UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Faculty of Engineering, Built Environment and Information Technology

Department of Computer Science
Faculty of Engineering, Built Environment & IT
University of Pretoria

COS301 - Software Engineering

Atbash

Software Requirements and Design Specifications

June 2, 2021

Item: Capstone Project - Demo 1

Team Name: Bit by Bit

Team Members:

Name	Surname	Student Number
Liam	Mayston	u19027801
Dylan	Pfab	u19003961 *
Connor	Mayston	u1906936
Joshua	Reddy	u19196042
Targo	Dove	u15020275

** - indicates team leader*

Contents

1 Project Owner

Mr Reinhardt Eiselen - email
Mr Matthew Gouws - email
Mr Peter Rayner - email
Amazon Web Services - email

2 Project Vision and Objectives

Atbash is a messaging application, where privacy of messages is top priority. Message content is only visible to the sender and the recipient.

3 Functional Requirements

The requirements of the system models the functionality that the Atbash system offers and should allow for the following functionality:

- R1: The system should allow the user to register an account and link their phone number
- R2: The system should allow the user to login securely
- R3: The system should allow the user to change their display name, status, and profile picture
- R4: The system should allow the user to add contacts
- R5: The system should allow the user to send private messages to their contacts

4 User Characteristics

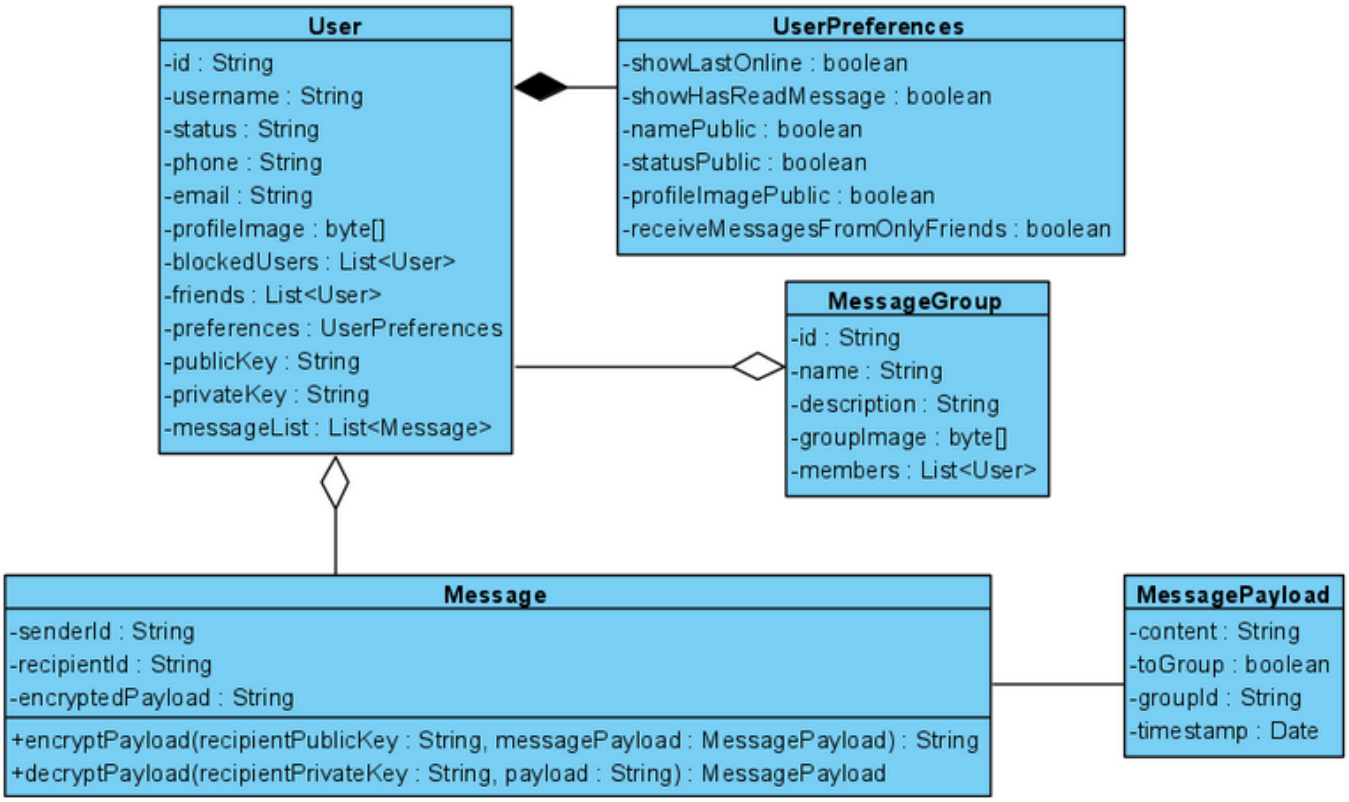
The user should be operating a smartphone to download and use the application. The user should have access to the internet and understand how to message. The Atbash system will be used by the following users:

4.1 Regular User

- Does not require any technical knowledge of the system or other similar systems in general.

- Is familiar with their smartphone and with messaging as a concept
- Is not familiar with the concept of end-to-end encryption

5 System Domain Model



5.1 Description

This is a very nice description that needs to be completed by Joshua.

6 Quality Requirements

- Q1: Security - The system must be secure. A user should not be able view another user's information. No one except the sender and recipient should be able to read their conversation.
- Q2: Scalability - The system should be scalable. An increase in the number of active users should not significantly slow down the performance of any particular user.
- Q3: Availability - The system should be able to be accessed anywhere anytime. This will require the system to have a down time of less than 1 hour in the case of an emergency or fault.

- Q4: Usability - The system must be usable. The regular user is assumed to be familiar with smartphones, but not with the concept of encryption. The system must educate the user about the encryption that the system uses.
- Q5: Flexibility - The system will be accessible for technological upgrades and updates in order to stay relevant with future technologies.

7 Subsystems

Below follows a description of the various subsystems that the system is composed of. Together with this the scope of each subsystem is represented by a use case diagram. For each use case a service contract can be designed which details preconditions, postconditions, invariants and interactions that each use case has in the system.

7.1 User

7.1.1 Use Cases

7.1.2 Domain Model

7.1.3 Service Contracts

7.2 Preferences

7.2.1 Use cases

7.2.2 Domain model

7.2.3 Service Contracts

8 Traceability Matrix