Password Keeper

Requirements Specification

Diego Menegaz, Michael Belmear, Joshua Elmore, Ben Heinze

Product Vision

FOR users on the internet

WHO want an accessible, secure place to create and store sensitive password information.

THE Password Keeper is a website with a secure environment to store passwords.

THAT is used to store all the user’s passwords while also letting the user generate ‘difficult-to-decode' passwords to ensure increased protection against cyber security threats.

UNLIKE traditional methods of keeping passwords such as on paper or a google document, it gives users access to a secure platform to encrypt and store their passwords, while also allowing auto generated password creation.

OUR product provides a secure platform with encrypted data so that malicious actors will have a harder time accessing the user’s passwords, while legitimate users have access to their passwords and corresponding websites.

Feature 1:

System securely stores the user's passwords.

Acceptance Criteria:

GIVEN I am a user who wants a centralized place to store all my passwords

WHEN I become a validated user of the Password Keeper system

THEN I can store all my online passwords in one location that is accessible from all my devices

User Stories:

US1-1. As a validated user who has multiple passwords for different websites, I want to be able to securely store and view all my passwords in one place so that it won't be hacked.

US1-2. As a security system administrator, I want only validated users to be able to use the system to access their passwords so that the possibility of third-party programs or cookies also having access is limited.

Feature 2:

Users can securely share their passwords.

Acceptance Criteria:

GIVEN I am a user who wants to share a password to personally selected users

WHEN I am a validated user of the Password Keeper system, and my recipient is chosen and validated

THEN I can share chosen passwords with validated user(s)

User Stories:

US2-1. As a validated user sharing an online subscription, I want to be able to securely share my password with another user, so that we can both have access without fearing that other malicious actors will gain access to our password.

US2-2. As a validated user, I want to securely share my Wi-Fi password with all my roommates, so that I don't want to have to worry about our neighbors stealing the password and using our Wi-Fi.

US2-3. As a system administrator, I want to be able to securely disclose passwords to users who request them so that I don't have to worry about our system security, giving me time to assist user's and their problems.

Feature 3:

Users can securely generate complex passwords.

Acceptance Criteria:

GIVEN I am a user who needs to update a password

WHEN I am a validated user of the Password Keeper system

THEN I can securely generate a new password that is hard to hash

User Stories:

US3-1. As a validated user, I want to be able to auto-generate a complex password that malicious actors will have a hard time hashing/hacking so that I don't have to spend time making my own password.

US3-2. As a system administrator, I want my users to have secure passwords that meet the necessary criteria and are hard to hash/hack so that they don't have to worry about their passwords being leaked by someone with mal intent.

Feature 4:

Users can securely export their passwords to a file.

Acceptance Criteria:

GIVEN I am a user who wants to print a paper copy or downloaded a file copy of my passwords

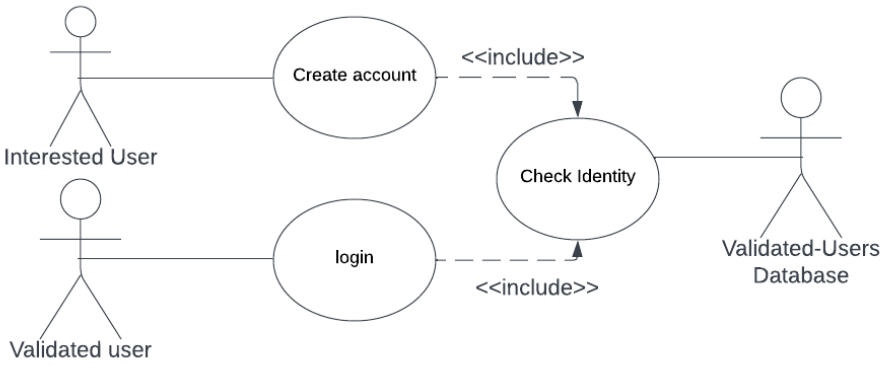
WHEN I am a validated user of the Password Keeper system

THEN I can export all my passwords to a downloadable encrypted file

User Stories:

US4-1. As a validated user for a company's network, I want to be able to export all our passwords to a file so that I can better distribute them to management and/or other people that need them.

