SMSEncryption Project
Requirements Specification

COS730 - Group 1

Version 1
April 12, 2014

1 History

Date	Version	Description	Updater
5 April	Version 0.1	Document Created	Henko
5 April	Version 0.2	Document layout added	Henko
10 April	Version 0.3	Added other sections	Henko
11 April	Version 0.4	Added parts to Introduction	Henko
12 April	Version 0.5	Added General Description	Henko

2 Group members

Vincent Buitendach	11199963
Luke Lubbe	11156342
Jaco Swanepoel	11016354
Hein Vermaak	11051567
Henko van Koesveld	11009315

Contents

3 Introduction

3.1 Purpose

This document describes the software requirements and specification for SMSEncryption mobile application.

The document will be used to ensure requirements are well understood by all stakeholders. It is therefore intended for all stakeholders of the project including the developers and customers.

3.2 Background

Reliable communication in certain parts of South Africa is not always possible in remote locations using GSM, 3G or other similar mediums.

Therefore, communication normally occur using SMS which generally is not very secure. This can cause a loss in confidentiality, integrity and availability of the communicators.

There is a need to develop a secure way of communicate using conventional mediums such as SMS.

3.3 Scope

The goal of this project is to create a mobile application which can be used on more than one platform(i.e. IOS and Android) and will be able to encrypt messages which can then be decrypted on the receiving end.

By using SMSEncryption, the user will be able to communicate securely with another user who also has the same application. The application will be secured using a password before the user can decrypt or encrypt a message.

The method of encryption will be an appropriate algorithm which will prevent the message from being decrypted by an unauthorised party who obtains the message.

The benefit of this application is that you are able to communicate securely,

knowing that you are reducing the risk of the confidential information being obtained by an unauthorised party. It allows for the use of convenient mediums of communication(such as SMS) which will be robust in remote areas with little signal.

3.4 Definitions, acronyms and abbreviations

- SMSEncryption - The current project which will allow secure communication once implemented.
- Message - The message intended to be sent from a sender to a receiver.
- Ciphertext - A message that has been changed into another form.
- Encrypt - The act of encoding messages into a ciphertext which only the authorised parties can read the content of the message.
- Decrypt - The act of decoding a ciphertext back into the orginal form before conversion took place.
- User - An authorised person who will interact with the application.
- Sender - The person who will send a message using the application.
- Receiver - The person who receives a message using the application.
- SMS - Short Message Service (SMS) is a text messaging service component of phone, Web, or mobile communication systems. This allows for short messages to be sent to other devices.
- GSM - Global System for Mobile Communications (GSM) is a second generation standard for protocols used on mobile devices.

3.5 Document Conventions

- Documentation formulation: LaTeX
- Naming convention: Crows Foot Notation

3.6 References

- Kyle Riley - MWR Info Security
  - face-to-face meeting
  - email
- Bernard Wagner - MWR Info Security
  - face-to-face meeting
  - email

3.7 Overview

The rest of the document will be organized to include General Description and Specific Requirements for SMSEncryption application.

The General Description will provide a background to the reader for SMSEncryption and contains sections: Product perspective, Product functions, User characteristics, Constraints and Assumptions and dependencies.

The Specific requirements contain requirements for SMSEncryption and is organised by features. This is done in such a way which will highlight the functions of the application.

The sections contained in Specific requirements include External interface requirements, System Features, Performance Requirements, Design constraints, Software system attributes, and Other requirements.

4 General description

4.1 Product perspective

4.1.1 Description

This is a new product which will be able to work together with other messaging capabilities, such as normal messaging on mobile devices, and also other applications capable of using the basic GSM character set.

GSM character set only allows a number of characters which may prevent the use of certain encryption. Many encryption algorithms greatly increase the number of characters, but this approach will be infeasable.

