LOW-LEVEL DESIGNS DOCUMENT

Hubba - Authentication

Version 1.1
Prepared By: Development Hell
Class: CECS 491-04
Date: December 14, 2022

Github Repository**:**
https://github.com/DevelopmentHellaHell/SeniorProject

Team Leader
Kevin Dinh
Members
Garrett Tsumaki
Bryan Tran
Jett Sonoda
Tien Nguyen
Darius Koroni

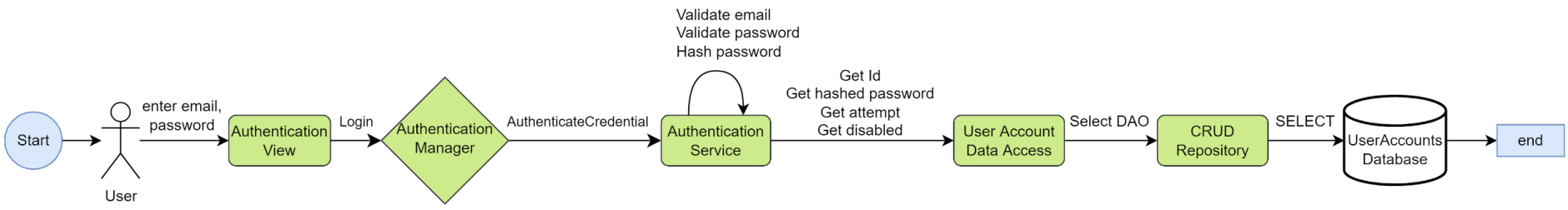
Revision History

Version	Overview	Date
v.1.0	Initial LLD	11/20/2022
v.1.1	Revision after Winter break	12/10/2022