US4-2. As a system administrator, I want businesses, private groups, and individuals to be able to download all their encrypted data so that they remain users and can customize their experience with the Password Keeper software system.



Use Case name: Create Account

Related requirements: US1-1

Goal in Context: Allow an interested user to create an account for Password Keeper

Preconditions:

1. The interested user has access to the internet.
2. The interested user has a valid form of ID

Successful End Condition: The interested user becomes a validated user

Failed End Condition: The interested user does not become a validated user

Primary Actors: Interested User

Secondary Actors: validated-users Database

Trigger: The interested user chooses to make a new account

Main Flow of Events:

1) interested user selects *Create account*

2) System asks user for ID information

3) The user gives the system ID information

Include::check identity

4) System performs validation

2) The system updates validated-*users database*

Extensions:

3.1) The interested user is rejected from creating a new account

Use Case name: Login

Related requirements: US1-1

Goal in Context: Allows validated members to access Password Keeper

Preconditions:

1) The validated user has access to the internet

2) The validated user has created an account and exists in the validated-*users database*

Successful End Condition: validated user gets access to all their passwords

Failed End Condition: validated user is not granted access to their passwords

Primary Actors: validated User

Secondary Actors: validated-users Database

Trigger: validated user chooses to login

Main Flow of Events:

1) validated User selects *login*

2) The system asks the user for ID information and compares it to the validated-*users database.*

Include::check identity

3) If the information matches the validated-*users database,* they are granted access to Password Keeper

Extensions:

3.1) The validated user enters wrong information.

Use Case name: check identity

Related requirements: US1-1

Goal in Context: Get information from the interested/validated user, and uses this information to compare information in the validated-*users database*

Preconditions:

1) The validated/interested user has access to the internet.

Successful End Condition: The validated/interested user now has access to Password Keeper

Failed End Condition: The validated/interested is not allowed to access to Password Keeper

Primary Actors: validated/interested user

Secondary Actors: validated-users Database

Trigger: The interested/validated user chooses to create-account/login

Main Flow of Events:

1) The interested/validated user chooses to login

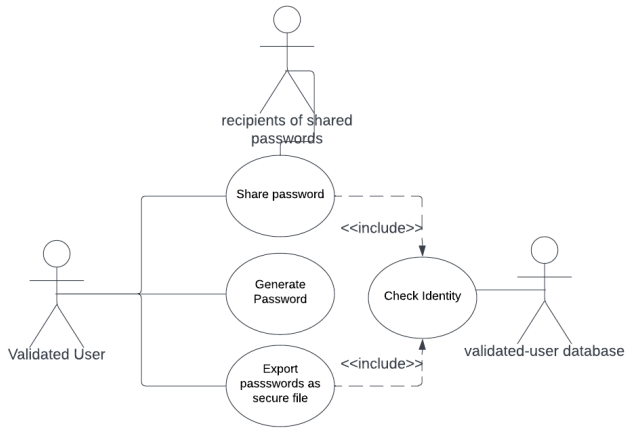
2) System asks for ID information

1) System performs validation check.

2) If success, they are granted access to Password Keeper

Extensions:

3.1) The validated/interested user enters incorrect information.



Use Case name: Share passwords

Related requirements: US 2-1

Goal in Context: A validated user of the Password Keeper can securely send website/password information to chosen recipients

Preconditions:

1) validated user is logged into Password Keeper

2) validated user has selected which passwords they would like to share

Successful End Condition: recipients chosen by the validated user now has access to the selected passwords.

Failed End Condition: validated user is not able to share passwords to chosen recipients

Primary Actors: validated user

Secondary Actors: validated User Database, recipients of shared passwords

Trigger: validated user opened Password Keeper and has chosen the passwords they would like to share.

Main Flow of Events:

1) validated user select which passwords they would like to share.

2) System identifies the passwords and stores them in secure file.

3) System sends secure file to chosen recipients.

Extensions:

3.1) validated-users database rejects identity

Use Case name: Generate Password

Related requirements: US 3-1

Goal in Context: A validated user of the Password Keeper can generate a secure password.

