Deliverable #1 Template : Software Requirement Specification (SRS)

SE 3A04: Software Design II – Large System Design

Tutorial Number: T03
Group Number: G06
Group Members:

- Virochaan Ravichandran Gowri
- Alex Yoon
- Noah Goldschmied
- Krish Dogra
- Leo Vugert

IMPORTANT NOTES

- Be sure to include all sections of the template in your document regardless whether you have something to write for each or not
  - If you do not have anything to write in a section, indicate this by the *N/A*, *void*, *none*, etc.
- Uniquely number each of your requirements for easy identification and cross-referencing
- Highlight terms that are defined in Section 1.3 (**Definitions, Acronyms, and Abbreviations**) with **bold**, *italic* or underline
- For Deliverable 1, please highlight, in some fashion, all (you may have more than one) creative and innovative features. Your creative and innovative features will generally be described in Section 2.2 (**Product Functions**), but it will depend on the type of creative or innovative features you are including.

1 Introduction

1.1 Purpose

This Software Requirement Specification has been created to specify the requirements needed to develop a secure communication app (VanklComm) for our organization. This SRS will ensure to cover functional requirements specifying how the app will perform the secure communication, including viewpoints from stakeholders and common business events and use cases and non-functional requirements outlining specifications of the system. Red text indicates a creative feature that goes beyond the project specifications.

1.2 Scope

The software product that will be produced is VanklComm, a secure chat application on Android. The product will allow for all employees of a company to communicate in a secure fashion, while also storing all texts in a database for security.

Users will be required to create an account on VanklComm and be verified by their company in order to begin chatting. The main function of the product is the person-to-person chat, however there will also be announcement boards that managers can use to notify all of their employees.

An objective of the software is to provide companies with secure chatting that prevents espionage from employees. Another objective of the software is that it must be easy to use, so that employees will have an easy transition over to the service. The last objective of the software is the encryption service. The software will provide end-to-end encryption on messages sent and received, which is what provides the secure chat.

1.3 Definitions, Acronyms, and Abbreviations

- API – Application Programming Interface
- ASDK – Android Software Developer Kit
- KDC – Key Distribution Centre
- VanklComm – Viro-Alex-Noah-Krish-Leo communication

1.4 References

[1] D. Nichols, "Coloring for Colorblindness," Davidmathlogic.com, 2019. Available: https://davidmathlogic.com/colorblind/#%23D81B60-%231E88E5-%23FFC107-%23004D40

[2] FeDev, "Why is Dark Mode more than just a trend?," Medium, Oct. 20, 2023. Available: https://bootcamp.uxdesign.cc/why-is-dark-mode-more-than-just-a-trend-224b8163acc6. Accessed: Feb. 14, 2024

[3] Washington University in St.Louis, "Performance Analysis of Data Encryption Algorithms," Wustl.edu, 2022. Available: https://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf

[4] Oracle, "Response Time Analysis Made Easy in Oracle Database 10g," Oracle.com, 2019. Available: https://www.oracle.com/technical-resources/articles/schumacher-analysis.html

[5] GPS.gov, "GPS.gov: GPS Accuracy," Gps.gov, 2019. Available: https://www.gps.gov/systems/gps/performance/accuracy

[6] Federal Trade Commission, "Use Two-factor Authentication to Protect Your Accounts," Consumer Advice, Sep. 12, 2022. Available: https://consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts#:~:text=Using%20two%2Dfactor%20authentication%20is

[7] “99.999% Uptime: Ensuring 5 Nines Uptime - Stratus Technologies,” Stratus — Zero-touch Edge Computing. Available: https://www.stratus.com/about/company-information/uptime-meter/#:~:text=Availability%20is%20normally%20expressed%20in

[8] L. Shinder and M. Cross, “Understanding Cybercrime Prevention,” Scene of the Cybercrime, pp. 505–554, 2008, doi: 10.1016/B978-1-59749-276-8.00012-1.

[9] “Google Play.” Accessed: Feb. 11, 2024. Online. Available: https://play.google.com/about/developer-distribution-agreement.html

[10] “Word list — Google developer documentation style guide — Google for Developers.” Accessed: Feb. 11, 2024. Online. Available: https://developers.google.com/style/word-list

[11] “SMS Compliance: A Comprehensive Look — Text-Em-All.” Accessed: Feb. 11, 2024. Online. Available: https://www.text-em-all.com/sms-compliance

[12] “Android App Quality Standards According to Google — by Badr Kouki — The Startup — Medium.” Accessed: Feb. 11, 2024. Online. Available: https://medium.com/swlh/android-app-quality-standards-according-to-google-5144137735b7

1.5 Overview

Section 2 provides an overview of the product's description in terms of the general factors that affect the product and its requirements. Section 3 includes our product's use case diagram that visually describes the actions taken by the system's actors to achieve a certain goal. Section 4 discusses all scenarios that are triggered by business events, organized by different viewpoints. Section 5 lists out the product's non-functional requirements along with their rationale.

