**Software design document**

**Introduction:**

Our password management app will provide a secure and convenient way for users to manage all their passwords in one place. With our app, users can easily generate complex passwords, securely store them, and access them on any device with ease. Our app will offer advanced features such as two-factor authentication, password sharing, and automatic password change reminders to ensure maximum security for our users.

**Requirements specification:**

Our target audience will be individuals and businesses who are concerned about the security of their online accounts and want an easy-to-use and reliable solution to manage their passwords. Our app will be suitable for people of all ages and professions who use online services and want to protect their personal information and data from unauthorized access.

****Overall Design:****

**Our app consists of 4 main interfaces, including login interface, login successful interface, edit password information interface and password information interface. Each interface is linked by buttons to make the conversion between pages smooth. The main functions of the app include: 1. User registration and login functions. 2. Create, edit, and delete accounts and account information. 3. Have a slider menu to delete the account, edit the information, and have an instant cancellation link to prevent users from deleting the account information by mistake. 4. Hidden password 5. It will be automatically filled to the landing page after registration 6. The account password can be stored and commented by app.**

****User Interface Design:****

**In the UI design part, we use black as the background, because we believe that black can better highlight the relevant information and content of the password, and at the same time, black can give people a sense of security. In addition, we also designed the avatar, there is a default avatar. Of course, users can also upload their own favorite avatar. In the lower right corner of the information page, we have added a "+" icon to make it easier for users to edit or add password information. Finally, we added ICONS to several popular apps.**

****Key technologies:****

**On a technical level, we write code in kotlin and apply what we learned in class to our app. For example: user registration login interface implementation and send data to another interface and return and so on. At the same time, we also learned some tips and solved some puzzles on the csdn website and GitHub. The main problems encountered by our technology include: 1. The sideslip menu does not respond to gesture sliding events. 2. Side sliding menu The content area covers the side sliding menu. 3. The data deletion operation is cancelled. 4. User interface design and user experience optimization.**

****Testing and User Experience Analysis:****

**Here are some user feedback and suggestions.**

**User A:**

**Feedback: The interface design is intuitive, but we want to add a search function to make it easy to find passwords quickly.**

**Improvement suggestion: Add a search box in the main interface, and support the function of searching passwords by keywords.**

**User D:**

**Feedback: The password backup and recovery function is not intuitive, wish there was a detailed tutorial or explanation.**

**Improvement suggestion: Provide a concise tutorial or instructions to help users properly use the backup and restore features.**

**User E:**

**Feedback: The password has security risks. You are advised to add permission Settings.**

**Improvement: Add permission Settings to password management to ensure that only authorized users can view and use shared passwords**

**User G:**

**Feedback: There is no password strength evaluation function, suggest improved algorithm.**

**Improvement suggestion: Design a password strength evaluation algorithm to provide more accurate password strength evaluation results.**

****Conclusion:****

**We learned a lot of knowledge in the process of app development and deepened it through practice. At the same time, the development of the app has made password management easier for users, and we are happy that we can implement most of the functions we designed. The difficulties and future development are described in detail below.**

1. **Password Protection Enhancement:**
2. **- Current Issue: The app utilizes a master password to protect user accounts and passwords. However, the security of the master password is crucial, as a compromised master password can jeopardize all user information.**

**- Proposed Solution: Implement additional security measures such as enforcing strong password requirements for the master password, including a combination of uppercase and lowercase letters, numbers, and special characters. Additionally, consider incorporating features like two-factor authentication or biometric authentication (e.g., fingerprint or face recognition) to add an extra layer of security.**

**2. Encryption and Secure Storage:**

**- Current Issue: The app stores user passwords, which need to be securely stored to prevent unauthorized access.**

**- Proposed Solution: Utilize strong encryption algorithms, such as AES (Advanced Encryption Standard), to encrypt user passwords before storing them in the database. Ensure that the encryption keys are securely managed and not stored within the app or easily accessible to unauthorized individuals. Additionally, consider implementing secure storage practices, such as storing the encrypted passwords in a separate secure database or utilizing keychain services provided by the operating system.**

**3. Regular Password Update Reminders:**

**- Current Issue: Users may forget to update their passwords regularly, increasing the risk of security breaches.**

**- Proposed Solution: Implement password update reminders or notifications to prompt users to change their passwords periodically. Allow users to set their preferred password update frequency and provide helpful tips on creating strong and unique passwords.**

**By incorporating these improvements, we can enhance the overall security of the app and protect user accounts and passwords from potential security threats. Additionally, by addressing the previously mentioned enhancements, such as passwor**