**Key Guardian: Requirements Specification Document**

**By Logan Ferguson**

**04/10/2023**

Table of Contents

[Key Guardian 3](#_Toc132006728)

[Requirements 4](#_Toc132006729)

[Functional: 4](#_Toc132006730)

[Look and Feel: 8](#_Toc132006731)

[Usability: 10](#_Toc132006732)

[Performance: 13](#_Toc132006733)

[Maintainability and Support: 17](#_Toc132006734)

[Security: 18](#_Toc132006735)

[Cultural: 20](#_Toc132006736)

# **Key Guardian**

Key Guardian is a password generator, checker, and manager of passwords which are stored securely on a local system. This software allows the user to choose the length of a password and to generate a secure password using upper and lower case letters, numbers, and symbols. Key Guardian will check any current passwords the user may have to see if it is secure and whether or not it has been exposed in a previous data breach. The security of passwords will be checked and rated on a scale of 1 to 5, and a friendly message will prompt a description of the security scale. Lastly, the user will be able to store passwords in a local database that will be encrypted with a master key, which is generated by Key Guardian. This will be the only password that users will need to keep in a safe place to unlock the rest of their passwords. Another feature of Key Guardian is the ability for the user to enter a certain time frame for when they want to change and update their passwords. They will then be reminded when that amount of time is ending and be prompted to change the password for that account. The purpose of this software is not to just create, check, and store passwords securely, but to educate users on how to better protect their online accounts.

**Description**

This document will list and describe the Requirements for the Key Guardian software and will represent a complete description of this project. Each of the requirements will include a requirement number and type, along with a description, rationale, fit criterion, priority, and the dependencies. The types of requirements that will be included are functional, look and feel, usability, performance, maintainability and support, security, and cultural. The priority scale is 1 to 10, with 1 being not a priority at all and 10 being of upmost importance for this software.

# **Requirements**

## **Functional:**

Requirement ID: 01

Description:

The software must prompt the user to create a master password on its first execution.

Rationale:

This will allow the user to lock their stored passwords with one master password.

Fit Criterion:

Upon running for the first time, the software prompts the user to create a master password before moving to the next window.

Priority: 10

Dependencies: None

Requirement ID: 02

Description:

The user can choose between three options on the main window.

Rationale:

The software has three major options that the user can choose from.

Fit Criterion:

The three options are viewable via buttons in the main window.

Priority: 9

Dependencies: 09

Requirement ID: 03

Description:

The software allows the user to generate a secure password and prints it in the window.

Rationale:

This partially fulfils the purpose of this password generator.

Fit Criterion:

User can successfully generate and view the password to the meet desired security policies.

Priority: 9

Dependencies: 27

Requirement ID: 04

Description:

The software allows the user to input a password to check it for security.

Rationale:

Users can secure their online accounts by ensuring that their passwords are safe and secure.

Fit Criterion:

Software takes a string as input and tests it for security.

Priority: 9

Dependencies: 27

Requirement ID: 05

Description:

The software will rate each checked password on a security scale of 1 to 5.

Rationale:

The user must be able to visually see the scale of security for their passwords.

Fit Criterion:

A security scale will print to the window and show the user the results of the assessment.

Priority: 7

Dependencies: 27

Requirement ID: 06

Description:

Each password checked by the software will be cross referenced with a breached passwords list.

Rationale:

The user must be able to identify whether or not their password has been contained in a data breach in the past.

Fit Criterion:

The password is used to scan through the breached word list to search for a matching word and notifies the user accordingly.

Priority: 8

Dependencies: None

Requirement ID: 07

Description:

The software allows the user to securely store passwords for any online account.

Rationale:

This allows the user to keep their passwords organized and stored securely in one place.

Fit Criterion:

The users’ passwords are stored in a local file and the user can view them at any time.

Priority: 10

Dependencies: None

Requirement ID: 08

Description:

The software allows the user to add/remove a password at any time and the local file is updated accordingly.

Rationale:

The user can move all their passwords over to this software and remove them as necessary.

Fit Criterion:

The user can add and remove any passwords from the local file.

Priority: 9

Dependencies: 07

## **Look and Feel:**

Requirement ID: 09

Description:

This software will be equipped with a full graphical user interface (GUI).

Rationale:

Allows for the ease of usability for the user.

Fit Criterion:

All functions are inserted into one user interface allowing the user to navigate the

features with ease.

Priority: 10

Dependencies: None

Requirement ID: 10

Description:

The appearance of the GUI will automatically match the system chosen theme.

Rationale:

The user will not have to manually edit the appearance of the interface.

Fit Criterion:

The GUI will be either in light, dark, or auto mode depending on what the user has selected on their host computer.

Priority: 5

Dependencies: 09

Requirement ID: 11

Description:

This software will have separate windows for each option selected by the user.

Rationale:

This keeps the software organized and easy for the user to interact with.

Fit Criterion:

A new window is displayed for each option the user selects in the main window.

Priority: 7

Dependencies: 09, 02

## **Usability:**

Requirement ID: 12

Description:

This software will be multi-platform, meaning that it will be available on Windows, MacOS, and Linux based systems.

Rationale:

This makes it easy for the user to use this software on any system listed above.