2 Overall Product Description

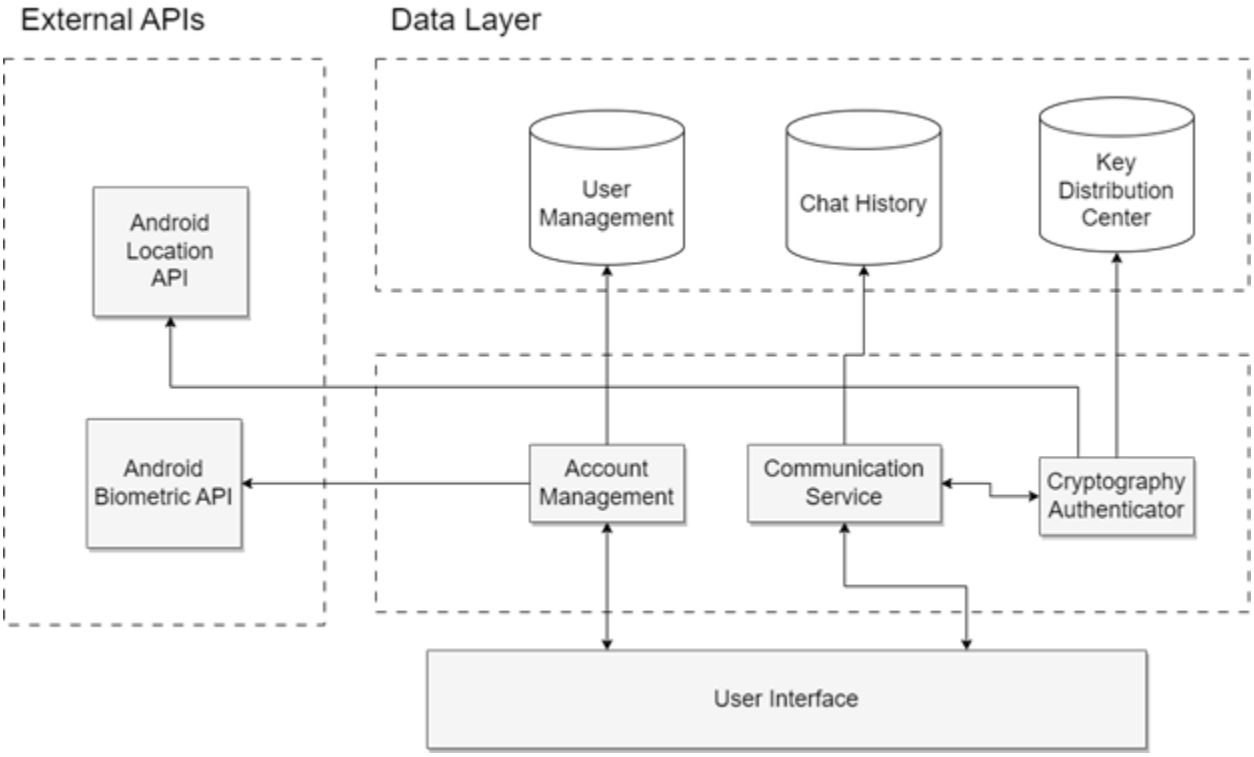
- This section should describe the general factors that affect the product and its requirements.
- It does not state specific requirements.
- It provides a *background* for those requirements and makes them easier to understand.

2.1 Product Perspective

VanklComm is a secure chat Application developed for Android and to be used solely on company devices. Other products similar to this app include other secure communication apps such as Signal and WhatsApp which allow for secure communication through End-to-End encryption of messages. VanklComm will have a focus on only allowing communication between registered agents (employees) within the company, allowing for a secure communication channel. The app will allow users to communicate securely through text and with a file sharing feature to securely transfer files between users. The user can store contacts within a contact book for fast access to other authorized users and past chat logs. The app will utilize geolocation software to ensure the app is only used in authorized locations and will utilize biometric identification for enhanced security through 2-Factor authentication.

The app will interface with Android APIs for biometric identification and geolocation. The biometric identification API will be used to allow entry into the application itself. The geolocation API will ensure usage of the app solely within the authorized locations allowed by the organization and will prompt users to reenter

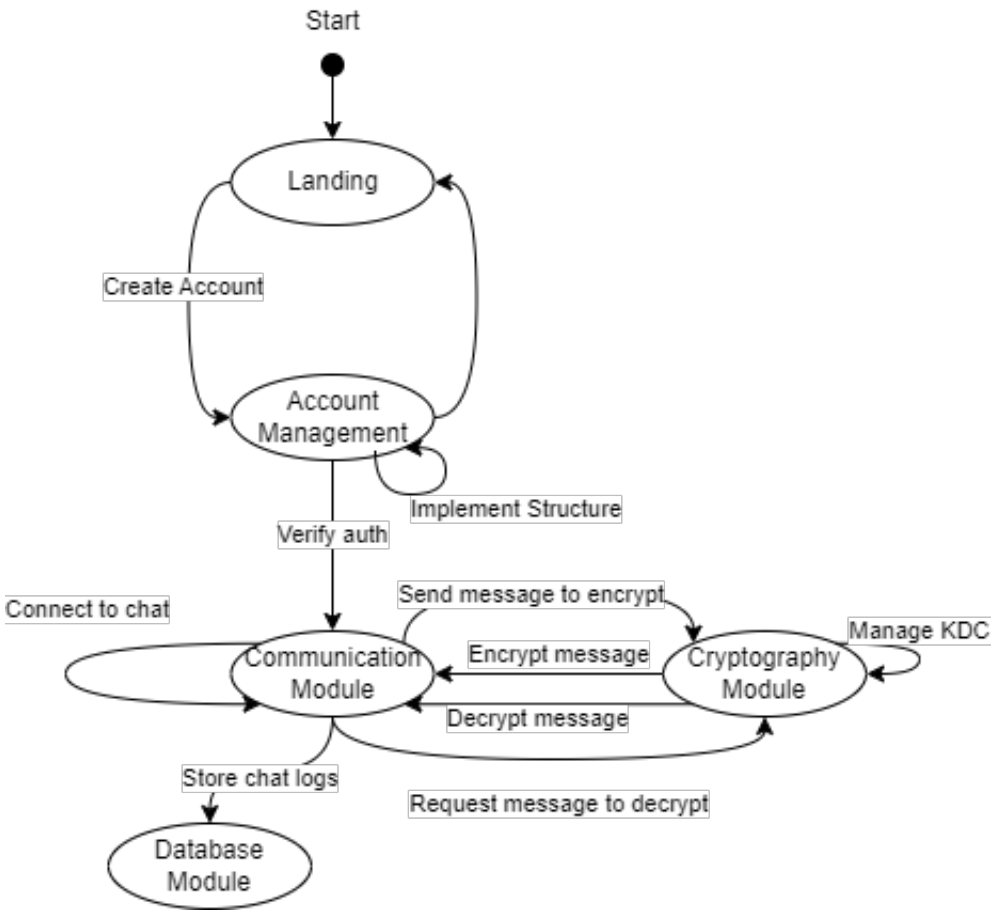
zones where they are allowed to use the app.



2.2 Product Functions

There are 4 main modules that are going to be implemented in VanklComm. These modules are the Communication module, the Account Management module, the Cryptography module, and the Database module. The Communication module will oversee most of the business value of the application, which includes chatting. The Account Management module will deal with creation and deletion of accounts, as well as implementing the company structure and verifying that the agents are authorized. The Cryptography module will deal with message encryption and decryption. The Database module will oversee how the chat logs are stored.

