|  |
| --- |
| SSk College of engineering and technology |
| Encryption Key Generator on Android |
| Software Requirement Specification |
|  |
| **A-TEAM** |
| **3/4/2012** |

|  |
| --- |
| An encryption key generator application for the Android platform. The application will replace smart cards for secure login to secure remote networks that employ periodic password change automatically on a timely basis. |

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Updated By** |
| 06/03/2012 | 1.0 | SRS Level 1 Review | A-TEAM |
|  |  |  |  |

**Document Approvals**

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Signature** |
| Mr. Muthukumar.G | Project Manager |  |
|  |  |  |

Contents

[1. Introduction 4](#_Toc318111679)

[1.1 Purpose of the Document 4](#_Toc318111687)

[1.2 Project Scope 4](#_Toc318111688)

[2. Requirements Analysis 5](#_Toc318111689)

[2.1 Models for Requirements Analysis 5](#_Toc318111690)

[2.2 System Description 5](#_Toc318111691)

[3 Functional Requirements 6](#_Toc318111692)

[3.1 Features in proposed System 6](#_Toc318111693)

[3.2 Non Functional and Performance Requirements 6](#_Toc318111694)

[3.4 Functional Flow Diagrams 6](#_Toc318111695)

[3.5 Data Dictionary 6](#_Toc318111696)

[4. General Requirements 9](#_Toc318111697)

[4.1 External Interfaces 9](#_Toc318111698)

[4.2 Scalability, Security and Performance Requirements 9](#_Toc318111699)

[5. Issue Management Strategy 9](#_Toc318111700)

[6. Open Issues 10](#_Toc318111701)

# 1. Introduction

## 1.1 Purpose of the Document

The purpose of this document is to present a detailed description of all the functions, specifications, requirements and constraints associated with the Encryption Key Generator application on Android. This document will outline the distinct advantages gained by the use of smartphones in encryption key generation process for securing access to protected remote networks.

## The contents detailed within this document is intended for use by the stakeholders for better understanding the advantages of the application from a business perspective as well as to detail an outline of the requirements and functional capabilities associated with it. It will also prove to be a guideline for the application development team to assist them in translating the clients’ needs into a quality software product.

## 1.2 Project Scope

The encryption key generator application is designated to be part of a larger framework of network security management suite - which is out of the scope for this document - that will provide a highly scalable and reliable architecture for corporate network security and remote access infrastructure.

The project will be developed for use on smartphones operating on the Android platform. It is to be applied in remote login and session management scenarios to allow easy and secure access for authorized personnel to the corporate network.

In essence, the encryption key generator application eliminates the need for employing smart cards to store the encryption function for generating the required encryption keys that allow the user to login to a secure session on the network remotely.

# 2. Requirements Analysis

## 2.1 Models for Requirements Analysis

Encryption is now viewed as a strategic issue with business leaders gaining greater influence over their organization’s encryption strategy. Studies show that the CIO, CTO or IT leader still tends to be the most important figure in deciding encryption strategy, but non-IT business managers have an increasing role in determining that strategy, demonstrating that encryption is no longer seen as just an IT issue but one that affects an entire organization.

IT administrators consider key management issues to be amongst the most important features of encryption technology, in particular the use of automated and centralized key management. Most interestingly, a good percentage of professionals believe that investments in key management have the potential to reduce operational costs within their organization.

Encryption is taking center stage as a strategic IT security issue, in order to mitigate the risk of data breaches and cyber-attacks and to protect an organization’s brand, reputation and credibility. Encryption is only a valuable tool if deployed correctly. It enables you to achieve high levels of assurance when deploying all forms of cryptography. By following the appropriate standards of due care you are able to reinforce the organization’s data security practices and protect its most valuable assets and business processes.

## 2.2 System Description

The encryption key generator application is intended to operate on the Android platform. The network uses asymmetric key cryptography ciphering techniques of sufficient key length to secure the all user communication including internal and remote sessions connected to it. The network policies are set up such that the encryption key will be periodically changed by the system.

The use of such a dynamic encryption key generation policy requires that the users accessing the system be provided with a safe and secure means of generating the changed password while maintaining a lower cost of implementation for the company. In this context, the key generator application is being developed to allow users to easily and securely generate the encryption key they require to successfully login to the network from remote locations.

The application uses only one main UI interface. Once the application is executed, it proceeds to generate the updated password for the user. This is provided to the user through the screen.

# 3 Functional Requirements

The application generates encryption key for secure login to remote networks without the need for using smartcard based systems.

