

DESIGN DOCUMENT

Hubba - OTP Authentication

Version 1.2

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

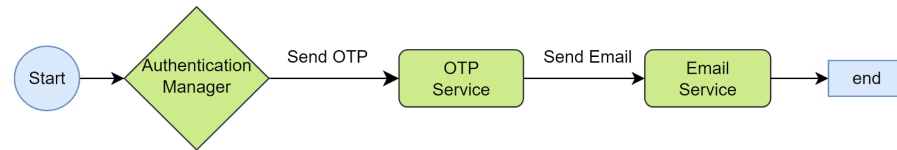
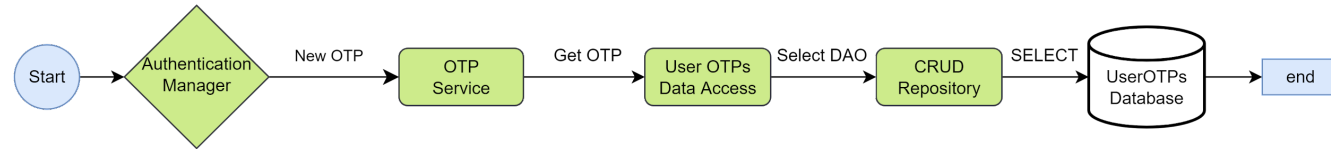
Version	Overview	Date
v1.0	Initial LLD	11/22/2022
v1.1	Small low-level adjustments	12/10/2022
v1.2	Integrated SendGrid	12/14/2022

Table of Contents

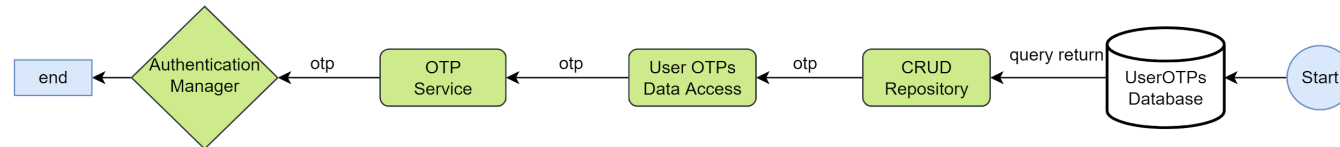
Table of Contents	3
High-Level Design	4
Low-Level Design	5
Relational Tables	5
Successful Case(s)	6
Failure Cases	7
References	9

High-Level Design

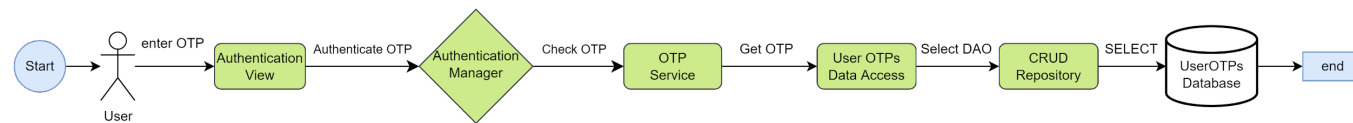
1. Activity flow - Authentication Manager request new OTP and send OTP to user's email:



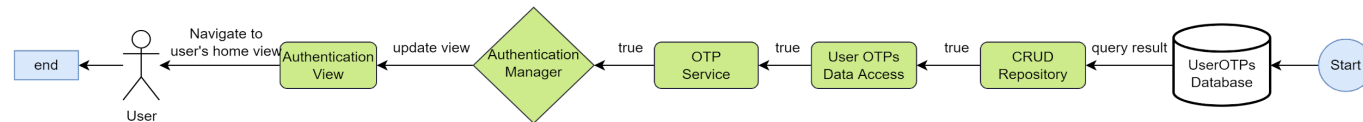
2. System's response:



