Scope Document

Bulk Bill Payment

GrameenPhone

Version 1.6

Comviva Internal

Table of Contents

Table of Contents 3

1 Introduction 5

1.1 Purpose 5

1.2 Scope 5

1.3 Audience 5

2 Bulk BillPayment Portal 6

2.1 Login Flow: 6

2.2 BillPayment Flow: 27

2.3 Password Management Flow: 34

2.4 Existing Flow Diagrams: 55

3 Technical Solution Requirement 58

3.1 Solution Overview 58

3.1.1 Tech stack to be used to deploy and run existing code 58

3.2 Deployment Specifications of existing module 58

3.2.1 DB Readiness 59

3.2.2 Application readiness 59

3.3 Project Specific Scope 59

3.3.1 Current Implemenation 59

3.3.2 Graphical User Interface 60

3.3.3 Training 60

3.3.4 Documentation 60

3.3.5 Postman Collection 60

3.4 Testing and Acceptance 61

3.4.1 System Integration Testing 61

3.4.2 User Acceptance Procedure 61

3.5 Risks, Impact and Mitigation 61

3.6 Responsibility Matrix 61

3.7 Out of Scope 61
3.8 Code management 61
3.9 Project handover 62
3.10 Project Timelines 62
3.11 Support and maintenance 62
4 Document Change History 63

1 Introduction

This document describes scope of work for Bulk BillPayment UI requirement for GrameenPhone

1.1 Purpose

It is the scope of work document for the changes needed in current Bulk BillPayment module of Grameenphone to integrate with upgraded mobiquity PayX Solution. This will give flexibility to admin users to fetch bill details of account holders in bulk and then pay all pending bills in bulk.

1.2 Scope

Grameenphone has already shared their code of existing Bulk BillPayment UI from old version and want same to be implemented in PayX solution provided by comviva in Phase B.

On existing feature, below are changes that need to be done:

- While fetching pending bill details of all bill account selected on UI : Change in existing integration logic and update to Mobiquity Integration API
- For Bill payment : Change in existing integration logic and update to Mobiquity Integration API
- Ambiguous payment handling scenarios(for enquiry and not reversal or refund) request will be routed to Mobiquity , for any dispute management
- Email and SMS handling should be there as per current setup : integration with Email server and SMSGW
- Login page to be created on WEB to enable user login with credentials. In old system, login page was from IDP. But in latest deployment Login feature should be created in Bulk UI itself.
- Password management (change and forgot password) feature has to be implemented on Bulk UI : Integration with Mobiquity for backend logic

Note : There are 2 UI for Bulk Bill Payment and Reporting. Current scope is just to give feature of Bulk Billpayment UI . Reporting UI requirements will be fulfilled from Pentaho which is part of Mobiquity solution.

1.3 Audience

Comviva technical teams, partner teams

-

2 Bulk BillPayment Portal

Admin user would be able to access Bulk BillPayment portal. Each of them will have their specific userId and password

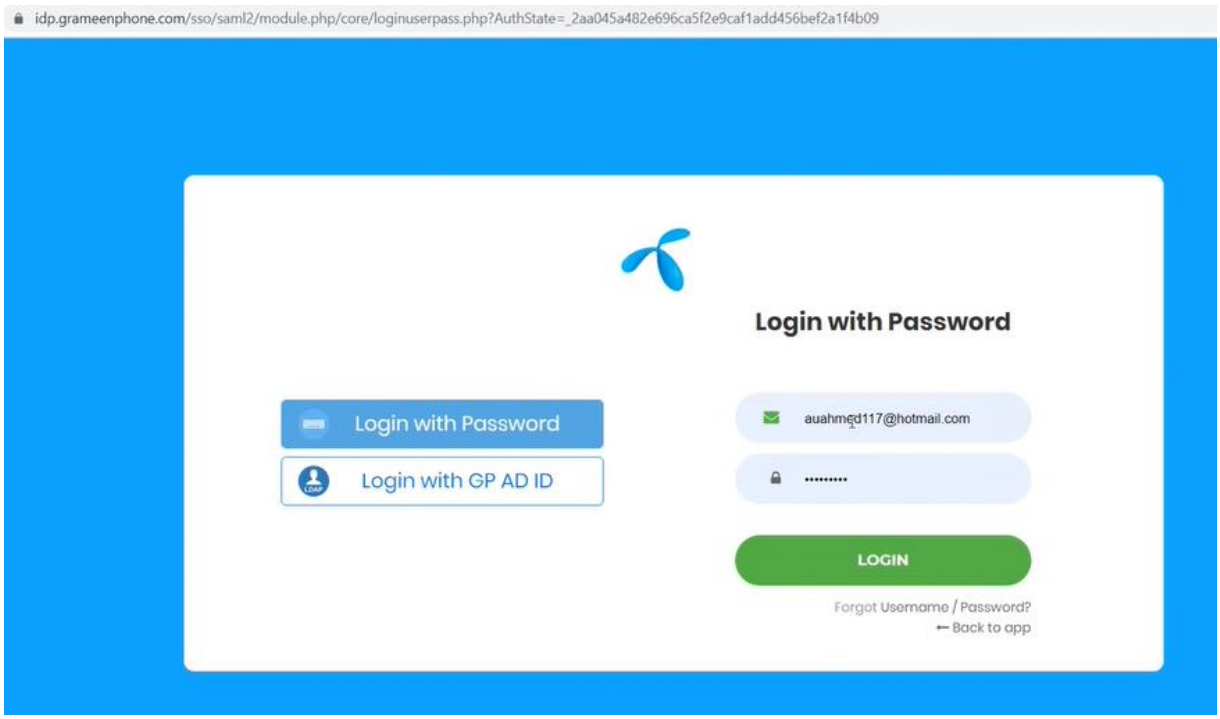
2.1 Login Flow:

Current Flow:

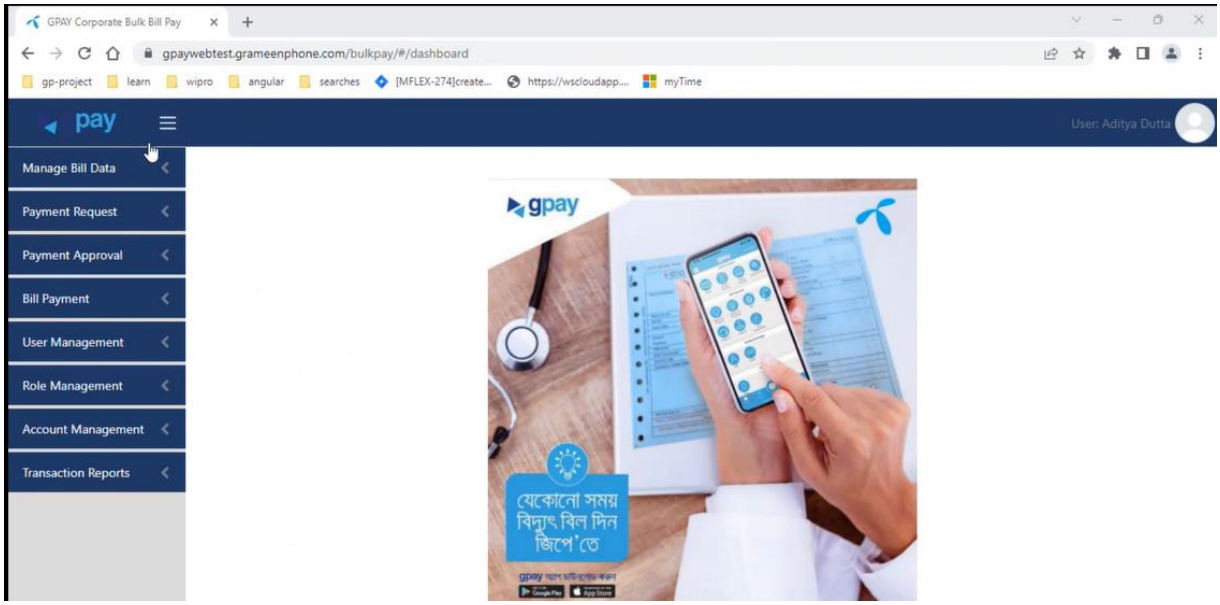
In old architecture, User authentication while Login is maintained by IDP. So whenever user is logging into the system, application routes user to login page of IDP. Where userid and password is asked from user.

IDP validated credentials, on success it calls Billpay Dashboard page and give access to admin user.

Login Page of IDP :



BillPay Dashboard snapshot is below:



New Flow:

Partner need to create this Login page into Bulk UI code itself. And w.r.t. authentication, hit is send to Mobiquity for user validation. Since there is no password storage in Bulk Bill mflex DB. Only userId and email id of users are stored. If user is verified by Mobiquity, then dashboard will be shown.

In order to support this approach, we must ensure that admin users who are present in mobiquity systems can only access bulk billpay dashboard. And they must need mobiquity login id and credentials only to login after registration in Bulk Billpay application. When any mobiquity user want access on Bulk Pay dashboard, then they have to get registered in BulkPay UI also with same login ID.
So login ID of user in mobiquity and BulkUI DB should match.

BulkUI application will send request to generate system token at time of login, once system token is fetched, login request will be sent with system token and login credentials and in return if user is valid in mobiquity system then userToken is sent in response to Login API along with refresh Token.

On receiving successful login, Bulk UI dashboard must be made visible to user.

Expections from Partner:

- Create Login page
- Integrate with mobiquity to fetch system token and Login validation
- Basis mobiquity Login API response, route request to already existing Bulk dashboard in system.

2.1.1 API Details:

2.1.1.1 Fetching System Token

Action: GET
Endpoint: /ums/v1/user/auth/web/system-token
Description
This API is used by the DFS container to generate grant type credentials for the user to login/access mobile or web application. By default, one grant type (system token) is associated with the system. This API helps in creating multiple grant types based on requirement.

Request:
curl --location 'https://mfsbaastest.grameenphone.com/mobiquitypay/oauth/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic Q29yZVdlYjphZGF5ZmNTV2NJ' \
--data-urlencode 'grant_type=client_credentials'

Response Body
Code: 200
Get System Token for Web Application.


```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzY29wZSI6WyJHRVRfVVNFUl9BTkRfQUNDT1VOVF9ERVRBSUxTIiwiU0VMRlNFVEFVVEhGQUNUT1IiLCJGRVRDSF9VU0VSX1FVRVNUSU9OIiwiVFhOQ09SUkVDVCIsIkFUTUNBU0hPVVQiLCJBVE1DQVNIT1VUX1Y0IiwiQURNVFhOUkVGSUQiXSwiZXhwIjoxNjk2OTk4ODM3LCJhdXRob3JpdGllcyI6WyJST0xFX0NMSUVOVCJdLCJqdGkiOiJiYWIxZjY2NC01NjA1LTQ4NDItYTEyYy0zMDE0NWRjNjZlNGYiLCJjbGllbnRfaWQiOiJDb3JlV2ViIn0.EhFA55EfQUDTrUSz1YuPRBE1lJmZjLARClc_PAVOfPtFVcvH_Np_yluShLMrsrH1JU71yAmi3gjIDka3-5bLq-o2JSLk_mc39QlBsXaZGYxR2CMpbxDkWrlNX8E1FF8RWPiW7Mk6xQI0rA6IJvD8y8JrFhvTyROhyuOzm1py3CG0ihM5kR4z_0KnA6ptzYJPVYbLzqVNQ9dFxxsEfQS0JQCZWMRbKEGuEOzbkCrmEGi1F7WTZ0SGm3speYqvRQMv_Cd5xo37q0YnPyp3boGkJq8wlgG3dFAv73fnAHzSm2ZwXM-nO19WKZhQNmqLpj64TZKAVJBplQeLwdCU2d6cAQ",
    "token_type": "bearer",
    "expires_in": 299,
    "scope": "GET_USER_AND_ACCOUNT_DETAILS SELFSETAUTHFACTOR FETCH_USER_QUESTION TXN CORRECT ATMCASHOUT ATMCASHOUT_V4 ADMTXNREFID",
    "jti": "bab1f664-5605-4842-a12c-30145dc66e4f"
}
```


Fields	Type	Description	Example/Allowed Values
LoginWithOTPResponseModel	Login response model with token		
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, ar, fr
lastLoginTime	String	Time stamp of last login of the user.	2020-10-13T02:47:56
message*	String	The API response message that	OTP validation is required.

Fields	Type	Description	Example/Allowed Values
		shows the type of information returned. No Specific length	Please enter OTP to continue
serviceFlow	String	A unique code that is internal to Comviva and identifies the business process flow associated to the API.	OTPLOGIN
serviceRequestId*	String	Whenever an API is called, Comviva generates an unique service request ID for the API request. This unique ID traverses' components in the business process flow. It is useful when the process flow is paused for the user input and needs to be resumed when user has provided the input. Length-36 characters (System generated)	f491f6b1-aa9b-43de-93b0-c85eda706a2c
status*	String	The status to show whether the API call is a success, failure, in progress, or paused.	SUCCEEDED, FAILED, INPROGRESS, or PAUSED
token	String	TokenData	

Fields	Type	Description	Example
`access_token` *	String	Access token is used for token based authentication to allow an application to access an API. The application receives an Access Token after a user successfully authenticates and authorizes access. User can then pass this access token as a credential to perform any transactions in the application.	asdfqwrtwy

Fields	Type	Description	Example/Allowed Values
		Access tokens are short-lived tokens.	
		`expires_in` — Integer ($int32) — Validity period (in seconds) for accessing the token.	299
		`refresh_token` — String — Once the access token expires, you can use the refresh token to get the new access token. Refresh tokens also expire but they are supposed to live much longer than the access token. Max Length-256 characters	asdfqwrtwy
transactionId*	String	The unique id generated by the Comviva platform for the transaction. Length-21 character	XX220316.0959.A15026
txnStatus	String	Defines the five different statuses of the transaction. Not Applicable for Non-Financial APIs TI – Transaction Initiated TS – Transaction Succeeded TF – Transaction Failure TP – Transaction Paused TA – Transaction Ambiguous	Success
userId	String	Unique ID generated by the system after successful user registration. Length-20 characters	US.k6GH1579603850092

Sample Response Body


```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzY29wZSI6WyJHRVRfVVNFUl9BTkRfQUNDT1VOVF9ERVRBSUxTIiwiU0VMRlNFVEFVVEhGQUNUT1IiLCJGRVRDSF9VU0VSX1FVRVNUSU9OIiwiVFhOQ09SUkVDVCIsIkFUTUNBU0hPVVQiLCJBVE1DQVNIT1VUX1Y0IiwiQURNVFhOUkVGSUQiXSwiZXhwIjoxNjk2NTcwODAwLCJhdXRob3JpdGllcyI6WyJST0xFX0NMSUVOVCJdLCJqdGkiOiIyY2ExYzlhYS1kYWE5LTRlNDEtOGI2OS1hNWY4OTdjNmUxMzAiLCJjbGllbnRfaWQiOiJDb3JlV2ViIn0.RXzx1CT19gAma-PuFUzR8zzq2pK-ezjY71sLdN_lx7nEodc8jz58m6QKTfqXHx2k9SUv5uCkZhJxF-OU7ChOkkMCdq3YiZcTxqvNs31LjTyxOMiT_c2s0x9H2WvSCEUUoXFx5c1RUfwuCYblBAsak4NfpAILvZZfaS7sUp4xjuwmz1CvGcL2rUAedxBSJBmHhYHPu4-9lGBEc9FLPXSKJz14fnX5wMBK37JbadIy4C-7C6XwRhYPyHG73RuPgnSG_-RbrlDkRoM9DS9h03V3Q35HesXXRTk7L5x5i9piMCwyM3dQJat8yzAZVAch9SaVZ2URjVF4MNyr49cg6XRbjw",
    "token_type": "bearer",
    "expires_in": 179,
    "scope": "GET_USER_AND_ACCOUNT_DETAILS SELFSETAUTHFACTOR FETCH_USER_QUESTION TXN CORRECT ATMCASHOUT ATMCASHOUT_V4 ADMTXNREFID",
    "jti": "2ca1c9aa-daa9-4e41-8b69-a5f897c6e130"
}
```


Error Codes

Error Code	Description
400	Bad request
500	Internal Server Error

2.1.1.2 Validating User Credential and Generate Token for Web

Action: POST

Endpoint: /ums/v3/user/auth/web/login

Description

This API is used to validate user login credentials based on login policy and generates token to access web application.

