**:** The app displays an error, and user is prompted to check the contact's identifier.

5 Non-Functional Requirements

5.1 Look and Feel Requirements

5.1.1 Appearance Requirements

LF-A1. The system shall use company branded colours.
Rationale: The main colours of the app will help to uniquely identify this app and associate it specifically with our company. If the buttons are a clear contrasting colour from the background it is easier to identify the buttons and interact with them accordingly.

LF-A2. Elements of the same type shall use the same font.
Rationale: The use of many fonts can be distracting for the user. This also allows this corporate app to maintain its formal nature and not come across as any typical social media app.

LF-A3. The system shall have the company logo in the app icon display.
Rationale: This is to indicate to users who the app belongs to and who the intended target is.

5.1.2 Style Requirements

LF-S1. The system shall be presented in a formal manner.
Rationale: This app is designed for formal and secure communication between employees.

LF-S2. The system shall use symbolic icons to guide users.
Rationale: The goal is for the users to be able to intuitively be able to navigate and utilize the app efficiently with the use of given contextual icons. Icons allow for the user to quickly recognize understand where to go navigate with a specified person, view previous chat logs, create a new chat, etc.

5.2 Usability and Humanity Requirements

5.2.1 Ease of Use Requirements

UH-EOU1. The app shall display only necessary elements to complete the user's task.
Rationale: The main purpose of this app is to permit secure messaging between employees and there is no need for excess visuals - it does not require a bright and colourful visual similar to that of a social media application.

UH-EOU2. Buttons shall be identified by users within 5 seconds of viewing a new screen.
Rationale: In order to interact with the app effectively, being able to locate the buttons easily and efficiently is ideal.

UH-EOU3. The system shall be able to guide users to their desired chat with minimal support or guidance.
Rationale: With the use of universal icons and the simplistic design, users will be able to instantly realize how they must interact with the app to navigate to the desired chat or begin messaging with someone new without needing to search up app functionalities or ask a colleague.

5.2.2 Personalization and Internationalization Requirements

UH-PI1. The system shall provide the option for users to receive push notifications for when they are receiving a message.
Rationale: This will allow users to stay up-to-date with conversations and be able to respond accordingly in quick succession. Without push notifications it would require users to frequently open the app and check for new messages. This gives the user an option for efficiency.

5.2.3 Learning Requirements

UH-L1. The system shall allow users to learn how to fully utilize the app and all of its features in under 10 minutes.
Rationale: The interface should be intuitive enough that users are easily able to create group chats, add members, view chat logs, delete chats and begin messaging right away. If the app takes users too long to learn how to send messages or create group chats they will be inclined to use a more intuitive app than take the time to learn the complicated process of this app. As well, if it is too complicated of a process to navigate and view previous chat logs, users will find another way of saving these logs and drive them away from this app.

5.2.4 Understandability and Politeness Requirements

UH-UP1. The system shall use icons that are clearly identifiable.
Rationale: The icons are meant to provide an easily identifiable way to quickly navigate the menus. In order to improve efficiency and best utilize the screen space, symbols must be very intuitive to understand (i.e. a house icon represents going to the home page).

5.2.5 Accessibility Requirements

UH-A1. The system shall follow the guidance of the ADOA.
Rationale: This ensures that users who may experience challenges accessing web content will be able to communicate with others through this product.[5]

5.3 Performance Requirements

5.3.1 Speed and Latency Requirements

PR-SL1. The latency between sending a message and another user receiving it should be less than 10 seconds.
Rationale: Users must be able to expect that they have received all messages and are dealing with complete information when making decisions. Extreme delay will cause uncertainty and distrust among users.

PR-SL2. Recommended text suggestions should appear within 2 seconds of a message being received.
Rationale: Users must be presented with quick response options so they can respond to a message very quickly.

5.3.2 Safety-Critical Requirements

N/A

5.3.3 Precision or Accuracy Requirements

PR-PA1. All received messages should match exactly what was sent by the user.
Rationale: Users have an expectation that the information they receive is complete and accurate. If the system does not guarantee this, it cannot be used to make business decisions.

PR-PA2. All saved message logs should match exactly what was sent by the user.
Rationale: Users have an expectation that the information they receive is complete and accurate. If the system does not guarantee this, it cannot be used to make business decisions.