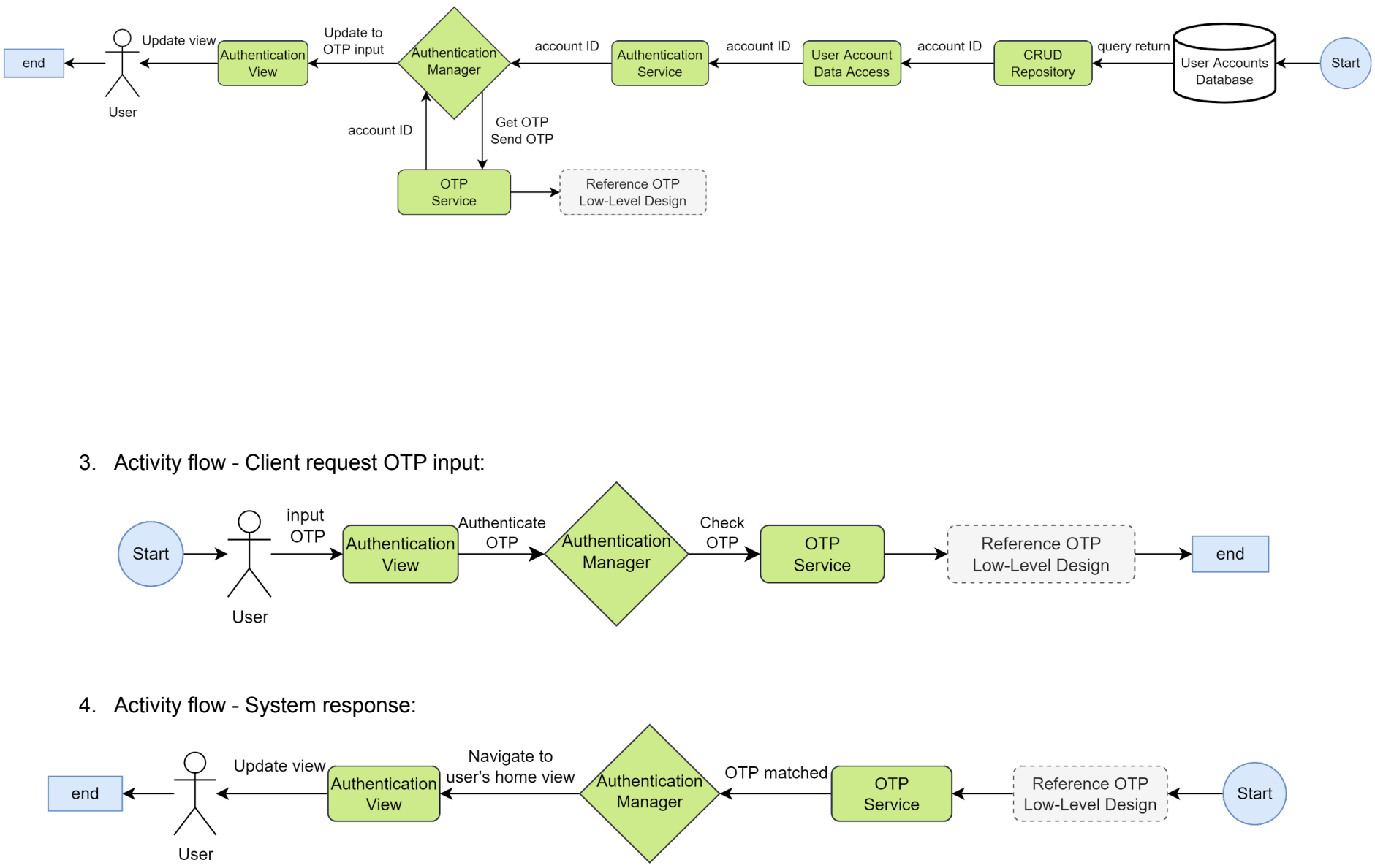
Table of Contents

High-Level Design

1. Activity flow - Client request Login:



2. Activity flow - System response and send OTP:



3. Activity flow - Client request OTP input:

4. Activity flow - System response:

Low-Level Design

User story: As a user, I can log in by providing valid security credentials including a username and a passphrase. Then I can complete the login process by entering a One Time Password which is sent to my registered email by the system.

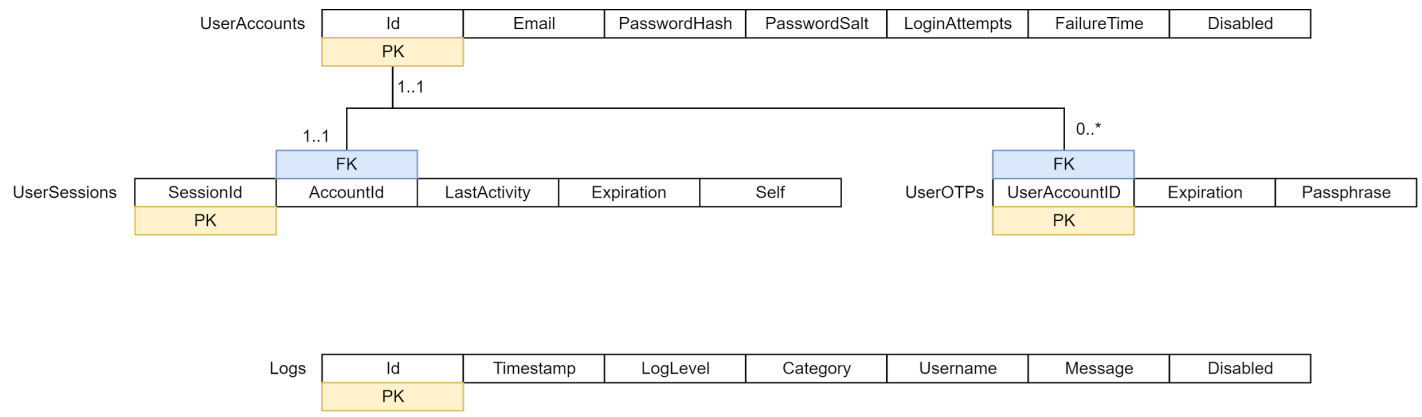
Business rules:

1. A valid username consists of:
    1.1. Minimum length of 8 characters
    1.2. 0-9
    1.3. a-z
    1.4. Allow these special characters: . - @
2. A valid passphrase satisfies the following constraints:
    2.1. Minimum length of 8 characters
    2.2. Consists of the following:
        - blank space
        - a-z
        - A-Z
        - 0-9
        - . , @ ! -
3. A valid OTP is defined in NIST SP 800-63b section 5.1.4.1
    3.1. OTP changed upon every successful case
    3.2. OTP expires every 2 minutes
    3.3. OTP satisfies the following constraints:
        - Minimum length of 8 characters
        - a-z
        - A-Z
        - 0-9
4. User is allowed to have a maximum of 3 failed attempts within 24 hours to log in.
    4.1. User's account will be disabled when exceeding the max attempts.
    4.2. 24 hours timer begins after the first failed attempt
    4.3. A successful login resets the 3 failed attempts
    4.4. A locked account can be enabled either by an Account Recovery request performed by the account owner, or by the system admin. Upon a successful Account Recovery, 3 failed attempts to login resets
    4.5. For each failed attempt, account undergoing authentication and the IP address of the device that requests the authentication will be recorded
5. System failure from this feature will not cause system to go offline.