Request body

curl --location 'https://mfsbaastest.grameenphone.com/mobiquitypay/ums/v3/user/auth/web/login' \

--header 'Content-Type: application/json' \

--header 'Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzY

29wZSI6WyJHRVRfVVNFUl9BTkRfQUNDT1VOVF9ERVRBSUxTIiwiU0VMRlNFVEF
VVEhGQUNUT1IiLCJGRVRDSF9VU0VSX1FVRVNUSU9OIiwiVFhOQ09SUkVDVCIsIk
FUTUNBU0hPVVQiLCJBVE1DQVNIT1VUX1Y0IiwiQURNVFhOUkVGSUQiXSwiZXhw
IjoxNjk2OTk5MjAzLCJhdXRob3JpdGllcyI6WyJST0xFX0NMSUVOVCJdLCJqdGkiOiJiM
mU1YzY5MC05ODBhLTQyNjUtYmQ0Mi05MzNhNTkxNGQyOGIiLCJjbGllbnRfaWQiOi
JDb3JlV2ViIn0.guCwI3T5L6MEtqVyuBKHjy12KEy01FvdK4JpYxO53GL2a3RUwwLjzM0
89QNNS1pzqrnlqoJZjjosNC54-
Uqzn4QQxhvZe7Lcr41yaysFUkdOlkUgowv7bm0eiclxMgohfE5MZAC7l0sCL2YEc8ArRHL
e6qOY8vcOfr-fXN1qD4Gl4RSo3EAPbNS2gmCwc7crm-
F9vh2ctxqCTW28eBjpUtuY70ByXxR44trS7g7IIeeNg5fzBb7hOrxvKGRIBq5fiVdK35ldXH
VBjBSQdYpyqTADhd38Q1TVxU3M4H3McVrReNK76ODFNQaur_KeHs2kDcN2S6MSqZ
ozGZiTa6X6GQ' \

```
--data-raw '{
    "bearerCode": "WEB",
    "language": "en",
    "workspaceId": "ADMIN",
    "identifierType": "LOGINID",
    "identifierValue": "Aman01",
    "authenticationValue": "Com@1357",
    "isTokenRequired": "Y",
    "deviceInfo": {
        "appName": "mobilePay",
        "appVersion": "V X.9",
        "deviceId": "ffed2d4608c5191f5086b2f2cf160afd",
        "browser": "Google Chrome",
        "isPublicDevice": "N",
        "latitude": "",
        "longitude": "",
        "mac": "",
        "model": "Desktop - Windows 10",
```

```
    "networkOperator": "",
    "networkType": "",
    "os": "",
    "providerIpAddress": "136.226.255.14"
  }
}'
```

Fields	Type	Description	Example/Allowed Values
LoginCriteriaRequest	String	Validate user login credential based on the criteria.	
AuthenticationValue*	String	PIN/Password of the user Default length of pin is 4 Min password length is 5 & Max password length is 10	2468
bearerCode *	String	Access bearer channel of user which includes Web, USSD, Core Web, Mobile App	Web, USSD, Core Web, Mobile App
deviceInfo *	DeviceDetailDTO Description: Representing the device details from where request raised.		

Fields	Type	Description	Example/Allowed Values
appName	String	Application name Length-40 character	mobiquity
appVersion	String	Version of the app that the user accessing. Length-20 character	10.2
browser	String	Browser compatibility of the application. Max Length-50 character	Chrome
deviceId *	String	Unique ID of the device from which the user is	excs-233-daca-312

Fields	Type	Description	Example/Allowed Values
		accessing the app. Max Length-50 character	
	`isPublicDevice` * String	Is the device public, Y/N	Y
	`latitude` String	Latitude geography of the device. Max Length-30 character	12.971599
	`longitude` String	Longitude geography of the device. Max Length-30 character	77.594566
	`mac` String	MAC address of the device. Max Length-30 character	00:1B:44:11:3A:B7
	`model` String	Model number of the device. Max Length-150 character	Oneplus10
	`networkOperator` String	Network operator of the device. Max Length-30 character	Orange
	`networkType` String	Network type of the device which includes 3G, 4G, 5G, etc. Max Length-30 character	4G
	`os` String	Operating system of the device. Max Length-20 character	Android10
	`providerIpAddress` String	IP address of the service provider.	172.56.76.89

Fields	Type	Description	Example/Allowed Values
		Max Length-50 character	
identifierType *	String	Access identifier type of the user/transactor	mobileNumber
identifierValue	String	Access identifier value associated with the identifier type selected. Mobile Number:8-15 Email: Max length-40 characters LOGINID-min length is 3 & max length is 20	777XXXXXX
isTokenRequired *	String	If token is required to access the app, select Y else select N	Y
language *	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, ar, fr
workspaceId *	String	Workspace is the classification of all users at high level. All users are clubbed together under three workspaces SUBSCRIBER/BUSINESS/ADMIN	SUBSCRIBER/BUSINESS/ADMIN

Sample Request

curl --location 'https://mfsbaastest.grameenphone.com/mobiquitypay/ums/v3/user/auth/web/login' \

--header 'Content-Type: application/json' \

--header 'Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzY29wZSI6WyJHRVRfVVNFUl9BTkRfQUNDT1VOVF9ERVRBSUxTIiwiU0VMRlNFVEFVVEhGQUNUT1IiLCJGRVRDSF9VU0VSX1FVRVNUSU9OIiwiVFhOQ09SUkVDVCIsIkFUTUNBU0hPVVQiLCJBVE1DQVNIT1VUX1Y0IiwiQURNVFhOUkVGSUQiXSwiZXhwIjoxNjk2NTcwODAwLCJhdXRob3JpdGllcyI6WyJST0xFX0NMSUVOVCJdLCJqdGkiOiIyY2ExYzlhYS1kYWE5LTRlNDEtOGI2OS1hNWY4OTdjNmUxMzAiLCJjbGllbnRfaWQiOiJDb3JlV2ViIn0.RXzx1CT19gAma-PuFUzR8zzq2pK-ezjY71sLdN_lx7nEodc8jz58m6QKTfqXHx2k9SUv5uCkZhJxF-OU7ChOkkMCdq3YiZcTxqvNs31LjTyxOMiT_c2s0x9H2WvSCEUUoXFx5c1RUfwuCYblBAsak4NfpAILvZZfaS7sUp4xjuwmz1CvGcL2rUAedxBSJBmHhYHPu4-9lGBEc9FLPXSKJz14fnX5wMBK37JbadIy4C-7C6XwRhYPyHG73RuPgnSG_-RbrlDkRoM9DS9h03V3Q35HesXXRTk7L5x5i9piMCwyM3dQJat8yzAZVAch9SaVZ2URjVF4MNyr49cg6XRbjw' \

--data-raw
'{"bearerCode":"WEB","language":"en","workspaceId":"ADMIN","identifierType":"LOGINID","identifierValue":"System01","authenticationValue":"Com@1357","isTokenRequired":"Y","deviceInfo":{"appName":"mobilePay","appVersion":"VX.9","deviceId":"ffed2d4608c5191f5086b2f2cf160afd","browser":"Google Chrome","isPublicDevice":"N","latitude":"","longitude":"","mac":"","model":"Desktop - Windows 10","networkOperator":"","networkType":"","os":"","providerIpAddress":"136.226.255.14"}}
'

Response Body

Code: 200

Validates credentials based on the login policy and generate token if request came from existing mapped device.

Fields	Type	Description	Example/Allowed Values
LoginWithOTPResponseModel	Login response model with token		
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, ar, fr
lastLoginTime	String	Time stamp of last login of the user.	2020-10-13T02:47:56
message *	String	The API response message that shows the type of information returned.	OTP validation is required. Please enter OTP to continue
serviceFlow	String	A unique code that is internal to Comviva and identifies the business process flow associated to the API.	OTPLOGIN
serviceRequestId *	String	Whenever an API is called, Comviva generates a unique service request ID for the API request. This unique ID traverses' components in the business process flow. It is useful when the process flow is paused for the user input and needs to be resumed when user has provided the input.	f491f6b1-aa9b-43de-93b0-c85eda706a2c
status *	String	The status to show whether the API call is a success, failure, in progress, or paused.	SUCCEEDED, FAILED, INPROGRESS, or PAUSED
token	String	TokenData	

Fields	Type	Description	Example/Allowed Values

Fields	Type	Description	Example/Allowed Values
access_token *	String	Access token is used for token based authentication to allow an application to access an API. The application receives an Access Token after a user successfully authenticates and authorizes access. User can then pass this access token as a credential to perform any transactions in the application. Access tokens are short-lived tokens.	asdfqwrtwy
expires_in	Integer ($int32)	Validity period (in seconds) for accessing the token.	299
refresh_token	String	Once the access token expires, you can use the refresh token to get the new access token. Refresh tokens also expire but they are supposed to live much longer than the access token.	asdfqwrtwy

Fields	Type	Description	Example/Allowed Values
		Length-256 characters	
transactionId *	String	The unique id generated by the Comviva platform for the transaction. Length-20 character	XX220316.0959.A15026
txnStatus	String	Defines the five different statuses of the transaction. Not Applicable for Non-Financial APIs TI – Transaction Initiated TS – Transaction Succeeded TF – Transaction Failure TP – Transaction Paused TA – Transaction Ambiguous	Transaction Success
userId	String	Unique ID generated by the system after successful user registration. Length-20 character	US.k6GH1579603850092

Sample Response Body

Below is the response body when two factor authentication is disabled:


```
{
    "serviceRequestId": "eff0d701-df67-4e77-b0ac-d11b6b0d36da",
    "message": "Login Successfully",
    "transactionId": null,
    "txnStatus": null,
    "serviceFlow": "LOGIN_POLICY",
    "status": "SUCCEEDED",
    "language": "en",
    "token": {
        "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHV
ibGljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiZWZmMGQ3MDEtZGY2Ny00ZTc3LWIwYWMtZDExYjZiMGQz
NmRhIiwidXNlcl9uYW1lIjoiZWZmMGQ3MDEtZGY2Ny00ZTc3LWIwYWMtZDExYjZiMGQzNmRhIiwiYXV0aG9y
aXphdGlvblByb2ZpbGVDb2RlIjoiTmV0YWRtaW5EZWZhdWx0IiwiaWRlbnRpZmllclZhbHVlIjoiU3lzdGVt
MDEiLCJpZGVudGlmaWVyVHlwZSI6IkxPR0lOSUQiLCJjYXRlZ29yeUNvZGUiOiJOV0FETSIsInVzZXJJZCI6
IlVTLjI5MjExNjg5MTQ1NTc1NzQyIiwiZGV2aWNlSWQiOm51bGwsImF1dGhvcml0aWVzIjpbIlJPTEVfVVNF
UiJdLCJjbGllbnRfaWQiOiJDb3JlV2ViIiwic2NvcGUiOlsiR0VUX1VTRVJfQU5EX0FDQ09VTlRfREVUQUlM
UyIsIlNFTEZTRVRBVVRIRkFDVE9SIiwiRkVUQ0hfVVNFUl9RVUVTVElPTiIsIlRYTkNPUlJFQ1QiLCJBVE1D
QVNIT1VUIiwiQVRNQ0FTSE9VVF9WNCIsIkFETVRYTlJFRklEIl0sIm5hbWUiOiJTeXN0ZW0gQWRtaW4iLCJi
```

```
ZWFyZXJDb2RlIjoiV0VCIiwiZXhwIjoxNjk2NTcwOTY0LCJqdGkiOiJjNGY5MTk5My1iZmQ3LTRhMmEtYjY0OS0zZjBmNmRlMjYwMWIifQ.yGxiN_4qhQDPAiuyzM-BsSPhuEZM3Tpd71G_cPduiD8dWd11b0sj3vXSKSBidwrup8pGO6t0DCIZQkK6RRtoOJPoiVlNCDcI78JopnohxvzYAuBMXU-zCCx8N5C084oWDAIq8_InxezRmN0KbbNCdUCd8M0vnDToXi6O6A9EYugRmCAcpgrQe__28qIUUyUtB8RJS5QWRftJTA-N_UqYUJr_5xMGowtdFG8qhLyVJNF4xBp2CAqUpTDBGn39Z0ZYU-RVveMrS_IYZD39wufaNChU9Q17jOVIgRtmJ2SzHzjTGjgy2he8NSlpstVoWAhrVGeSmXlY3tp1rBbSOQvlYA",
        "expires_in": 299,
        "refresh_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiZWZmMGQ3MDEtZGY2Ny00ZTc3LWIwYWMtZDExYjZiMGQzNmRhIiwidXNlcl9uYW1lIjoiZWZmMGQ3MDEtZGY2Ny00ZTc3LWIwYWMtZDExYjZiMGQzNmRhIiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiTmV0YWRtaW5EZWZhdWx0IiwiaWRlbnRpZmllclZhbHVlIjoiU3lzdGVtMDEiLCJpZGVudGlmaWVyVHlwZSI6IkxPR0lOSUQiLCJjYXRlZ29yeUNvZGUiOiJOV0FETSIsInVzZXJJZCI6IlVTLjI5MjExNjg5MTQ1NTc1NzQyIiwiZGV2aWNlSWQiOm51bGwsImF1dGhvcml0aWVzIjpbIlJPTEVfVVNFUiJdLCJjbGllbnRfaWQiOiJDb3JlV2ViIiwic2NvcGUiOlsiR0VUX1VTRVJfQU5EX0FDQ09VTlRfREVUQUlMUyIsIlNFTEZTRVRBVVRIRkFDVE9SIiwiRkVUQ0hfVVNFUl9RVUVTVElPTiIsIlRYTkNPUlJFQ1QiLCJBVE1DQVNIT1VUIiwiQVRNQ0FTSE9VVF9WNCIsIkFETVRYTlJFRklEIl0sImF0aSI6ImM0ZjkxOTkzLWJmZDctNGEyYS1iNjQ5LTNmMGY2ZGUyNjAxYiIsIm5hbWUiOiJTeXN0ZW0gQWRtaW4iLCJiZWFyZXJDb2RlIjoiV0VCIiwiZXhwIjoxNjk2NjAwNjY0LCJqdGkiOiI5YzZiNDg4Zi0wOWNiLTRiMTYtOGNhZS0xNzI3ZTNmOGZlNmYifQ.cniKvyqMjBLe5ez-j-K0y9Ytfs1_37pe50AnTmCBS-fM-eSK0wPiV9FjdBUbxYR_0Y4vz6k8B-D7RbIHGWQ81krWX_OqNEwpw3ZRwghTl1Nhj8erf9QHWyU8xp7bIP1Yir6MIaOu_u4flXRNjv82q1sUZjSOJaasfA9qsYtzCY1Qqb0A0GeCqAywnMg7NfUtmQNnTqwL6pMsCemOvoL0JB0dsJ5a-fWbugVU8EImNuEldoXA6BbV8NVyMEwug-ryC1da37LRBzTeajQZzSpt6Ls5Ymi26yc1a3XD_jkXzcA2Qbtb8kSv7rmSrmsySPSbU8f57BcNnZcCHLxSt63w1w"
    },
    "lastLoginTime": "2023-10-04T10:31:28",
    "userId": "US.29211689145575742",
    "sessionIdList": [
        "fd4e5489-3280-4aa7-b1d0-596570277b2f"
    ]
}
```


Below is the response body when two factor authentication is enabled:


```
{
    "serviceRequestId": "d8b7d414-b4d0-4d02-9f42-d1c3edb6459b",
    "message": "OTP validation is required. Please enter OTP to continue",
    "transactionId": null,
    "txnStatus": null,
    "serviceFlow": "LOGIN_POLICY",
    "status": "PAUSED",
    "language": "en",
    "code": "otp.validation.required",
    "mfsTenantId": "mfsPrimaryTenant",
    "transactionTimeStamp": "2023-02-09T10:18:56"
}
```

Error Codes

Error Code	Description
400	Bad request
500	Internal Server Error

Error scenario:

Http error code: 400.
Error Code: Authen01- Invalid credentials.