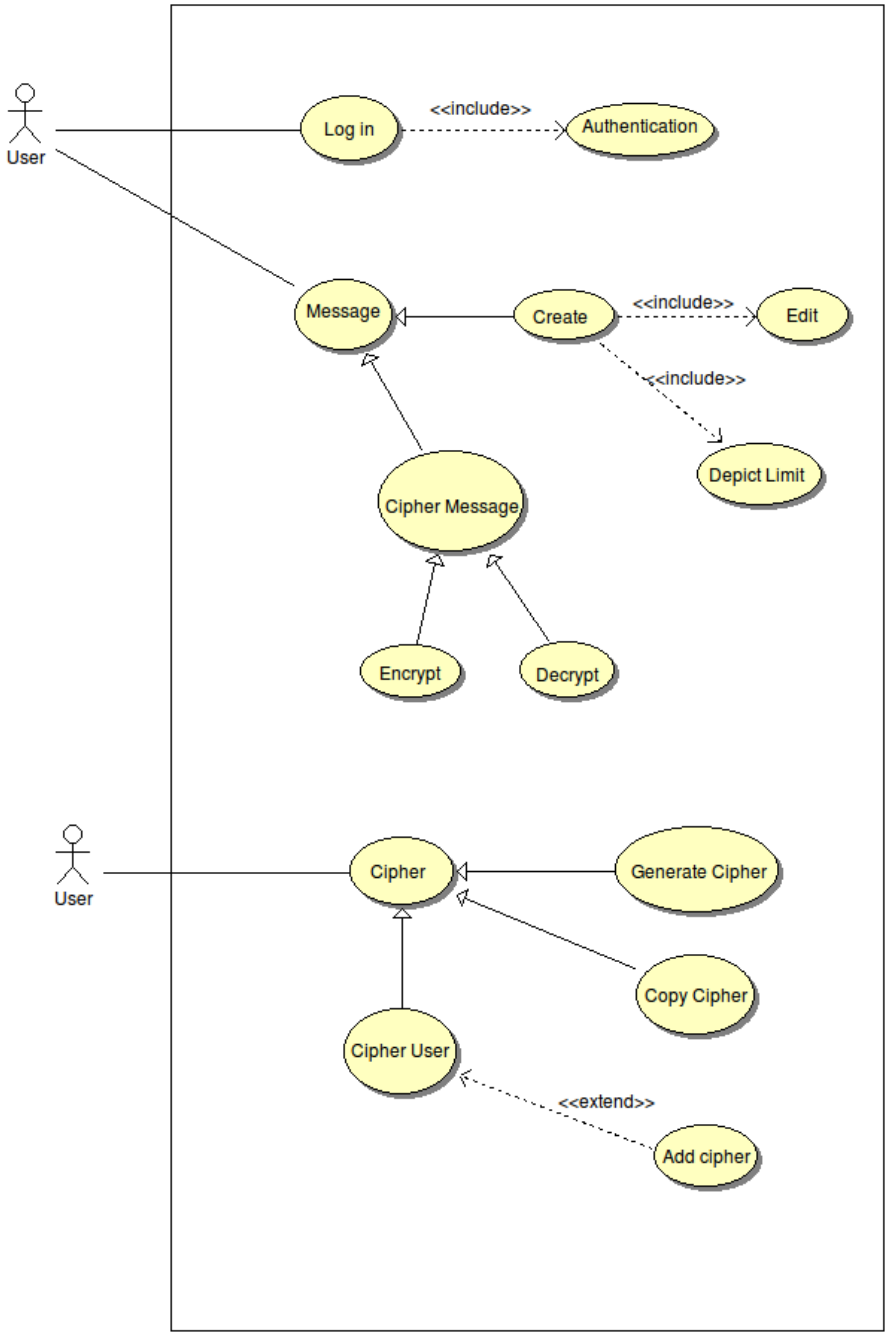
Software interface - The software interface will make use of the clipboard functionality on the phone in order to copy and paste messages or ciphertexts.

User interface - The user interface is what will allow the user to encrypt a message and decrypt a message which has been sent by other users of this application.

Hardware Interface - The software will run on a mobile device with touch screen capabilities.

4.1.2 Use Cases

SMSEncryption Use case diagram



4.2 Product features

4.2.1 Log In

- The application will ask the user for login details which he/she must then enter in correctly.
- If it is incorrect, the application will close preventing access for an unauthorised user.

4.2.2 Message

Create

- The user can create a message using this application.
- The application will also allow the user to edit the message which is currently being typed in.
- The limit of the message will be displayed while the user is entering a message.

Cipher Message

- The message can be encrypted to obtain the cipher text which the user can send to the other user.
- The cipher text can be sent after copying the message to the clipboard and pasting it into a message such as SMS or other similar applications.
- The user who receives a message will be able to decrypt the message afterwards showing the original message before encryption.

4.2.3 Cipher

- The user can generate a cipher which will influence how it is encrypted and decrypted by the sender and receiver.

- This cypher can be copied and can be used in other places such as add cipher.
- The user can add a cipher to the application determining how the message will be encrypted and decrypted which allows communication between two users.

4.3 User characteristics

- There will be only one user class who will have full access to all the features provided by the application.
- It is assumed that the user has proficient knowledge on how to copy items from messages such as SMS and paste it within this application.

4.4 Constraints

- The application must make use of the basic GSM character set.
- The application will be delivered as a prototype if time permits.

4.5 Assumptions and dependencies

- It is assumed that the amount of characters in the basic GSM character set is 128 for the 7-bit encoding used in GSM.

5 Specific requirements

5.1 External Interface Requirements

5.1.1 User interfaces

5.1.2 Hardware interfaces

5.1.3 Software interfaces

5.1.4 Communications interfaces

5.2 System Features

5.2.1 Create message : FRQ1 (Source: Bernard Wagner, Priority: High)

- A message must be creatable in the application.
- The message must be editable.

5.2.2 Encrypt message : FRQ2 (Source: Bernard Wagner, Priority: High)

- After that the message must be encrypted using a suitable encryption method.
- The user must be able to select and copy the message to the clipboard in order to be sent using the method the user wants to.

5.2.3 AppSomething : FRQ3 (Source: Bernard Wagner, Priority: High)

- The application must use a password to log on in order to ensure confidentiality.

5.3 Performance Requirements

5.4 Design constraints

5.5 Software system attributes

5.6 Other requirements