3. User enter OTP received via email:



4. System's 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.

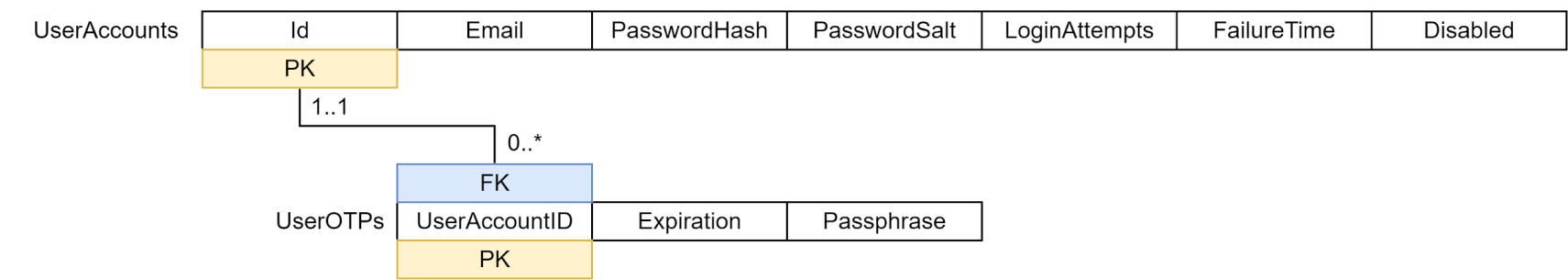
Business rules:

- 1. A valid OTP is defined in NIST SP 800-63b section 5.1.4.1
 - 1.1. OTP changed upon every successful case
 - 1.2. OTP expires every 2 minutes
 - 1.3. OTP satisfies the following constraints:
 - Minimum length of 8 characters
 - a-z
 - A-Z
 - 0-9
- 2. System failure from this feature will not cause system to go offline.

Preconditions:

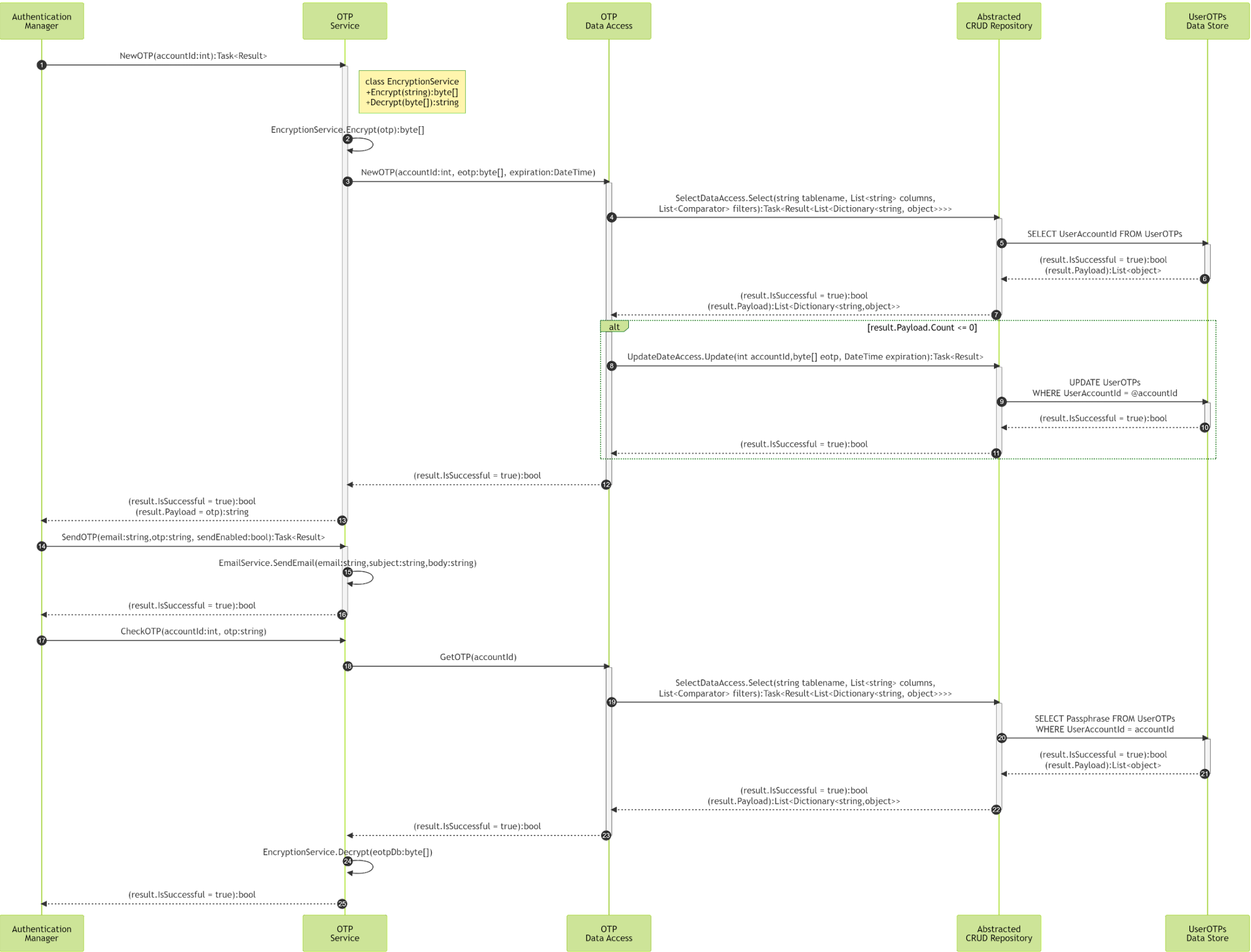
- 1. User must not be authenticated already on the current device. If a user has signed in already, this authentication process is not possible.
- 2. User must be on login view or navigated to login view when attempting to access a protected resource (refer to Authorization Requirement)

