Daniyal Murtaza SP23-BSE-001

Use Case: Reset Password

Use Case Name	Reset Password
Primary Actor	Hostel Management System User (e.g., Student, Staff, Admin)
Stakeholders and Interests	- **Users**: Want a secure and easy way to regain access to their accounts if they forget their password. - **System Admin**: Wants to ensure password reset process is secure to prevent unauthorized access.
Preconditions	- User must have an existing account in the system. - User must have provided a valid email or phone number during registration.
Postconditions	- The user’s password is updated and they can log in using the new password.
Trigger	User clicks on "Forgot Password" link on the login page.

Main Success Scenario (Basic Flow)

1. **User** clicks on "Forgot Password?" on the login screen.
2. **System** prompts user to enter their registered email or phone number.
3. **User** enters the email/phone number and submits the form.
4. **System** validates the input and checks if it is associated with a registered account.
   - **Success**: The email/phone number is registered in the system.
5. **System** generates a password reset token or OTP (One-Time Password) and sends it to the user's email or phone number.
6. **User** receives the token/OTP and enters it on the password reset screen.
7. **System** verifies the token/OTP.
   - **Success**: The token/OTP is valid and not expired.
8. **System** prompts the user to enter a new password and confirm it.
9. **User** enters and confirms the new password.
10. **System** validates the new password format (e.g., length, complexity).
    - **Success**: Password meets the complexity requirements.
11. **System** updates the user’s password in the database.
12. **System** displays a success message and redirects the user to the login page.

Alternate Flows (Alternate Scenarios)

4a. Invalid email/phone number entered

- **Step 4a1**: System displays an error message: “No account found with this email/phone.”
- **Step 4a2**: User is prompted to try again or contact support.
    - **Alternative**: User may choose to go back to the login screen and try again or request additional help.

6a. Invalid or expired token/OTP

- **Step 6a1**: System displays an error message: “Invalid or expired token.”
- **Step 6a2**: User can request a new token/OTP.
    - **Alternative**: User may need to re-enter their email or phone number to receive a new token/OTP.

10a. Passwords do not match or do not meet complexity rules

- **Step 10a1**: System displays an error message: “Passwords do not match” or “Password must contain at least 8 characters, a number, and a symbol.”
- **Step 10a2**: User is prompted to re-enter the new password and confirm it.
    - **Alternative**: If the user forgets the complexity rules, the system can display the exact criteria for password strength.

Additional Success Case Scenarios and their Alternatives

Success Case Scenario 1: Password reset completed successfully and logged in immediately

- **Step 12**: After resetting the password, the system automatically logs the user in with their new credentials.
- **Alternative Case**:
    - If the auto-login fails (e.g., incorrect password entered or session issues), the system redirects the user to the login screen with an appropriate message: “Password reset successful, please log in with your new password.”

Success Case Scenario 2: User chooses to reset password via email

- **Step 5**: The user receives an email with a password reset link.
    - **Success**: User clicks the link and is redirected to the password reset form.
    - **Alternative**: If the email fails to arrive or gets delayed, the user can manually click "Resend Link" to receive a new reset link.
- **Step 6**: User enters the token received from the email and follows the steps outlined in the main success scenario.

Success Case Scenario 3: User resets password via phone OTP

- **Step 5**: The system sends an OTP via SMS to the registered phone number.
    - **Success**: The user receives the OTP and enters it correctly.
    - **Alternative**: If the user does not receive the SMS, they can choose to re-request the OTP or use an alternate method (e.g., email).

Special Requirements

- Reset link/token should expire within a specified timeframe (e.g., 15 minutes).
- Passwords must follow security standards (e.g., min. 8 characters, upper/lowercase, number, symbol).
- All sensitive data (tokens, passwords) should be transmitted securely using HTTPS and stored securely (e.g., hashed passwords).
- Option to limit the number of reset attempts to prevent brute force attacks.

