SMSEncryption Project
Requirements Specification

COS730 - Group 1

Version 1.0
April 21, 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
21 April	Version 0.6	Modification of current document and IEE compliance adjustment	Jaco and Luke
21 April	Version 0.7	Added to some empty sections	Jaco and Luke
21 April	Version 0.8	Added appendix A	Hein
21 April	Version 0.9	Added appendix B	Hein
21 April	Version 1.0	Added appendix C	Hein

2 Group members

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

Contents

3 Introduction

3.1 Purpose

This document describes the software requirements and specification for the 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). This application will be able to encrypt messages which can then be decrypted on the receiving end.

By using SMSEncryption, the user will be able to encrypt messages which can only be decrypted using the same application. The user will require local authentication to access the access the appliaction and make use of it's features.

The benefit of this application is that you can use SMS technology to send messages containing confidential information which only you and the desired recipient can read in an unencrypted form.

3.4 Definitions, acronyms and abbreviations

- SMSEncryption - The current project which will allow you to encrypt and decrypt text with the purpose of it being sent as a message via messaging applications eg. WhatsApp, SMS etc.
- Message - The text intended to be sent from a sender to a receiver or stored once said message has been encrypted via SMSEncryption.
- Plaintext - Is information a sender wishes to transmit to a receiver.
- Ciphertext - Is the result of encryption performed on plaintext using an algorithm, called a cipher.
- Encrypt - To alter the plaintext using an algorithm so as to be unintelligible to unauthorized parties.
- 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 authored and intends to send a messagethat has been encrypted via the application.
- Receiver - The intended party who receives a message which has been encrypted via 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 over a network which is not controlled by the sender or receiver.
- GSM - Global System for Mobile Communications (GSM) is a second generation standard for protocols used on mobile devices.
- Entropy - The expected value of the information contained in a message.

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 can be used in conjunction with any mobile text manipulation service, be this provided by the operating system or another application, capable of using the basic GSM character set, should you require encryption and decryption functionality.

The GSM character set only contains certain characters which limits which encryption methods we can make use of. Many encryption algorithms greatly increase the number of characters, but this approach will be infeasable.

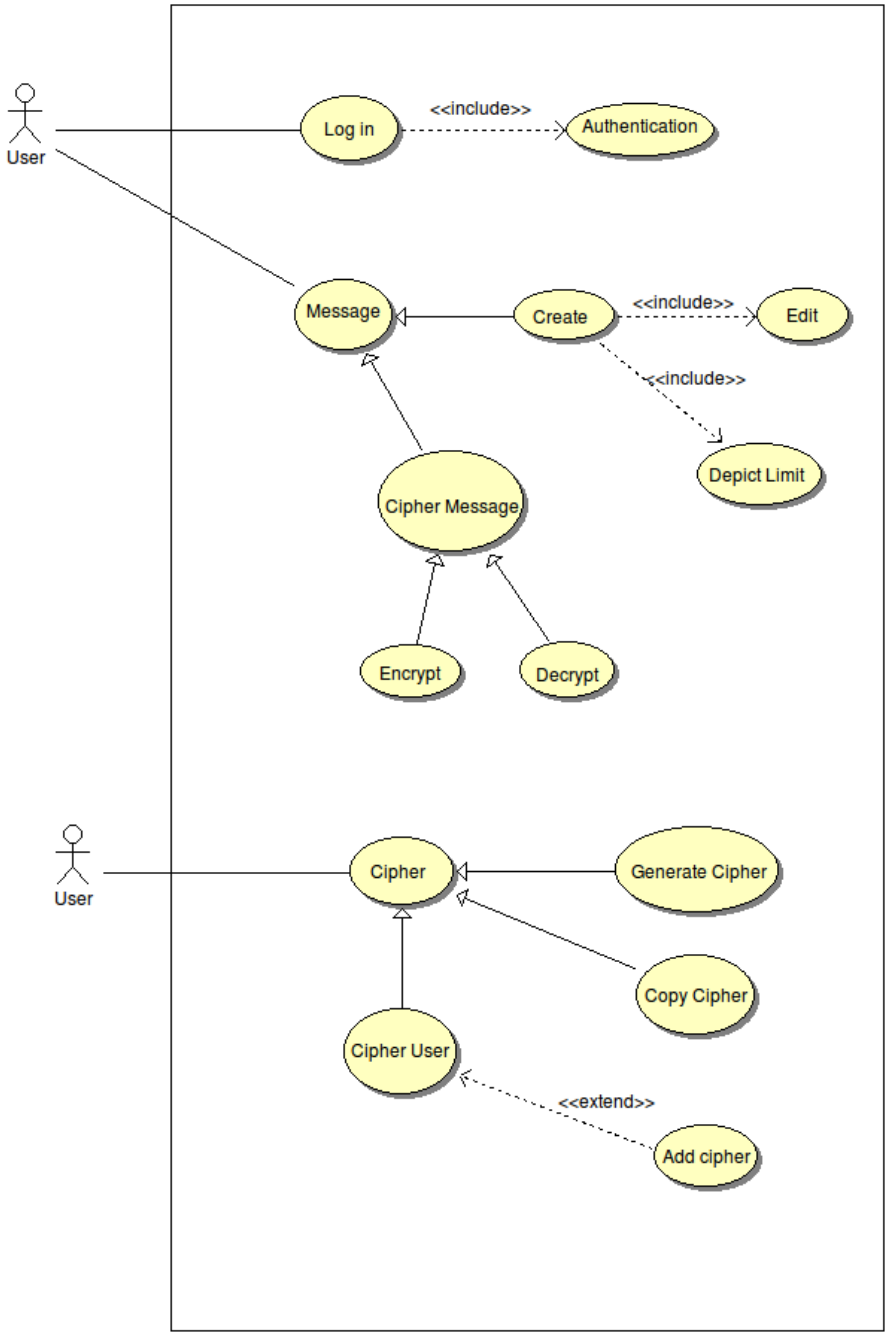
Software interface - The software interface will make use of operating system features such as a clipboard on the device to facilitate copying and pasting of messages or ciphertexts.

