**GROUP 7 - LOCKIT**

**Features**

* 1 master key password to log in to the app - **Implemented**
* If the master password is forgotten the user will receive a temporary password through an email account. As soon as this temporary password is entered in the desktop app will open the login screen requesting to change your password. **Not implemented ( as Emile Ohan suggested we didn’t implement this feature)**
* The application will have a feature that forces the user to change their master password every 3 months by having the master password expire every 90 days-**Implemented with more flexibility for the user. The user can select the security level(not secure,low,medium or high)**
* Copy button next to each password so the user can easily copy it and place it in the corresponding web, software, etc.-**Implemented**
* Add new password entry to the manager.  -**Implemented**
* Remove password entry from the manager  -**Implemented**
* Password Generator –-**Implemented**
* Decrypt password to see plain text –-**Implemented**
* Auto password renewal – **Not implemented** – however the user will get an error if password is expired and need to renew the password. If password is the same the date is not updated therefor you cant save the same password if expired. If new password entered the new date is saved in the database.
* Alert system that warns if the password is frequently used in several websites - -**Implemented**
* Share information with friends or family members – **Not implemented**
* Link to the project source code on GitHub repository - **Implemented**
* Update master key password  **-Implemented**
* Encrypt and store files, images, and notes -**Implemented**

**New Master Key Page**

* Master Key Entry Box - This page will have a text entry box for a new master key to be setup with the software. **-Implemented**
* GitHub Icon - This will be in the left corner of the page to a GitHub page containing our project. **-Implemented**
* Master Key Help Box - Clicking this button will give a detailed description of telling the user what to do and what a master key will be. **-Implemented**
* Password Hint Entry Box - This box will be on the new master key page to be setup with a master key (optional). **-Implemented**
* Password Hint Color - A color from a menu of standard colors (red, blue, green, purple..etc) will be picked by the user and will be set up alongside the password hint entry box.- **Not implemented**

**Login with Master Key Page**

* Login with the master key page - This page will have a text entry box to enter your master key password. **-Implemented**
* Show key button - This page will have a button to show the text being typed inside the text entry box.- **-Not implemented**
* Page explainer - This explainer will have a detailed description of what input the program is expecting from the user.-**Not implemented, user can log in and check the documentation in the Help menu**
* Master Key Hint - This will output the hint you have entered into your database during the initial master key setup. **-Implemented**
* GitHub Icon - This will be in the left corner of the page to a GitHub page containing our project. **-Implemented**

**Initial Security Page**

* View Data Icon Checkbox - This will lock the view icon button behind the master password if enabled. **-Implemented**
* Copy Button Checkbox -  This will lock the copy button behind the master password if enabled. **-Implemented**
* Auto logout Checkbox - This will enable an auto-logout timer to log out the user after 5 minutes of inactivity**-Implemented – added more flexibility , the user can select between 1-10 minutes**

**New Password Entry Page**

This page will have text boxes to enter password entry name, login name, password, security answers, category and save button.

* ‘Entry name' textbox - the user can input alphabetical characters or numeric, and there will be a constraint on the number of characters in the textbox. (Maximum 35 characters) -**Implemented**
* ‘Website’ textbox – this field is optional; the user can input a valid website to the account. -**Implemented**
* Account ‘username’ textbox - the user can input alphabetical characters or numeric, and there will be a constraint on the number of characters in the textbox. (Maximum 50 characters) -**Implemented**
* ‘Password’ textbox - the user can input alphabetical characters, numeric, special characters and there will be a constraint on how many characters the user can provide. (Maximum 25 characters) -**Implemented – minimum 6 character .. no max characters**
* ‘Security Question’ radio button- the user has to select yes/no if he would like to enter security answers-**Implemented**
* ‘Number Security Answers’ drop down – if the user selects yes to security question radio button a drop-down displays with a number indicating the number of security answers. The user must select the number of security answers he would like to enter. -**Implemented**
* ‘Security answers’ text box – the number of text boxes depends on the number that is selected in the drop-down menu. The user can input alphabetical characters, numeric, special characters and there will be a constraint on how many characters the user can provide. (Maximum 50 characters) -**Implemented**
* ‘Show’ button – this button located near the password textbox, if a user clicks this button the user will be able to see the password in plain text. If this button is not clicked the password that the user enters displayed in dots. -**Implemented**
* ‘Generate Password’ button - this button located near the password textbox, if a user clicks this button the software automatically will generate a strong password and enters it in the password text box. In order to view the password, the user needs to click the Show button. -**Implemented**
* Password indicator – located below the password text box. It indicates how strong is the password. -**Implemented**
* ‘Password security level’ drop down – user must select level of security for the password. The drop-down options are: no need to update the password, change every month, change every 3 months, change every 6 months. Depends on user selection the software will generate timer for each password entry. -**Implemented**
* ‘Save’ Button – when the user clicks this, the system will check the database to see if there are no duplicates in the database. If entry name match with another entry name in the database it will display an error and the user must select a different entry name. If the password matches another password in the database it will display a warning message. If the password matches more than 3 passwords in the database, an error message will be displayed and the user must enter a different password. If the form is filled with no error messages the system will create new password entry in the database and present the success message. -**Implemented – no warning message if password matches only error if more than 3 passwords are the same. Entry name should be unique within a category**
* ‘Return’ Button – discard all the input text and returns to the previous menu. -**Implemented**

