Not for terrorists secure messaging app

Table of Contents

1 Introduction

* 1. Purpose
  2. Scope
  3. Definitions
  4. Overview

...

3.3 Non-Functional Requirements

Introduction

1.1 Purpose

The purpose of this document is to explain in detail the requirements for the “Not for terrorists secure messaging app”. This document will also explain the purpose of the aforementioned system. In conclusion, this document will act as a proposal to customers as well as a reference for the development team.

1.2 Scope

The purpose of this application is to be able to send highly secure messages to those with the same app. Messages will be deleted at least 5 minutes after being read, and will automatically delete after 8 hours. Customers will be able to add encryption to their messages, as well as ten-point security patterns. The makers of this app will not have a way to view these messages, and will have minimal access to the back-end. Passwords will be only be kept on the developers servers, under standard encryption. Accounts can only be created by admins; usernames and passwords will be randomized and be at least 10 characters.

This application needs data-service or Wi-Fi to send messages.

1.3 Definitions

1.4 Overview

The document consists of a UML case diagram of all identifiable use cases, with detailed descriptions of each. Furthermore, each use case will have a corresponding sequence diagram. The next section gives a detailed UML class diagram, showing all actors, relations, etc. A brief description will also be provided.

Next will be two state machines for use cases of interest. Functional and non-functional requirements will be documented. Use case stories will be next, followed lastly by the appendix, containing minutes from the stakeholder meetings.

Use Cases

For Admins

UC-0001 Create Account

Creating an account for another User

Actors: Admin, System

Pre-Conditions: Admin is logged into an Administration account, user who is receiving new profile has passed company security checks.

Post-Conditions:

1. Admin clicks on ‘Create Account’ button in the toolbar
2. System generates a random 10-15 digit number ID.
3. System checks to see if number matches an existing account\*
4. System generates a random password using numbers letters and special characters
5. System checks if password matches an existing account\*
6. System returns ID and password to Admin.
7. System asks Admin to confirm creation.
8. Admin confirms
9. System creates account with generated ID and password

3a. System finds a match

3b. System generates new ID

5a. System finds a match

5b. System generates new password

User Use Cases

\*These cases are also usable by Admins

UC-0002 Login

User logs into their account

Actors: User, System, Admin

Pre-Conditions: User has an account; User has downloaded the app onto their mobile device

Post-Conditions:

1. User opens app
2. User types in ID and password
3. System checks account data for a match\*
4. App unlocks and shows received messages

3a. User incorrectly enters data

3b User incorrectly enters data 3 times

3c. System locks the app

3d. User must contact Admin outside of app to unlock

UC-0003 Send Message

User sends a message to another User

Actors: User, System

Pre-Conditions: Both Users have accounts and are logged in. Both Users must have an agreed upon encryption code and or security pattern

Post-Conditions:

1. User types in recipient ID or opens chat with desired recipient
2. User types a message into the message bar
3. User chooses time after message is read that it should be deleted.
4. User chooses whether to add encryption
5. User chooses whether to add pattern
6. User hits send button
7. System sends message to recipient ID

UC-0004 Adding a new contacts

Actors: User, System, Admin

Pre-Conditions: User has an account;...

Post-Conditions:

1. User selects the contact list optional
2. User types in recipient ID
3. User chooses whether to add default encryption
4. User chooses whether to add default pattern
5. User types additional notes about the recipient

2a. User types incorrect ID

UC-0005 Unlocking locked accounts

Actors: User, System, Admin

Pre-Conditions:

Post-Conditions:

1. User selects the “contact admin” option in the starting menu
2. User selects the option “unlock my account”
3. User types in the ID of his/her account and the reason it was locked.
4. The admin analyzes the customer’s request
5. The admin sends a confirmation to the customer’s default email with a link to unlock the accounts

4a. Admin denies request

5a. Customer doesn’t have access anymore to his/her default email

UC-0006 Deleting account (customer request)

Actors: User, System, Admin

Pre-Conditions:

Post-Conditions:

1. The customer logs in (UC-0002)
2. The customer selects the option “delete account”
3. System brings up the information from the current user’s accounts
4. System logs customer out
5. System deletes customer’s info and accounts

UC-0007 Log out

Actors: User, System

Pre-Conditions:

Post-Conditions:

UC-0008 Open Message

Actors: User

Pre-Conditions: The user received a message.

Post-Conditions: User opened the message.

1. User is notified that a message was received

2. User opens the app

3. User selects the unopened message

4. If the message wasn't encrypted, the user opens and reads the unencrypted message

5. Else the app will prompt the user to enter the encryption key or pattern

6. The message is decrypted and displayed

5a. Key or pattern is incorrect and the app prompts again for it

5b. Key or pattern is entered incorrectly too much and the message is deleted

3.3 Non-Functional Requirements

* Security - Obviously security is a top priority for the app. Messages and accounts should be highly protected.
* Limited Accessibility - The app should only be installed on select devices, and accounts cannot be created without an admin.
* Limited Backup - Messages should not be stored on any server and should be deleted on devices after a set amount of time.
* Disaster Recovery - Should an account be hacked or a device be stolen, admins should be able to lock that account.
* Minimal Exploitability - Due to the sensitive nature of the information being exchanged, there shouldn't be any way the system can be exploited to expose that information.
* No Backend (optional) - It would be desirable to not utilize a back end for the transfer of messages.