Response:


```
{"txnStatus":"TF","status":"FAILED","language":"en","mfsTenantId":"mfsPrimaryTenant","errors":[{"code":"AUTH_06","message":"Invalid login credentials. Please try again.","componentName":"user-authentication"}],"transactionTimeStamp":"2023-07-06T20:30:00","errorCode":"Authen01","traceId":"19422597-1711-4bc6-bcab-baf6734549a8","step":"get.userid.service","errorUserMsg":"Invalid credentials.","httpErrorCode":"400"}
```


2.1.1.3 Confirm OTP and Generate Token

Action: POST
Endpoint : /ums/v3/user/auth/login-confirm
Description
This API is used to confirm OTP and mapped device information and then generate token. This is used when the user login authentication requires OTP to access Web Application.

Request body
curl --location
'https://mfsbaastest.grameenphone.com/mobiquitypay/ums/v3/user/auth/web/login-confirm' \
--header 'Accept: application/json, text/plain, */*' \
--header 'Accept-Language: en-US,en;q=0.9,hi;q=0.8' \
--header 'Connection: keep-alive' \
--header 'Content-Type: application/json;charset=UTF-8' \
--header 'Cookie: unq=c4dPpSLPIgO9yPZM;
refresh_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiNjQzNjZmYWUtZTFlYy00YmU4LTg0YzEtMzVmZmM4ZWU5ZTIxIiwidXNlcl9uYW1lIjoiNjQzNjZmYWUtZTFlYy00YmU4LTg0YzEtMzVmZmM4ZWU5ZTIxIiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiTmV0YWRtaW5EZWZhdWx0IiwiaWRlbnRpZmllclZhbHVlIjoiU3lzdGVtMDEiLCJpZGVudGlmaWVyVHlwZSI6IkxPR0lOSUQiLCJjYXRlZ29yeUNvZGUiOiJOV0FETSIsInVzZXJJZCI6IlVTLjI5MjExNjg5MTQ1NTc1NzQyIiwiZGV2aWNlSWQiOm51bGwsImF1dGhvcml0aWVzIjpbIlJPTEVfVVNFUiJdLCJjbGllbnRfaWQiOiJDb3JlV2ViIiwic2NvcGUiOlsiR0VUX1VTRVJfQU5EX0FDQ09VTlRfREVUQUlMUyIsIlNFTEZTRVRBVVRIRkFDVE9SIiwiRkVUQ0hfVVNFUl9RVUVTVElPTiIsIlRYTkNPUlJFQ1QiLCJBVE1DQVNIT1VUIiwiQVRNQ0FTSE9VVF

9WNCIsIkFETVRYTlJFRklEIl0sImF0aSI6IjVmY2UxYzIwLTc2ZGMtNDYwOS04YzljLTRmNTgxOWIyYjI4NyIsIm5hbWUiOiJTeXN0ZW0gQWRtaW4iLCJiZWFyZXJDb2RlIjoiIiwiZXhwIjoxNjk3MTI0NjYwLCJqdGkiOiJjYTgxM2U4My03YTBlLTQ0MTctODMyZC0zOTFhNTA2OGFjZDUifQ.vHZkp9nDpybGdUnn1wnnv2x0XWcpYpr34ggGY0oC2P9voWEK0Bqh59b4zcvrz2S-ImycNL8RwesvTVsRWrLRs9QIVJcPdqo6b3zVH5AN3zNeOwsfGJsROY7m3VQZ-8prfD_1GAC6cC--B6B1GnmScJ9dxaRDsYfOImXbQtieG-sVGq2SRfWyRemJD2PBH3s4UZCgQDkTMDsImPvnKDkqmatHGwCjYWLJJk9ajG6G-k1CLlSkBXtUyaL29x16SJGBhRR6owoweQ54OY12wXccnUDOGQ0QFCaH32Ocfh6rE5vM_HusBvP2o6ILuu-2ciAyCYGiMgQDkE5sMOLVOERiCw;
TS01e8828b=01f85cdc3cd65aade26503bb357b0fc85a8faa097255d642a34a905953db6030a15d9e297f47e18dea0ea8d6548b527164ba3d8426f964e35115b2f556c7b0230681e273b902423e76e1f61c7374644fb29562bd0756dc0ec47fd9e4860f67109e14ee50b4927689e34f8b6c7a5e93bd9d2f84e091;
TS33367916027=085664378eab20005f6d552a0e3dcb6ab482c61a4463475d56d440134d92d17e2c4ff95db0e1c46708fb9cec231130007c72543bf19e84e4e91c371dad89deff56eeb5d037ea6a02e0b398369e567544b5f10c16fc6c5651a3e6352f28ef26be;
TS01e8828b=01f85cdc3cff0747976a3b309e1e7297735cdc6cc36e3b6f955ff1e6cbeb69ded4b585246362c3f44bded9c9fc0812471342b42029;
TS33367916027=085664378eab2000517ad57c223838ab294f8bf5ed07f3dfe99ad6cbf0244793433db33afaec416b085438d37b1130005ef5407a7073e9db4193aface6a2ece13b06a1342a44bad1429f720d7014b7dc125ab80cf95559e7efa777608bf8fc05' \
--header 'Nonce: d17f187090ede6ab' \
--header 'Origin: https://mfsbaastest.grameenphone.com' \
--header 'Referer: https://mfsbaastest.grameenphone.com/dfscontainer/app.html' \
--header 'Sec-Fetch-Dest: empty' \
--header 'Sec-Fetch-Mode: cors' \
--header 'Sec-Fetch-Site: same-origin' \
--header 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36' \
--header 'sec-ch-ua: "Google Chrome";v="117", "Not;A=Brand";v="8", "Chromium";v="117"' \
--header 'sec-ch-ua-mobile: ?0' \
--header 'sec-ch-ua-platform: "Windows"' \
--data '{"resumeServiceRequestId":"0a24aaa1-3e71-4468-a7a7-e7bc8aef6d31","otp":"560727","serviceCode":"LOGIN_POLICY"}'

<table>
<tr><th>Fields</th><th>Type</th><th>Description</th><th>Example/Allowed Values</th></tr>
<tr><td>loginValidateRequest</td><td colspan="3">API to validate OTP and generate token for device login.
<table>
<tr><th>Fields</th><th>Type</th><th>Description</th><th>Example/Allowed Values</th></tr>
<tr><td>otp *</td><td>String</td><td>OTP received on registered mobile number.

Length-6 digit</td><td>213131</td></tr>
<tr><td>resumeService</td><td>String</td><td>Whenever an API is called,</td><td>9ee59b43-46ac-</td></tr>
</table></td></tr>
</table>

Fields	Type	Description	Example/Allowed Values
	RequestId *	Comviva generates a unique service request ID for the API request. This unique ID traverses' components in the business process flow. It is useful when the process flow is paused for the user input and needs to be resumed when user has provided the input. Length-36 characters	4d75-b1c0-b1b10b187abd

Sample Request Body


```
{"resumeServiceRequestId":"0a24aaa1-3e71-4468-a7a7-e7bc8aef6d31","otp":"560727","serviceCode":"LOGIN_POLICY"}
```


Response Body

Code: 200

Access token generated successfully.

Fields	Type	Description	Example/Allowed Values
LoginWithOTPResponseModel	Login response model with token		
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, ar, fr
lastLoginTime	String	Time stamp of last login of the user.	2020-10-13T02:47:56
message *	String	The API response message that shows the type of information returned.	OTP validation is required. Please enter OTP to continue
serviceFlow	String	A unique code that is internal to Comviva and identifies the business process flow associated to the API.	OTPLOGIN
serviceRequestId *	String	Whenever an API is called, Comviva generates a unique service request ID for the API request. This unique ID traverses' components in the business process flow. It is useful when the process flow is paused for the user input and needs to be resumed when user has provided the input. Length-36 characters	f491f6b1-aa9b-43de-93b0-c85eda706a2c
status *	String	The status to show whether the	SUCCEEDED, FAILED,

Fields	Type	Description	Example/Allowed Values
		API call is a success, failure, in progress, or paused.	INPROGRESS, or PAUSED
token	String	TokenData	

Fields	Type	Description	Example/Allowed Values
access_token *	String	Access token is used for token based authentication to allow an application to access an API. The application receives an Access Token after a user successfully authenticates and authorizes access. User can then pass this access token as a credential to perform any transactions in the application. Access tokens are short-lived tokens.	asdfqwrtwy
expires_in	Integer ($int32)	Validity period (in seconds) for accessing the token.	299
refresh_token	String	Once the access token expires, you can use the refresh token to get the new access token. Refresh tokens also expire but they are supposed to live much	asdfqwrtwy

Fields	Type	Description	Example/Allowed Values
		longer than the access token. Max Length-256 characters	
transactionId *	String	The unique id generated by the Comviva platform for the transaction. Length-20 characters	XX220316.0959.A15026
txnStatus	String	Defines the five different statuses of the transaction. Not Applicable for Non-Financial APIs TI – Transaction Initiated TS – Transaction Succeeded TF – Transaction Failure TP – Transaction Paused TA – Transaction Ambiguous	Transaction Success
userId	String	Unique ID generated by the system after successful user registration. Length-20 characters	US.k6GH1579603850092

Sample Response Body


```
{
    "serviceRequestId": "8dd2d378-21d2-4bf8-a363-f023792e15bb",
    "message": "Login Successfully",
    "transactionId": null,
    "txnStatus": null,
    "serviceFlow": "LOGIN_POLICY",
    "status": "SUCCEEDED",
    "language": "en",
    "token": {
        "access_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.
eyJzZXJ2aWNlUmVxdWVzdElkIjoiOGY5NmRiYzQtZWRkMS00NWNiLWI2YjEtMWUzYTc2ZjQy
ZTBjIiwidXNlcl9uYW1lIjoiOGY5NmRiYzQtZWRkMS00NWNiLWI2YjEtMWUzYTc2ZjQyZTBj
IiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiU3Vic0RlZmF1bHQiLCJpZGVudGlmaWVy
VmFsdWUiOiI3Nzc0Njg0MzU5IiwiaWRlbnRpZmllclR5cGUiOiJNU0lTRE4iLCJjYXRlZ29y
eUNvZGUiOiJTVUJTIiwidXNlcklkIjoiVVMuNTMwMTY3NTM5OTE5ODU5NCIsImRldmljZUlk
IjpudWxsLCJhdXRob3JpdGllcyI6WyJST0xFX1VTRVIiXSwiY2xpZW50X2lkIjoiQ29yZVdl
YiIsInNjb3BlIjpbIkdFVF9VU0VSX0FORF9BQ0NPVU5UX0RFVEFJTFMiLCJTRUxGU0VUQVVU
```

```
SEZBQ1RPUiIsIkZFVENIX1VTRVJfUVVFU1RJT04iLCJUWE5DT1JSRUNUIiwiQVRNQ0FTSE9V
VCIsIkFUTUNBU0hPVVRfVjQiLCJBRE1UWE5SRUZJRCJdLCJuYW1lIjoiU3Vic2NyaWJlciBI
YWdlbmVzIiwiYmVhcmVyQ29kZSI6IldFQiIsImV4cCI6MTY3NTkyMTU2NiwianRpIjoiMzM5
ODRmYTYtNzFhYi00MmVmLTgyZDYtMTY1ZWUwZDRlMmZlIn0.WFcZiMSapOAMdouIKj2bKkmU
dtWST78bY71-
gN8OIpGIFmJXFJMx9AwwhEPtB6vsqJ5RQebVyn26OlMopD_IzRKdSxx4V5hfaFgx1kcIQocv
lvgmGx14aW-
QcUJxcqVoIU3hPddj0iZ1Hz0Tlab8czJ5edOkk0qIDTh8BvutwVKLAOYHl6dpKwxn6_PHSzF
poH9qi9jb6fgEFXBDIKhDbj9CqPUUl7iAvbEBD42wkJQyemqu4-
9eETbsbugX5PVjol2_CYUdbLAJgmGwwlEYlFOQ2GTk6bPdfzG5ImhNRigv9P9kK5aeCdb2rM
3qZcqQ2GI_FvLFlUQS0zDVhNKWnA",
        "expires_in": 2999,
        "refresh_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.
eyJzZXJ2aWNlUmVxdWVzdElkIjoiOGY5NmRiYzQtZWRkMS00NWNiLWI2YjEtMWUzYTc2ZjQy
ZTBjIiwidXNlcl9uYW1lIjoiOGY5NmRiYzQtZWRkMS00NWNiLWI2YjEtMWUzYTc2ZjQyZTBj
IiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiU3Vic0RlZmF1bHQiLCJpZGVudGlmaWVy
VmFsdWUiOiI3Nzc0Njg0MzU5IiwiaWRlbnRpZmllclR5cGUiOiJNU0lTRE4iLCJjYXRlZ29y
eUNvZGUiOiJTVUJTIiwidXNlcklkIjoiVVMuNTMwMTY3NTM5OTE5ODU5NCIsImRldmljZUlk
IjpudWxsLCJhdXRob3JpdGllcyI6WyJST0xFX1VTRVIiXSwiY2xpZW50X2lkIjoiQ29yZVdl
YiIsInNjb3BlIjpbIkdFVF9VU0VSX0FORF9BQ0NPVU5UX0RFVEFJTFMiLCJTRUxGU0VUQVVU
SEZBQ1RPUiIsIkZFVENIX1VTRVJfUVVFU1RJT04iLCJUWE5DT1JSRUNUIiwiQVRNQ0FTSE9V
VCIsIkFUTUNBU0hPVVRfVjQiLCJBRE1UWE5SRUZJRCJdLCJhdGkiOiIzMzk4NGZhNi03MWFi
LTQyZWYtODJkNi0xNjVlZTBkNGUyZmUiLCJuYW1lIjoiU3Vic2NyaWJlciBIYWdlbmVzIiwi
YmVhcmVyQ29kZSI6IldFQiIsImV4cCI6MTY3NTk0ODU2NiwianRpIjoiZmUzNDFlYmItN2Nl
YS00MTBjLWFkZmItZmJmYjA2MmI0NjFlIn0.UrYcUPmNEjr78tegJ6nGt897SVPF1_MRz5as
J-
1Epj62SqV3djq97fgivov5tvcSWxbDFNeT4cXINKHnIuI6rZUuu5G6q2E_fFI3DH4b4PIifv
TJ58BQnvGlDlL6XD14I3y4YQ3n4Cm4WkmMzRFTyDiyvzSC2Yg31qx9bqLW4G7_w80A6vn0SY
ZqFd2jEPt7WQCTspceK952vp9OWg6JFzVMZaZ49YuounMBLgBEBwxQaMrnfGSbI4_0DBwrb2
9buS0I4EG_SMroyrZMjkX-
lqkVISXKZJjPdu3ZvULniY54wxjN2uUUeYr1MKlR7X6qXkE11rO5lBeCaPzCQzuKNg"
    },
    "lastLoginTime": null,
    "userId": "US.5301675399198594",
    "sessionIdList": null
}
```


Error Codes

Error Code	Description
400	Bad request
500	Internal Server Error

Error scenario:

Http error code: 400.

Error Code: Generic06- Invalid input.