Module	Function
Communication Module	• Connect to chat – Allows user to connect to the chat • Send and receive messages – Allows user to send and receive messages from other users • Send and receive files – Allows user to send and receive files from other users • Receive announcement board posts – Allows user to receive messages from managers through the announcement board • Report inappropriate messages – Allows user to report inappropriate messages to admin
Account Management Module	• Create account – Allows user to create account • Delete account – Allows user to delete account • Create a contact list – Allows user to have a contact list with their frequently contacted co-workers • Manage Geolocation – Verifies that user is in the correct location • Verify agents are authorized – Oversees correct user credentials to allow signing in – Verify user using biometrics
Cryptography Module	• Manage the KDC – Ensures that the KDC works as expected • Encrypt sent messages – Encrypts the sent messages • Decrypt received messages – Decrypts the received messages
Database Module	• Store chat logs – Stores all chat logs in a secure database



2.3 User Characteristics

Education Skills: Basic Reading and Writing Skills

- Users are expected to have a basic understanding of the language used in the app, to be able to navigate different parts of the app, and to talk and text through the app

Experience: No specific experience required

- Users could be familiar with common messaging applications, but the application will be intuitive and user-friendly for anyone, even those who don't have much experience with messaging applications.

Technical Skills: Should be able to use a smartphone

- Users should have a basic understanding of how to use a smartphone, download apps and navigate different features of the hardware to be able to use the app and communicate through it.

Roles

Managers

- Managers will be able to send announcements through to many employees in a one way communication channel.

Employee

- Basic communication abilities, can message, call, share files, etc. with others. Can not make announcements like managers.

2.4 Constraints

- Provide a general description of any constraints that will limit the developer's options

2.5 Assumptions and Dependencies

- List any assumptions you made in interpreting what the software being developed is aiming to achieve
- List any other assumptions you made that, if it fails to hold, could require you to change the requirements
  - **Example**: An assumption may be that a specific operating system will be available on the hardware designated for the software product. If, in fact, the operating system is not available, the SRS would then have to change accordingly.

2.6 Apportioning of Requirements

1. Cross-Platform Compatibility:

The initial version of the secure chat application will be strictly developed for the Android platform. However, we will consider extending support to iOS and other mobile operating systems in later versions. This will allow our application to cater to a wider variety of users.

2. Secure Group Chat Communication:

The initial version of our application will only provide encrypted one-on-one communication between company employees. Future versions may introduce a group chat feature, which allows multiple users to communicate in a group setting, all the while ensuring a safe and secure platform. This will benefit users by allowing them to efficiently coordinate tasks with many employees, including file transfer, calendar scheduling, and more.

3. Secure Video Conferencing:

The app's initial version only considers communication in terms of text-based messages and file sharing between users. However, later versions could support an integration with secure video conferencing systems, allowing users to interact in encrypted video calls for a more immersive experience.

3 Use Case Diagram

- Provide the use case diagram for the system being developed.
- You do not need to provide the textual description of any of the use cases here (these will be specified under "Highlights of Functional Requirements").

4 Highlights of Functional Requirements

Main Business Events: List out all the main business events you are presenting. If you sub-divided into smaller ones, you don't need to include the smaller ones in this list.

- BE1 Secure Communication
- BE2 Chat History Log
- BE3 Contact Book
- BE4 Secure File Sharing

- BE5 Broadcasting Channel
- BE6 User Registration
- BE7 Authentication Protocol
- BE8 Key Updates
- BE9 Biometric Authentication
- BE10 Geolocation

Viewpoints: List out all the viewpoints you will be considering.

- VP1 User
- VP2 Tech Support/IT
- VP3 KDC Administrator
- VP4 Security Auditors/Cybersecurity
- VP5 Legal Department
- VP6 Board of Directors

Interpretation: Specify any liberties you took in interpreting business events, if necessary.

Business Events:

1BE. Secure Communication #1

Precondition:

The secure chat application has already been installed on an Android device, and the user has an account.

1VP. User #1

Main Success Scenario:

1. The user logs into the VANKL secure chat application.
2. The system authenticates the user.
3. Once authenticated, the user may engage in various tasks, including secure communication, accessing the chat's history log, utilizing the contact book, sharing files securely, and receiving broadcasts from higher authority.

Secondary Scenarios:

2i. The system fails to authenticate the user.

2i.1 The system will prompt the user to retry for authentication.

2i.2 If the issue persists, then the user will be redirected to contact tech support.

3i. The user experiences delays when trying to access the chat's history log, due to server overload issues.

3i.1 The system provides a display message to inform the user of this delay and apologizes for the inconvenience.

3i.2 The system will continuously attempt to alleviate the increased demand, by utilizing backup servers, caching, and load balancing.

2VP. Tech Support/IT #2

2i. The system fails to authenticate Tech Support/IT.

3i. Tech Support/IT faces challenges during debugging and troubleshooting, due to an unexpected server outage.

3VP. KDC Administrator #3

N/A

4VP. Security Auditors/Cybersecurity #4

2i. The system fails to authenticate the Security Auditors/Cybersecurity.

3i. The Security Auditors/Cybersecurity encounter issues while accessing specific logs, due to a temporary system glitch.

5VP. Legal Department #5

N/A

6VP. Board of Directors #6

2i. The system fails to authenticate the Board of Directors.

3i. The Board of Directors encounter delays while sending a one-way message in the broadcasting channel, due to server overload.

Global Scenario:

Precondition:

The secure chat application has already been installed on an Android device, the user has an account, and all necessary configurations have been made.

Main Success Scenario:

1. The user, Tech Support/IT, Security Auditors/Cybersecurity, Legal Department, and the Board of Directors all log into the VANKL secure chat application (not necessarily simultaneously).
2. The system authenticates each entity successfully.
3. Each entity performs their respective tasks and actions within the application.

Secondary Scenarios:

2i. The system fails to authenticate any entity.

2i.1 The system will prompt that entity to retry for authentication.

2i.2 If the issue persists, then that entity will be redirected to contact their respective support department (not necessarily Tech Support/IT).

3i. An entity faces issues related to the various functionalities of the application, due to server problems.

3i.1 The system provides a global display message to acknowledge the issue(s), and assures the entity(s) that Tech Support/IT is working on a resolution.

2BE. Chat History Log #2

Precondition:

The secure chat application has already been installed on an Android device, and the user has an account.

1VP. User #1

Main Success Scenario:

1. The user logs into the VANKL secure chat application.
2. The system authenticates the user.
3. Once authenticated, the user can access their chat's history log.
4. The system displays specific identifiers, date, time, and an up-to-date chat transcript for each conversation.

Secondary Scenarios:

2i. The system fails to authenticate the user.