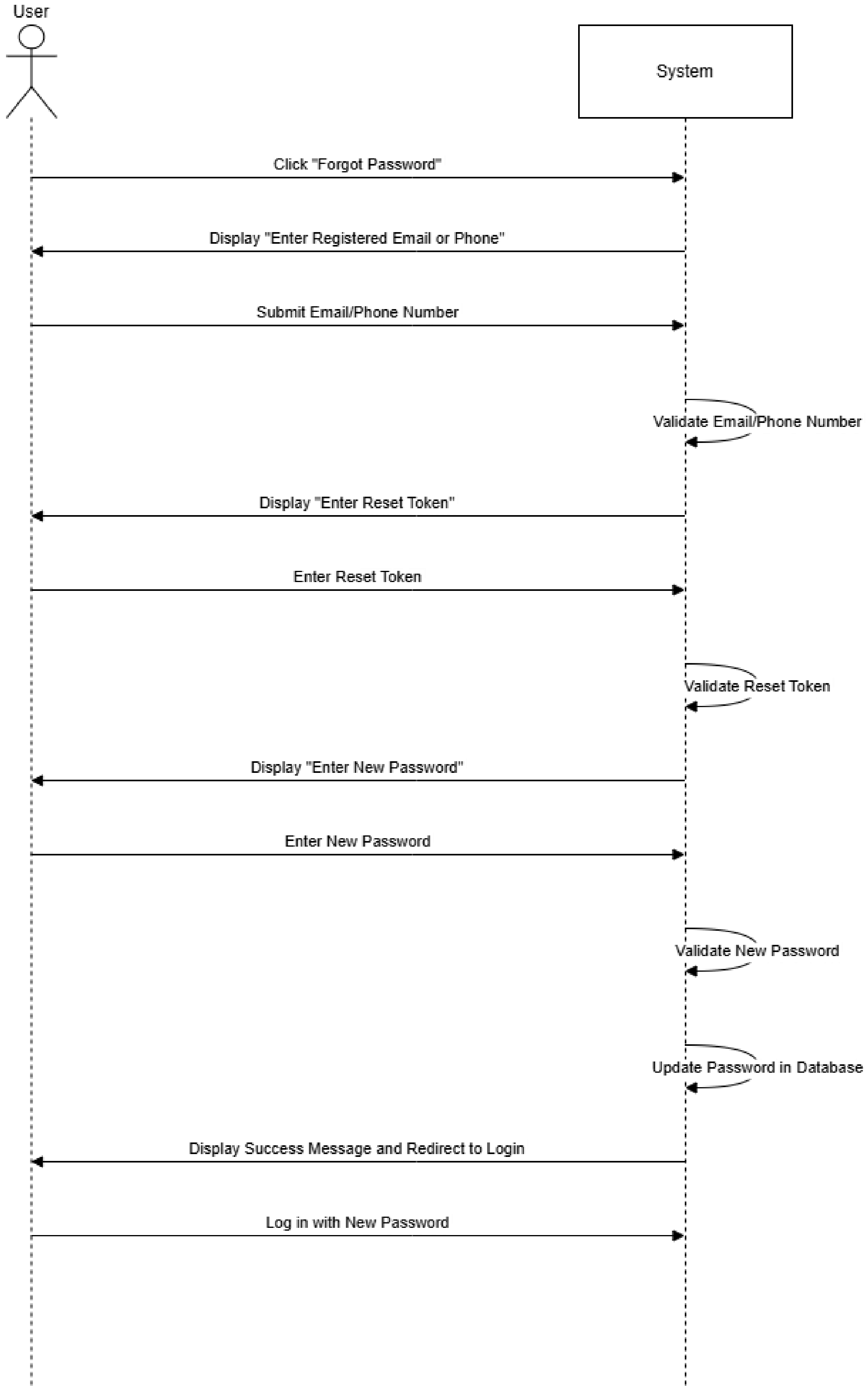
Frequency of Use

- Occasional: Typically when a user forgets their password or wants to update it for security.

