Software Requirements Specification

for

Passworder

Version 1.0

Prepared by :

Abhijit Parida (1541012143)
Arabinda Bal (1541012551)
Deepak Kumar Singh (1541012511)
Sandeep Dash (1541012568)
Sourav Bastia (1541012453)
Swaraj Laha (1541012021)

Institute of Technical Education and Research
SIKSHA 'O' ANUSANDHAN (Deemed to be University)

20th July 2018

Table of Contents

Table of Contents 2

Revision History 3

1. Introduction 4

1.1 Purpose 4

1.2 Document Conventions 4

1.3 Intended Audience and Reading Suggestions 4

1.4 Product Scope 5

1.5 References 5

2. Overall Description 5

2.1 Product Perspective 5

2.2 Product Functions 6

2.3 User Classes and Characteristics 6

2.4 Operating Environment 6

3. External Interface Requirements 6

3.1 User Interfaces 6

3.2 Hardware/Software Interfaces 7

4. System Features 7

4.1 Set Master Password 7

4.2 Add Password Entry 7

4.3 View Passwords 7

5. Other Nonfunctional Requirements 8

5.1 Safety Requirements 8

5.2 Security Requirements 8

Appendix A: Glossary 8

Appendix B: Analysis Models 8

Revision History

Name	Date	Reason For Changes	Version
Initial version	20/06/2018	Initial version	1.0

1. Introduction

1.1 Purpose

This document includes software requirements for *Passworder*, release number 1.0. Passworder is a password manager providing resolution to two major problems faced by users concerned about their online privacy: memorizing secure passwords and accessing stored passwords across all of their devices. The former is addressed by offering secure storage of passwords; and the latter is addressed by generating passwords based on a *master password*. As passwords can be predictably generated (based on the master password) across devices, this essentially eliminates the need of using a database/internet connection to sync passwords. Users can unlock the password manager either by entering the master password, or by using their fingerprint. Lastly, the password manager will allow users to view the strength of their master password and warn them against using commonly used passwords.

1.2 Document Conventions

- When writing this document it was inherited that all requirements have the same priority.
- First there is presented an overall view about the Passworder and then all features and functions are analyzed in details.

1.3 Intended Audience and Reading Suggestions

This document was intended for the following audience:

1) **Developers:** in order to be sure they are developing the right project that fulfills requirements provided in this document.

2) **Testers:** in order to have an exact list of the features and functions that have to respond according to requirements and provided diagrams.

3) **Users:** in order to get familiar with the idea of the project and suggest other features that would make it even more functional.

4) **Documentation writers:** to know what features and in what way they have to explain. What security technologies are required, how the system will response in each user's action etc.

5) **Advanced end users, end users/desktop and system administrators:** in order to know exactly what they have to expect from the system, right inputs and outputs and response in error situations.

1.4 Product Scope

Passwords managers available in the market can broadly be divided into free password managers and paid password managers. Free password managers don't usually provide the ability to sync passwords across multiple devices and thus, users have to resort to their own means like using dropbox or private FTP servers.

Passworder offers the facility of predictably generating passwords across devices based on a master password. This essentially eliminates the need of syncing passwords using an online database.

Other than the above mentioned, Passworder will also provide basic features of a password manager such as secure storage of the master password, ability to view password strength and warn users of weak & commonly used passwords.

1.5 References

- *https://en.wikipedia.org/wiki/List_of_password_managers#Features*

  Feature comparison of various password managers available in the market.

- *https://material.io/design/*

  Material design guidelines offered by Google for a modern and consistent user interface.

2. Overall Description

2.1 Product Perspective

The password manager described in this document is a follow-on member of the existing line of password managers; distinguishing from other products by being very minimalistic & lightweight, and most importantly allowing access across devices regardless of internet connectivity.

As passwords can be predictably generated (based on the master password) across devices, this essentially eliminates the need of using a database/internet connection to sync passwords. Users can unlock the password manager either by entering the master password, or by using their fingerprint.

Lastly, the password manager will allow users to view the strength of their master password and warn them against using commonly used passwords.