Preconditions:

1) validated user is logged into Password Keeper

Successful End Condition: validated user is given a unique password

Failed End Condition: validated user cannot generate a new password

Primary Actors: validated user: user that has logged in successfully to Password Keeper

Secondary Actors: none

Trigger: validated user chooses to generate a new password

Main Flow of Events:

1) validated user chooses to generate password

2) System shows validated user the generated password

3) if validated user accepts password, the password database updates with added information

Extensions:

1) System fails to generate password

Use Case name: export passwords as secure file

Related requirements: US4-1

Goal in Context: A validated user of the Password Keeper can export their complete list of passwords as a secure/encrypted file

Preconditions:

1) validated user is logged into Password Keeper

Successful End Condition: validated user gets a secure/encrypted file of their passwords

Failed End Condition: validated user does not get a secure/encrypted file of their passwords

Primary Actors: validated user

Secondary Actors: validated-users database

Trigger: validated user chooses to download their passwords

Main Flow of Events:

1) validated User chooses to download their passwords

2) The system reaffirms the user's choice to download passwords

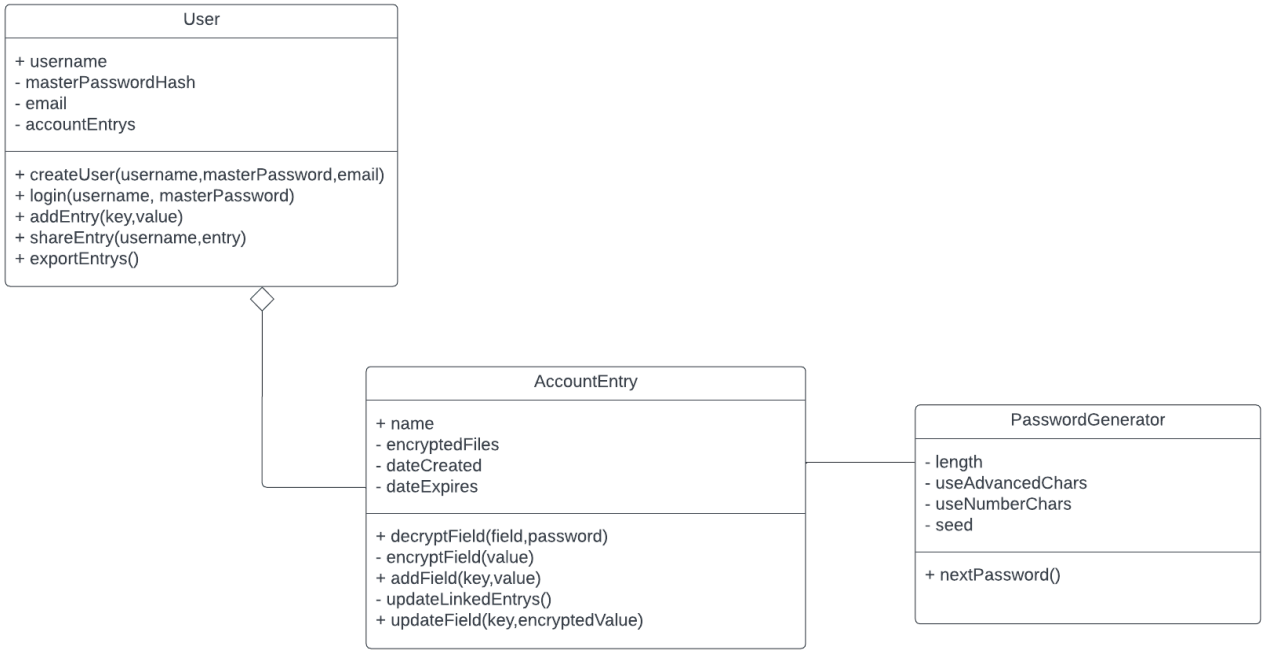
2) if the affirmation passes, a secure/encrypted file of the passwords will be downloaded.