Relational Tables



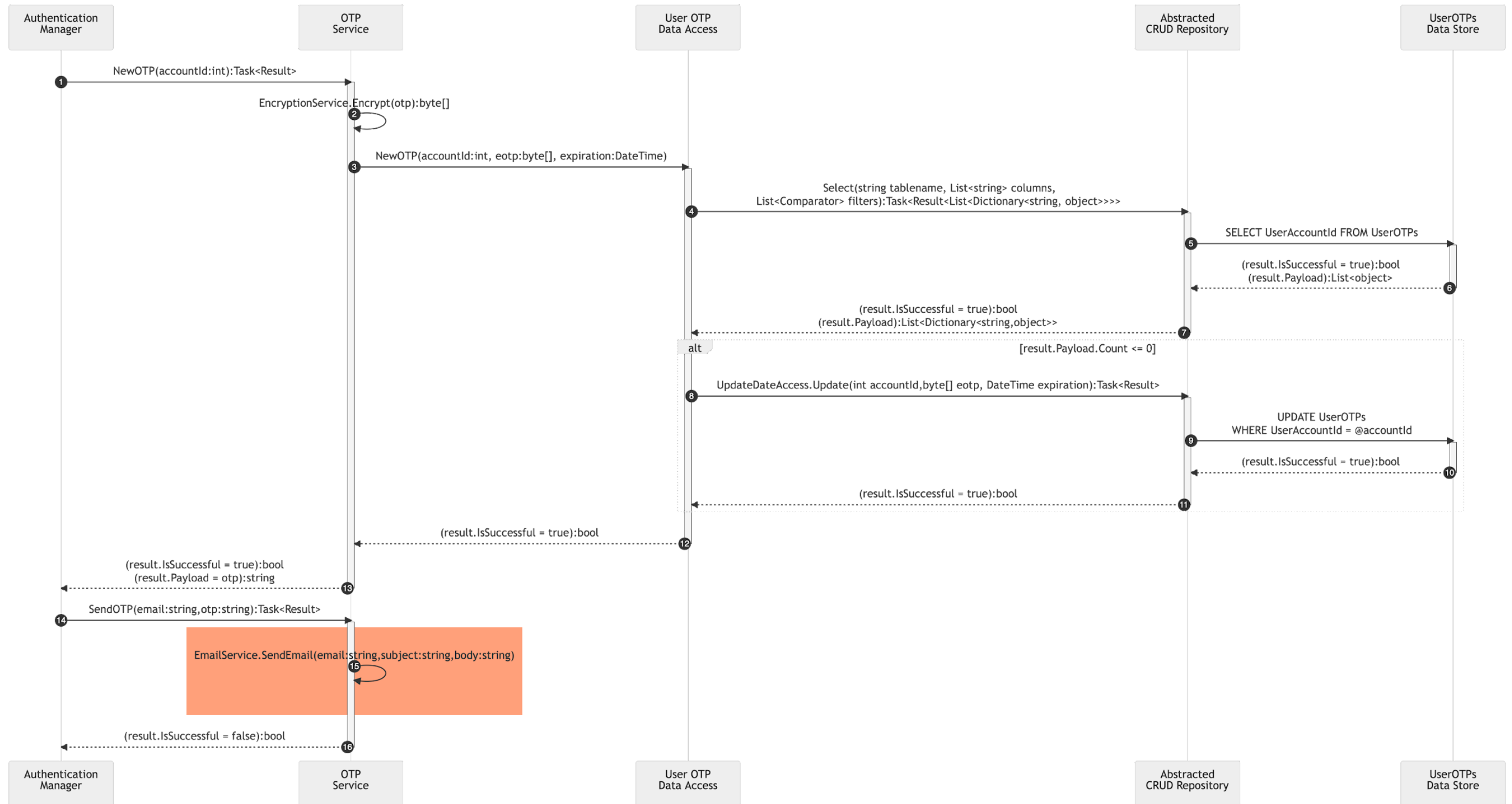
Successful Case(s)

- 1. Authentication Manager performs Login, email and password are valid and authenticated. Authentication Manager requests a new OTP and send it to user's email
- 2. User provides a valid OTP sent by the system. System check if OTP is satisfied then navigates to user's home view.