Response:


```
{
  "status": "FAILED",
  "errors": [
    {
      "code": "sfm.errors.invalid.resume.service.request.id",
      "message": "resume request id mandatory cannot have null or empty
value",
      "componentName": "SFM"
    }
```

```
  ],
  "errorCode": "Generic06",
  "errorUserMsg": "Invalid input.",
  "httpErrorCode": "400"
}
```

2.2 BillPayment Flow:

Current Flow:

- On UI (named as CBP / web-portal-application) : to fetch bill details of accounts and to pay pending bills in bulk, request is initiated from UI and it is stored in CBP DB for further processing. At this point request is just queued, no fetching or processing has take place.
- Second component scheduler will then pick these request from DB on timely basis and communicates with communicator component which will make hit to backend financial system(mobiquity) for Payment and third party system(Biller platform) for actual processing

New Flow:

Process flow will be similar to existing approach , but only change in integration.

- On UI (named as CBP / web-portal-application) : to fetch bill details of accounts and to pay pending bills in bulk, request is initiated from UI and it is stored in CBP DB for further processing. At this point request is just queued, no fetching or processing has take place.
- Second component scheduler will then pick these request from DB on timely basis and communicates with communicator component which will make hit to backend financial system(mobiquity) to fetch bill details or Payment request instead of Biller Platform.

  Refer section 2.2.1.1 for API to fetch bill details
- In fetch bill details it is simple API hit to mobiquity to fetch bill details instead of biller platform.
- For Payment also, communicator will send payment hit to just mobiquity. Not to biller. Mobiquity will in turn send hit to biller platform for any kind of third party integration. Communicator will not interact with biller platform.

  Refer section 2.2.1.2 for API to pay for Bill
- While sending hit to mobiquity, CBP has to ensure a unique reference ID is created, stored in mflex DB corresponding to each bill request and is sent to mobiquity to manage for any disputes in future.
- Communicator will just wait for Mobiquity response of Payment API. Response handling is mentioned below:
  - If it is Failed, then payment is also marked failed in mflex DB.
  - If success/pending or fulfilment initiated : then it is assumed that request is properly posted in mobiquity and now to check status of payment etc. mobiquity DB/ reports has to be inspected. All mobiquity reports will show corresponding unique ID created by CBP so as to track the transaction in mobiquity.
  - If no response from mobiquity for payment request, then all such transactions will be enquired in mobiquity with unique reference ID created at time of payment.
  - If success/fail response of enquiry then status is cleared in mFlex DB.
  - But if no response of enquiry, for a predefined configurable retries, then those are left uncleared in mflex DB, and all such transactions can be checked in Mobiquity reports.

Note :

Scheduler will pick only those records for enquiry for which they didn't get response back from mobiquity platform. No retry feature will be available in this scenario. If scheduler gets response back for payment API, then also any reference to the payments and third party response should be from mobiquity reports. It should not be checked from Bulk Billpay UI.

Expectations from partner :

- Communicator code need to be updated so it can now integrate with new mobiquity platform with updated API specifications to fetch bill details and for payment. These will be routed to mobiquity instead of direct biller integration.
- Logic of unique ID creation to be sent in mobiquity payment APIs
- Mobiquity response handling and Ambiguous payments settlement logic (enquiry , **not refund**) need to be updated accordingly in BillPay code.
- Email and SMS handling should be there as per current setup : integration with Email server and SMSGW

Note: During payment initiation, PIN of client is entered on UI and is validated. API to be used for this is mentioned in 2.2.1.3

2.2.1 API Details:

2.2.1.1 Fetch Bill Details:

Request

```
curl --location --
request POST 'https://mfsbaastest.grameenphone.com/extensibility/fetchPendingBillsFormAggregator' \
--header 'Content-Type: application/json' \
--data-raw '{
"utility": "DSCO",
"consumer_id": "17021270" ,
"thirdParty" : "aggregator",VA
"params":{
   "MOB_NO":"9810036587"
   }
}'
```

Response

Case1: When multiple bills are pending

```
{
   "message": "OK",
   "code": 200,
   "utility": "DSCO",
   "account_no": "17021270",
   "bill_list": [
      {
         "bill_number": "012331291314",
         "due_date": "2023-08-14",
         "amount": 110.0,
         "service_charge": 0.0,
```

```
    "detail": {
      "accountNo": "31291311",
      "billNo": "012331291314",
      "billMonth": "07",
      "billYear": "2023",
      "totalKwh": "333",
      "amount": "100.0",
      "lpc": "10.0",
      "vat": "10.0",
      "issueDate": "14-07-2023",
      "dueDate": "14-08-2023",
      "paymentStatus": "UNPAID"
    }
  },
  {
    "bill_number": "022331291311",
    "due_date": "2023-03-16",
    "amount": 220.0,
    "service_charge": 0.0,
    "detail": {
      "accountNo": "31291311",
      "billNo": "022331291311",
      "billMonth": "2",
      "billYear": "2023",
      "totalKwh": "262",
      "amount": "200.0",
      "lpc": "20.0",
      "vat": "20.0",
      "issueDate": "15-02-2023",
      "dueDate": "16-03-2023",
      "paymentStatus": "UNPAID"
    }
  },
  {
    "bill_number": "032331291311",
    "due_date": "2023-04-12",
    "amount": 330.0,
    "service_charge": 0.0,
    "detail": {
      "accountNo": "31291311",
      "billNo": "032331291311",
      "billMonth": "3",
      "billYear": "2023",
      "totalKwh": "31",
      "amount": "300.0",
```

```
            "lpc": "30.0",
            "vat": "30.0",
            "issueDate": "14-03-2023",
            "dueDate": "12-04-2023",
            "paymentStatus": "UNPAID"
         }
      }
   ]
}
```


Case2: When single bill is pending


```
{
 "message": "OK",
   "code": 200,
   "utility": "JGDCL",
   "account_no": "1233",
   "bill_list": [
      {
         "bill_number": "3265725864641415",
         "due_date": null,
         "amount": 430.0,
         "service_charge": 0.0,
         "detail": null
      }
   ]

}
```


Case3: When no bills are pending


```
{
   "message": "OK",
   "code": 200,
   "utility": "JGDCL",
   "account_no": "601130401",
   "bill_list": []
}
```


Case4: When mandatory field consumer ID is missing


```
{
   "message": "Consumer Id can not be empty",
   "code": 422
}
```


Case5: Invalid Utility


```
{
```

```
  "message": "This API is not applicable for the specific utility",
  "timestamp": 1695725748098,
  "status": 403
}
```


2.2.1.2 Pay Bill:

Request:


```
curl --location 'https://mfsbaastest.grameenphone.com/jigsaw/v1/order/billpay' \
--header 'Content-Type: application/json' \
--header 'Cookie: TS01e8828b=01f85cdc3c45009be88b8dc2907cb422c9dbc891322e3041a5eaaddab62191ca993f8f9770073e7f762285741e428429f81081c459' \
--data '{
   "bearerCode": "MOBILE",
   "currency": 101,
   "deviceInfo": {
      "appVersion": 10.2,
      "deviceId": 990000862471854,
      "lattitude": 12.971599,
      "logitude": 77.594566,
      "mac": "00:1B:44:11:3A:B7",
      "model": "Oneplus10",
      "networkOperator": "Orange",
      "networkType": "4G",
      "os": "Android10",
      "providerIpAddress": "172.56.76.89"
   },
   "initiator": "sender",
   "language": "en",
   "partnerData": {"billAccountNumber":"12345","billNumber":"12345","surcharge":"surcharge1","vat":"vat1","other1":"other1","other2":"other2","billerName":"TTAS","billerCode":"TTAS"},
   "receiver": {
      "idType": "mobileNumber",
      "idValue": "01788886666",
      "productId": 12
   },
   "remarks": "remarks",
   "sender": {
```

```
      "idType": "mobileNumber",
      "idValue": "01755555555",
      "mpin": 13579,
      "paymentInstruments": [
        {
          "instrumentType": "WALLET",
          "amount": 1,
          "productId": 12
        }
      ],
      "userRole": "Channel"
    },
    "serviceFlowId": "BILLPAYOAP"
}'
```

Response:

Successfully initiated payment:


```
{
    "code": "process.fulfilment",
    "message": "Order is placed successfully",
    "orderId": "169647-825021-446643",
    "orderStatus": "PENDING",
    "serviceRequestId": "96c7bed5-e9bf-4f5e-96a4-3eaed32bddd3",
    "transactionTimeStamp": "2023-10-05T09:57:31"
}
```


Failed Response:


```
{
    "status": "FAILED",
    "language": "en",
    "mfsTenantId": "mfsPrimaryTenant",
    "errors": [
        {
            "code": "AUTH03",
            "message": "Provided Password Authentication is invalid. Remaining attem
pts: 3",
            "componentName": "user-authentication"
        }
    ],
    "transactionTimeStamp": "2023-10-05T09:58:43",
    "errorCode": "Authen01",
    "traceId": "79f0dc48-3ecb-441e-b70c-4adaab4d722c",
    "step": "validate.initiator:E.update.order.initiator.authentication.failed",
    "errorUserMsg": "Invalid credentials.",
    "orderId": "169647-832294-424111",
```

```
    "orderStatus": "FAILED",
    "orderState": "VALIDATION_FAILED",
    "httpErrorCode": "400"
}
```


2.2.1.3 Validate MPIN of client:

Request :


```
curl --location 'https://mfsbaastest.grameenphone.com/mobiquitypay/v1/user/auth/validate_credentials_no_token' \
--header 'Content-Type: application/json' \
--header 'Cookie: TS01e8828b=01f85cdc3c6eb1a33f17df6b5974b2ae4dd530e8f034e58b0567c0ff3ef8be4986bd83a1b350f11f7446259154f3f494ed88757d30' \
--data '{
   "workspace": "BUSINESS",
   "identifierType": "MSISDN",
   "language": "en",
   "authenticationValue": "13579",
   "identifierValue": "01755555555",
   "isTokenRequired": "Y"
}'
```


Response:

Successful:


```
{"status":200,"payload":{"token":{"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiZGUyYWJiODUtNGRlNS00NzE5LTk3NWUtMjdhN2RlZDU4OThhIiwidXNlcl9uYW1lIjoiZGUyYWJiODUtNGRlNS00NzE5LTk3NWUtMjdhN2RlZDU4OThhIiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiV2hvbGVzYWxlckRlZmF1bHQiLCJpZGVudGlmaWVyVmFsdWUiOiIwMTc1NTU1NTU1NSIsImlkZW50aWZpZXJUeXBlIjoiTVNJU0ROIiwiY2F0ZWdvcnlDb2RlIjoiV0hTIiwidXNlcklkIjoiVVMuNzM4NjE2ODk4NTM0MTg0MTUiLCJkZXZpY2VJZCI6bnVsbCwiYXV0aG9yaXRpZXMiOlsiUk9MRV9VU0VSIl0sImNsaWVudF9pZCI6IkNvcmVXZWIiLCJzY29wZSI6WyJHRVRfVVNFUl9BTkRfQUNDT1VOVF9ERVRBSUxTIiwiU0VMRlNFVEFVVEhGQUNUT1IiLCJGRVRDSF9VU0VSX1FVRVNUSU9OIiwiVFhOQ09SUkVDVCIsIkFUTUNBU0hPVVQiLCJBVE1DQVNIT1VUX1Y0IiwiQURNVFhOUkVGSUQiXSwibmFtZSI6Im51bGwiLCJiZWFyZXJDb2RlIjoibnVsbCIsImV4cCI6MTY5ODkxMjM5MCwianRpIjoiYmI0M2RjM2QtYzFkNy00NmNjLTgzNGEtMjA0NWQ2NWI3OGU1In0.k1ejMY2QEB_fYsRR3I6CZYEP81RNosr1xjapyLfMlTZ4B2wZL4D7bPpJSEg4r73T2t0WV41WNoXdChOLZFYPQeVugmiL8zCcHfSSqDb5Z3rrP8ZhYzAZLw2FIlLzn26P3wdrFULhaQasyRbPQi5Z3pacbJ1mdv7yyC7u28mAGMLGxFCDu0uXZoYPyaKnWU5Y7fVOJzfkxDelaIttjw8rkqflbuiXElLo4x42gs0BxfVUkHEKR3TKHCN7Nsxv6_7NHhi1wY136mPObW60y2HjCzYpOMEbqyFAGK_hDjnwRWZ0YZVCr2Yv6IRWwisTDFO32xLAkim-AtjSNHtl7rDKWQ","expires_in":299,"refresh_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiZGUyYWJiODUtNGRlNS00NzE5LTk3NWUtMjdhN2RlZDU4OThhIiwidXNlcl9uYW1lIjoiZGUyYWJiODUtNGRlNS00NzE5LTk3NWUtMjdhN2RlZDU4OThhIiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiV2hvbGVzYWxlckRlZmF1bHQiLCJpZGVudGlmaWVyVmFsdWUiOiIwMTc1NTU1NTU1NSIsImlkZW50aWZpZXJUeXBlIjoiTVNJU0ROIiwiY2F0ZWdvcnlDb2RlIjoiV0hTIiwidXNlcklkIjoiVVMuNzM4NjE2ODk4NTM0MTg0MTUiLCJkZXZpY2VJZCI6bnVsbCwiYXV0aG9yaXRpZXMiOlsiUk9MRV9VU0VSIl0sImNsaWVudF9pZCI6IkNvcmVXZWIiLCJzY29wZSI6WyJHRVRfVVNFUl9BTkRfQUNDT1VOVF9ERVRBSUxTIiwiU0VMRlNFVEFVVEhGQUNUT1IiLCJGRVRDSF9VU0VSX1FVRVNUSU9OIiwiVFhOQ09SUkVDVCIsIkFUTUNBU0hPVVQiLCJBVE1DQVNIT1VUX1Y0IiwiQURNVFhOUkVGSUQiXSwibmFtZSI6Im51bGwiLCJiZWFyZXJDb2RlIjoibnVsbCIsImV4cCI6MTY5ODkxMjM5MCwianRpIjoiYmI0M2RjM2QtYzFkNy00NmNjLTgzNGEtMjA0NWQ2NWI3OGU1In0.k1ejMY2QEB_fYsRR3I6CZYEP81RNosr1xjapyLfMlTZ4B2wZL4D7bPpJSEg4r73T2t0WV41WNoXdChOLZFYPQeVugmiL8zCcHfSSqDb5Z3rrP8ZhYzAZLw2FIlLzn26P3wdrFULhaQasyRbPQi5Z3pacbJ1mdv7yyC7u28mAGMLGxFCDu0uXZoYPyaKnWU5Y7fVOJzfkxDelaIttjw8rkqflbuiXElLo4x42gs0BxfVUkHEKR3TKHCN7Nsxv6_7NHhi1wY136mPObW60y2HjCzYpOMEbqyFAGK_hDjnwRWZ0YZVCr2Yv6IRWwisTDFO32xLAkim-AtjSNHtl7rDKWQ","scope":"READ WRITE","token_type":"bearer"},"responseCode":"SUCCESS"}}
```

QURNVFhOUkVGSUQiXSwiYXRpIjoiYmI0M2RjM2QtYzFkNy00NmNjLTgzNGEtMjA0NWQ2NWI3OGU1IiwibmFtZSI6Im51bGwiLCJiZWFyZXJDb2RlIjoibnVsbCIsImV4cCI6MTY5ODk0MjA5MCwianRpIjoiMTBkNmEyNjgtYThhNi00YmM0LTllMjMtNGVmNjlmOGViY2Y3In0.qdRM7ZJRpExwIFBcL8GSP1u9lyYxQ30G0fgiR7EBy4bHGEbb27CMqTAoHTwsgzI1d_MZBgJ4Wysr0C8mnjCtFOa2RTeW2UXQXsWMJ9FRpXfTz_hLn3Aroeitm3mx5hm3b_B18KeGB21ZoCMpATBQylUa1_TcbiaGJD19hNzvrE2Ygxp1KPdQaCmPNvc0dHH3fYrDFbpALcMz13-fZHa1wj1skPco1UYN2Dq97riMVk5RekjzYfuj4g-BnMlU5C6-bJp1jWjugiDoTtw2kdGT_tG4Yf2K6JD1zXlOHEk2BU0vOPD-D2UZIaDNlmU3JdukKu4aYoUZXSRAD0dOyEHZcw"},"userId":"US.73861689853418415","identifierType":"MSISDN","identifierValue":"01755555555","workspace":"BUSINESS","userIdentifierDTO":{"identifierId":"ID.96281689853418532","identifierValue":"01755555555","identifierType":"MSISDN","workspaceId":"BUSINESS","categoryId":"WHS","authenticationId":"AU.16511689853418533","isDifferentAuthFactor":"Y","userId":"US.7386168985 3418415","status":"Y","createdOn":1689853418516,"createdBy":"US.4111687939118897","modifiedOn":1698195610421,"modifiedBy":"US.29211689145575742","primaryIdentifier":"Y","profileCode":"SP.1319","authorizationProfileCode":"WholesalerDefault"}},"authenticationBlocked":"No","remainingAttempt":-99999}

Fail:

{"status":400,"error":{"code":"AUTH03","message":"Provided PIN Authentication is missing or invalid. Remaining attempts: 3"},"authenticationBlocked":"No","remainingAttempt":3}

2.3 Password Management Flow:

When any user forgets his password then user should have flexibility to get these reset via forget password feature on login page. Also once he login, then user can change his password on his own.

