

COS730 PROJECT REQUIREMENTS SPECIFICATION

Group 1

Version 1
April 11, 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

2 Group members

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

Contents

1	History	1
2	Group members	1
3	Introduction	4
3.1	Purpose	4
3.2	Background	4
3.3	Scope	4
3.4	Definitions, acronyms and abbreviations	5
3.5	Document Conventions	5
3.6	References	5
3.7	Overview	6
4	General description	7
4.1	Product perspective	7
4.2	Product functions	7
4.3	User characteristics	7
4.4	Constraints	7
4.5	Assumptions and dependencies	7
5	Specific requirements	8
5.1	External Interface Requirements	9
5.1.1	User interfaces	9

5.1.2	Hardware interfaces	9
5.1.3	Software interfaces	9
5.1.4	Communications interfaces	9
5.2	System Features	10
5.2.1	Create message : FRQ1 (Source: Bernard Wagner, Priority: High)	10
5.2.2	Encrypt message : FRQ2 (Source: Bernard Wagner, Priority: High)	10
5.2.3	AppSomething : FRQ3 (Source: Bernard Wagner, Priority: High)	10
5.3	Performance Requirements	11
5.4	Design constraints	11
5.5	Software system attributes	11
5.6	Other requirements	11
6	System Description	12

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.
- 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 original 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.

3.5 Document Conventions

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

3.6 References

- Kyle Riley - MWR Info Security
- Bernard Wagner - MWR Info Security

3.7 Overview

4 General description

4.1 Product perspective

4.2 Product functions

4.3 User characteristics

4.4 Constraints

4.5 Assumptions and dependencies

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

6 System Description

Use Cases

Use case 1

Use case 2

Flow diagram

Flow 1

Flow 2