Preconditions:

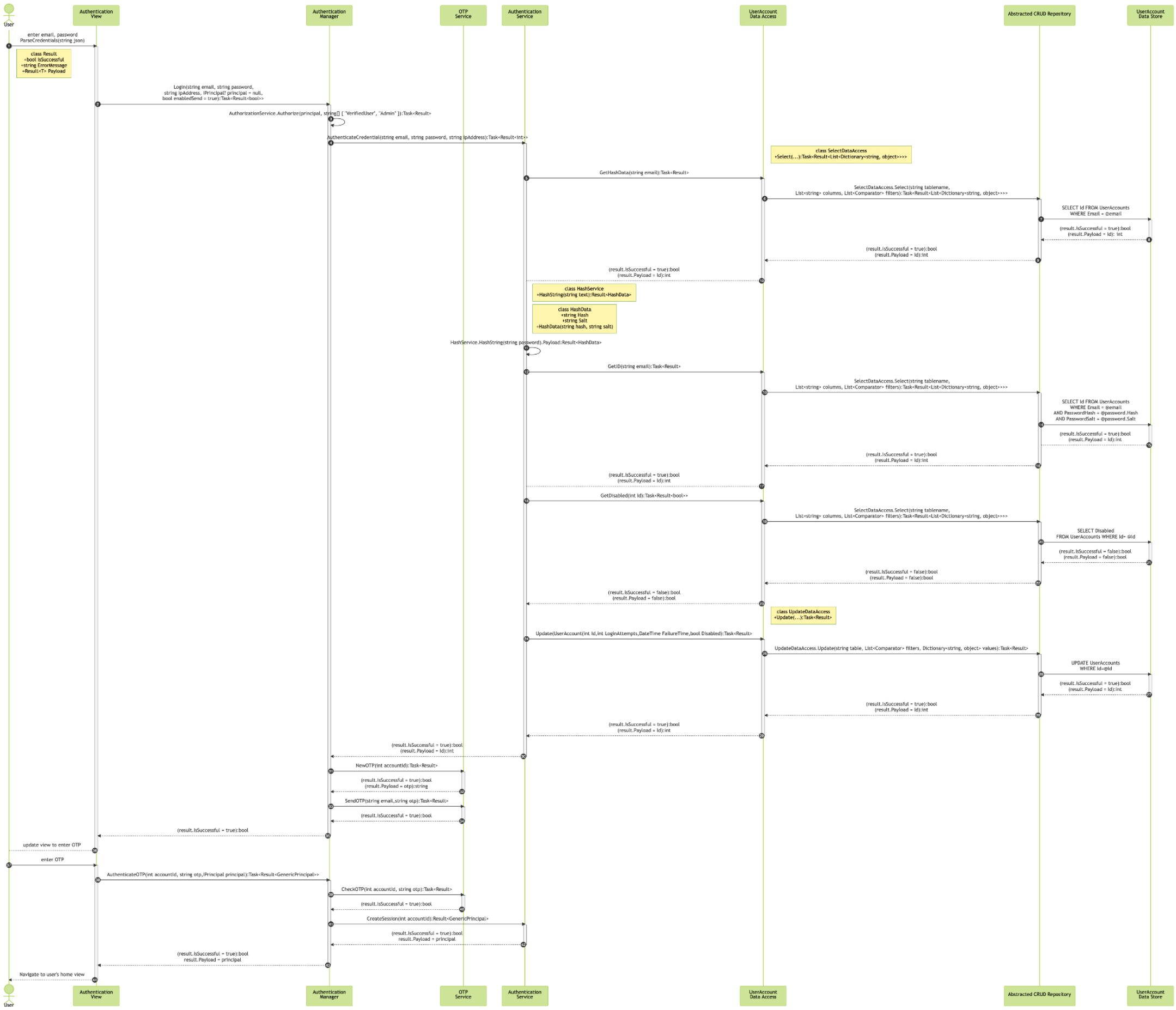
1. User must not be authenticated already on the current device. If a user has signed in already, this authentication process is not possible.
2. User must be on login view or navigated to login view when attempting to access a protected resource (refer to Authorization Requirement)