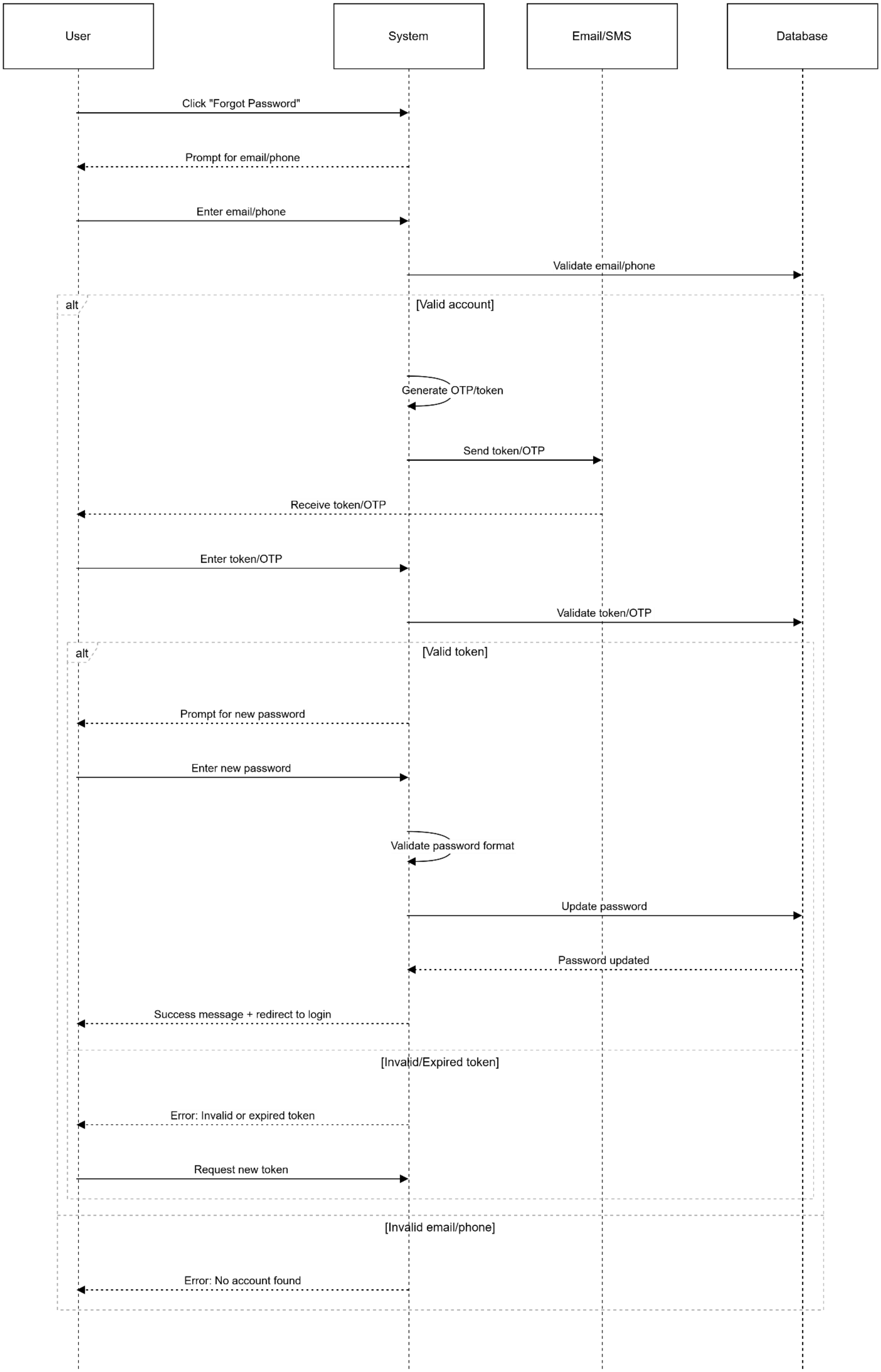
Open Issues

- Should the system allow password reset using both email and phone?
- Should the user be notified via email/phone after a successful reset for security awareness?

SSD For Reset Use case:


User
System
Click "Forgot Password"
Display "Enter Registered Email or Phone"
Submit Email/Phone Number
Validate Email/Phone Number
Display "Enter Reset Token"
Enter Reset Token
Validate Reset Token
Display "Enter New Password"
Enter New Password
Validate New Password
Update Password in Database
Display Success Message and Redirect to Login
Log in with New Password

SDD:


User
System
Email/SMS
Database
Click "Forgot Password"
Prompt for email/phone
Enter email/phone
Validate email/phone
alt
[Valid account]
Generate OTP/token
Send token/OTP
Receive token/OTP
Enter token/OTP
Validate token/OTP
alt
[Valid token]
Prompt for new password
Enter new password
Validate password format
Update password
Password updated
Success message + redirect to login
[Invalid/Expired token]
Error: Invalid or expired token
Request new token
[Invalid email/phone]
Error: No account found