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 that allows user interaction.

4.1.2 Use Cases

SMSEncryption Use case diagram



4.2 Product features

4.2.1 Log In

- On first use a password must be created for future use by the user of the application.
- The application will ask the user for login details which he/she must then enter correctly.
- If it is incorrect, the application will close preventing access for an unauthorised user.

4.2.2 Message

Create

- The plaintext is created independently by the user and input into the application
- The plaintext can be created and edited within the application.

Cipher Message

- The user will select a relevant contact, that contacts details will then be used to perform encryption or decryption.
- The message will be encrypted to obtain the cipher text which the user can then copy out and send to the desired receiver via any messaging method.
- The desired receiver will be able to decrypt the message into its plaintext.

4.2.3 Device Synchronization

- In order for communication to take place between two devices they need to be synchronized.

- A user adds what is called a contact, it will ask the name of the contact as well as generate a unique word to be provided to the other person and an input box where the unique word appearing on the contacts phone.
- Both users must add each other at the same time, because they need each other unique word that will be generated for their communication. This will synchronize communication between the devices.

4.3 User characteristics

- There will be only one user class who will have full access to all the features provided by the application after local authentication.
- 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.
- Assumed that the users performed the device synchronization phase correctly as there is no way for the device to know.

4.4 Constraints

- The application must make use of the basic GSM character set.

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.
- It is assumed that the devices being used allows for copy and pasting of text between different interfaces and applicaitons.

5 Specific requirements

5.1 External Interface Requirements - Hein and Henko input

5.1.1 User interfaces

5.1.2 Hardware interfaces

5.1.3 Software interfaces

5.1.4 Communications interfaces

5.2 Product Functions

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

- A message must be able to be typed in the application.
- The message must be editable.

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

- 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 Local Authentication : FRQ3 (Source: Bernard Wagner, Priority: High)

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

5.3 Performance Requirements

- The application should operate in a timely manner, the user should not be made to wait an unreasonable amount of time (this variable can be affected by the system environment e.g. resource availability).
- The encryption method must be secure.

5.4 Design constraints

5.4.1 Message length : DC1 (Source: Bernard Wagner, Priority: High)

- Due to the fact that the primary messaging service which the client intends to use is SMS this limits the input size of the text to 160 characters. To maintain consistency we enforce this as the maximum length of messages which the application can encrypt and decrypt.

5.4.2 The usable character : DC2 (Source: Bernard Wagner, Priority: High)

- The usable character which can be encrypted by the application is the GSM character set because the primary intended messaging service that the client wishes to use is SMS.

5.4.3 Application resource requirementsr : DC3 (Source: Bernard Wagner, Priority: High)

- The application should function efficiently with the least amount of resource usage.

5.5 Software system attributes

5.5.1 Reliability

- The application should run until the user closes it.

- Any information stored in the application should be static and exist as long as the application is open or said information is removed/edited.
- The Cypher text should decrypt into its plaintext.

5.5.2 Availability

- The user should be able to use the application as long as it is running and should not be made to wait while the application performs a function.
- The application should not interfere with any other applications which are running on the device.

5.5.3 Security

- A secure encryption and decryption method with entropy of no more than one percent will have to be used.

5.5.4 Maintainability

- The source code should be maintainable (simplistic and readable/documented).
- The application should not act in unpredictable ways.

5.5.5 Portability

- The client has requested that different versions of the application be developed to execute on different operating systems namely Android and IOS.

6 Appendix A - RSA

Introduction

Method

Result

Discussion

Conclusion

References

7 Appendix B - One time pads

Introduction

Method

Result

Discussion

Conclusion

References

8 Appendix C - Protocol

8.1 Diagrams

8.1.1 Work flow diagram

8.2 Description