40104/Secrets Manager

Requirements Engineering "**Secrets Manager"**

Task

Describe your project or any project neatly using the methods of Requirements Engineering.

Project Description

This is my base pet project of application for keep secrets. This small application should have a client connected to the backend and store the secrets encrypted in the database. In the process of completing this project, I would like to get acquainted with the Golang programming language.

Functional requirements

Aa Name	👥 Assign	🗓 Date	☼ Status
Authorization and Authentication		@January 23, 2024 → January 30, 2024	Done
Storage and encryption		@January 23, 2024 → January 30, 2024	Done
Generation		@January 23, 2024 → January 30, 2024	Done
Copy and paste		@January 23, 2024 → January 30, 2024	Done
Search and filtering		@January 23, 2024 → January 30, 2024	In progress
Synchronization		@January 23, 2024 → January 30, 2024	Not started
Plugin		@January 23, 2024 → January 30, 2024	Not started
Analysis and Statistics		@January 23, 2024 → January 30, 2024	Not started
Exchange and sharing		@January 23, 2024 → January 30, 2024	In progress

Aa Name	👥 Assign	📅 Date	⟳ Status
Notifications		@January 23, 2024 → January 30, 2024	In progress

Functional requirements

Functional requirements

Aa Name	👥 Assign	📅 Date	⟳ Status
Authorization and Authentication		@January 23, 2024 → January 30, 2024	Done
Storage and encryption		@January 23, 2024 → January 30, 2024	Done
Generation		@January 23, 2024 → January 30, 2024	Done
Copy and paste		@January 23, 2024 → January 30, 2024	Done
Notifications		@January 23, 2024 → January 30, 2024	In progress
Exchange and sharing		@January 23, 2024 → January 30, 2024	In progress
Search and filtering		@January 23, 2024 → January 30, 2024	In progress
Synchronization		@January 23, 2024 → January 30, 2024	Not started
Plugin		@January 23, 2024 → January 30, 2024	Not started
Analysis and Statistics		@January 23, 2024 → January 30, 2024	Not started

☐ **Authorization and Authentication**

- The web application must allow the user to create, log in and out of an account using their username and password.

- The web application should also support password recovery, password change, and two-factor authentication for enhanced security.

☐ S**torage and encryption**

- The web application should allow the user to save, edit, delete and view passwords for different sites or services.

- The web application must also encrypt and decrypt passwords using a strong algorithm and a key that is kept only by the user.

☐ G**eneration**

- The web application should allow the user to generate random and complex passwords using various parameters such as length, characters, numbers.

- The web application must also check the strength and uniqueness of passwords using various criteria such as entropy, dictionary, frequency.

☐ **Synchronization**

- The web application should allow the user to sync their passwords between different devices and browsers using cloud storage or other methods.

- The web application should also allow the user to export and import their passwords in different formats such as CSV, JSON, XML, etc.

☐ S**earch and filtering**

- The web application should allow the user to quickly and easily find the required passwords by searching by keywords, tags, categories.

- The web application should also allow the user to filter passwords based on various criteria such as creation date, modification date, expiration date.

☐ **Copy and paste**

- The web application should allow the user to easily copy and paste passwords into other applications or sites using hotkeys, context menu, toolbar.

- The web application should also allow the user to configure the clipboard lifetime so that passwords do not remain in memory after use.

☐ **Plugin**

- The web application should allow the user to automatically fill and enter passwords on different sites or services using browser extensions, applications for mobile devices, fingerprint scanners.

- The web application should also allow the user to configure rules and exceptions for autofill and autologin.

☐ **Analysis and Statistics**

- The web application should allow the user to analyze and track various aspects related to passwords, such as average strength, category distribution, change history, usage frequency.

- The web application should also allow the user to view and export various reports and graphs based on passwords.

☐ **Exchange and sharing**

- The web application should allow the user to securely exchange and share passwords with other users using encryption, one-time links, expiration dates.

- The web application should also allow the user to control other users' access and rights to their passwords.

☐ **Notifications**

- The web application should allow the user to receive notifications and reminders about various password-related events such as expiration, suspicious activity, need to change password.

- The web application should also allow the user to customize the frequency and method of receiving notifications and reminders.

Non-functional requirements

Non Functional requirements

Aa Name	👥 Assign	📅 Date	🔆 Status
High availability		@January 23, 2024 → January 30, 2024	Not started
Reliability		@January 23, 2024 → January 30, 2024	Not started
Security		@January 23, 2024 → January 30, 2024	Done

Aa Name	👥 Assign	🗓 Date	⟳ Status
<u>Performance</u>		@January 23, 2024 → January 30, 2024	In progress
<u>Usability</u>		@January 23, 2024 → January 30, 2024	In progress

Non Functional requirements

Aa Name	👥 Assign	🗓 Date	⟳ Status
<u>High availability</u>		@January 23, 2024 → January 30, 2024	Not started
<u>Reliability</u>		@January 23, 2024 → January 30, 2024	Not started
<u>Security</u>		@January 23, 2024 → January 30, 2024	Done
<u>Performance</u>		@January 23, 2024 → January 30, 2024	In progress
<u>Usability</u>		@January 23, 2024 → January 30, 2024	In progress

☐ **Security**

- The web application must protect sensitive user data such as passwords from unauthorized access, hacking, leakage or loss.

- The web application must use strong encryption, authentication, backups, auditing, and other security measures.