2.2 Product Functions

- Secure password storage
- Password generation based on a master password

2.3 User Classes and Characteristics

Passworder is primarily targeted towards users who are concerned about their privacy and keeping their online presence secure. Passworder helps remember use different passwords for different online services/websites.

2.4 Operating Environment

Hardware/Software: Passworder should work on Android devices running Android 4.0.3 (Ice Cream Sandwich) and above.

3. External Interface Requirements

3.1 User Interfaces

The user interface includes activities consisting of forms and lists. Various activities of the app are listed below:

1. **Login activity:** In this activity, the user will enter the master password which is required to unlock the application.

2. **Password List activity:** In this activity, a list of website names and passwords will be shown. The passwords would initially be hidden (masked by asterisks ‘*’) and will be visible after a button is pressed to reveal them. A button to copy passwords will also be present.

3. **Add Password activity:** Users will be able to generate new passwords in this activity.

3.2 Hardware/Software Interfaces

The standard Android API is used for displaying the user interface and storing data such as the master password, and list of websites.

4. System Features

4.1 Set Master Password

4.1.1 Description and Priority

The user is prompted to set a master password on launching the application for the first time.

4.1.1 Stimulus/Response Sequences

1. User opens the app for the first time.
2. User enters the master password.
3. A password strength meter is shown.
4. User is warned if the password is weak or commonly used.
5. The master password is saved in the database.

4.1.2 Functional Requirements

The master password entered by the user must be hashed before being stored.

4.2 Add Password Entry

4.1.1 Description and Priority

The user can add a new password entry in the database.

4.1.1 Stimulus/Response Sequences

1. User opens the add password activity.
2. User enters the name of the website.
3. The entry is added and shown in the password list activity.

4.1.2 Functional Requirements

The password is generated based on the master password and website name.

4.3 View Passwords

4.1.1 Description and Priority

The user can view a list passwords.

4.1.1 Stimulus/Response Sequences

1. User opens the password list activity.
2. User taps on the reveal password button to view a particular password.

4.1.2 Functional Requirements

The password is generated based on the master password and website name.

5. Other Nonfunctional Requirements

5.1 Safety Requirements

Care must be taken that the master password must be strong enough so that it cannot be brute forced or easily guessed by malicious users.

Users must be warned against using weak and commonly used passwords.

5.2 Security Requirements

The master password given by the user must be hashed using a cryptographically secure hashing algorithm before storing it.

Appendix A: Glossary

Password Manager: A software application used to store passwords securely.

Master Password: A single password used by the user to access other passwords.