2i.1 The system will prompt the user to retry for authentication.

2i.2 If the issue persists, then the user will be redirected to contact tech support.

3i. The user experiences delays when trying to access the chat's history log, due to server overload issues.

3i.1 The system provides a display message to inform the user of this delay and apologizes for the inconvenience.

3i.2 The system will continuously attempt to alleviate the increased demand, by utilizing backup servers, caching, and load balancing.

4i. While viewing a specific conversation, the system experiences a temporary glitch, which results in missing or incomplete messages.

4i.1 The system provides a display message to inform the user of this issue, and apologizes for the inconvenience.

4i.2 The system then advises the user to refresh the chat log or contact Tech Support/IT, if the problem still persists.

2VP. Tech Support/IT #2

N/A

3VP. KDC Administrator #3

N/A

4VP. Security Auditors/Cybersecurity #4

N/A

5VP. Legal Department #5

N/A

6VP. Board of Directors #6

N/A

Global Scenario:

Precondition:

The secure chat application has already been installed on an Android device, the user has an account, and all necessary configurations have been made.

Main Success Scenario:

1. The user, Tech Support/IT, Security Auditors/Cybersecurity, Legal Department, and the Board of Directors all log into the VANKL secure chat application (not necessarily simultaneously).
2. The system authenticates each entity successfully.
3. Each entity accesses their respective chat history log that has accurate and up-to-date conversation records.

Secondary Scenarios:

2i. The system fails to authenticate any entity.

2i.1 The system will prompt that entity to retry for authentication.

2i.2 If the issue persists, then that entity will be redirected to contact their respective support department (not necessarily Tech Support/IT).

3i. An entity faces delays in accessing specific chat history logs, due to server problems.

3i.1 The system provides a global display message to acknowledge the issue(s), and assures the entity(s) that Tech Support/IT is working on a resolution.

4i. An entity faces system glitches, resulting in missing or incomplete messages while viewing conversations.

4i.1 The system provides an error message and advises the entity(s) to report this issue to management (Board of Directors), who will in turn contact Tech Support/IT for investigating this issue.

3BE. Contact Book #3

Precondition:

The secure chat application has already been installed on an Android device, and the user has an account.

1VP. User #1

Main Success Scenario:

1. The user logs into the VANKL secure chat application.
2. The system authenticates the user.
3. Once authenticated, the user can access their contact book.
4. The system provides saved agents' contact information for easier communication access.
5. The user can easily add, edit, and/or delete contacts as required.

Secondary Scenarios:

2i. The system fails to authenticate the user.

2i.1 The system will prompt the user to retry for authentication.

2i.2 If the issue persists, then the user will be redirected to contact tech support.

3i. The user experiences delays when trying to access their contact book, due to server overload issues.

3i.1 The system provides a display message to inform the user of this delay, and apologizes for the inconvenience.

3i.2 The system will continuously attempt to alleviate the increased demand, by utilizing backup servers, caching, and load balancing.

4i. When searching for an employee's contact, the system experiences a temporary glitch, which leads to missing contact information.

4i.1 The system provides a display message to inform the user of this error, and apologizes for the inconvenience.

4i.2 The system advises the user to refresh the contact book or contact Tech Support/IT, if the issue still persists.

5i. When accessing the contact book to add, edit, and/or delete contacts, the system faces a navigation malfunction.

5i.1 When the user attempts to access the contact book feature, the system runs into a malfunction with the navigation subsystem.

5i.2 The system provides an error message to the user apologizing for the inconvenience and logs an incident report for the tech team to assess and resolve.

2VP. Tech Support/IT #2

N/A

3VP. KDC Administrator #3

N/A

4VP. Security Auditors/Cybersecurity #4

N/A

5VP. Legal Department #5

N/A

6VP. Board of Directors #6

N/A

Global Scenario:

Precondition:

The secure chat application has already been installed on an Android device, the user has an account, and all necessary configurations have been made.

Main Success Scenario:

1. The user, Tech Support/IT, Security Auditors/Cybersecurity, Legal Department, and the Board of Directors all log into the VANKL secure chat application (not necessarily simultaneously).
2. The system authenticates each entity successfully.
3. Only the users can access the contact book and view their saved agents' information for easier communication access.

Secondary Scenarios:

2i. The system fails to authenticate any entity.

2i.1 The system will prompt that entity to retry for authentication.

2i.2 If the issue persists, then that entity will be redirected to contact their respective support department (not necessarily Tech Support/IT).

3i. A user faces issues when trying to open their contact book, such as accessing delays or missing/incomplete contact information.

3i.1 The system provides a display message to acknowledge that Tech Support/IT is working on a resolution.

3i.2 The system advises the user to refresh the contact book or access it at a later time.

4BE. Secure File Sharing #4

Precondition:

The secure chat application has already been installed on an Android device, and the user has an account.

1VP. User #1

Main Success Scenario:

1. The user logs into the VANKL secure chat application.
2. The system authenticates the user.
3. Once authenticated, the user can initiate secure file sharing.
4. The system will encrypt the file and facilitate secure transmission.
5. The file recipient will then decrypt and access the shared file.

Secondary Scenarios:

2i. The system fails to authenticate the user.

2i.1 The system will prompt the user to retry for authentication.

2i.2 If the issue persists, then the user will be redirected to contact tech support.

3i. The user experiences delays when trying to initiate secure file transfer, due to server overload issues.

3i.1 The system provides a display message to inform the user of this delay, and apologizes for the inconvenience.

3i.2 The system will continuously attempt to alleviate the increased demand, by utilizing backup servers, caching, and load balancing.

4i. When encrypting the file, the system experiences a temporary glitch, which leads to a delay in the transmission process.

4i.1 The system provides a display message to inform the user of this error, and apologizes for the inconvenience.

4i.2 The system advises the user to retry file sharing or contact Tech Support/IT, if the issue still persists.

2VP. Tech Support/IT #2

N/A

3VP. KDC Administrator #3

N/A

4VP. Security Auditors/Cybersecurity #4

N/A

5VP. Legal Department #5

N/A

6VP. Board of Directors #6

N/A

Global Scenario:

Precondition:

The secure chat application has already been installed on an Android device, the user has an account, and all necessary configurations have been made.

Main Success Scenario:

1. The user, Tech Support/IT, Security Auditors/Cybersecurity, Legal Department, and the Board of Directors all log into the VANKL secure chat application (not necessarily simultaneously).
2. The system authenticates each entity successfully.
3. Only the users can initiate secure file transfer between the employees of the company.