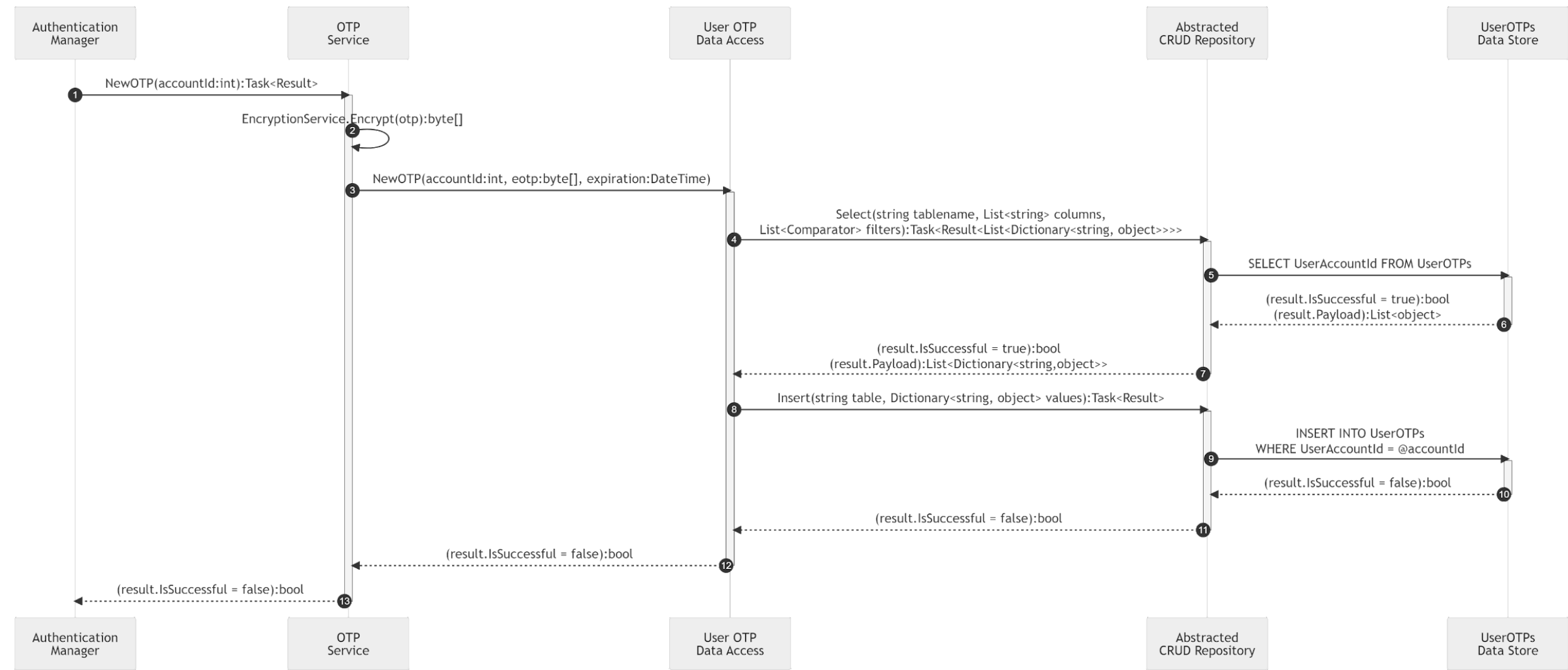


Failure Cases

1. New OTP is provided by the system. Email was not sent successfully. Display message “Error. Retry or contact system admin”.



2. New OTP was not entered into the data store. Email was not sent. Return result was not successful.



References

This document elaborates client's requirements¹ for one of the product's core components - AUTHENTICATION. The requirement is designed based on the system architecture provided in High-Level Design Document². The diagrams included in this document utilized diagrams.net³ and Mermaid.js⁴.

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/#/>