Appendix B: Analysis Models

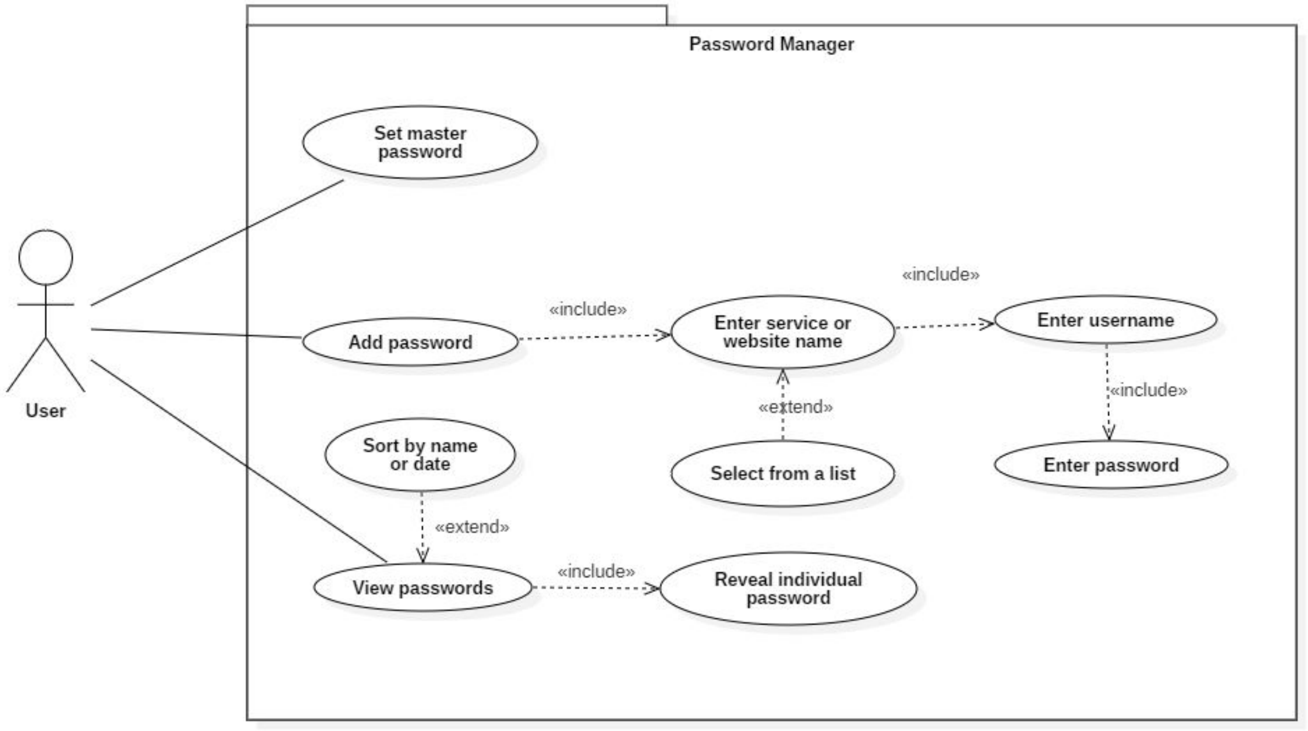

Fig. 1: Use case diagram

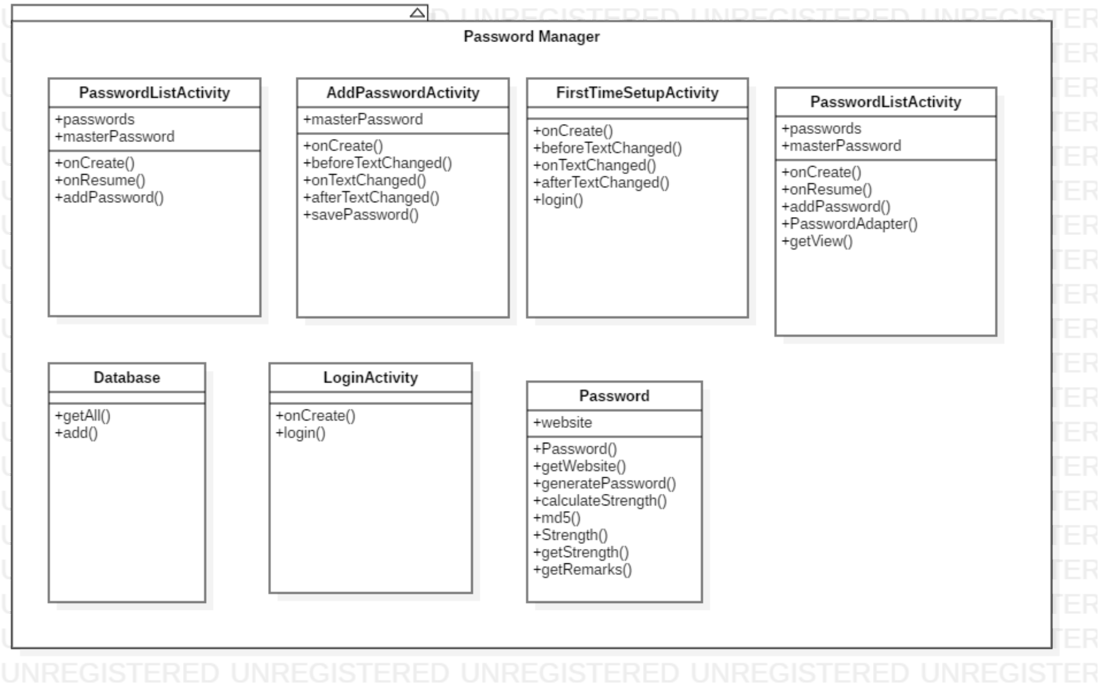

Fig 2: Class diagram