Secondary Scenarios:

2i. The system fails to authenticate any entity.

2i.1 The system will prompt that entity to retry for authentication.

2i.2 If the issue persists, then that entity will be redirected to contact their respective support department (not necessarily Tech Support/IT).

3i. A user faces delays in the secure file sharing process, due to server issues.

3i.1 The system provides a display message to acknowledge that Tech Support/IT is working on a resolution.

3i.2 The system advises the user to retry the file transfer or try again at a later time.

4i. The system faces temporary glitches resulting in missing/incomplete file transfer.

4i.1 The system provides a display message to acknowledge that Tech Support/IT is working on a resolution.

4i.2 The system advises the user to retry the file transfer when the glitches have been fixed at a later date.

5BE. Broadcasting Channel #5

Precondition:

The secure chat application has already been installed on an Android device, and the user has an account.

1VP. User #1

Main Success Scenario:

1. The user logs into the VANKL secure chat application.
2. The system authenticates the user.
3. Once authenticated, the user can access the one-way broadcasting channel feature.
4. The system allows users to view the broadcasted announcements sent out by their superiors (i.e. Board of Directors).

Secondary Scenarios:

2i. The system fails to authenticate the user.

2i.1 The system will prompt the user to retry for authentication.

2i.2 If the issue persists, then the user will be redirected to contact tech support.

3i. The user experiences delays when trying to access the broadcasting channel, due to server overload issues.

3i.1 The system provides a display message to inform the user of this delay, and apologizes for the inconvenience.

3i.2 The system will continuously attempt to alleviate the increased demand, by utilizing backup servers, caching, and load balancing.

4i. The system experiences a temporary glitch, which leads to missing one-way messages in the broadcasting channel.

4i.1 The system provides a display message to inform the user of this issue, and apologizes for the inconvenience.

4i.2 The system advises the user to report this issue to Tech Support/IT.

2VP. Tech Support/IT #2

N/A

3VP. KDC Administrator #3

N/A

4VP. Security Auditors/Cybersecurity #4

N/A

5VP. Legal Department #5

N/A

6VP. Board of Directors #6

2i. The system fails to authenticate a Board of Directors member.

3i. The Board of Directors member experiences delays when trying to access the broadcasting channel, due to server overload issues.

4i. The system experiences a temporary glitch, which leads to missing one-way messages (that a member has sent) in the broadcasting channel.

Global Scenario:

Precondition:

The secure chat application has already been installed on an Android device, the user has an account, and all necessary configurations have been made.

Main Success Scenario:

1. The user, Tech Support/IT, Security Auditors/Cybersecurity, Legal Department, and the Board of Directors all log into the VANKL secure chat application (not necessarily simultaneously).
2. The system authenticates each entity successfully.
3. Only the users and the Board of Directors can utilize the broadcasting channel feature, where users (i.e. employees) can view one-way messages and board members can send one-way messages.

Secondary Scenarios:

2i. The system fails to authenticate any entity.

- **2i.1** The system will prompt that entity to retry for authentication.
- **2i.2** If the issue persists, then that entity will be redirected to contact their respective support department (not necessarily Tech Support/IT).

3i. An entity faces delays in accessing the broadcasting channel, due to server issues.

- **3i.1** The system provides a display message to acknowledge that Tech Support/IT is working on a resolution.
- **3i.2** The system advises the entity(s) to refresh the broadcasting channel or try again at a later time.

4i. The system faces temporary glitches resulting in missing/incomplete one-way messages in the broadcasting channel.

- **4i.1** The system provides a display message to acknowledge that Tech Support/IT is working on a resolution.
- **4i.2** The system advises the entity(s) to access the broadcasting channel when the glitches have been fixed at a later date.

6BE. User Registration #6

Precondition:

- User does not have an account
- User was granted access to company issued device/email
- User is connected to company WIFI
- The KDC server is operational

1VP. User #1

Main Success Scenario:

1. User gains access to make an account
2. User initiates sign in
3. User inputs information
4. User is provided key from KDC
5. User is prompted with success message

Secondary Scenarios:

2i. User inputs incorrect information

2i.1 User submits incorrect information
2i.2 Prompts user to recheck information and resubmit

2VP. Tech Support/IT #2

1i. IT provides the app with authorization for user's information and provided email

3VP. KDC Administrator #3

4i. KDC provides key

4i.1 KDC checks users authorization status
4i.2 KDC generates encryption key

4i. User inputted incorrect information

4i.1 KDC checks user authorization status
4i.2 Denies access and does not generate key

4VP. Security Auditors/Cybersecurity #4

N/A

5VP. Legal Department #5

N/A

6VP. Board of Directors #6

N/A

Global Scenario:

Precondition:

- User does not have an account
- User was granted access to company issued device/email
- User is connected to company WIFI
- The KDC server is operational

Main Success Scenario:

1. User gains access to make an account
2. User initiates sign in
3. User inputs information
4. User is provided key from KDC
5. User is prompted with success message

Secondary Scenarios:

2i. User inputs incorrect information

2i.1 User submits incorrect information
2i.2 Prompts user to recheck information and resubmit

7BE. Authentication Protocol #7

Precondition:

- User attempts to access the chat application
- Initiates authentication process

1VP. User #1

Main Success Scenario:

1. The user opens the chat application
2. The user provides their username and password to sign in to the chat application
3. The application authenticates the user's credentials
4. Upon successful authentication, the user gains access to the application's features

Secondary Success Scenario:

2i. User inputs incorrect information

2i.1 Prompted to re-enter information

2VP. Tech Support/IT #2

2i. User has too many failed attempts to authenticate

2i.1 IT support is notified of the failed attempts
2i.2 IT support will contact the user to assist with the authentication process
2i.3 IT support will reset the user's password if necessary

3VP. KDC Administrator #3

N/A

4VP. Security Auditors/Cybersecurity #4

N/A

5VP. Legal Department #5

N/A

6VP. Board of Directors #6

N/A

Global Scenario:

Precondition:

- User attempts to access the chat application
- Initiates authentication process

Main Success Scenario:

1. User opens the chat application
2. User provides their username and password
3. The application authenticates the user's credentials
4. Upon successful authentication, the user gains access to the application's features

Secondary Success Scenario:

2i. User inputs incorrect information

2i.1 Prompted to re-enter information

8BE. Key Update #8

Precondition:

- The KDC has new keys to distribute for secure communication.