Current Flow:

In current platform, all password management is done at IDP page.

New Flow and Expectations from Partners:

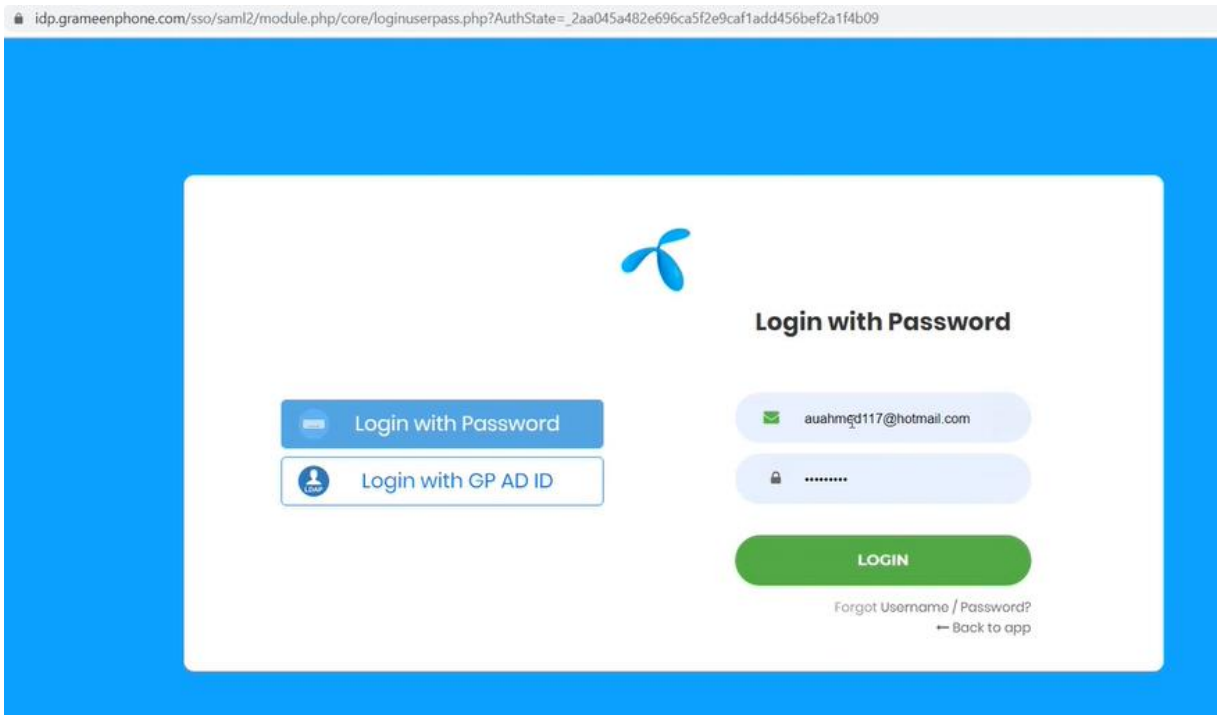
Password management to be incorporated on Bulk UI portal in 2 ways:

1. Give forgot password option on login page.
2. User himself once logged in, can be given with Change password option

All 2 APIs need to have direct integration with Mobiquity for forgot password and change password.

Mobiquity will share APIs to achieve same. Partner can design pages.

Forgot password option may come like below:



Change Own password or reset password pages are new.

2.3.1 API Details:

2.3.1.1 Change Authentication Factor

Action: POST
Endpoint: /ums/v2/user/auth/change-credential
Description
Self-initiated change authentication (Pin/Password). User can change his old password to new password without answering security questions. This API is usually called for changing the default password given by mobiquity system for the first login after successful user registration.
Request body

Fields	Type	Description	Example/Allowed Values
Authorization	String	Authorization Token to pass header	eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1r
changeAuthenticationFactorModel	String	Change Authentication service body. Cannot be empty.	
ChangeAuthenticationFactorModel	String	Change Authentication Request Model	
requestedBy*	String	SELF for self request else unique ID of Requestor from	SELF

Fields	Type	Description	Example/Allowed Values
		Mobiquity System.	
workspaceId*	String	Workspace is the classification of all users at high level. All users are clubbed together under three workspaces SUBSCRIBER/BUSINESS/ADMIN	SUBSCRIBER/BUSINESS/ADMIN
identifierType*	String	Access identifier type of the user like MSISDN/EMAIL/LOGINID/OTHERID to perform reset.	MSISDN/EMAIL/LOGINID/OTHERID
identifierValue*	String	Access identifier value associated with the identifier type selected. Mobile Number:8-15 Email: Max length-40 characters LOGINID-min length is 3 & max length is 20	7766990546
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, Fr, Ar
oldauthenticationValue*	String	Old authentication value (PIN/Password) Of the user. Default length of pin is 4 Min password length is 5 & Max password length is 10 Pin/password also can be configured using security profile	4568
newauthenticationValue*	String	New authentication value (PIN/Password) Of the user. Default length of pin is 4 Min password length is 5 & Max password length is 10 Pin/password also can be configured using security profile	1357
confirmedauthenticationValue*	String	Re-Enter new authentication value to confirm.	1357

Fields	Type	Description	Example/Allowed Values
		Default length of pin is 4 Min password length is 5 & Max password length is 10 Pin/password also can be configured using security profile	

Sample Request Body

```
curl --location
    'https://mfsbaastest.grameenphone.com/jigsaw/ums/v2/user/auth/change-
    credential' \

--header 'Accept: application/json, text/plain, */*' \

--header 'Accept-Language: en-US,en;q=0.9,hi;q=0.8' \

--header 'Connection: keep-alive' \

--header 'Content-Type: application/json;charset=UTF-8' \

--header 'Cookie: unq=c4dPpSLPIgO9yPZM;
    refresh_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcH
    VibGljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiMzM5YWM4ZTgtNGI3MS00NmM4LWIwOTY
    tNzE0MjMzNWZhZTNhIiwidXNlcl9uYW1lIjoiMzM5YWM4ZTgtNGI3MS00NmM4LWIwOTYtNzE
    0MjMzNWZhZTNhIiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiTmV0YWRtaW5EZWZhdWx
    0IiwiaWRlbnRpZmllclZhbHVlIjoiQW1hbjAxIiwiaWRlbnRpZmllclR5cGUiOiJMT0dJTkl
    EIiwiY2F0ZWdvcnlDb2RlIjoiTldBRE0iLCJ1c2VySWQiOiJVUy4zMzU2NTI0OTM0NjM4MzE
    1IiwiZGV2aWNlSWQiOm51bGwsImF1dGhvcml0aWVzIjpbIlJPTEVfVVNFUiJdLCJjbGllbnR
    faWQiOiJDb3JlV2ViIiwic2NvcGUiOlsiR0VUX1VTRVJfQU5EX0FDQ09VTlRfREVUQUlMUyI
    sIlNFTEZTRVRBVVRIRkFDVE9SIiwiRkVUQ0hfVVNFUl9RVUVTVElPTiIsIlRYTkNPUlJFQ1Q
    iLCJBVE1DQVNIT1VUIiwiQVRNQ0FTSE9VVF9WNCIsIkFETVRYTlJFRklEIl0sImF0aSI6IjV
    iN2FlMWU4LWMxZTMtNDRjMS05MmFjLWRjYzY2OTE4MmM4YiIsIm5hbWUiOiJBbWFuIEFtYW4
    iLCJiZWFyZXJDb2RlIjoiIiwiZXhwIjoxNjk3MjIxMDQ3LCJqdGkiOiIzZDRjNWQ2OS02N2N
    iLTQzYzQtYjNhYy01MWI3MTQ1ZTA2MmYifQ.RvvCz02WwzcYyU92deafO3D9kkVvkXs6sNGa
    rN_H4ItQMdxi2UHZrtuM4HgavZj5ybwudhnkx23Ur-
    tkegluYo9600Fbc3on5JVyGvDCRf_n3IEzPzP_Xv1wQxpqYeGgp-xBIqsltej-
    2lQsk565jV5fma9SIKYPKBbdjVRWrfZR64XkrxTfpG66xL3153xTzsQNpKSMJaX-
    oqxL67vpfB9zmkbnf49mEip9codyDOqyAnMF5ziF8oxxiC_HDh6QOF2Hitc6BX_ugdm0236B
    JNcpYO352aPnlgHs5kAmfFehYTnklshIwtjtG1YHwpluczGawEZ254x_i5lT-u61CA;
    TS01e8828b=01f85cdc3c4193144a5196e34f94886729188b50dbcd9ec0d5d08bd867791
    82ec116b1db77c6ddc5d76348eb13924f6240cdba354cd1deeecf9f2ccac165cd22d4e81
    869d850cd9be48aa3275c1409b087a17ff8b5f4cb35d6eddcc53ce38b63df121247f267f
    f06bcfe074a2dd498e13632799080;
    TS33367916027=085664378eab2000fece8b7e6a08c8882c2e810760347737e490a304a7
    d3574cf1c41f4082f0ad3008f1616e6c1130000450cd062c9ac8b5daedca2182a5c7012d
    b2a7e432503b71294fa52c3223d20c6ae44ffa7dcdb4eb65611d3c32bb4b98;
    TS01e8828b=01f85cdc3cb66a0320431ff33def6c6f15239030a5f4308df07469cb2c115
    9d161c56ad0de44cc0bc2af109d59d22822de5da01e3c;
    TS33367916027=085664378eab2000429722169bda1acba71172edfb2be1771ab6943a3e
    a22507d34364023cd87fb408edfa74ce113000fafde979033332c3b37bcf3f686fc1b43e
    2625b196d9b583c860fc23197fabbb2e148ffb5bb827a709eb1b7280e36750' \
```

```
--header 'Nonce: 490ded18fa1b019b' \

--header 'Origin: https://mfsbaastest.grameenphone.com' \

--header 'Referer:
   https://mfsbaastest.grameenphone.com/dfscontainer/app.html' \

--header 'Sec-Fetch-Dest: empty' \

--header 'Sec-Fetch-Mode: cors' \

--header 'Sec-Fetch-Site: same-origin' \

--header 'Signature:
   958a3a3bef29cd787973abd32fbbf4e716a5eebf763d6dead65ed4d1ff6c09b7' \

--header 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36' \

--header 'sec-ch-ua: "Google Chrome";v="117", "Not;A=Brand";v="8",
   "Chromium";v="117"' \

--header 'sec-ch-ua-mobile: ?0' \

--header 'sec-ch-ua-platform: "Windows"' \

--data-raw '{

    "requestedBy": "SELF",

    "oldAuthenticationValue": "Com@8989",

    "newAuthenticationValue": "Com@4545",

    "confirmedAuthenticationValue": "Com@4545",

    "language": "en",

    "workspaceId": "ADMIN",

    "identifierType": "LOGINID",

    "identifierValue": "OTP01"

}'
```

Response Body

{

"serviceRequestId": "79143bb4-9be3-4315-8cd8-33ee63703911",

"message": "Authentication factor is successfully changed",

"serviceFlow": "CHANGEAUTHFACTOR",

"status": "SUCCEEDED",

"userId": "US.462873139693364",

"userName": null,

"workspaceId": "ADMIN",

"identifierType": "LOGINID",

"identifierValue": "OTP01",

"sessionIdList": [

"dcbccb29-4aad-407d-a8b1-4738e53f478b"

]

}

Fields	Type	Description	Example/Allowed Values
AuthenticationResponse	String	User Authentication Response Model	
identifierType*	String	Access identifier type of the user like MSISDN/EMAIL/LOGINID/OTHERID to perform reset.	MSISDN/EMAIL/LOGINID/OTHERID
identifierValue*	String	Access identifier value associated with the identifier type selected. Mobile Number:8-15 characters Email: Max length-40 characters LOGINID-min length is 3 & max length is 20	7766990546
message*	String	The API response message that shows the type of information returned. *No Specific length*	Your password is changed successfully.

Fields	Type	Description	Example/Allowed Values
serviceFlow	String	A unique code that is internal to Comviva and identifies the business process flow associated to the API.	CHANGEAUTHFACTOR/ RESETAUTHFACTOR/ RESETAUTHBYADMIN
serviceRequestId*	String	Whenever an API is called, Comviva generates a unique service request ID for the API request. This unique ID traverses' components in the business process flow. It is useful when the process flow is paused for the user input and needs to be resumed when user has provided the input. *Length-36 charachters*	f491f6b1-aa9b-43de-93b0-c85eda706a2c
status*	String	The status to show whether the API call is a success, failure, in progress, or paused.	SUCCEEDED, FAILED, INPROGRESS, or PAUSED
workspaceId*	String	Workspace is the classification of all users at high level. All users are clubbed together under three workspaces SUBSCRIBER/BUSINESS/ADMIN	SUBSCRIBER/BUSINESS/ADMIN
userId*	String	Unique ID generated by the system after successful user registration. Length-20(System generated)	US.k6GH1579603850092
userName	String	Name of the user.	Not set in response
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, Fr, Ar