Relational Tables



Successful Use Cases

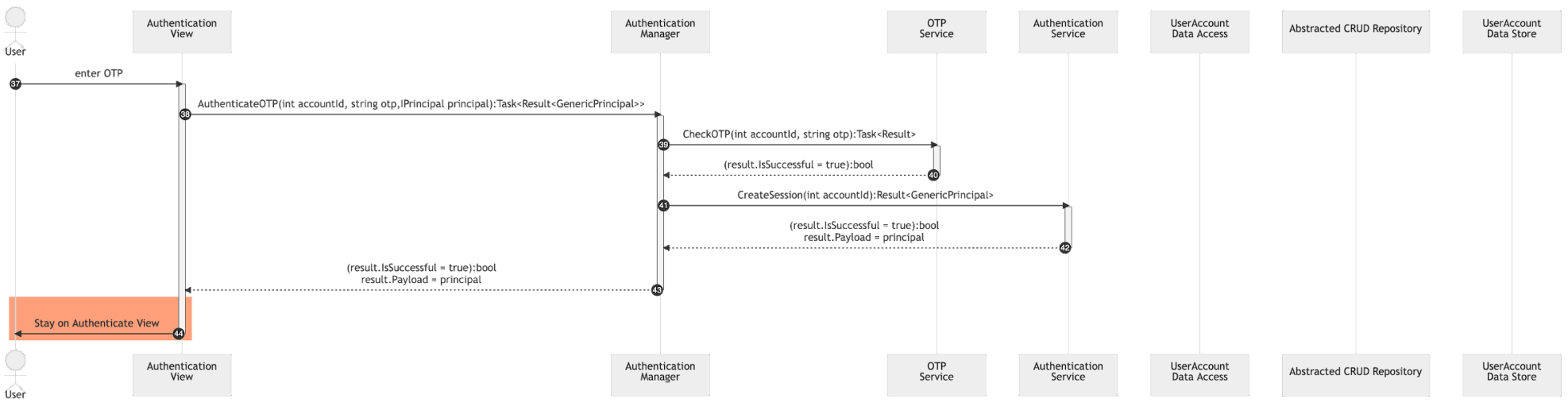
1. User submits valid security credentials. The user is automatically navigated to the user's home view.
   If user is already authenticated, the user should not be able to reach login view.



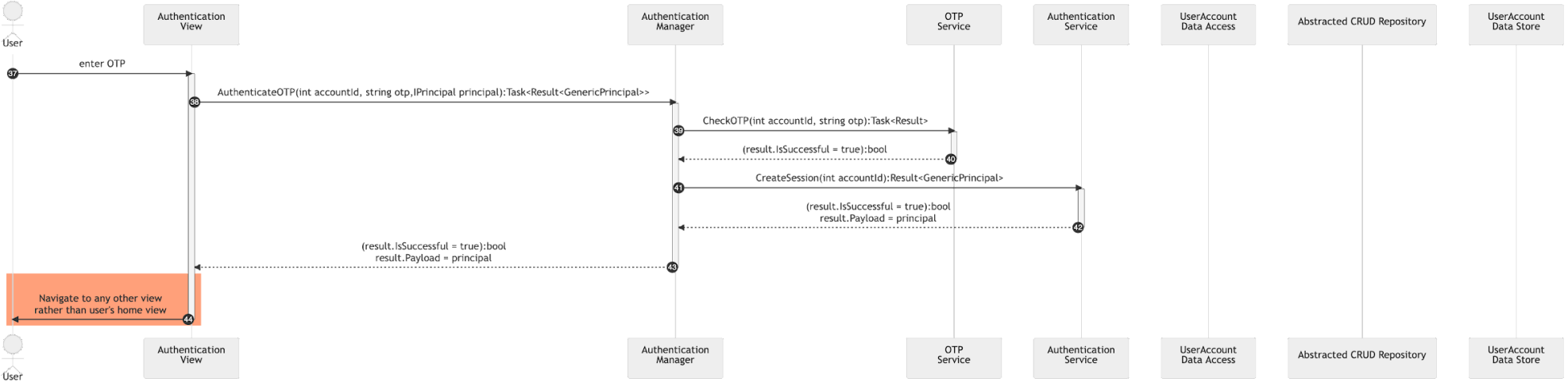
- Steps 31-34 and 39-42, reference OTP Low-Level Design Document

