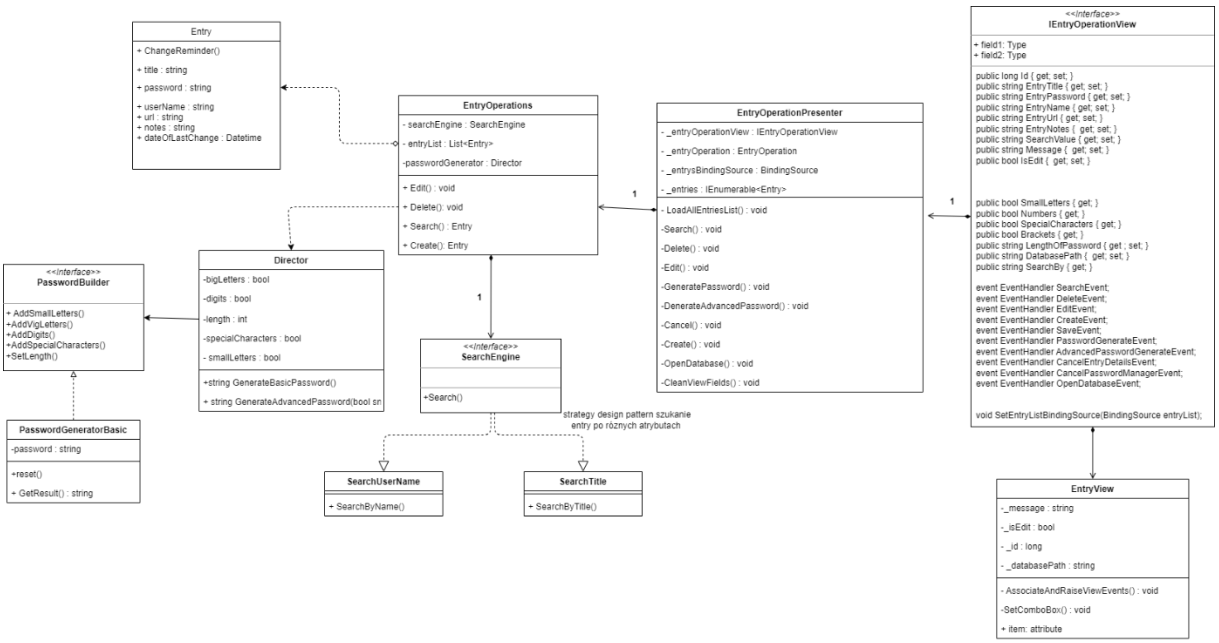
Password Manager

1. Diagram UML



2. Objaśnienia
   2.1. Wejście – klasa Entry zawierająca w sobie pola przedstawione na powyższym diagramie UML.
   2.2. Tytuł – nazwa strony lub cokolwiek innego co pomoże nam w organizacji wejść.
3. Opis
   Password Manager przechowuje hasła wraz z loginami, adresami stron internetowych, tytułami oraz notatkami, które mogą pomóc nam w organizacji.
   Password Manager ma takie funkcje jak: dodaj wejście, usuń wejście, edytuj wejście, wyszukaj wejście. Aplikacja ma także wbudowany password generator który po wciśnięciu przycisku „Add” automatycznie uzupełnia hasło. Możemy, także przejść do zaawansowanego password generatora gdzie możemy wybrać jakie znaki mają pojawiać się w naszym haśle oraz ustalić jego długość. Password manager ma także opcje edycji lub usunięcia zaznaczonego wejścia. Możemy także wyszukać interesujące nas wejście na podstawie tytułu lub nazwy użytkownika.
4. Zastosowane wzorce
   4.1. Builder – Password generator. Gdy tworzymy nowe wejście automatycznie generowane jest hasło. W przypadku gdy otwieramy stronę password generatora wtedy tworzymy zaawansowane hasło zaznaczając odpowiednie boxy. Dwie funkcje do tworzenia hasła GeneratePassword oraz GenerateAdvancedPassword.
   4.2. Strategy – SearchEngine. Gdy chcemy wyszukać odpowiednie wejście możemy zrobić to za pomocą tytułu jaki nadaliśmy naszemu wejściu lub za pomocą nazwy użytkownika. W combo boxie wybieramy co ma nam posłużyć przy wybieraniu wejścia.
   4.3. MVP – Model View Presenter – wzorzec architektoniczny umożliwi podział odpowiedzialności w programie. Model w odpowiedzialny za logikę biznesową. View implementuje interfejs użytkownika. Presenter, który odpowiedzialny jest za odpowiednie przetworzenie danych wejściowych i przekazanie ich dalej do modelu oraz na odwrót przekazywanie outputu do widoku.

5. Funkcjonalności
    5.1. zaimplementowane funkcjonalności:
        5.1.1. dodawanie wejścia zawierającego tytuł, hasło, nazwę użytkownika, url strony, notatki, datę ostatniej zmiany hasła.
        5.1.2. Automatycznie generujące się hasło – po wciśnięciu przycisku „add” przekierowywani jesteśmy do strony entry Details gdzie od razu pojawia się odpowiednio silne hasło
        5.1.3. Zaawansowany password generator, w którym możemy ustawić długość hasła oraz czy ma zawierać: małe litery, cyfry, nawiasy, specjalne znaki.
        5.1.4. Edytowanie już utworzonych wejść.
        5.1.5. Usuwanie wejść
        5.1.6. Wyszukiwanie wejścia po nazwie użytkownika lub po tytule jaki nadaliśmy danemu wejściu
    5.2. Funkcjonalności w trakcie implementacji
        5.2.1. Otwieranie innej już istniejącej bazy danych z poziomu programu
    5.3. Funkcjonalności nie zaimplementowane:
        5.3.1. Szyfrowanie wejść które przechowywane są w bazie danych
        5.3.2. Tworzenie nowej bazy danych z poziomu programu
        5.3.3. Ocenianie jakości hasła
        5.3.4. Przypomnienie o zmianie hasła po upływie określonego czasu od ostatniej zmiany
    5.4. Prawdopodobnie porzucone funkcjonalności:
        5.4.1. Możliwość logowania się do bazy danych poprzez wybranie odpowiednich zdjęć – łatwy atak Brute Force.