**AUTHENTICATION OF USER ACTIONS**

**5th JULY 2020**

**Version 1.0.0**

| REVISION HISTORY | | | |
| --- | --- | --- | --- |
| DATE | VERSION | DESCRIPTION | AUTHOR |
| 5/7/2020 | 1.0.0 | Documentation Created | Surbhi Kumar |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[AUTHENTICATION OF USER ACTIONS 1](#_Toc44871896)

[5th JULY 2020 1](#_Toc44871897)

[Version 1.0.0 1](#_Toc44871898)

[INTRODUCTION 3](#_Toc44871899)

[PURPOSE 3](#_Toc44871900)

[INTENDED AUDIENCE 3](#_Toc44871901)

[PROJECT SCOPE 3](#_Toc44871902)

[DESCRIPTION 3](#_Toc44871903)

[PRODUCT PERSPECTIVE 3](#_Toc44871904)

[FEATURES NEED TO BE BUILT 3](#_Toc44871905)

[ASSUMPTIONS 3](#_Toc44871906)

[DOCUMENTATION 3](#_Toc44871907)

[API DESCRIPTION AND DOCUMENTATION 4](#_Toc44871908)

[OTP generation 4](#_Toc44871909)

[Resend OTP 5](#_Toc44871910)

[Validate OTP 5](#_Toc44871911)

[ADVANTAGES 6](#_Toc44871912)

[DISADVANTAGES 6](#_Toc44871913)

# INTRODUCTION

## PURPOSE

To specify technical documentation for BOODMO interview Round 2 for the feature of User Authentication on a list of actions

## INTENDED AUDIENCE

Boodmo technical/product team

## PROJECT SCOPE

To describe relevant benefits, objectives, goals, disadvantages of the proposed solution.

# DESCRIPTION

## PRODUCT PERSPECTIVE

Considering there is an e-commerce platform that sells books. A user enters the ecommerce platform and performs various operations like addition of products to cart, wish list, creation of user account etc. Now while performing certain actions the user need to be authenticated, i.e. an OTP (one time password) needs to be sent to the user via SMS and the OTP shall stay valid for a period of 2 minutes.

The actions where this type of authentication is needed are:

* When the user tries to login via mobile number
* When the user wants to checkout from the cart via COD(cash on delivery) payment mode
* When the user wants to opt for a free subscription of an e-magazine

## FEATURES NEED TO BE BUILT

A user authentication service needs to be build which will perform the following action:

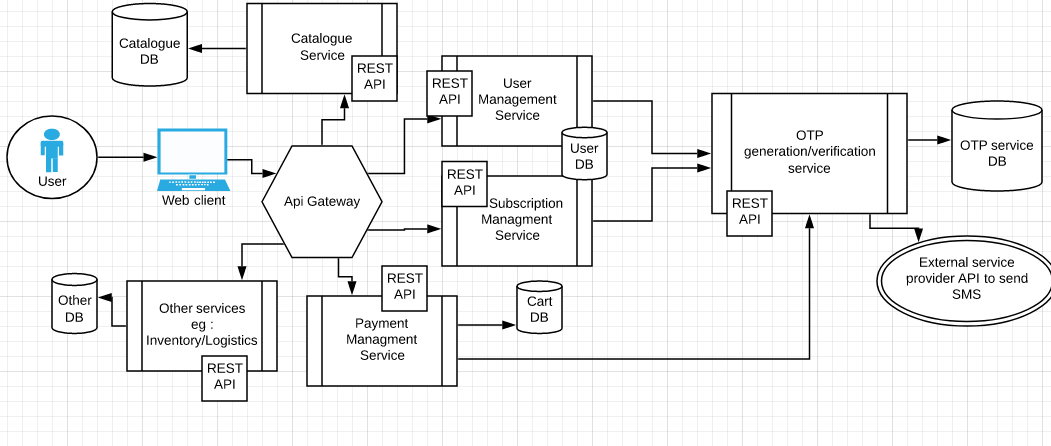
* OTP generation
* OTP verification
* Resending the OTP

## ASSUMPTIONS

The e-commerce platform is already having several other micro services to perform other operations like : inventory management, logistics, user management etc.

## DOCUMENTATION

A microservice called OTP\_generation\_verification needs to be created to manage OTP related operations that will interact with other services via REST APIs and it shall maintain its own DB. This microservice shall also call the external SMS service provider API to send SMS.



## API DESCRIPTION AND DOCUMENTATION

For actual request / response /Api end points, please visit the apiDocs.html page in the repository or visit

<https://app.swaggerhub.com/apis/OtpApiDoc_Surbhi/requestOTP/1.0.0>

### OTP generation

|  |  |
| --- | --- |
| **DESCRIPTION** | An OTP generation rest API shall be created, which generates a random 4 digit number and send the OTP as an SMS to the user |
| **RESPONSE** | The API Shall return a response with the response code, success message/ failure message and an api status which is a Boolean value |
| **FUNCTIONAL REQUIREMENTS** | The API is required to perform the following actions :   1. Generate a 4 digit random number, along with the valid from and valid to fields in the DB, valid\_to shall be calculated as valid\_from+2 minutes 2. Save the API requestor information 3. Call an external service provider API to send SMS and store its response also |

### Resend OTP

|  |  |
| --- | --- |
| **DESCRIPTION AND PRIORITY** | An OTP resend rest API shall be created, which checks whether the user has requested to resend the OTP in a valid time frame, if yes, then resend OTP SMS, else regenerate a 4 digit random OTP and send the SMS to the user |
| **STIMULUS / RESPONSE SEQUENCES** | The API Shall return a response with the response code, success message/ failure message and an api status which is a Boolean value |
| **FUNCTIONAL REQUIREMENTS** | The API is required to perform the following actions :   * Check if the requestor has requested for the API in the valid time frame , if yes ,just resend SMS, , else regenerate a 4 digit random OTP and send the SMS to the user * Save the API requestor information * Call an external service provider API to send SMS and store its response also |

### Validate OTP

|  |  |
| --- | --- |
| **DESCRIPTION AND PRIORITY** | The API shall verify the OTP based on the phone\_number and otp received and will also check if the OTP has not expired |
| **STIMULUS / RESPONSE SEQUENCES** | The API Shall return a response with the response code, success message/ failure message and an api status which is a Boolean value |
| **FUNCTIONAL REQUIREMENTS** | The API is required to perform the following actions :   * Verify the OTP against phone number * Verify Time frame(if the current time is in between valid\_from and valid\_to range) |

## ADVANTAGES

1. Easy fault analysis : Since code is small, it is easier to identify bugs and issues
2. Scalability : Can be integrated with any other service if required in future(eg: User registration )
3. Fast Deployments : Smaller code will lead to quicker deployment
4. Easy to maintain and understand
5. Small databases and datasets

## DISADVANTAGES

1. Poor performance as when microservices communicate with each other, it causes network latency
2. More the number of applications, harder it becomes to manage
3. Retry mechanism/fault handling systems need to be built while performing communication between 2 micro services**(NOTE : even in my solution a queuing mechanism can be built to avoid any loss of requests if the system goes down,but since the OTP is valid only for 2 minutes, it does not make sense as the user will not wait idle on the screen for 2 minutes if he/she does not receive an SMS, instead regerate a request which will keep getting queued in case the system is down )**
4. It is harder to maintain transaction safety