Extensions:

3.1) validated user denies reaffirmation

3.2) System has no passwords to export

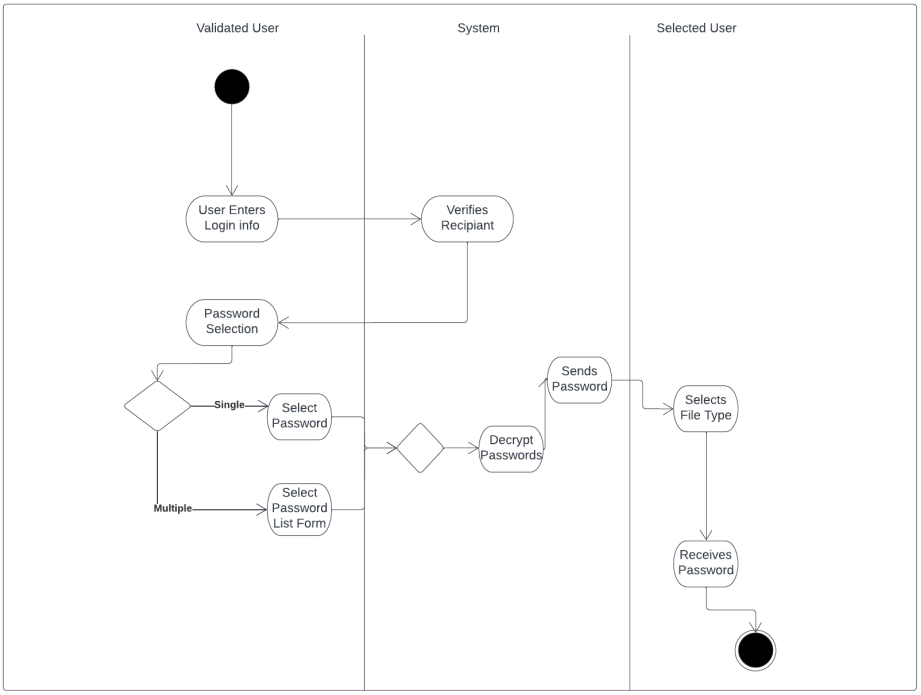
Class Diagram



Activity Diagrams:

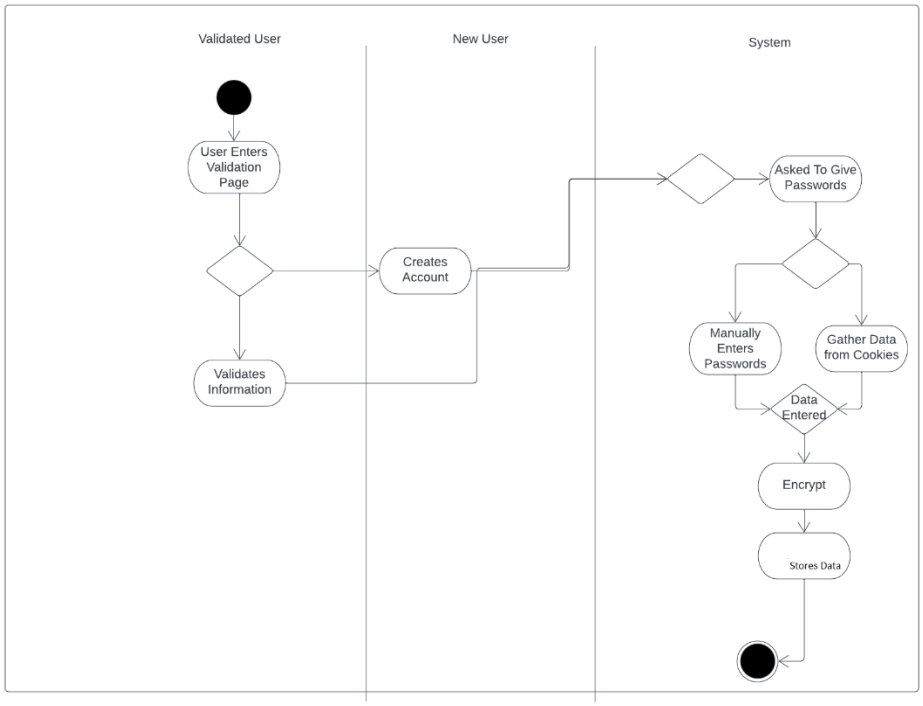
Covers: US2-(1,2,3), US4-(1,2)

Sending a File to a Select User



Covers: US1-(1,2)

Gathering Existing Passwords



Covers US3-(1,2)

Create New Password (Auto-Password Generation)