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

- Provide an overview of the document/SRS.

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.

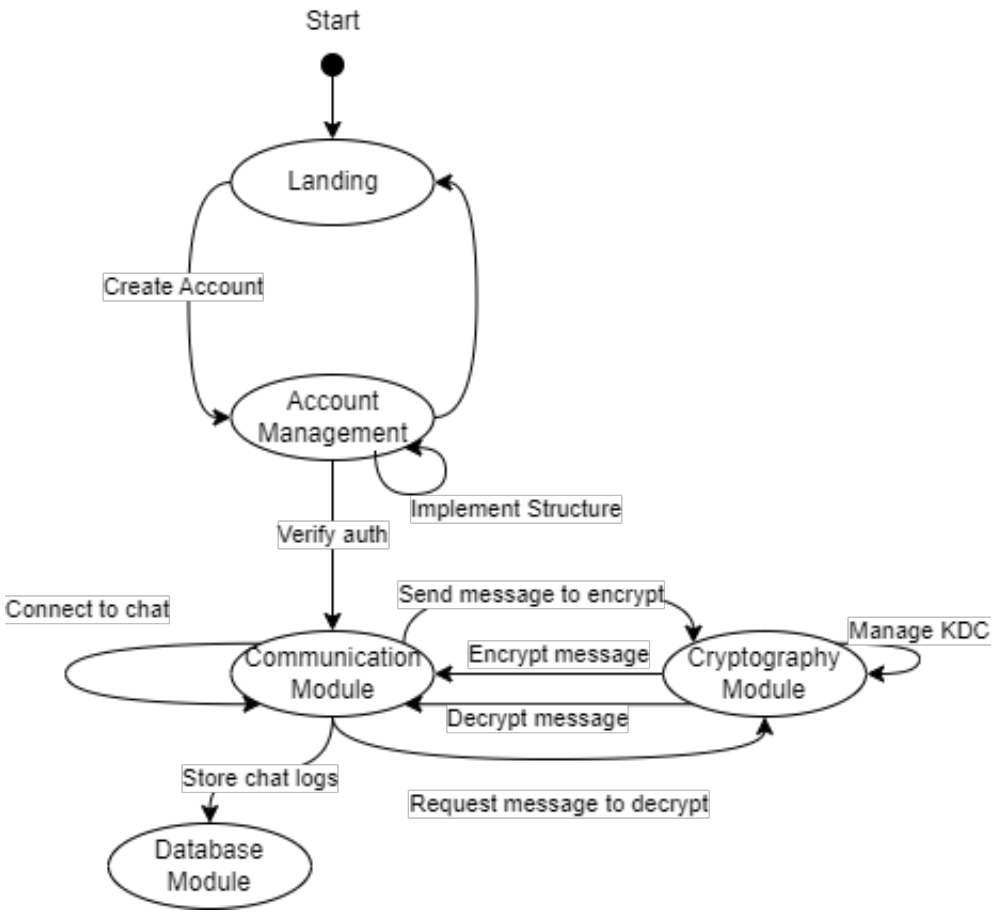
2.1 Product Perspective

- Put the product into perspective with other related products, i.e., context
- If the product is independent and totally self-contained, it should be stated here
- If the SRS defines a product that is a component of a larger system, then this subsection should relate the requirements of that larger system to the functionality of the software being developed. Identify interfaces between that larger system and the software to be developed.
- A block diagram showing the major components of the larger system, interconnections, and external interfaces can be helpful

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

- Describe those general characteristics of the intended users of the product including educational level, experience, and technical expertise
- Since there will be many users, you may wish to divide into different user types or personas

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

- Identify requirements that may be delayed until future versions of the system

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

- Specify all use cases (or other scenarios triggered by other events), organized by Business Event.
- For each Business Event, show the scenario from every Viewpoint. You should have the same set of Viewpoints across all Business Events. If a Viewpoint doesn't participate, write N/A so we know you considered it still. You can choose how to present this - keep in mind it should be easy to follow.
- At the end, combine them all into a Global Scenario.
- Your focus should be on what the system needs to do, not how to do it. Specify it in enough detail that it clearly specifies what needs to be accomplished, but not so detailed that you start programming or making design decisions.
- Keep the length of each use case (Global Scenario) manageable. If it's getting too long, split into sub-cases.
- You are *not* specifying a complete and consistent set of functional requirements here. (i.e. you are providing them in the form of use cases/global scenarios, not a refined list). For the purpose of this project, you do not need to reduce them to a list; the global scenarios format is all you need.
- Red text below is just to highlight where you need to insert a scenario - don't actually write it all in red.

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.

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

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

BE1. Business Event Name #1

VP1. Viewpoint Name #1
Insert Scenario Here

VP2. Viewpoint Name #2
Insert Scenario Here

Global Scenario:
Insert Scenario Here

BE2. Business Event Name #2

VP1. Viewpoint Name #1
Insert Scenario Here

VP2. Viewpoint Name #2
Insert Scenario Here

Global Scenario:
Insert Scenario Here

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.

5.2.2 Personalization and Internationalization Requirements

UH-PI1.

5.2.3 Learning Requirements

UH-L1.

5.2.4 Understandability and Politeness Requirements

UH-UP1.

5.2.5 Accessibility Requirements

UH-A1.

5.3 Performance Requirements

5.3.1 Speed and Latency Requirements

PR-SL1.

5.3.2 Safety-Critical Requirements

PR-SC1.

5.3.3 Precision or Accuracy Requirements

PR-PA1.

5.3.4 Reliability and Availability Requirements

PR-RA1.

5.3.5 Robustness or Fault-Tolerance Requirements

PR-RFT1.

5.3.6 Capacity Requirements

PR-C1.

5.3.7 Scalability or Extensibility Requirements

PR-SE1.

5.3.8 Longevity Requirements

PR-L1.

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.