Sample Response Body

```
curl --location
'https://mfsbaastest.grameenphone.com/jigsaw/ums/v2/user/auth/change-
credential' \
--header 'Accept: application/json, text/plain, */*' \
--header 'Accept-Language: en-US,en;q=0.9,hi;q=0.8' \
--header 'Connection: keep-alive' \
--header 'Content-Type: application/json;charset=UTF-8' \
--header 'Cookie: unq=c4dPpSLPIgO9yPZM;
refresh_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVib
GljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiMzM5YWM4ZTgtNGI3MS00NmM4LWIwOTYtNzE0M
jMzNWZhZTNhIiwidXNlcl9uYW1lIjoiMzM5YWM4ZTgtNGI3MS00NmM4LWIwOTYtNzE0MjMzNWZh
ZTNhIiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiTmV0YWRtaW5EZWZhdWx0IiwiaWRlbnR
```

```
pZmllclZhbHVlIjoiQW1hbjAxIiwiaWRlbnRpZmllclR5cGUiOiJMT0dJTklEIiwiY2F0ZWdvcn
lDb2RlIjoiTldBRE0iLCJ1c2VySWQiOiJVUy4zMzU2NTI0OTM0NjM4MzE1IiwiZGV2aWNlSWQiO
m51bGwsImF1dGhvcml0aWVzIjpbIlJPTEVfVVNFUiJdLCJjbGllbnRfaWQiOiJDb3JlV2ViIiwi
c2NvcGUiOlsiR0VUX1VTRVJfQU5EX0FDQ09VTlRfREVUQUlMUyIsIlNFTEZTRVRBVVRIRkFDVE9
SIiwiRkVUQ0hfVVNFUl9RVUVTVElPTiIsIlRYTkNPUlJFQ1QiLCJBVE1DQVNIT1VUIiwiQVRNQ0
FTSE9VVF9WNCIsIkFETVRYTlJFRklEIl0sImF0aSI6IjViN2FlMWU4LWMxZTMtNDRjMS05MmFjL
WRjYzY2OTE4MmM4YiIsIm5hbWUiOiJBbWFuIEFtYW4iLCJiZWFyZXJDb2RlIjoiIiwiZXhwIjox
Njk3MjIxMDQ3LCJqdGkiOiIzZDRjNWQ2OS02N2NiLTQzYzQtYjNhYy01MWI3MTQ1ZTA2MmYifQ.
RvvCz02WwzcYyU92deafO3D9kkVvkXs6sNGarN_H4ItQMdxi2UHZrtuM4HgavZj5ybwudhnkx23
Ur-tkegluYo9600Fbc3on5JVyGvDCRf_n3IEzPzP_Xv1wQxpqYeGgp-xBIqsltej-
2lQsk565jV5fma9SIKYPKBbdjVRWrfZR64XkrxTfpG66xL3153xTzsQNpKSMJaX-
oqxL67vpfB9zmkbnf49mEip9codyDOqyAnMF5ziF8oxxiC_HDh6QOF2Hitc6BX_ugdm0236BJNc
pYO352aPnlgHs5kAmfFehYTnklshIwtjtG1YHwpluczGawEZ254x_i5lT-u61CA;
TS01e8828b=01f85cdc3c4193144a5196e34f94886729188b50dbcd9ec0d5d08bd86779182e
c116b1db77c6ddc5d76348eb13924f6240cdba354cd1deeecf9f2ccac165cd22d4e81869d85
0cd9be48aa3275c1409b087a17ff8b5f4cb35d6eddcc53ce38b63df121247f267ff06bcfe07
4a2dd498e13632799080;
TS33367916027=085664378eab2000fece8b7e6a08c8882c2e810760347737e490a304a7d35
74cf1c41f4082f0ad3008f1616e6c1130000450cd062c9ac8b5daedca2182a5c7012db2a7e4
32503b71294fa52c3223d20c6ae44ffa7dcdb4eb65611d3c32bb4b98;
TS01e8828b=01f85cdc3cb66a0320431ff33def6c6f15239030a5f4308df07469cb2c1159d1
61c56ad0de44cc0bc2af109d59d22822de5da01e3c;
TS33367916027=085664378eab2000429722169bda1acba71172edfb2be1771ab6943a3ea22
507d34364023cd87fb408edfa74ce113000fafde979033332c3b37bcf3f686fc1b43e2625b1
96d9b583c860fc23197fabbb2e148ffb5bb827a709eb1b7280e36750' \
--header 'Nonce: 490ded18fa1b019b' \
--header 'Origin: https://mfsbaastest.grameenphone.com' \
--header 'Referer:
https://mfsbaastest.grameenphone.com/dfscontainer/app.html' \
--header 'Sec-Fetch-Dest: empty' \
--header 'Sec-Fetch-Mode: cors' \
--header 'Sec-Fetch-Site: same-origin' \
--header 'Signature:
958a3a3bef29cd787973abd32fbbf4e716a5eebf763d6dead65ed4d1ff6c09b7' \
--header 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36' \
--header 'sec-ch-ua: "Google Chrome";v="117", "Not;A=Brand";v="8",
"Chromium";v="117"' \
--header 'sec-ch-ua-mobile: ?0' \
--header 'sec-ch-ua-platform: "Windows"' \
--data-raw '{
    "requestedBy": "SELF",
    "oldAuthenticationValue": "Com@8989",
    "newAuthenticationValue": "Com@4545",
    "confirmedAuthenticationValue": "Com@4545",
    "language": "en",
    "workspaceId": "ADMIN",
    "identifierType": "LOGINID",
    "identifierValue": "OTP01"
}'
```

Error Codes

Error Code	Description
400	Bad request
500	Internal Server Error

Error scenario:

Http error code: 400

Error Code: Generic04- Mandatory field can't be empty.

Response:


```
o {
  "txnStatus": "TF",
  "status": "FAILED",
  "language": "en",
  "mfsTenantId": "mfsPrimaryTenant",
  "errors": [
    {
      "code": "WORK02",
      "message": "Workspace is mandatory",
      "componentName": "user-authentication"
    }
  ],
  "transactionTimeStamp": "2023-03-30T01:23:13",
  "errorCode": "Generic04",
  "traceId": "352e62e0-7053-497d-8f2d-0ce13d1ac446",
  "step": "get.userid.service",
  "errorUserMsg": "Mandatory field can't be empty",
  "httpErrorCode": "400"
}
```


2.3.1.2 Forget Authentication API

This section will tell you all APIs to be called in sequence to reset login credentials

1. Initiate reset authentication via OTP
2. Validate OTP
3. Confirm new authentication values

2.3.1.2.1 Validate Self-Set Authentication Value with OTP

Action: POST
Endpoint: /v2/ums/user/auth/self-set-auth/initiate
Description
This API is used to initiate change authentication value (Pin/Password) with two factor authentication (OTP).
Request body

Fields	Type	Description	Example/Allowed Values
Authorization	String	Authorization Token to pass header	eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1r
adminResetAuthenticationFactorModel	String	Self-initiated change authentication with otp service body. Cannot be empty.	
SelfSetAuthenticationFactorWithOtpModel	String	Self-Set Authentication with OTP Request Model	

Fields	Type	Description	Example/Allowed Values
bearerCode *	String	Access bearer channel from which the request is raised.	Web, USSD, Core Web, Mobile App
identifierType*	String	Access identifier type of the user like MSISDN/EMAIL/LOGINID/ OTHERID to perform reset.	MSISDN/EMAIL/LOGINID/ OTHERID
identifierValue*	String	Access identifier value associated with the identifier type selected. Mobile Number:8-15 Email: Max length-40 characters LOGINID-min length is 3 & max length is 20	7766990546
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, Fr, Ar
workspaceId*	String	Workspace is the classification of all users at high level. All users are clubbed together under three workspaces SUBSCRIBER/BUSINESS/ADMIN	SUBSCRIBER/BUSINESS/ADMIN

Sample Request Body

```
curl --location
'https://mfsbaastest.grameenphone.com/mobiquitypay/v2/ums/user/auth/self-set-auth/initiate' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzY29wZSI6WyJHRVRfVVNFUl9BTkRfQUNDT1VOVF9ERVRBSUxTIiwiU0VMRlNFVEFVVEhGQUNUT1IiLCJGRVRDSF9VU0VSX1FVRVNUSU9OIiwiVFhOQ09SUkVDVCIsIkFUTUNBU0hPVVQiLCJBVE1DQVNIT1VUX1Y0IiwiQURNVFhOUkVGSUQiXSwiZXhwIjoxNjk3MTkwMzI3LCJhdXRob3JpdGllcyI6WyJST0xFX0NMSUVOVCJdLCJqdGkiOiI4NzMzMmUxMy1iMzBhLTQxNTgtOWYyMi1hMWZhOGZkYWY1ZDQiLCJjbGllbnRfaWQiOiJDb3JlV2ViIn0.D4uTGHwmziIVbZgUPa85BR2wQzcU6DbcAc_oMyjwAUPOVXt4N2ti91EotTI6GpApAtwCXbIjhpPlk8HipPXq1me5Ui6zKu7kZAlkEUqZT8R5iEkVthPKxXKhHvH2XYOU3Iq9ol1o8XGFM5L12Hc_wb5iUfn7Sl4IFro-8Kt4muun0L-ai4o8Eqh7-ZKBAyKVdRQqKD_1M-D7oYIJXlkRBUmjHwwAVJSf5kFybVVlpV8U6ldYrUqt_uyTbVf8PzGkm5GvQq4MNlDaVvyJZ-SmSNBLJQSGGoanYerpCUG73kp_bOYlAHKVO7afHLN67mYu8Ck59S8l-ycv3XIgxLqh4g' \
--header 'Cookie:
TS01e8828b=01f85cdc3c457214bcde5852bf9c955be3074eb2238e8122302b6b9ebb50a15e
```

```
56d81e8a03cd979693acc4df7bb0b5dd63081d0822;
TS33367916027=085664378eab20002075bddbba8e81e1840f3ebc2f3cd2aea7bdbf72cffe2
d381dd6ee61ce92fcf708e57e2907113000fd0d73614c37dfc97541eb8291406460f5dcb46f
08728a412e5d86bb95d6364d63eec9acad2e5ae8b2fd7c35f938da39' \
--data
'{"requestedBy":"SELF","workspaceId":"ADMIN","identifierType":"LOGINID","id
entifierValue":"OTP01","language":"en","bearerCode":"WEB","deviceInfo":{"ap
pName":"MobiquityPayChannel","appVersion":"10.03.0.01","deviceId":"17cf27d2
-871b-42d2-aa4c-2930bed0f5e6","isPublicDevice":"N","model":"Google
sdk_gphone_x86","os":"ANDROID"}} Response'
```

Response Body


```
{
  "serviceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634",
  "mfsTenantId": "mfsPrimaryTenant",
  "language": "en",
  "serviceFlow": "SELFSETAUTHMFA",
  "transactionTimeStamp": "2023-10-13T15:42:03",
  "originalServiceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634",
  "code": "otp.validation.required",
  "message": "OTP validation is required. Please enter OTP to continue",
  "status": "PAUSED"
}
```


Fields	Type	Description	Example/Allowed Values
SelfSetAuthenticationFactorWithOtpResponse	String	Self-Set Authentication with OTP Response model.	
Code	String	Step code where the request is paused for user input.	otp.validation.required OR security.answer.required
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, Fr, Ar
message*	String	The API response message that shows the type of information returned.	OTP validation is required. Please enter “OTP” to continue OR “Answer” for security question is required. Please enter the correct answer to continue.
mfsTenantId	String	MFS Tenant ID of the user	mfsPrimaryTenant
originalServiceRequestId *	String	The Original Service Request ID Length-36 charachters	da371e6e-db02-472b-94c3-2ad2f79dfd09
serviceFlow	String	A unique code that is internal to Comviva and identifies the business	SELFSETAUTHMFA

Fields	Type	Description	Example/Allowed Values
		process flow associated to the API.	
serviceRequestId*	String	Whenever an API is called, Comviva generates a unique service request ID for the API request. This unique ID traverses' components in the business process flow. It is useful when the process flow is paused for the user input and needs to be resumed when user has provided the input. Length-36 charachters	f491f6b1-aa9b-43de-93b0-c85eda706a2c
status*	String	The status to show whether the API call is a success, failure, in progress, or paused.	SUCCEEDED, FAILED, INPROGRESS, or PAUSED
transactionTimeStamp *	String	The date and time of transaction in the format YYYY-MM-DD and HH:MM:SS respectively.	2023-01-31T15:49:45

Sample Response Body


```
{
    "serviceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634",
    "mfsTenantId": "mfsPrimaryTenant",
    "language": "en",
    "serviceFlow": "SELFSETAUTHMFA",
    "transactionTimeStamp": "2023-10-13T15:42:03",
    "originalServiceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634",
    "code": "otp.validation.required",
    "message": "OTP validation is required. Please enter OTP to continue",
    "status": "PAUSED"
}
```


Error Codes

Error Code	Description
400	Bad request
500	Internal Server Error

Error scenario:

Http error code: 400.

Error Code: invalid.value- Unexpected value 'QR_CODE_TYPE_DYNAMIC'.

Response:


```
{"traceId":null,"errorUserMsg":"Bad Request","errors":[{"code":"invalid.value","message":"Unexpected value 'LOGINI'"}],"step":null,"referenceId":null,"status":"FAILED","httpErrorCode":"400"}
```

2.3.1.2.2 Validate OTP for Self-Set Authentication Value

Action: POST
Endpoint: /v2/ums/user/auth/self-set-auth/validate-otp
Description
This API is used to validate the OTP entered for self-initiated change authentication value (Pin/Password).

Sample Request body :

curl --location 'https://mfsbaastest.grameenphone.com/mobiquitypay/v2/ums/user/auth/self-set-auth/validate-otp' \
--header 'Accept: application/json, text/plain, */*' \
--header 'Accept-Language: en-US,en;q=0.9,hi;q=0.8' \
--header 'Connection: keep-alive' \
--header 'Content-Type: application/json;charset=UTF-8' \
--header 'Cookie: unq=c4dPpSLPIgO9yPZM;
refresh_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcHVibGljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiMzM5YWM4ZTgtNGI3MS00NmM4LWIwOTYtNzE0MjMzNWZhZTNhIiwidXNlcl9uYW1lIjoiMzM5YWM4ZTgtNGI3MS00NmM4LWIwOTYtNzE0MjMzNWZhZTNhIiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiTmV0YWRtaW5EZWZhdWx0IiwiaWRlbnRpZmllclZhbHVlIjoiQW1hbjAxIiwiaWRlbnRpZmllclR5cGUiOiJMT0dJTklEIiwiY2F0ZWdvcnlDb2RlIjoiTldBRE0iLCJ1c2VySWQiOiJVUy4zMzU2NTI0OTM0NjM4MzE1IiwiZGV2aWNlSWQiOm51bGwsImF1dGhvcml0aWVzIjpbIlJPTEVfVVNFUiJdLCJjbGllbnRfaWQiOiJDb3JlV2ViIiwic2NvcGUiOlsiR0VUX1VTRVJfQU5EX0FDQ09VTlRfREVUQUlMUyIsIlNFTEZTRVRBVVRIRkFDVE9SIiwiRkVUQ0hfVVNFUl9RVUVTVElPTiIsIlRYTkNPUlJFQ1QiLCJBVE1DQVNIT1VUIiwiQVRNQ0FTSE9VVF9WNCIsIkFETVRYTlJFRklEIl0sImF0aSI6ImQ2NGRjMDU4LWM1MjgtNGYyNy1hMDI2LTMzZGRjZGJjZDZkZCIsIm5hbWUiOiJBbWFuIEFtYW4iLCJiZWFyZXJDb2RlIjoiIiwiZXhwIjoxNjk3MjE3NTg1LCJqdGkiOiJhNzA3MGM3Ni04ZDg2LTQ3MmUtYTYxOS03YWMyMTJjYTViNmYifQ.jPBlVRKmPMl2Z_-trAWWLxajZzDRh2KjCmsX-kwVHKXr3DPOMN17G9VW1PiY2ZaEqR3Y2H6nRxIkFXz6MOoIll30UEqljuOpB6V95l9cNURFq06evqFwIasfs6jIzmxV7by1iNlHNR5m1KMMF42D8L9en8h0lAVf9Hb4VaX_I_GL2GAnbUjyn7SM28njVx3Q9ZF6UDORlrAQVTbdW1uzimGXKLhoYtzE_nupf-w2ksToC0dOKsY5fKB7U9aO-qjXnPBBXJIrmUvM25J9fPmyNCiP0YNGeCktyIbASOAwIbV9HyEu1-VOWnSKA1w06KeUIaS3bebf5maPznh88J1GgQ;
TS01e8828b=01f85cdc3ceaccb0e0dd4d85ebf7b7dddaea5ae0f3944a191229a40ce8bad051d541990c8462523f2db0fe252be3d31f3cdb37758fde55c4845375f9941e6e3d38e3141a71228d43f32497bf609ae9f1c048bf4aeea2e051d3b0030cee573634d855d3616a3a9d7319297d1dd455fff7d420a65643;
TS33367916027=085664378eab20003e46c7461c225006eba2cd3cb988d1c6eea59dd23027e627bc15326ac15e177f081689eb9c113000bbb3fc5fd604827c4e734e6887a45fbc9205a19d46fd6b3959b0dbf2bc96af9228efe46927ad4ed0deddc47a7050ebbc;
TS01e8828b=01f85cdc3cc4c735ef2d04975ee799b43c280a5acda09245bf7e07a400768132bf99bd0fcf0fa6db3629c68a2c243e3fe394e2521d;
TS33367916027=085664378eab200030e7e937866eff56d79adfc2e3953b18afaa55d66c416cf3

```
87b180f4d11ac3a408364762be1130006bae8939e0d4fa429f87dfe7f9c417e75552f134113441
63a739081e1395ef08a0cfe5a4cf6325c271c6efd08467b62f' \
--header 'Nonce: b03c046cdf821a64' \
--header 'Origin: https://mfsbaastest.grameenphone.com' \
--header 'Referer: https://mfsbaastest.grameenphone.com/dfscontainer/app.html' \
--header 'Sec-Fetch-Dest: empty' \
--header 'Sec-Fetch-Mode: cors' \
--header 'Sec-Fetch-Site: same-origin' \
--header 'Signature:
7066ce421a0d842145c11be84e53dd5d3fdc8868c34d65d7dc8d36504fd6dba7' \
--header 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36' \
--header 'sec-ch-ua: "Google Chrome";v="117", "Not;A=Brand";v="8",
"Chromium";v="117"' \
--header 'sec-ch-ua-mobile: ?0' \
--header 'sec-ch-ua-platform: "Windows"' \
--data '{
   "language": "en",
   "otp": "655336",
   "resumeServiceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634"
}'
```