## 3.1 Features in proposed System

* Encryption key generation
* Security
* Unique key generation for each session

## 3.2 Non Functional and Performance Requirements

* Android programming Tutorials (Text reference and online services)
* Java programming Tutorials (Text and online references)
* Android smartphone running OS version 2.2 or above (for testing)

## 3.4 Functional Flow Diagrams

## 

Figure 1 : Use Case Diagram

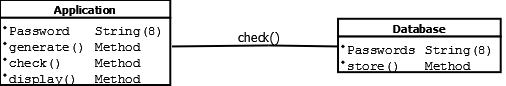


Figure 2 : Class Diagram

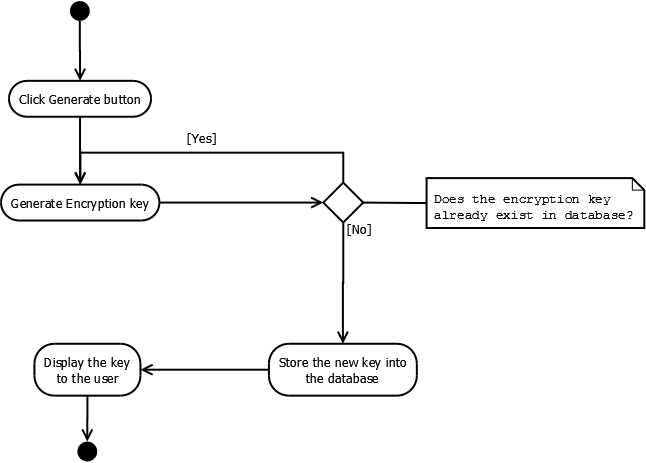


Figure 3 : Activity Diagram

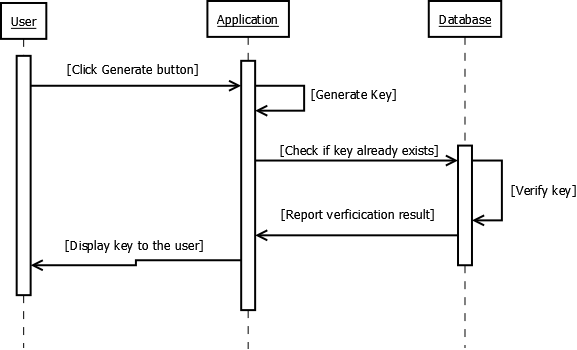


Figure 4 : Sequence Diagram

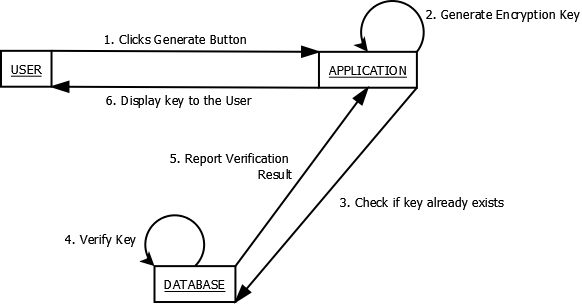


Figure 5 Collaboration Diagram

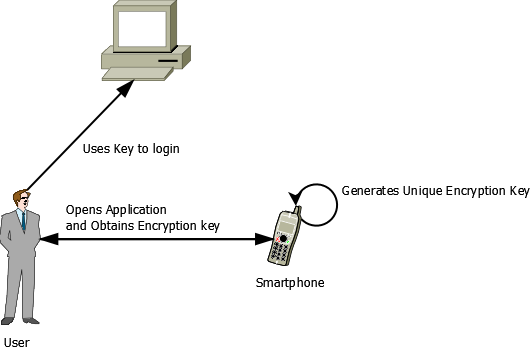


Figure 6 Deployment Diagram

# 4. General Requirements

## 4.1 External Interfaces

* Bluetooth
* USB
* WI -FI

## 4.2 Scalability, Security and Performance Requirements

* Smartphone operating on Android Platform
* Android version 2.2 or above
* 800Mhz Processor or above
* 30MB of free RAM
* 50MB ROM for installation

# 5. Issue Management Strategy

* Key duplication occurs

The encryption key once generated is ideally not intended to be regenerated by the system. In such a case, the issue will be regarded with a priority level 3 (medium) as the application may still remain usable. The issue will be followed upon within one business day and a solution can be expected within seven days.

* Application fails to execute

This issue may either be due to the application itself or with other factors prevalent on the device. This condition will be assigned with a priority level 1 (urgent) and the customer will receive suitable response within the same day as the issue is reported.

# 6. Open Issues

* The encryption key strength is relatively less secure compared to industry standard security solutions
* The application requires Android version 2.2 (froyo) or above for proper execution.