1VP. User

Main Success Scenario:

1. KDC sends new key updates to user's device
2. User receives a notification about the availability of new keys.
3. User's device automatically updates the keys without requiring manual intervention
4. User continues to use the secure chat application with updated keys

Secondary Success Scenario:

2i. User misses notification/update because they were disconnected

2i.1 User can manually hit update button and update keys

2VP. Tech Support/IT #2

N/A

3VP. KDC Administrator #3

1i. KDC generates new keys and pushes notifications for key updates

1i.1 KDC sends new key updates to user's device

1i.2 KDC sends a notification about the availability of new keys

4VP. Security Auditors/Cybersecurity #4

1i. Security Auditors/Cybersecurity monitors the key update process

1i.1 Security Auditors/Cybersecurity checks the integrity of the new keys

1i.2 Security Auditors/Cybersecurity ensure the new keys are distributed securely

5VP. Legal Department #5

N/A

6VP. Board of Directors #6

N/A

Global Scenario:

Precondition:

- The KDC has new keys to distribute for secure communication.

Main Success Scenario:

1. KDC sends new key updates to user's device
2. User receives a notification about the availability of new keys.
3. User's device automatically updates the keys without requiring manual intervention
4. User continues to use the secure chat application with updated keys

Secondary Success Scenario:

2i. User misses notification/update because they were disconnected

2i.1 User can manually hit update button and update keys

9BE. Biometric Authentication #9

Preconditions:

- User has biometric authentication enabled
- Device has methods of biometric authentication built-in
- Chat application supports biometric authentication

1VP. User

Main Success Scenario:

1. User opens the app
2. The app prompts the user for biometric authentication (ex. fingerprint, facial recognition)
3. User provides biometric data
4. The app verifies the biometric data and grants access to the app upon successful authentication

Secondary Success Scenario:

4i. Biometric data fails

4i.1 Prompts user to enter password
4i.2 Grants access to app with correct password

2VP. Tech Support/IT

N/A

3VP. KDC Administrator

N/A

4VP. Security Auditors/Cybersecurity

4i. Security Auditors/Cybersecurity ensure biometric data and authentication is secure

4i.1 Biometric data is provided by the user
4i.2 Biometric data is encrypted and stored securely on the device

5VP. Legal Department

N/A

6VP. Board of Directors

N/A

Global Scenario:

Preconditions:

- User has biometric authentication enabled
- Device has methods of biometric authentication built-in
- Chat application supports biometric authentication

Main Success Scenario:

1. User opens the app
2. The app prompts the user for biometric authentication (ex. fingerprint, facial recognition)
3. User provides biometric data
4. The app verifies the biometric data and grants access to the app upon successful authentication

Secondary Success Scenario:

4i. Biometric data fails

4i.1 Prompts user to enter password

4i.2 Grants access to app with correct password

10BE. Geolocation #10

Preconditions:

- The app is installed on the user's device
- The device has location services enabled
- The company defines specific areas where access to the application is allowed

1VP. User

Main Success Scenario:

1. User launches the app
2. The app detects the user's location using geolocation services
3. If the user is within the designated area, access to the application is granted
4. User can use the application as usual

Secondary Success Scenario:

3i. User is outside the designated area

3i.1 They are notified that they are outside the designated area

3i.2 Access to the application is restricted

2VP. Tech Support/IT

N/A

3VP. KDC Administrator

N/A

4VP. Security Auditors/Cybersecurity

2i. The app detects the users location

2i.1 The application securely stores the user's location data and checks if the user is within the designated area, locally, on the device

5VP. Legal Department

N/A

6VP. Board of Directors

N/A

Global Scenario:

Preconditions:

- The app is installed on the user's device
- The device has location services enabled
- The company defines specific areas where access to the application is allowed

Main Success Scenario:

1. User launches the app
2. The app detects the user's location using geolocation services
3. If the user is within the designated area, access to the application is granted
4. User can use the application as usual

Secondary Success Scenario:

3i. User is outside the designated area

3i.1 They are notified that they are outside the designated area

3i.2 Access to the application is restricted

5 Non-Functional Requirements

- For each non-functional requirement, provide a justification/rationale for it.
  Example:
  SC1. *The device should not explode in a customer's pocket.*
  Rationale Other companies have had issues with the batteries they used in their phones randomly exploding [insert citation]. This causes a safety issue, as the phone is often carried in a person's hand or pocket.
- If you need to make a guess because you couldn't really talk to stakeholders, you can say "We imagined stakeholders would want...because..."
- Each requirement should have a unique label/number for it.
- In the list below, if a particular section doesn't apply, just write N/A so we know you considered it.

5.1 Look and Feel Requirements

5.1.1 Appearance Requirements

LF-A1.

5.1.2 Style Requirements

LF-S1.

5.2 Usability and Humanity Requirements

5.2.1 Ease of Use Requirements

UH-EOU1. Users should be allowed to report errors and areas of improvement through the organization's in-app feedback tool.
Rationale: The system will provide a way of reporting bugs and errors and provide general feedback or areas of improvement which the organization can then act upon. It will be done through the organization to provide maximum transparency for all stakeholders involved and keep them in the loop about future developments.

UH-EOU2. On first download, users should be given a short tutorial on the correct usage of the app.
Rationale: The tutorial will allow every employee to have a base understanding of the usage of the app and will protect the organization to make sure users properly authenticate before communicating. The tutorial will also indicate certain accessibility features for users that require it to ensure effective usage of the app.

UH-EOU3. The system should provide users with a help section including FAQs and recapping the Tutorial.
Rationale: While using the app, if a user should face difficulty or forget the location or usage of certain features, they can use the help section to see if their question or problem can be resolved. It will also recap the tutorial including basic usage and accessibility features of the app.

5.2.2 Personalization and Internationalization Requirements

UH-PI1. The system should allow users to change the language to any of the provided languages based on their preferences.
Rationale: Users must be able to utilize the app effectively, so it is crucial they understand the different headings and labels within the app. This is also represented within the tutorial as it will be translated into the provided languages. We will only provide languages that the organization uses in day-to-day work as there is an expectation that the employees will understand these languages.

UH-PI2. The user should be allowed to change the font based on one's own preference.
Rationale: Allows the user to customize the font which will apply to all facets of the app for an overall better experience. Some people like different fonts for readability and giving them this option can only raise the overall user experience of using the app.