Request body :

Fields	Type	Description	Example/Allowed Values
adminResetAuthenticationFactorModel	String	Validate OTP for self-initiated change authentication with OTP service body. Cannot be empty.	
ValidateOtpSelfSetAuthenticationFactorWithOtpModel	String	Self Set Authentication with OTP Request Model	
language *	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, Fr, Ar
otp *	String	OTP received on registered mobile number. Length-6	213131
resumeServiceRequestId *	String	Whenever an API is called, Comviva generates a unique service request ID for the API request. This unique ID traverses' components in the business process flow. It is useful when the process flow is paused for the user	f491f6b1-aa9b-43de-93b0-c85eda706a2c

Fields	Type	Description	Example/Allowed Values
		input and needs to be resumed when user has provided the input. Length-36 characters (System generated)	

Sample Request Body

```
{
    "language": "en",
    "otp": "655336",
    "resumeServiceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634"
}
```

Response Body

Code: 200

Self-set authentication with OTP response.

Fields	Type	Description	Example/Allowed Values
ValidateOtpSelfSetAuthenticationFactorWithOtpResponse	String	Self-Set Authentication with OTP Response model.	
Code	String	Step code where the request is paused for user input.	new.authentication.value.required
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, Fr, Ar
message*	String	The API response message that shows the type of information returned.	new authentication value is required. Please enter new & confirmation values to continue.
mfsTenantId	String	MFS Tenant ID of the user	mfsPrimaryTenant
originalServiceRequestId *	String	The Original Service Request ID Length-36 characters	da371e6e-db02-472b-94c3-2ad2f79dfd09
serviceFlow	String	A unique code that is internal to Comviva and identifies the business process flow associated to the API.	SELFSETAUTHMFA
serviceRequestId*	String	Whenever an API is called, Comviva generates a unique service request ID for the API request. This unique	f491f6b1-aa9b-43de-93b0-c85eda706a2c

Fields	Type	Description	Example/Allowed Values
		ID traverses' components in the business process flow. It is useful when the process flow is paused for the user input and needs to be resumed when user has provided the input. Length-36 characters	
status*	String	The status to show whether the API call is a success, failure, in progress, or paused.	SUCCEEDED, FAILED, INPROGRESS, or PAUSED
transactionTimeStamp *	String	The date and time of transaction in the format YYYY-MM-DD and HH:MM:SS respectively.	2023-01-31T15:49:45

Sample Response Body


```
{
    "serviceRequestId": "a25e5e96-4f0e-4f89-af3d-1a6244f57441",
    "mfsTenantId": "mfsPrimaryTenant",
    "language": "en",
    "serviceFlow": "SELFSETAUTHMFA",
    "transactionTimeStamp": "2023-10-13T15:46:12",
    "originalServiceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634",
    "code": "new.auth.value.required",
    "message": "New authentication value is required. Please enter new and confirmat
ion values to continue",
    "status": "PAUSED"
}
```


Error Codes

Error Code	Description
400	Bad request
500	Internal Server Error

Error scenario:

Http error code: 400.
Error Code: Generic05- No data found.

Response:


```
{
  "status": "FAILED",
  "errors": [
    {
      "code": "sfm.errors.resume.service.request.id.not.found",
      "message": "resume request id not found",
      "componentName": "SFM"
    }
  ],
  "errorCode": "Generic05",
  "errorUserMsg": "No data found",
```

```
  "httpErrorCode": "400"
}
```


2.3.1.2.3 Confirm Authentication Values after OTP Validation

Action: POST
Endpoint: /v2/ums/user/auth/self-set-auth/confirm
Description
This API is used to confirm new authentication value for self-initiated change authentication value (Pin/Password) after OTP validation.

Request body :

Fields	Type	Description	Example/Allowed Values
adminResetAuthenticationFactorModel	String	set authentication value for Self-set authentication with otp service body. Cannot be empty.	
SetAuthenticationValueWithOtpModel	String	Self-Set Authentication with OTP Request Model	
confirmedAuthenticationValue*	String	Re-enter new password for confirmation. Default length of pin is 4 Min password length is 5 & Max password length is 10 Pin/password also can be configured using security profile	1234
newAuthenticationValue*	String	Enter new password/PIN Can be configured using security profile Default length of pin is 4	1234

Fields	Type	Description	Example/Allowed Values
		Min password length is 5 & Max password length is 10 Pin/password also can be configured using security profile	
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, Fr, Ar
resumeServiceRequestId*	String	System Generated Unique Id which determines the service flow Length- 36 characters (System generated)	f491f6b1-aa9b-43de-93b0-c85eda706a2c

Sample Request Body

```
curl --location
    'https://mfsbaastest.grameenphone.com/mobiquitypay/v2/ums/user/auth/self
    -set-auth/confirm' \

--header 'Accept: application/json, text/plain, */*' \

--header 'Accept-Language: en-US,en;q=0.9,hi;q=0.8' \

--header 'Connection: keep-alive' \

--header 'Content-Type: application/json;charset=UTF-8' \

--header 'Cookie: unq=c4dPpSLPIgO9yPZM;
    refresh_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imp3cy1rZXktcH
    VibGljLTEifQ.eyJzZXJ2aWNlUmVxdWVzdElkIjoiMzM5YWM4ZTgtNGI3MS00NmM4LWIwOTY
    tNzE0MjMzNWZhZTNhIiwidXNlcl9uYW1lIjoiMzM5YWM4ZTgtNGI3MS00NmM4LWIwOTYtNzE
    0MjMzNWZhZTNhIiwiYXV0aG9yaXphdGlvblByb2ZpbGVDb2RlIjoiTmV0YWRtaW5EZWZhdWx
    0IiwiaWRlbnRpZmllclZhbHVlIjoiQW1hbjAxIiwiaWRlbnRpZmllclR5cGUiOiJMT0dJTkl
    EIiwiY2F0ZWdvcnlDb2RlIjoiTldBRE0iLCJ1c2VySWQiOiJVUy4zMzU2NTI0OTM0NjM4MzE
    1IiwiZGV2aWNlSWQiOm51bGwsImF1dGhvcml0aWVzIjpbIlJPTEVfVVNFUiJdLCJjbGllbnR
    faWQiOiJDb3JlV2ViIiwic2NvcGUiOlsiR0VUX1VTRVJfQU5EX0FDQ09VTlRfREVUQUlMUyI
    sIlNFTEZTRVRBVVRIRkFDVE9SIiwiRkVUQ0hfVVNFUl9RVUVTVElPTiIsIlRYTkNPUlJFQ1Q
    iLCJBVE1DQVNIT1VUIiwiQVRNQ0FTSE9VVF9WNCIsIkFETVRYTlJFRklEIl0sImF0aSI6ImQ
    2NGRjMDU4LWM1MjgtNGYyNy1hMDI2LTMzZGRjZGJjZDZkZCIsIm5hbWUiOiJBbWFuIEFtYW4
    iLCJiZWFyZXJDb2RlIjoiIiwiZXhwIjoxNjk3MjE3NTg1LCJqdGkiOiJhNzA3MGM3Ni04ZDg
    2LTQ3MmUtYTYxOS03YWMyMTJjYTViNmYifQ.jPBlVRKmPMl2Z_-
    trAWWLxajZzDRh2KjCmsX-
    kwVHKXr3DPOMN17G9VW1PiY2ZaEqR3Y2H6nRxIkFXz6MOoIll30UEqljuOpB6V95l9cNURFq
```

```
    06evqFwIasfs6jIzmxV7by1iNlHNR5m1KMMF42D8L9en8h0lAVf9Hb4VaX_I_GL2GAnbUjyn
    7SM28njVx3Q9ZF6UDORlrAQVTbdW1uzimGXKLhoYtzE_nupf-w2ksToC0dOKsY5fKB7U9aO-
    qjXnPBBXJIrmUvM25J9fPmyNCiP0YNGeCktyIbASOAwIbV9HyEu1-
    VOWnSKA1w06KeUIaS3bebf5maPznh88J1GgQ;
    TS01e8828b=01f85cdc3ceaccb0e0dd4d85ebf7b7dddaea5ae0f3944a191229a40ce8bad
    051d541990c8462523f2db0fe252be3d31f3cdb37758fde55c4845375f9941e6e3d38e31
    41a71228d43f32497bf609ae9f1c048bf4aeea2e051d3b0030cee573634d855d3616a3a9
    d7319297d1dd455fff7d420a65643;
    TS33367916027=085664378eab2000d2ee20e60cf6c69918ee90b02feaaf93e0e1ffc7b9
    4c3ea9010a09a12655b26108fcaf43b211300097d606c789d778d91e619c5e775d098504
    73bc9e887e877d6ba64d43ea0a5977896f8096ba5f5917dce41e3f45421521;
    TS01e8828b=01f85cdc3cc4c735ef2d04975ee799b43c280a5acda09245bf7e07a400768
    132bf99bd0fcf0fa6db3629c68a2c243e3fe394e2521d;
    TS33367916027=085664378eab2000e2f861779ca922a47ea0f5d303868474fdb5400199
    295ee2257cb0ba988681a308f3d4df8711300094fad75a80452f7924d9a853bbabc5e0f7
    cebcf61d31f5fec0eb4349217b9d417c42b90b507173c5887a0750835a5c4a' \

--header 'Nonce: f086e5d8266d1303' \

--header 'Origin: https://mfsbaastest.grameenphone.com' \

--header 'Referer:
    https://mfsbaastest.grameenphone.com/dfscontainer/app.html' \

--header 'Sec-Fetch-Dest: empty' \

--header 'Sec-Fetch-Mode: cors' \

--header 'Sec-Fetch-Site: same-origin' \

--header 'Signature:
    5a86ee76514b9513d49dab829365cecdf9f5eabc7c91b026c1fc6fe34f430681' \

--header 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36' \

--header 'sec-ch-ua: "Google Chrome";v="117", "Not;A=Brand";v="8",
    "Chromium";v="117"' \

--header 'sec-ch-ua-mobile: ?0' \

--header 'sec-ch-ua-platform: "Windows"' \

--data-raw '{

    "confirmedAuthenticationValue": "Com@0822",

    "language": "en",

    "newAuthenticationValue": "Com@0822",

    "resumeServiceRequestId": "a25e5e96-4f0e-4f89-af3d-1a6244f57441"

}'
```

Response Body


```
{
   "serviceRequestId": "c7c35c94-6f8a-4709-8667-7ac77bf728ed",
   "mfsTenantId": "mfsPrimaryTenant",
   "language": "en",
   "serviceFlow": "SELFSETAUTHMFA",
   "transactionTimeStamp": "2023-10-13T15:48:19",
   "originalServiceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634",
   "code": "AUTH_04",
   "message": "Authentication factor is successfully changed",
   "status": "SUCCEEDED"
}
```


Fields	Type	Description	Example/Allowed Values
SetAuthenticationValueWithOtpResponse	String	Self Set Authentication with OTP Response model	
language	String	Preferred language of the user. By default, system supports 3 languages English/French/Arabic.	En, Fr, Ar
message*	String	The API response message that shows the type of information returned.	Authentication factor is successfully changed
mfsTenantId	String	MFS Tenant ID of the user	mfsPrimaryTenant
originalServiceRequestId *	String	The Original Service Request ID Length-36 characters	da371e6e-db02-472b-94c3-2ad2f79dfd09
serviceFlow	String	A unique code that is internal to Comviva and identifies the business process flow associated to the API.	SELFSETAUTHMFA
serviceRequestId*	String	Whenever an API is called, Comviva generates a unique service request	f491f6b1-aa9b-43de-93b0-c85eda706a2c

Fields	Type	Description	Example/Allowed Values
		ID for the API request. This unique ID traverses' components in the business process flow. It is useful when the process flow is paused for the user input and needs to be resumed when user has provided the input. Length-36 characters	
status*	String	The status to show whether the API call is a success, failure, in progress, or paused.	SUCCEEDED, FAILED, INPROGRESS, or PAUSED
transactionTimeStamp*	String	The date and time of transaction in the format YYYY-MM-DD and HH:MM:SS respectively.	2023-01-31T15:49:45

Sample Response Body


```
{
    "serviceRequestId": "c7c35c94-6f8a-4709-8667-7ac77bf728ed",
    "mfsTenantId": "mfsPrimaryTenant",
    "language": "en",
    "serviceFlow": "SELFSETAUTHMFA",
    "transactionTimeStamp": "2023-10-13T15:48:19",
    "originalServiceRequestId": "cfd43988-7adf-4168-bdcd-0523ce0a8634",
    "code": "AUTH_04",
    "message": "Authentication factor is successfully changed",
    "status": "SUCCEEDED"
}
```


Error Codes

Error Code	Description
400	Bad request
500	Internal Server Error

Error scenario:

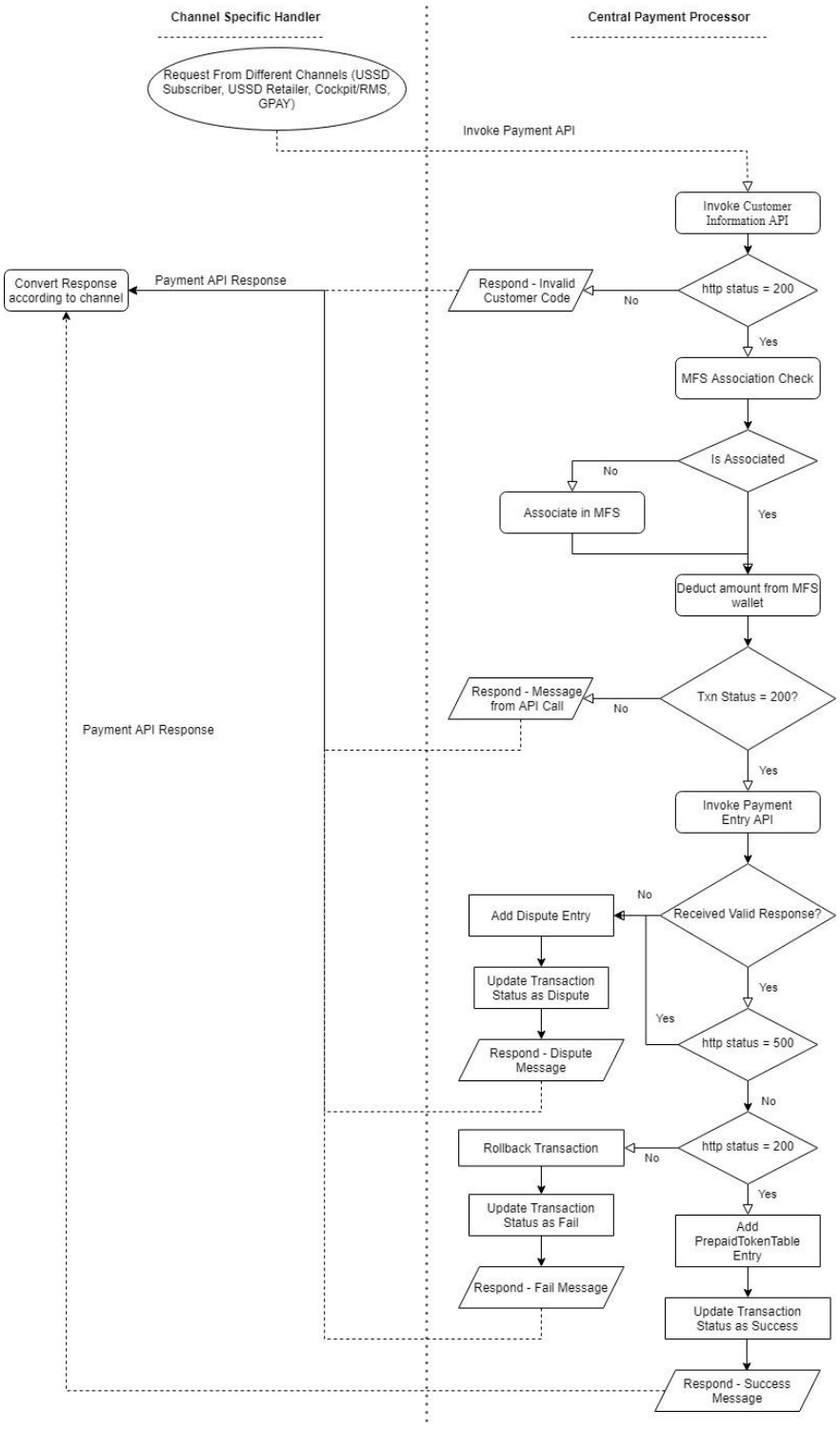
Http error code: 400
Error Code: Generic05- No data found.