☐ **Performance**

- The web application must provide fast and stable access to user data, without delays, glitches or errors.

- The web application must use optimal algorithms, data structures, caching, load balancing and other optimization techniques.

☐ **Reliability**

- The web application must be able to operate in a variety of environments and situations without loss of functionality or quality.

- The web application must use redundancy, recovery, testing, monitoring, and other reliability techniques.

☐ High availability

- The web application must be fault-tolerant and continue to provide service to users in the event of failure of one or more nodes.

- The web application must support clustering and load balancing of frontend, backend and database

☐ Usability

- The web application should be easy and intuitive for users, without complexity or inconvenience.

- The web application must use a simple and beautiful interface, support for different languages, customization to user preferences and other convenience factors

Transition requirements

Transition requirements

Aa Name	⧉ Assign	▦ Date	⟳ Status
Data migration		@January 23, 2024 → January 30, 2024	Not started
Adapt to Change		@January 23, 2024 → January 30, 2024	Not started
User Training		@January 23, 2024 → January 30, 2024	Not started
Testing		@January 23, 2024 → January 30, 2024	In progress
Support and Maintenance		@January 23, 2024 → January 30, 2024	In progress

Transition requirements

Aa Name	⧉ Assign	▦ Date	⟳ Status
Data migration		@January 23, 2024 → January 30, 2024	Not started
Testing		@January 23, 2024 → January 30, 2024	In progress
Adapt to Change		@January 23, 2024 → January 30, 2024	Not started
User Training		@January 23, 2024 → January 30, 2024	Not started
Support and Maintenance		@January 23, 2024 → January 30, 2024	In progress

☐ **Data migration**

- The web application should allow the user to migrate their passwords from other sources such as files, other password managers, browsers.

- The web application must support different data import and export formats such as CSV, JSON, XML, etc., and ensure data security and integrity during migration.

☐ **Testing**

- The web application must be tested against functional requirements such as authorization, storage, generation, synchronization.

- The web application must be tested for resistance to various types of attacks such as hacking, leaking, spoofing, denial of service.

- The web application must be tested for its ability to handle large volumes of data and requests without losing speed or stability.

- The web application must be tested for its ability to work under various conditions and situations, without loss of functionality or quality.

☐ **Adapt to Change**

- The web application must be able to adapt to changes in requirements, technologies, standards, etc., without losing functionality or quality.

- The web application must use flexible and modular architectures, support updates and patches, be testing and responsive.

☐ **User Training**

- The web application should provide users with the necessary information and instructions on how to use the web application, as well as answers to frequently asked questions.

- The web application must have a simple and understandable interface, support for different languages, a help system, video tutorials, etc.

☐ **Support and Maintenance**

- The web application should provide users with the necessary support and maintenance in case of problems, questions or requests.

- The web application must have support, feedback, warranty, backup, recovery.

Interface requirements

Interface requirements

Aa Name	👥 Assign	🗓 Date	Status
Navigation and Orientation		@January 23, 2024 → January 30, 2024	Not started
Feedback and Interaction		@January 23, 2024 → January 30, 2024	Not started
Design and Aesthetics		@January 23, 2024 → January 30, 2024	In progress
Adaptability and Accessibility		@January 23, 2024 → January 30, 2024	In progress
Data Input and Output		@January 23, 2024 → January 30, 2024	Done

Interface requirements

Aa Name	👥 Assign	🗓 Date	Status
Navigation and Orientation		@January 23, 2024 → January 30, 2024	Not started
Design and Aesthetics		@January 23, 2024 → January 30, 2024	In progress
Data Input and Output		@January 23, 2024 → January 30, 2024	Done
Feedback and Interaction		@January 23, 2024 → January 30, 2024	Not started
Adaptability and Accessibility		@January 23, 2024 → January 30, 2024	In progress

☐ **Design and Aesthetics**

- The web application should have a simple and beautiful design that matches the theme and purpose of the web application and also attracts and holds the user's attention.

- The web application must use colors, fonts, images, icons, animations and other visual design elements that harmoniously combine with each other and create a unified style.

☐ **Navigation and Orientation**

- The web application should provide easy and intuitive navigation across different pages and sections of the web application, and allow the user to easily determine their current position and available actions.

- The web application must use menus, breadcrumbs, links, buttons, tabs, headers, footers and other navigation elements that clearly and unambiguously indicate the structure and functionality of the web application.

☐ **Data Input and Output**

- The web application should allow the user to easily and securely input, output, edit and delete data related to passwords and other sensitive information.

- The web application must use forms, fields, checkboxes, radio buttons, drop-down lists, tables, dialog boxes and other data input and output elements that provide validation, confirmation, encryption and protection of data from unauthorized access.

☐ **Feedback and Interaction**

- The web application must provide the user with the necessary feedback and interaction that validates, informs, guides and motivates the user.

- The web application must use messages, notifications, prompts, instructions, sounds, vibrations and other feedback and interaction elements that respond to the user's actions, requests and errors, and also offer help, advice and recommendations to the user.

☐ **Adaptability and Accessibility**

- The web application must be able to adapt to different devices, browsers, resolutions, orientations, networks and other factors that affect the display and operation of the web application, without loss of quality or functionality. The web

application must use adaptive and responsive design, media queries, frameworks, libraries and other technologies that allow the web application to adapt to different conditions and usage scenarios.