UH-PI3. The user should be allowed to change the background of the chat and home screens.
Rationale: Provides users with greater customization to make the app more personal to them. Increasing the options available to the user can improve the user experience and make the app more personal to them.

5.2.3 Learning Requirements

UH-L1. Users should be able to set up and use the app within 10 minutes of downloading.
Rationale: The process for registering a user's account and then using the app after watching the tutorial should be able to be completed within 10 minutes of the first usage of the app. Keeping the whole set up process short increases user retention using the app and a short, yet comprehensive tutorial ensures that information on usage is more easily understood.

5.2.4 Understandability and Politeness Requirements

UH-UP1. Symbols for messaging and adding users should be universally recognized and the standard for all mobile apps.
Rationale: To properly utilize the app the user must be able to understand all iconograph. By matching our icons with the ones that are used in other similar apps we can ensure that the average user will be able to seamlessly make the transition to using our app without confusion and contribute to a lower learning curve for the app.

5.2.5 Accessibility Requirements

UH-A1. The user should be allowed to change font size for better visibility.
Rationale: This feature should be implemented to ensure ease of use for persons who are more visually impaired. This font size should be global for the app to ensure that users with visual difficulties can always understand what is on the screen.

UH-A2. Implement a colorblind mode which changes the color palette to use more accessible colours.
Rationale: This feature should be implemented to ensure ease of use for persons who are colour blind and have difficulty differentiating between colours. The color-blind mode should utilize the Deuteranomaly friendly colour palette so the user can differentiate the colours displayed. [1]

UH-A3. A high contrast/dark color mode should be implemented for better visibility and for usage during nighttime.
Rationale: This feature should be implemented to ensure ease of use for people who are more visually impaired and require better distinctions between certain colours. Can be a tool for people who want a dark mode as well and provide better distinction between icons, symbols, and lettering when being used during nighttime or in low lighting. Including a dark mode will greatly increase user experience and provide further customization for the user. [2]

UH-A4. The system should implement an on-screen reader for the visually impaired.
Rationale: An on-screen reader is essential for visually impaired people as it allows them to utilize the app more effectively. The on-screen reader should allow for easier navigation through the app as well as provide text-to-speech conversion of messages.

UH-A5. The system should implement a dictation feature which converts voice to messages.
Rationale: Provides the user with more methods of performing communication and sending messages. Can help persons with limited dexterity in their fingers by providing an alternative method of communication.

5.3 Performance Requirements

5.3.1 Speed and Latency Requirements

PR-SL1. The KDC should have less than a 2-second response time when returning keys.
Rationale: The KDC should be able to return keys within 2 seconds of receiving the request from an agent. This time is more than enough to send the key as it does not consider the generation/rotation of keys. This will also ensure agents do not spend a long time waiting to enter a chat due to the KDC having large delays providing a seamless experience.

PR-SL2. The time taken to encrypt and decrypt using key should be less than 2s.
Rationale: After receiving the key, the encryption and decryption of data should not take longer than 2 seconds since the payload of the data is quite small ranging in the kilobytes of size. We can see that through experimental testing of the algorithms 2 seconds should be more enough to encrypt and decrypt payloads of this size and this represents the worst-case scenario. [3]

PR-SL3. The message should be received by the receiving communicating agent in less than 10s after being sent.
Rationale: We want to ensure that global standards are met for delivering and receiving messages, but it also needs to be taken into account that these messages are being encrypted and decrypted, which adds extra time. This is why we believe 7.5 seconds is a good realistic timespan in which it doesn't introduce that large of a delay between send and receive while maintaining a high level of security.

PR-SL4. Time taken to access chat logs from the database server should be less than 10 seconds.
Rationale: Should an administrator require access to a certain chat log this should be done in a prompt manner and querying data should be fast and efficient. This can aid in Incident Response should there be a security breach, or some other concern related to an employee's behavior aiding in a fast investigation. 10 seconds provides both a realistic timeframe for querying through large amounts of data while still being prompt in the response time. [4]

5.3.2 Safety-Critical Requirements

PR-SC1. N/A

5.3.3 Precision or Accuracy Requirements

PR-PA1. The app must be only used in accepted locations with an error of location of maximum of 20 meters.
Rationale: Most Android Devices utilize some sort of GPS software to ensure accurate location of the device. The average accuracy of GPS enabled devices is around 5m but this can worsen due to location and spotty cell/Wi-Fi service. [5] By expanding the range to 20 meters we account for potential inaccuracies while still maintaining security.

PR-PA2. Fingerprint identification should have 99% accuracy in identifying users.
Rationale: The biometric identification feature should have a 99% accuracy to ensure only authorized users are able to gain entry to the access. This high level of accuracy ensures security by not misidentifying users while still attempting to minimize the total time taken to enter the app by fast identification. It also enables us to use 2-Factor Authentication which is a much more secure method of identification. [6]

5.3.4 Reliability and Availability Requirements

PR-RA1. The app should have a scheduled downtime of a maximum of 1 hour every 6 months to ensure proper functionality.
Rationale: Provides enough time for required maintenance on the app as necessary while maintaining a high level of availability. This higher time of downtime is justified due to the clandestine nature of the app and security being of utmost priority. Since this is a company-wide app it is easy to inform individuals using the app of the scheduled downtime limiting the risk and inconvenience.

PR-RA2. The Database server should maintain a backup of the data in cold data storage.
Rationale: Ensuring that we keep a backup of the data but stored in cold data storage to save resources as hopefully we will not be needed to access the backup. The accessing of the data in the backup may take a long time if necessary and is primarily used just to ensure data security.

PR-RA3. The app should strive for 99.999% availability during normal operation.
Rationale: When the app is being used during standard situations, we should aim for it to have 99.999% availability as it will ensure that all members of the company remain connected. 99.999% or 5 nines uptime is industry standard and the highest realistic uptime necessary for the app to maintain continuous availability. [7]

5.3.5 Robustness or Fault-Tolerance Requirements

PR-RFT1. The app should function as long as there is cell service in the area.
Rationale: The app should be able to work on mobile data and is not limited to only Wi-Fi. This ensures that communication will still work when Wi-Fi networks are down, ensuring employees can remain connected.

5.3.6 Capacity Requirements

PR-C1. The KDC should be able to handle 20% of the userbase's requests at the same time.
Rationale: Ensures that the KDC meets capacity while also considering scalability in terms of requests. We could say a fixed number such as 20 but if the company has 10000 people with the app there is a high likelihood that more than 20 people request keys at the same time during peak usage of the app. By maintaining this requirement as a percentage, we can maintain both scalability and have good capacity throughput.