Failure Cases

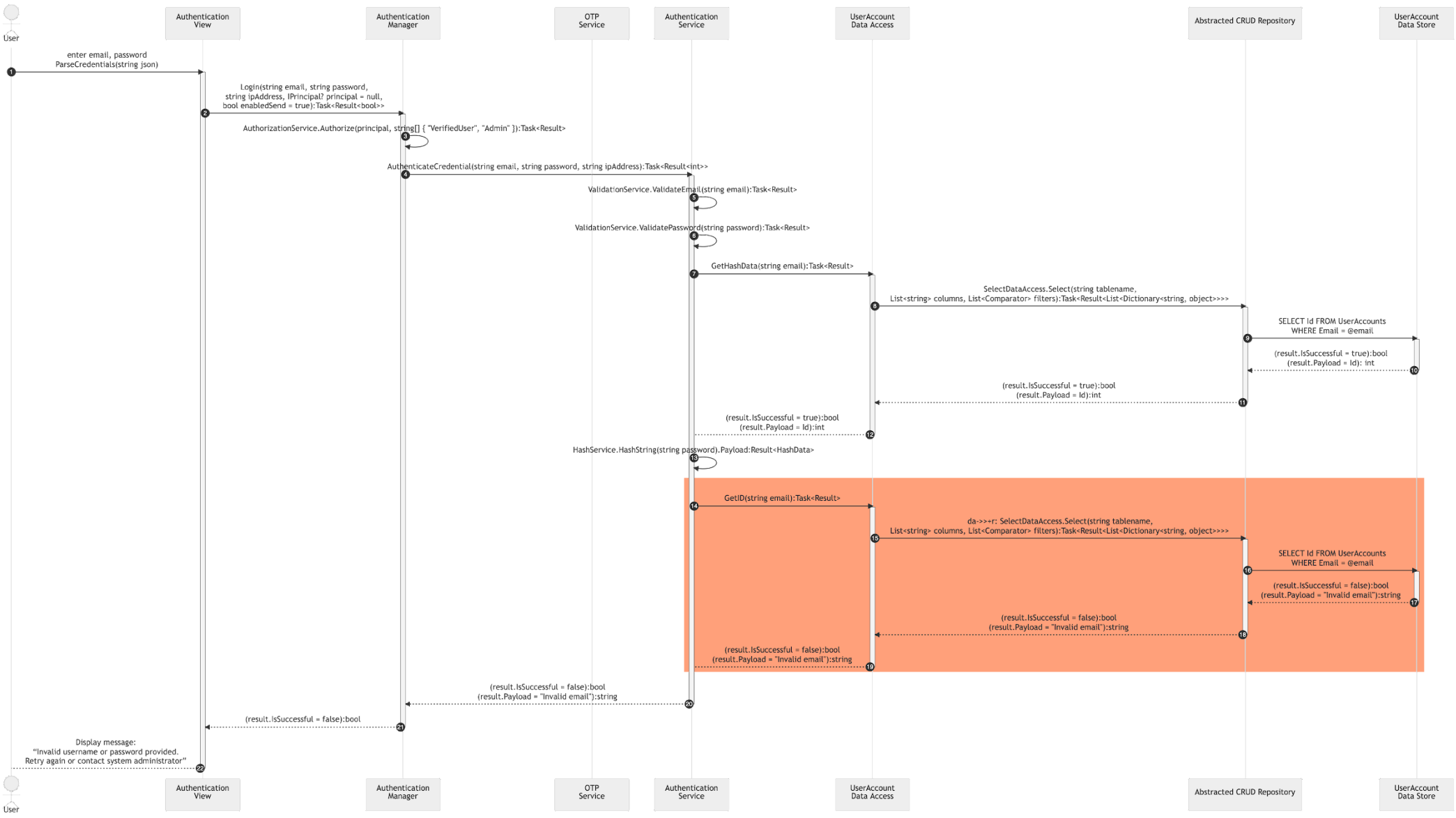
1. User submits valid security credentials. Automatic navigation does not take place.
    - Step 1-39: reference Successful Case sequence diagram (page 8, 9)



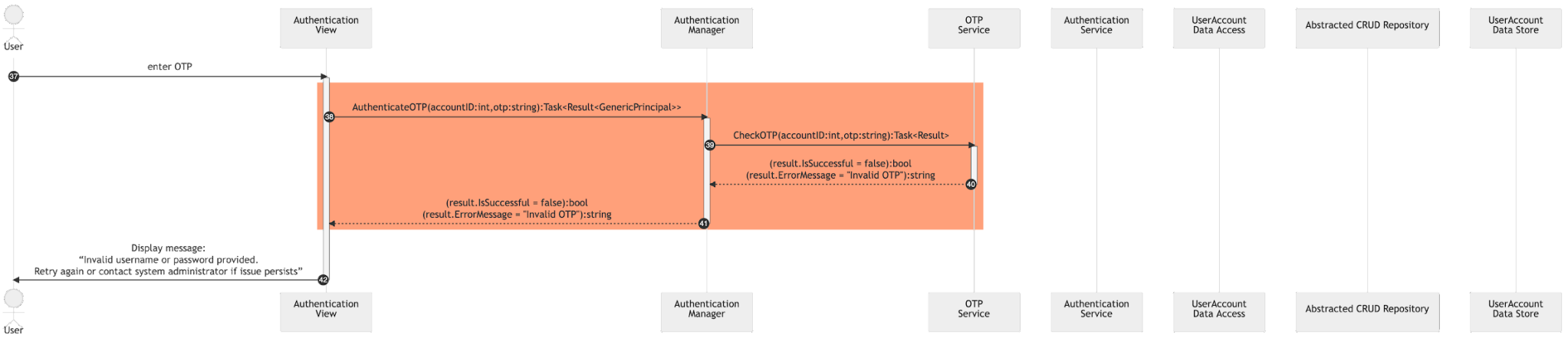
2. User submits valid security credentials. The user is automatically navigated to a view other than the user's home view.
    - Step 1-39: reference Successful Case sequence diagram (page 8, 9)



