Password Authenticator Tool – Use Case Description

Actors:

1. **User** – The sole user who sets up, accesses, and manages passwords within the app.
2. **System** – The Password Authenticator Tool that handles authentication, password generation, storage, and security analysis.

Use Cases and Descriptions:

1. First-Time Setup & Authentication

1. A first-time user (new user) is guided through a welcome screen along with a tutorial explaining the app's features.
2. After the tutorial, the user sets up authentication using:
    1. Password
    2. Passcode
    3. Biometric data (fingerprint, face recognition, etc.)
3. Once setup is complete, the app locks behind the chosen authentication method.
4. An existing user only needs to enter their password, passcode, or biometric data to gain access.

2. Generate Secure Password

1. The User can request the app to generate a strong password.
2. The System creates a secure, random password based on predefined security rules (length, character types, etc.).
3. The generated password can be copied or saved within the app.

3. Store User Passwords

1. The User can save passwords for different accounts inside the app.

2. The System securely stores these passwords locally on the device using encryption.
3. Stored passwords can only be accessed after successful authentication.

4. Password Strength Checker

1. The User can enter a password to analyze its strength.
2. The System evaluates the password based on factors like:
    1. Length
    2. Use of uppercase/lowercase letters, numbers, and special characters
    3. Predictability and common patterns
3. The app provides feedback on how strong the password is and how likely it is to be cracked.
4. If the password is weak, the System suggests improvements.

5. Reset Forgotten Password (if applicable)

1. If the **User** forgets their password/passcode and hasn't set up biometrics, recovery might not be possible.
2. If the app includes a **recovery method**, it could involve security questions or a backup code set during the first-time setup.

Relationships and Interactions:

- The User interacts with all functions of the app.
- The System manages authentication, password generation, secure storage, and password strength analysis.
- The app operates offline, meaning no internet connection is required for authentication or password storage.