PR-C2. The Initial Database Server should have a minimum of 1TB storage before scaling.
Rationale: We want to have a large base server size to ensure that we do not need to start scaling unnecessarily expending valuable resources on maintaining the database. 1TB of storage can store multiple years worth of data without

5.3.7 Scalability or Extensibility Requirements

PR-SE1. The app should maintain at least 5% of the database empty to ensure space for future chat logs.
Rationale: Allow for scalability to store more chat logs in the future. Ensure that we never reach a situation where there are chats coming in but not being stored due to the full capacity in the database server. 5% also provides a good buffer space if there is a sudden influx of data providing time for the database to scale to the new capacity.

5.3.8 Longevity Requirements

PR-L1. The app in its first iteration must be able to last a minimum of 2 years with avenues for extension or improvement.
Rationale: Current iteration should be usable by employees and based on feedback and bug reporting we can provide future updates or overhauls. This process could take a long time so it is important the current iteration lasts at least 2 years for feedback to be collected and updates developed.

5.4 Operational and Environmental Requirements

5.4.1 Expected Physical Environment

OE-EPE1.

5.4.2 Requirements for Interfacing with Adjacent Systems

OE-IA1.

5.4.3 Productization Requirements

OE-P1.

5.4.4 Release Requirements

OE-R1.

5.5 Maintainability and Support Requirements

5.5.1 Maintenance Requirements

MS-M1.

5.5.2 Supportability Requirements

MS-S1.

5.5.3 Adaptability Requirements

MS-A1.

5.6 Security Requirements

5.6.1 Access Requirements

SR-AC1. User must be logged into the application to access any information.
Rationale: This is to ensure that only users that have verified their credentials have access to any potentially sensitive information or features.

SR-AC2. User must be a part of the company verified list.
Rationale: For a user to join any chats or announcement boards they must be a verified member of the company that oversees the chats.

SR-AC3. User must not have access to ant chats, files or announcements that they do not belong to.
Rationale: To maintain the secure aspect of the application, only users that belong to certain chats, files or announcements may view them.

SR-AC4. User must consent to have their location being used.
Rationale: To ensure that the user is within a verified geolocation, the app needs permission to use their GPS location to determine if the location is verified.

SR-AC5. User must consent to have their biometric data being used.
Rationale: To utilize biometric data for effective two-factor authentication, the app needs permission to use the biometric data to determine if the user is who they say they are.

5.6.2 Integrity Requirements

SR-INT1. The system will use an industry accepted end-to-end symmetric-key cryptosystem algorithm.
Rationale: To ensure that the messages being sent back and forth are not being modified in the middle, an end-to-end encryption is necessary. The algorithm to be used will be one of the industry standard algorithms (AES, 3-DES) [8].

SR-INT2. Chat logs will be stored separately from the rest of the system.
Rationale: To ensure that the chat logs are not tampered with, they will be stored on a database that is separate from the system that only admins have access to.

SR-INT3. Users should not change their name unless company allows it.
Rationale: To verify that users know who they are chatting to, users should not be allowed to change their name unless given permission by the company.

5.6.3 Privacy Requirements

SR-P1. The application will adhere to the Google Play Developer Distribution Agreement.
Rationale: As this app is going to be developed for android, adhering to the GPDDA is a step to ensure that privacy is being kept [9].

SR-P2. Personal information of users should not be displayed to anyone outside of themselves.
Rationale: To keep information such as age, gender, an employees department, etc. private, this information should not be displayed to those they are chatting to.

SR-P3. Notifications should not display message content.
Rationale: To maintain the purpose of secure communication, notifications should not contain sensitive information, and rather have a message similar to "you have a notification from VanklComm, you have 8 unread messages".

5.6.4 Audit Requirements

SR-AU1. The app must comply with company guidelines for auditing employee chats.
Rationale: To allow for the company to regulate the chats that their employee's send, the app must provide a way for them to audit effectively.

5.6.5 Immunity Requirements

SR-IM1. Verify with the KDC that the user is authorized.
Rationale: To protect against malware or bad actors, only users authorized by the KDC may use the app.

5.7 Cultural and Political Requirements

5.7.1 Cultural Requirements

CP-C1. No offensive imagery will be used in the composition of the app.
Rationale: To make the app a safe space for all users, any imagery that is known to be offensive to any group of people must be erased from the app.

CP-C2. The app will not send messages that contain inappropriate words.
Rationale: Using Google's Word list [10] the use of inappropriate words will not be tolerated.

CP-C3. Users can report hateful and/or abusive language to the admin.
Rationale: In order to maintain the safety of users, any inappropriate messages not caught by the word list can be reported by a user.

5.7.2 Political Requirements

CP-P1. Users may only send direct messages to those who they are authorized to message.
Rationale: A low level factory worker should not be messaging the CEO unless they have permission granted to do so.

CP-P2. Employees may send a message request to those they are unauthorized to message.
Rationale: Similar to Facebook Messenger, if an employee is unauthorized, their message should go to a separate inbox that does not flood the receiver, but they can check to see the request.

5.8 Legal Requirements

5.8.1 Compliance Requirements

LR-COMP1. The app will be SMS compliant [11].
Rationale: To follow the law, the app must be SMS compliant as it is technically a text messaging service.

5.8.2 Standards Requirements

LR-STD1. The app will comply with the Android App Quality Standards [12].
Rationale: To maintain good standards, the app will follow the standards given by Android.

A Division of Labour

Include a Division of Labour sheet which indicates the contributions of each team member. This sheet must be signed by all team members.

Virochaan Ravichandran Gowri:

- 1.1 - Purpose
- 2.1 - Product Perspective
- 2.1 - Block Diagram showcasing product connections
- 5.2, 5.3 - Usability and Humanity + Performance Non Functional Requirements.
- Reviewed the whole document as a group

Krish Dogra:

- Section 4 - Highlights of Functional Requirements (Business Events 1 - 5)
- Section 2.6 - Apportioning of Requirements
- Reviewed the whole document as a group

Leo Vugert:

- Section 2.3 - User Characteristics and Roles
- Section 3 - The Use Case Diagram
- Section 4 - Highlights of Functional Requirements (Business Events 6 - 10)
- Reviewed the whole document as a group