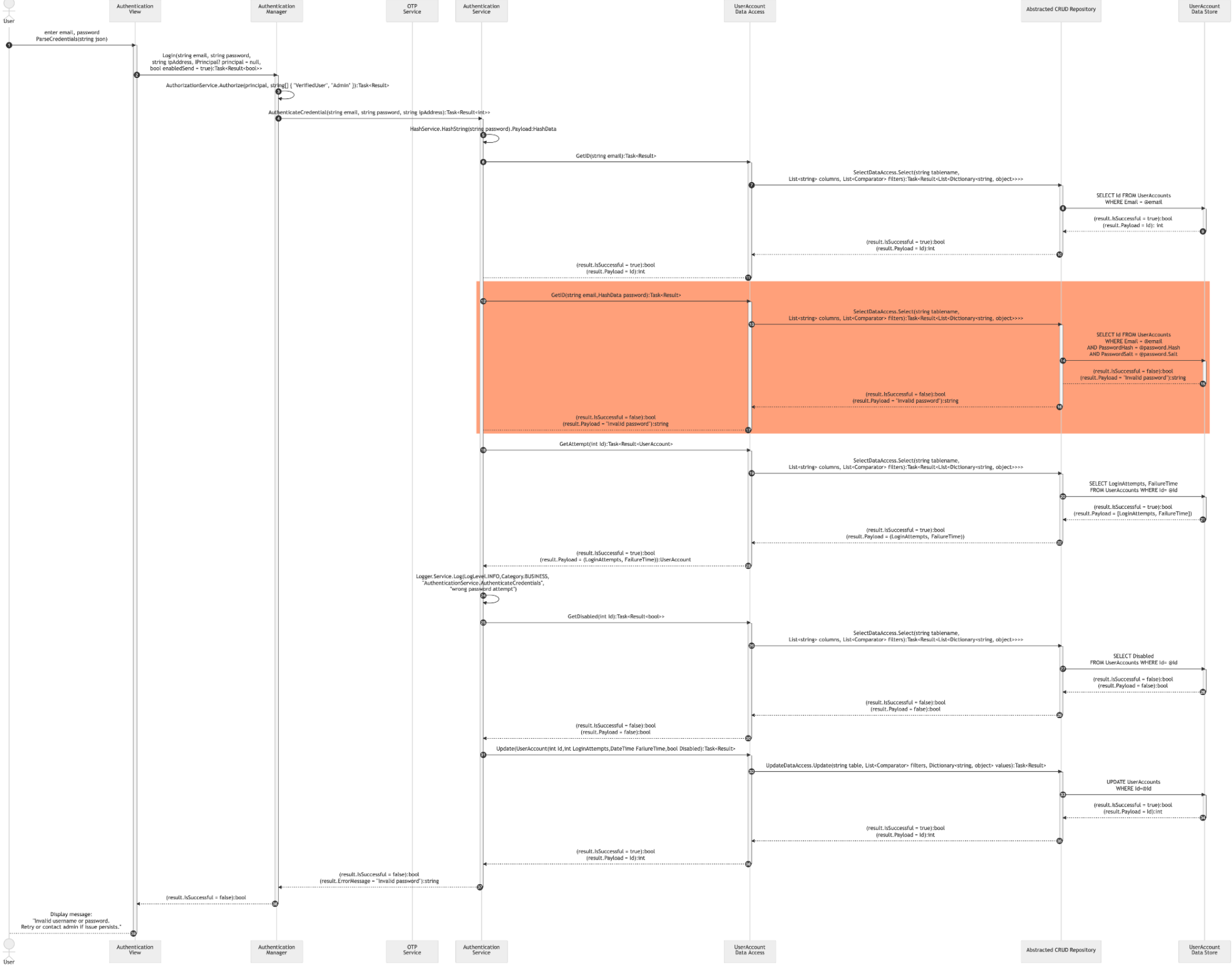
3. User submits invalid username. A system message displays "Invalid username or password provided. Retry again or contact system administrator".