**Additional features implemented**

**Notes textbox – to input notes related to the entry**

**Modify Password Entry Page**

On this page, the user can modify existing password entry

* ‘Entry name’ textbox - the user can input alphabetical characters or numeric, and there will be a constraint on the number of characters in the textbox. (Maximum 35 characters) -**Implemented**
* ‘Website’ textbox – this field is optional; the user can input a valid website to the account. -**Implemented**
* Account ‘username’ textbox - the user can input alphabetical characters or numeric, and there will be a constraint on the number of characters in the textbox. (Maximum 50 characters) -**Implemented**
* ‘Current password’ textbox - the user can view current passwords. -**Implemented**
* ‘Change password’ button – if user clicks this button a new window pops up with new password textbox requesting to enter a new password.  -**Implemented. There is no new window popup. If user click generate password the old password will be cleared from the textbox and populated with the new password.**
* Pop up window - ‘New password’ textbox - the user can input alphabetical characters or numeric, and there will be a constraint on how many characters the user can provide. (Maximum 25 characters) - **Not Implemented – the user can do it on the Modify Password Screen**
* Pop up window - ‘Generate Password’ button - this button located near the password textbox, if the user clicks this button the software automatically will generate a strong password and enters it in the password text box. In order to view the password, the user needs to click the Show button. **Not Implemented – the user can do it on the Modify Password Screen**
* Pop up window- ‘Password indicator’ – located below the password text box. It indicates how strong is the password. **Not Implemented – it is displayed on Modify Password Screen**
* Pop up window- ‘Show’ button – this button located near the password textbox, if the user clicks this button the user will be able to see the password in plain text. If this button is not clicked the password that the user enters displayed in dots. **Not Implemented – it is displayed on the Modify Password Screen**
* Pop up window -’Save’ button - when the user clicks this, the system will check If the password matches another password in the database. If it matches another password in the database it will display a warning message. If the password matches more than 3 passwords in the database, an error message will be displayed and the user must enter a different password. The system will update the new password to the database and close the popup window. The new password will be displayed in the password textbox. **Not Implemented – the user can do it on the Modify Password Screen, no warning message if password matches only error if more than 3 passwords are the same.**
* ‘Security Question’ radio button- the user has to select yes/no if he would like to enter security answers- **Implemented.**
* ‘Number Security Answers’ drop down – if user selects yes to security question radio button, a drop-down displays with a number indicating the number of security answers. The user must select the number of security answers he would like to enter. **Implemented.**
* ‘Security answers’ text box – the number of text boxes depends on the number that is selected in the drop-down menu. The user can input alphabetical characters, numeric, special characters and there will be a constraint on how many characters the user can provide. (Maximum 50 characters) **Implemented.**
* ‘Show’ button – this button located near the password textbox, if user clicks this button the user will be able to see the password in plain text. If this button is not clicked the password that the user enters displayed in dots. **Implemented.**
* ‘Password Security Level’ drop down – user must select the level of security for the password. The drop-down options are: not secure - no need to update the password, high - change every month, medium-change every 3 months, low- change every 6 months. Depends on user selection the software will generate timer for each password entry. **Implemented.**
* ‘Save’ button – when the user clicks this, the system will check the database to see if there are no duplicates in the database. If entry name match with another entry name in the database it will display an error and the user must select a different entry name. If the form is filled with no error messages the system will create modify password entry in the database and present the success message. **Implemented. Entry name should be unique within a category**
* ‘Return’ button – discard all the changes and returns to the previous menu. **Implemented.**
* ‘Delete Entry’ button – removes the entry from the database. If the user clicks this button pop up window displays with a warning message asking the user to approve the deletion. If the user selects ‘yes’ to delete password entry the system will delete password entry from the database. **Implemented.**
* **Additional features implemented**
* **Notes textbox – to input notes related to the entry**

**View Password Entry Page**

On this page, the user can view all the information related to the password entry.