5.3.4 Reliability and Availability Requirements

PR-RA1. The messaging system should be available 99.99% of the time from 8:00am to 7:00pm EST.
Rationale: Users must be able to expect the messaging function will be operational during work hours.

5.3.5 Robustness or Fault-Tolerance Requirements

PR-RFT1. The system should securely store chat logs, even in the event of database failure.
Rationale: Users have an expectation that the information they receive is complete and accurate. If the system does not guarantee this, it cannot be used to make business decisions.

5.3.6 Capacity Requirements

PR-C1. The system should be able to handle a user base of [size of company]
Rationale: The System must be able to tolerate the traffic generated by all the members of the company.

PR-C2. Group chats should be able to handle up to 10 users.
Rationale: The System must be able to tolerate large groups of user communicating. Groups larger than 10 would likely benefit from switching to another medium such as email.

5.3.7 Scalability or Extensibility Requirements

PR-SE1. The system should be built to grow at the same pace as the company hires. Capacity for the system should grow 5% per year for the next 4 years.
Rationale: The current company growth rate is 5% per year. To ensure the system can handle the new employees, it must be designed to increase capacity by this amount each year.

5.3.8 Longevity Requirements

PR-L1. System should securely store logs for duration of longest record retention date.
Rationale: The system is legally required to store certain chat logs for a period of time, in the event an audit is conducted. The system should guarantee those logs are recoverable until the last record is permitted to be deleted.

5.4 Operational and Environmental Requirements

5.4.1 Expected Physical Environment

OE-EPE1. The app shall support a range of Android devices including smartphones and tablets with varying screen-sizes.
Rationale: The NFR ensures that the app supports users with varying personal device and accessibility preferences.

5.4.2 Requirements for Interfacing with Adjacent Systems

OE-IA1. The app shall interface with third-party authentication services, ensuring a secure and seamless user login experience.
Rationale: Using third-party auth services guarantees security through proven protocols and provides familiar login experiences for the user.

OE-IA2. The app shall be compatible with Android push notifications.
Rationale: Notifications are essential for real-time communication.

5.4.3 Productization Requirements

OE-P1. The app shall include scalable server architecture to accommodate a growing user base.

5.4.4 Release Requirements

OE-R1. The app shall undergo thorough security auditing before each major release to identify and mitigate vulnerabilities.
Rationale: Security checks ensures that the app remains secure against potential threats and maintains user trust.

OE-R2. The app shall provide release notes for each update, detailing new features, improvements, and known issues to keep users informed.
Rationale: Transparency about updates and known issues fosters user trust manages expectations.

5.5 Maintainability and Support Requirements

5.5.1 Maintenance Requirements

MS-M1. The system shall have software updates weekly during off peak hours.
Rationale: As the chat application contains sensitive information, it is vital that the software is free of bugs and vulnerabilties. This will help with the maintainability of the app.

5.5.2 Supportability Requirements

MS-S1. The system shall have access to a Frequently Asked Questions (FAQ) page.
Rationale: The FAQ will allow users to troubleshoot common problems at any hour of the day, decreasing the number of technical support problems issued to the IT Team.

5.5.3 Adaptability Requirements

MS-A1. The system shall be compatabile with Android devices (Android 10 and later).
Rationale: The devices issued within the organization are Android devices. Therefore, it is important that the application can run on the Android operating system.

5.6 Security Requirements

5.6.1 Access Requirements

SR-AC1. The app shall enforce role-based access control (RBAC) to ensure users have access only to the features and data necessary for their role.
Rationale: RBAC minimizes the rist of accidental or malicious access to sensitive data.

5.6.2 Integrity Requirements

SR-INT1. The app shall use end-to-end encryption (E2EE) for all messages to ensure that only the communicating users can read the messages.
Rationale: E2EE protects against data tampering and eavesdropping.

5.6.3 Privacy Requirements

SR-P1. The app shall not store unencrypted messages on servers.
Rationale: Encrypted storage provides users privacy with their data and ensures that private conversations are not susceptible to security breaches.