Fit Criterion:

The software is executable on any version of Windows, MacOS, or any distribution of Linux.

Priority: 8

Dependencies: None

Requirement ID: 13

Description:

Each user can create their own personal database of passwords saved locally on their system.

Rationale:

The user will no longer need to write passwords down and wonder if they are secure or

not.

Fit Criterion:

The user can add and remove passwords to be stored in the local file.

Priority: 8

Dependencies: 07, 08

Requirement ID: 14

Description:

User friendly messages will be printed to the screen throughout the software that educate the user on best practices for password security.

Rationale:

Allows the user to learn about how to keep their online accounts secure.

Fit Criterion:

Periodic messages print informing the user on what makes a certain password secure or unsecure.

Priority: 5

Dependencies: None

Requirement ID: 15

Description:

This software is easy to use for anyone and guides the use through each step.

Rationale:

Anyone can use the software because of its simple yet functional design.

Fit Criterion:

Every option and window are clearly labeled on the interface and guides the user through each selection.

Priority: 7

Dependencies: 09, 11

Requirement ID: 16

Description:

Anyone is free to install this software from the GitHub repository and use it on their system.

Rationale:

The purpose of this software is to be usable to anyone and help them store their

passwords and learn about password security.

Fit Criterion:

The software can be downloaded from the repository and run on any system with the correct packages installed.

Priority: 9

Dependencies: None

## **Performance:**

Requirement ID: 17

Description:

The software will not have any latency noticeable to the user.

Rationale:

Allows the user to quickly generate, check, and store their passwords locally.

Fit Criterion:

The software is not connected to the internet in any way and is completely local to each system allowing for little to no latency.

Priority: 8

Dependencies: None

Requirement ID: 18

Description:

The software will scan through the previously breached passwords list as efficiently as possible.

Rationale:

The software must scan through millions of passwords in order to accurately determine if

the password has been exposed.

Fit Criterion:

Latency exists but will not be overly conspicuous to the user.

Priority: 7

Dependencies: 06, 17

Requirement ID: 19

Description:

The software will be designed to be as precise as possible when generating passwords, checking their security, and storing them efficiently.

Rationale:

This will ensure the software is reliable and a useful password manager for everyone.

Fit Criterion:

The software will validate a generated password to certify that it meets the security requirements, ensures the whole breached wordlist is scanned, and makes sure that a password the user wishes to store does not already exist in their password database.

Priority: 8

Dependencies: 27, 06

Requirement ID: 20

Description:

The software will check any user input for validity and inform the user of any incorrect input.

Rationale:

Allows the software to be robust and to handle any erroneous input.

Fit Criterion:

All input fields that require it will be validated to ensure no syntax errors are present.

Priority: 7

Dependencies: None

Requirement ID: 21

Description:

The amount of passwords stored will not have a max capacity and is only dependent on the storage of the local system.

Rationale:

Every password the user has for online accounts can be stored in this software.

Fit Criterion:

The software will allow the user to store as many passwords as they wish.

Priority: 7

Dependencies: 07

Requirement ID: 22

Description:

The software is designed in such a way that new features can be added with ease.

Rationale:

To allow the software to have extensibility and longevity.

Fit Criterion:

New features can be added to the software.

Priority: 8

Dependencies: None

## **Maintainability and Support:**

Requirement ID: 23

Description:

Any updates or bug fixes for the software will be added to the GitHub repository.

Rationale:

Allows the software to be properly maintained.

Fit Criterion:

Updates for the software and to the breached wordlist are available through the repository.

Priority: 5

Dependencies: None

## **Security:**

Requirement ID: 24

Description:

The software can only be accessed with the user created master password.

Rationale:

Allows for only the owner of the stored passwords to view them.

Fit Criterion:

The software is unlocked and the passwords are accessible by the user upon correct entry of the password.

Priority: 9

Dependencies: 01

Requirement ID: 25

Description:

The database file storing the user’s passwords will be encrypted and will only be decrypted when the software is unlocked.

Rationale:

Maintains the privacy and integrity of the software.

Fit Criterion:

The file is encrypted when the software is not running and is only decrypted when the user is signed in.

Priority: 7

Dependencies: 01, 24

Requirement ID: 26

Description:

This software will record every successful and unsuccessful login attempt.

Rationale:

Allows the software to maintain an audit for security purposes.

Fit Criterion:

Each successful and unsuccessful login attempt is logged by the software.

Priority: 3

Dependencies: 01, 24

Requirement ID: 27

Description:

The password complexity requirements will include a minimum length of 10 characters, at least 2 upper case letters, 3 numbers, 2 special characters, and at least 30 bits of entropy.

Rationale:

The software will use this policy to generate secure passwords and to check user

passwords for the level of security.

Fit Criterion:

A generated password will not be given to the user unless it meets these requirements and each password checked by the user will be rated using the security scale based on this policy.

Priority: 9

Dependencies: None

## **Cultural:**

Requirement ID: 28

Description:

The goal of this software is to focus on the quality of the product to reduce faults and increase user satisfaction.

Rationale:

Allowing the software to be reliable and enjoyed by the users.

Fit Criterion:

The software is refined and the updates and user support are readily available.

Priority: 8

Dependencies: 23