* ‘Entry name’ textbox - the user can view entry name. **Implemented.**
* ‘Website’ textbox - the user can view the website name. **Implemented.**
* ‘Go to website’ button – displays only if the website is in the database. If the user clicks this button, the system will open a Browser and take the user to the corresponding website. **Implemented. If no website warning message popup telling that website is not exist in the entry**
* ‘Username’ textbox - the user can view account name. **Implemented.**
* ‘Password’ textbox – password is displayed with dots.  **Implemented.**
* ‘Show’ button – this button located near the password textbox, if user clicks this button the user will be able to see the password in plain text. **Implemented.**
* ‘Copy’ Button - this button located near the password textbox, if user clicks this button the user copies the password and can paste it in the corresponding website. **Not Implemented – can be done in View Passwords inside the Category screen**
* ‘Security answers’ text box – the user can view security answers. **Implemented.**
* ‘Password Security Level’ drop down – user can view the security level the password is set to. **Implemented.**
* Timer- depends on security level that is set for the password indicating how many days left to change the password. **Implemented in View Passwords inside Category screen**
* ‘Modify’ button – when the user clicks this button ‘Modify Password Entry Page’ will pop up. **Implemented.**
* ‘Return’ button – returns to the previous menu. **Implemented.**
* ‘Delete Entry’ button – removes the entry from the database. If the user clicks this button pop up window displays with a warning message asking the user to approve the deletion. **Implemented.**

**Additional features implemented**

* **Notes textbox – to view notes related to the entry**
* **Exclamation mark next to password entry when password is expired**
* **Auto fill username and password if click visit website ( not adjusted for every website- as it is a lot to cover but has that functionality for myseneca,google,rbc bank working)**

**View Passwords Page**

On this page, the user can see all the passwords that belong to the selected category.

On each category the password entry will be presented in the following way:

**Category**

Password entry name, Username, Password in dots,

* ‘Copy’ Button - this button located near the password textbox, if the user clicks this button the user copies the password and can paste it in the corresponding website. – **Implemented in pop up menu – right click on entry row.**
* ‘Show’ button – this button located near the password textbox, if user clicks this button the user will be able to see the password in plain text.– **Implemented in pop up menu – right click on entry row.**
* ‘Go to website’ button –displays only if the website is in the database. if user clicks this button, the system will open a Browser and takes the user to the corresponding website. – **Implemented in pop up menu – right click on entry row.**
* ‘View’ button – if user clicks this button, “View Password Entry Page” will be open. – **Implemented– double click on entry row.**
* ‘Modify’ button - if user clicks this button, “Modify Password Entry Page” will be open. – **Implemented – double click on entry row and click ‘Modify Password’**
* Timer **-** depends on security level that is set for the password indicating how many days left to change the password. – **Implemented**

**Additional features implemented**

* **Notes textbox – to view notes related to the entry**
* **Exclamation mark next to password entry when password is expired**
* **Auto fill username and password if click visit website ( not adjusted for every website- as it is a lot to cover but has that functionality for myseneca,google,rbc bank working)**
* **If password is expired the user unable to view/copy password and pop up message shows to change the password**
* **Username is encrypted and displayed in \*\*\*\*\*\*. When user click show password in the pop up menu the username and the password are decrypted.**

**Create category/Modify Category Page**

On this page the user has the option of creating a category, choosing a default category or modifying an existing category.

The page includes the following:

* Categories - clickable button user clicks this to bring down a drop-down list which contains default categories & previously saved categories. **Implemented – no drop down all categories are displayed in the page**
* New category - clickable button user clicks to create a new category. – **Implemented**
* New category box - Alphabetical characters allowed up to 35 characters. – **Implemented**
* Character limit - if user tries to put more than 35 characters, the cursor will stop at 15 characters . – **Not** **Implemented**
* Category limit - Only 15 user-defined categories can be saved at any one time on the drop-down list . – **Implemented**
* Prompt - If there are already 15 categories and the user tries to add one more than pop up box will ask the user to remove at least one from the list . – **Implemented**
* Modify category - clickable button that prompts the user to select which category to edit. – **Implemented – right click on the category and select modify**
* Delete category - clickable button which allows the user to remove the category he/she no longer requires . – **Implemented – right click on the category and select delete**
* Duplicate category - if creating a new category or modifying an old category creates a duplicate category than the system will automatically pop an alert requesting the user to change the password **–** – **Implemented. The pop up alert request to change the category name/color**

**Additional features implemented**

* **User must select unique color for each category**
* **If color is duplicate error message displayed**

**Add Image / document**

On this page, the user has the option to save documents or images on the application and have the encrypted for extra security.

The page will include the following:

* Insert Image -> this is a clickable button that will have a pop up asking where the user is adding the image form. **Implemented.**
* Insert Document -> this is similar to the insert image that will ask the user for document location to insert from. **Implemented.**
* Error message -> the application will prompt an error if either document is not supported by the encryption type. **Not Implemented – our software supports all file documents**
* Save media -> this will be a clickable button that will save the document or image into the application’s database. **Implemented.**
* delete media ->this is another clickable button that will allow the user to permanently delete an item from the data store. **Implemented.**
* Create Folder -> the user is able to create a separate folder for each set of documents or images that they save onto the application. **Implemented.**
* View image/document ->when this is clicked it will decrypt the chosen item and allow it to be viewed by the user. **Implemented.**
* Decrypt and Send media -> this will first decrypt the media and be sent by email to the user’s contact. **Implemented. Only send media from database to computer.**

**Additional features implemented**

* **Extra protection to view document/image by requesting Master Key if it is set up in the security settings**
* **Mini file system is implemented. Can store images and document inside folder and navigate to the main page**