5.6.4 Audit Requirements

SR-AU1. The app shall maintain secure, time-stamped logs of security-relevant events (e.g., login attempts, configuration changes).
Rationale: Time-stamped logs enables effective tracking and investigation of potential security incidents.

SR-AU2. The app shall support secure, controlled access to audit logs for authorized personnel only, ensuring the confidentiality and integrity of audit data.
Rationale: Restricting audit log access prevents tampering and unauthorized disclosure of sensitive information

5.6.5 Immunity Requirements

SR-IM1. The app shall incorporate rate limiting and other anti-automation mechanisms.
Rationale: Protects against brute-force attacks.

5.7 Cultural and Political Requirements

5.7.1 Cultural Requirements

CP-C1. N/A

5.7.2 Political Requirements

CP-P1. The application must comply with local and international data privacy regulations.
Rationale: Adherence to data privacy regulations is crucial to maintain legal compliance and protect sensitive information. Failure to comply may lead to legal consequences and damage the organization's reputation.

5.8 Legal Requirements

5.8.1 Compliance Requirements

LR-COMP1. The application must comply with relevant cybersecurity standards and best practices.
Rationale: Adhering to established cybersecurity standards ensures the application's robustness against potential threats, reducing the risk of security breaches and unauthorized access to sensitive information.

5.8.2 Standards Requirements

LR-STD1. The application must follow Android platform guidelines and best practices.
Rationale: Adhering to platform-specific guidelines ensures a consistent user experience, compatibility with future updates, and integration with other Android applications. This contributes to the overall stability and reliability of the secure chat application.

LR-STD2. The application must comply with encryption standards recommended by recognized security authorities.
Rationale: Using established encryption standards ensures the confidentiality and integrity of communications, aligning with industry best practices and protecting against potential cryptographic vulnerabilities.

A Division of Labour

Section	Team Member	Delivered on	Reviewed by	Reviewed on
1.1	Rosa	2024-02-8	Edward	2024-02-13
1.2	Rosa	2024-02-8	Edward	2024-02-13
1.3	Team	2024-02-13		
1.4	Aidan	2024-02-08	Daniel	2024-02-14
1.5	Kyle	2024-02-11	Rosa	2024-02-13
2.1	Aidan	2024-02-07	Daniel	2024-02-14
2.2	Kyle and Edward	2024-02-06	Rosa	2024-02-13
2.3	Daniel	2024-02-13	Kyle	2024-02-16
2.4	Rosa	2024-02-13	Kyle	2024-02-16
2.5	Rosa	2024-02-13	Kyle	2024-02-16
2.6	N/A			
3	Daniel	2024-02-12	Kyle	2024-02-16
4.BE1	Daniel	2024-02-06	Kyle	2024-02-11
4.BE2	Daniel	2024-02-06	Kyle	2024-02-11
4.BE3	Rosa	2024-02-8	Edward	2024-02-13
4.BE4	Rosa	2024-02-8	Edward	2024-02-13
4.BE5	Kyle	2024-02-06	Rosa	2024-02-13
4.BE6	Kyle	2024-02-06	Rosa	2024-02-13
4.BE7	Aidan	2024-02-07	Daniel	2024-02-16
4.BE8	Edward	2024-02-8	Aidan	2024-02-12
4.BE9	Edward	2024-02-8	Aidan	2024-02-12
5.1	Daniel	2024-02-06	Kyle	2024-02-13
5.2	Daniel	2024-02-06	Kyle	2024-02-13
5.3	Kyle	2024-02-06	Rosa	2024-02-13
5.4	Edward	2024-02-8	Aidan	2024-02-12
5.5	Rosa	2024-02-8	Edward	2024-02-13
5.6	Edward	2024-02-8	Aidan	2024-02-10
5.7	Aidan	2024-02-07	Daniel	2024-02-14
5.8	Aidan	2024-02-07	Daniel	2024-02-14
Appendix	Kyle	2024-02-16	Daniel	2024-02-17
Formatting	Kyle	2024-02-16	Daniel	2024-02-17

We certify the above information is correct and complete.

Kyle Jordan Ball McMaster

Daniel David Franze-Da Silva

Rosa Chen

Aidan Froggatt

Aidan Edward Froggatt

Edward Gao