Response:

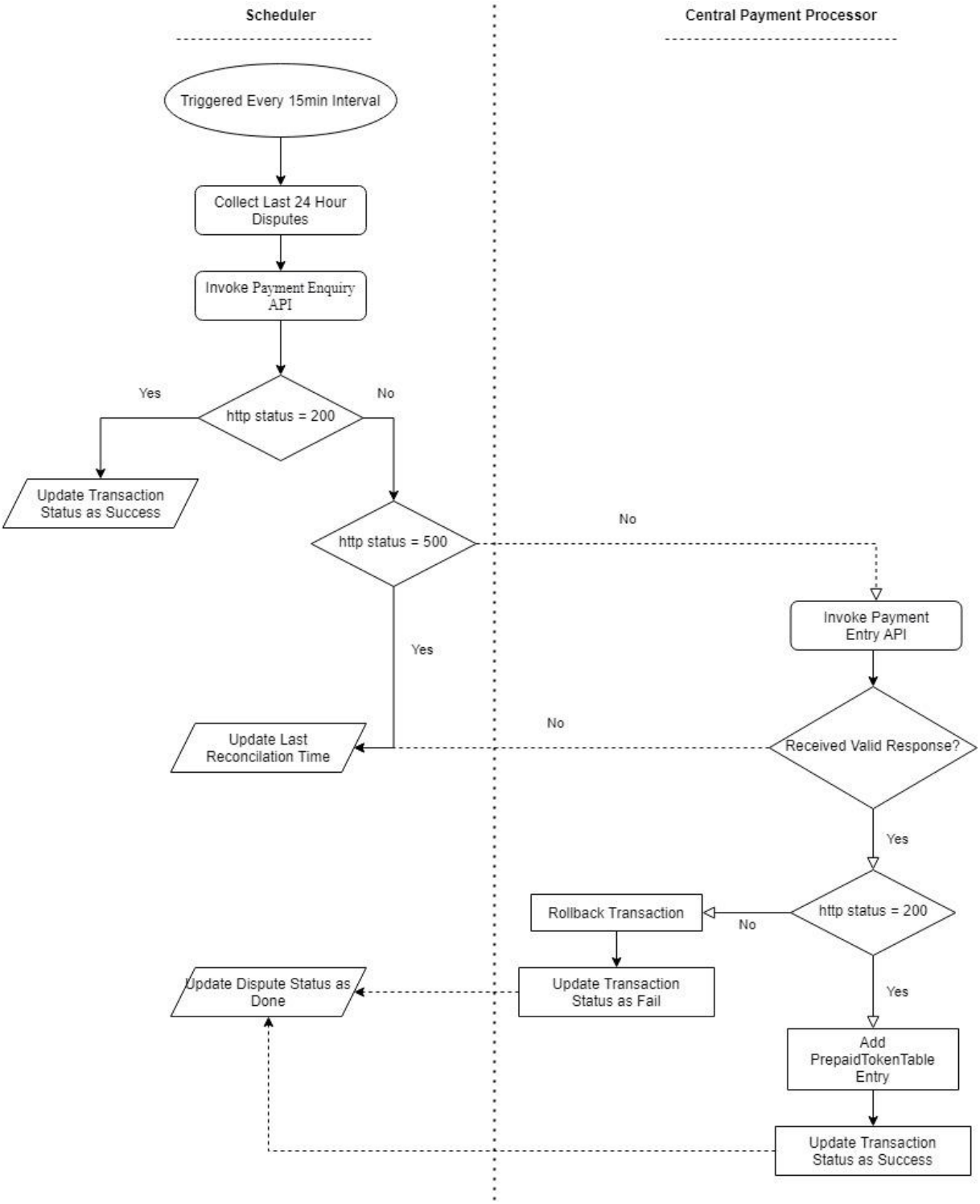

```
{
  "status": "FAILED",
  "errors": [
    {
      "code": "sfm.errors.resume.service.request.id.not.found",
      "message": "resume request id not found",
      "componentName": "SFM"
    }
  ],
  "errorCode": "Generic05",
  "errorUserMsg": "No data found",
  "httpErrorCode": "400"
}
```


2.4 Existing Flow Diagrams:

Flow diagram of Billpayment Request



Call flow of scheduler : to pick bulk request(fetch bill and payment) initiated from UI



Note:

- All technical training session happened with Wipro will be shared with partner that will give detailed view of current implemented request flow .
- Postman collection of existing system APIs is also shared.
- Git code link of existing system will be shared by Comviva to partner

2.5 User Management:

Important points to be noted:

Multiple users in bulk pay system can be linked to a single client

When users initiates payment req from their portal, it is client's wallet which is debited. User has no wallet to it.

In payment API to mobiquity : sender wallet will have client ID details associated to it.

SO in Bulk Pay module, first a client needs to be created under "Account Management". The MSISDN associated to client is mapped to actual Channel User present in mobiquity system. He can be of any category (wholeseller, merchant etc)

All users getting onboarded in Bulk system, has to be present as systemadmin in mobiquity with limited access of roles in mobiquity system and no wallets attached to them.

When a user is created in bulk system, then he is linked with a client (msisdn of channel user in mobiquity) and during payment MSISDN and PIN of this client ID is sent in API to mobiquity for wallet debit.

3 Technical Solution Requirement

3.1 Solution Overview

the solution must be created using open-source technologies widely accepted and used by the industry.

3.1.1 Tech stack to be used to deploy and run existing code

Comviva suggest to use below listed technology stack for the development of the application:

Angular 9.1.1
npm 6.13.4
Node 12.16.1
tomcat 9 or above
Jdk 14
MySql

3.2 Deployment Specifications of existing module

The solution must be deployed with below steps in order.

3.2.1 DB Readiness

- Install MySql in your local system.
- Install MySql Workbench in your local system.
- execute Below all the files in MySQL Workbench for setup database in your local system.

mflex_bulk_bill.sql

mflex_core.sql

mflex_report.sql z

3.2.2 Application readiness

- There are Four Modules which need to be deployed in same order
- 1. web application
- 2. async job
- 3. mfs-communication
- 4. gpay-C

Steps to deploy:

- (Web Application – master)
  - Go in this folder
    1. cd src/ng
    2. open command prompt or git bash
    3. npm init -y
    4. npm install
    5. npm run dev
  - Now, open the project and do some changes in .properties (DB configuration, etc…)
  - run main class which have @SpringBootAplication annotations.
  - open any Browser and hit : http://localhost:8080/

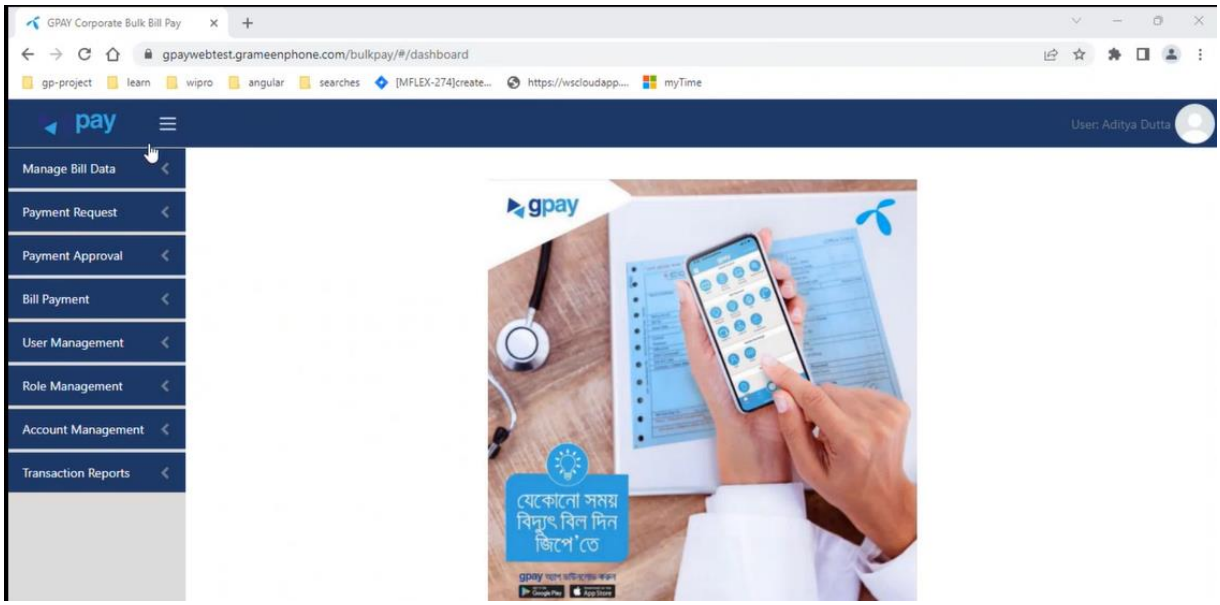
3.3 Project Specific Scope

3.3.1 Current Implemenation

All technical hands-on recording will be shared with Parner

3.3.2 Graphical User Interface

GUI should be as below:



Rest can be referred from Recordings:

3.3.3 Training

Once the application is delivered on site, the partner must conduct technical training to the Comviva development team and provide necessary information and code walk through for changes made in existing Code.

3.3.4 Documentation

Flow diagram has been attached above to explain process flow of Request

3.3.5 Postman Collection

Attached is postman collection is existing system APIs to integrate within system and with biller platform

Communicator copy.postman_colle

Desco-postpaid.po stman_collection.jso

Note: Comviva will share it's API (Fetch bill, payment, ambiguous settlement)

3.4 Testing and Acceptance

3.4.1 System Integration Testing

Application must pass all the test cases defined by partner's internal QA. Comviva QA will audit the report and also may execute their own designed cases as per the functionalities if required, Partner must fix all issues raised by Comviva QA.

Note: Any bug identified during QA testing which is present in existing/new code must be fixed by Partner.

3.4.2 User Acceptance Procedure

Once the application in cleared by Comviva QA, it must be offered to customer for their testing and acceptance. User acceptance test cases must be shared by partner and passed in order to get user acceptance certificate. All UAT defects must be fixed by Partner.

3.5 Risks, Impact and Mitigation

Partner must identify and define all the risks and share its impact as well as mitigation plan.

3.6 Responsibility Matrix

Partner must prepare and share responsibility matrix for various tasks required to be executed during the lifecycle of this project.

3.7 Out of Scope

Third party (Biller)APIs integration would be out of scope for partner, though partner must define their own list of out of scope items and share with us.

All third party integrations will be under mobiquity scope. Partner has to just integrate with Mobiquity Payment APIs.

Reporting UI shown in demo is out of scope of partner . Mobiquity will support all report related need through existing reports present in product.

3.8 Code management

Partner must commit and update all the codes, designs, and documents into Comviva version control systems (GIT) and provide necessary access information for Comviva development team. Partner should adhere to all the Comviva software development guidelines and follow GDPR processes.

3.9 Project handover

Once the project is completed, partner must handover updated software to Comviva and conduct various workshops (technical, functional, non-functional etc.) for teams and provide them hands on experience and KT to enable them to take care of future change requests as well as bug fixes. This will be for changes done by Partner on top of existing code.

3.10 Project Timelines

This project must be completed within the defines and agreed timelines. The project is expected to be completed within 30 days.

3.11 Support and maintenance

- Partner will be responsible for UAT as well as production defects
- Partner must provide technical support and maintain the project upto 1 year after delivery.
- Partner must assign a dedicated team to develop and support this project
- Production defects must be fixed with in defined SLA.

4 Document Change History

Version	Change Type (A/M/D)	Change Description	Prepared By	Reviewer	Approved by	Date
1.0	A	Initial version	Anshika Aggarwal	Pranay Agrawal	Kamal Kishor Arya	27-July-2023

Disclaimer

Copyright © 2021: Comviva Technologies Limited 5th, 7th & 8th floor, Capital CyberScape, Village Ullahwas, Sector 59, Golf Course Extn. Road, Gurugram – 122102, Haryana, India.

All rights about this document are reserved and shall not be , in whole or in part, copied, photocopied, reproduced, translated, or reduced to any manner including but not limited to electronic, mechanical, machine readable ,photographic, optic recording or otherwise without prior consent, in writing, of Comviva Technologies Ltd (the Company).

The information in this document is subject to changes without notice. This describes only the product defined in the introduction of this documentation. This document is intended for the use of prospective customers of the Company Products Solutions and or Services for the sole purpose of the transaction for which the document is submitted. No part of it may be reproduced or transmitted in any form or manner whatsoever without the prior written permission of the company. The Customer, who/which assumes full responsibility for using the document appropriately. The Company welcomes customer comments as part of the process of continuous development and improvement.

The Company, has made all reasonable efforts to ensure that the information contained in the document are adequate, sufficient and free of material errors and omissions. The Company will, if necessary, explain issues, which may not be covered by the document. However, the Company does not assume any liability of whatsoever nature , for any errors in the document except the responsibility to provide correct information when any such error is brought to company's knowledge. The Company will not be responsible, in any event, for errors in this document or for any damages, incidental or consequential, including monetary losses that might arise from the use of this document or of the information contained in it.

This document and the Products, Solutions and Services it describes are intellectual property of the Company and/or of the respective owners thereof, whether such IPR is registered, registrable, pending for registration, applied for registration or not.

The only warranties for the Company Products, Solutions and Services are set forth in the express warranty statements accompanying its products and services. Nothing herein should be construed as constituting an additional warranty. The Company shall not be liable for technical or editorial errors or omissions contained herein.

The Company logo is a trademark of the Company. Other products, names, logos mentioned in this document , if any , may be trademarks of their respective owners.

Copyright © 2021: Comviva Technologies Limited. All rights reserved.

Thank You

Visit us at *www.comviva.com*