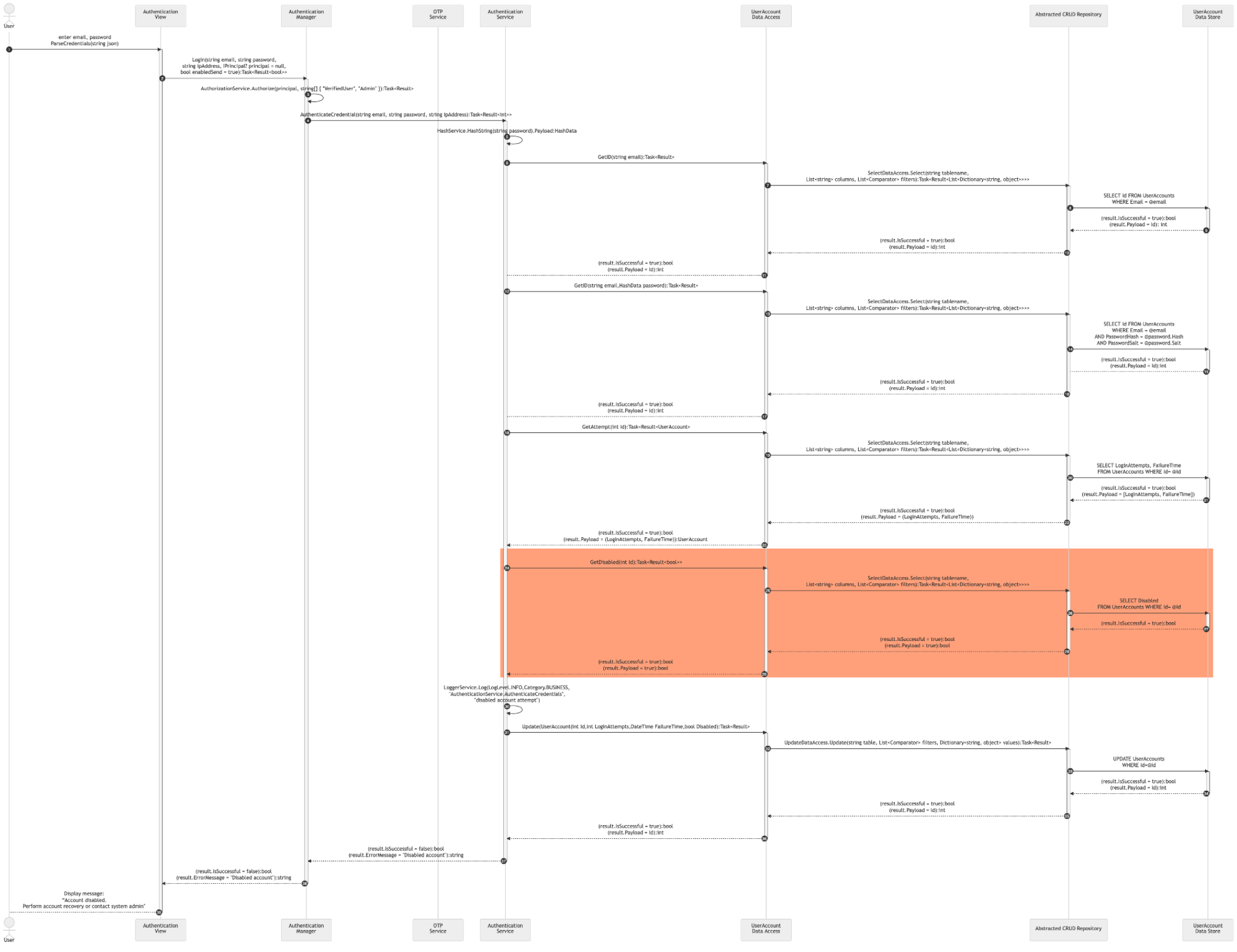
4. User submits invalid OTP. A system message displays “Invalid username or password provided. Retry again or contact system administrator if issue persists”.
    - Step 1-39: reference Successful Case sequence diagram (page 8, 9)



