COS730 Project Requirements Specification

Group 1

Version 1
April 10, 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

2 Group members

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

Contents

3   References

- Kyle Riley - MWR Info Security

- Bernard Wagner - MWR Info Security

4   Overview

4.1   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, availability and integrity to the communicators.

4.2   Document Conventions

- Documentation formulation: LaTeX

- Naming convention: Crows Foot Notation

4.3   Project 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. Thereby reducing the risk of the confidential information being obtained by an unauthorised party.

5 Functional Requirements

Messaging

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

- A message must be creatable in the application.

- The message must be editable.

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.

Application

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

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

6 Quality Requirements

7 System Description

Use Cases

Use case 1

Use case 2

Flow diagram

Flow 1

Flow 2

8   Glossary

- Encryption - The act of encoding a message in a way that only authorized parties can read it