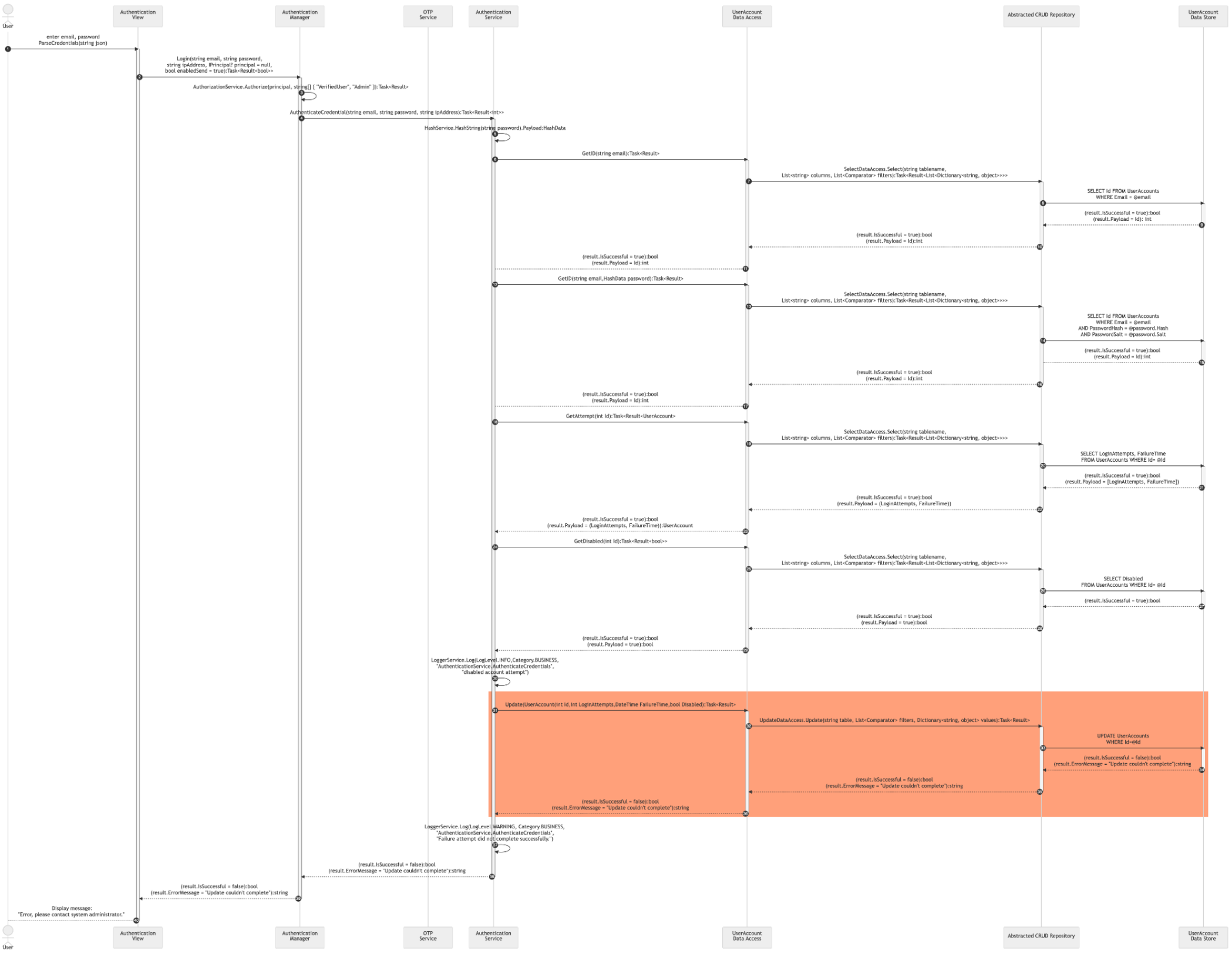
5. User submits invalid security credentials. A system message displays “Invalid username or password provided. Retry again or contact system admin”.
    - Step 27-28: reference Low-Level Design - Logging Document



6. User submits valid security credentials for a disabled account. A system message displays “Account disabled. Perform account recovery or contact system admin”. The failure attempt is recorded accurately.



7. User submits valid security credentials for a disabled account. A system message displays “Account disabled. Perform account recovery or contact system admin”. The failure attempt is not recorded accurately. The system attempts to log that the failure attempt did not complete successfully.



References

This document elaborates client’s requirements[1] for one of the product’s core components - AUTHENTICATION.
The requirement is designed based on the system architecture provided in High-Level Design Document[2].
The diagrams included in this document utilized diagrams.net[3] and Mermaid.js[4].

[1] Client’s email, 10/17/2020
[2] High-Level Design Document, URL: https://github.com/DevelopmentHellaHell/SeniorProject/blob/b43182c4076d471ef03520052675f1f88371dafd/docs/HL%20Design/DevelopmentHell%20HLD%20v1.2.pdf
[3] https://www.diagrams.net/
[4] https://mermaid-js.github.io/mermaid/#/