apigateMint API Specification [Northbound] – Identity:OTP

Document Reference No.: APIGATE/MINT/APIS-NB-IDN-OTP

Version: 1.1

Issued: 8 March 2019

Table of Contents

Glossary

Abbreviation	Definition
API	Application programming interface
SP	Service Provide
MC	Mobile Connect
OIDC	Open ID Connect
HE	Header Enrichment
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
SSL	Secure Sockets Layer
TLS	Transport Layer Security
JWT	JSON Web token
T&C	Terms and Conditions

1. Introduction

This document describes Identity:OTP (IDN-OTP) API specification for Client/Service Provider mobile app. The API is to allow mobile app to authenticate its users via a One Time PIN (OTP) based on MSISDN. This variation of the Identity service still uses the basic Mobile Connect standard, but uses a OTP sent via SMS for the End User authentication.

Client/SP App must implement

- GUI screens to accommodate MSISDN input, new user registration, Terms and Conditions, OTP input, displaying response result for end user.
- Logical check to prevent bad attempts e.g. **requesting for OTP several times**, **unsuccessful OTP validation**, etc

2. Summary of Identity:OTP flow for Mobile App

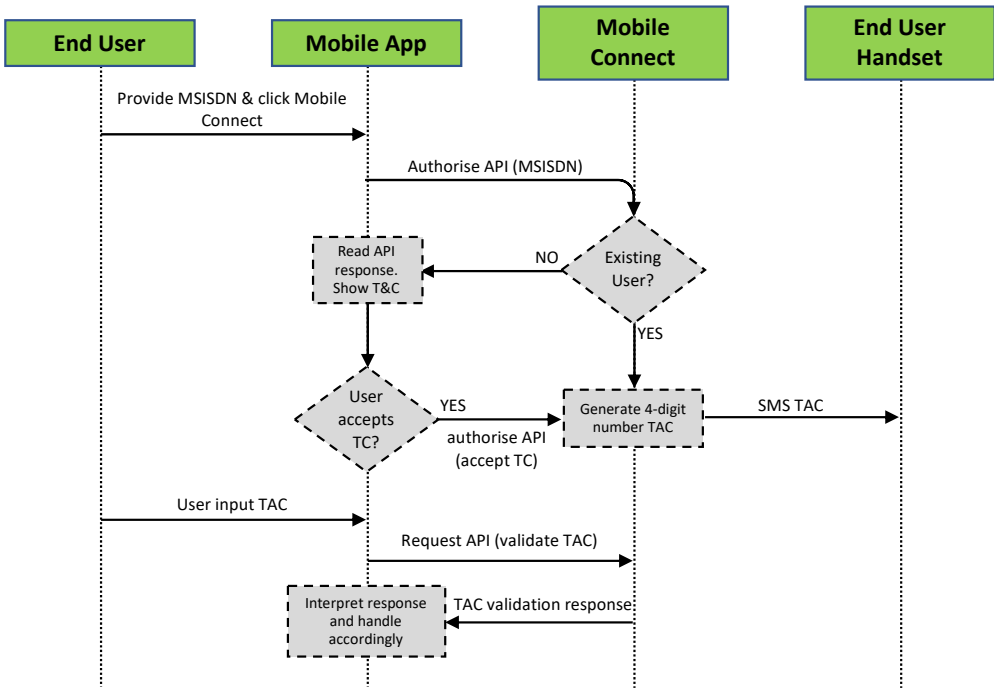

Figure 1: Identity:OTP flow for Mobile App

The Mobile App sends an authorize API requests when user clicks on the “Mobile Connect” button in app. MSISDN must be included as part of request parameters together with others.

Mobile Connect checks whether user has login before.

- It generates a 4-digit numeric one-time-pin (OTP) and sends to user handset via SMS if user MSISDN exists in MC database. The result is sent back to App as API response
- It shall respond user status if user MSISDN is not found registered with MC.

In case user has not login to MC, App shall display registration screen with Terms and Conditions. Once user has agreed to T&C and registered, App send authorize API request to register. Mobile Connect generates 4-digit OTP and sends it to user MSISDN via SMS.

App provides an input screen for user to validate OTP. App sends API request OTP validation. MC responds to App on validation result e.g. valid/invalid code, expired.

3. Authorization request endpoint

This API endpoint is called when user clicks on “Mobile Connect” in-app button

Endpoint name: `/app/authorize`

Method: GET

The request parameters are added using Query String Serialization. The following table lists the parameters required for Mobile Connect authorization request.

Parameter	Required	Type (max length)	Description	Value
`msisdn`	Mandatory	Numeric	User’s MSISDN	Standard MSISDN format, **numeric (no +, -, space, special character)** e.g. 60131234567
`response_type`	Mandatory	String (20)	To indicate the grant type flow to be used is authorization code	Must set to **`code`**
`client_id`	Mandatory	String (50)	SP identifier For authorization request validation	Value will be provided to SP after it is configured in MC server
`scope`	Mandatory	String (20)	List of ASCII strings for authorization scope request	Must set to **`openid mc_authz phone`**
`redirect_uri`	Mandatory	String (100)	URI where response will be sent to.	SP provide redirect_uri URI in request parameter must match pre-registered redirect_uri configured in MC server
`version`	Mandatory	String(10)		Must set to **`2.2`**
`state`	Mandatory	String(50)	Security mechanism to prevent Cross-Site Request Forgery	**SP generates unique value for every new authorization request.** **This is an alpha-numeric field, at least 16 characters in length with no space in between. The value must be unique for each SP**
`acr_values`	Mandatory	String(10)	Indicate LoA	**2**
`client_name`	Mandatory	String (50)	SP’s name	TDB

binding_message	Mandatory	String (45)	Reference ID to be displayed on Consumption device and Authorization device	SP generates unique Reference ID
mode	Mandatory	Numeric	Indicate authorization request is for login or transaction	1: Login 2: Transaction
accept_tc	Optional	Numeric	Indicate user has agreed to T&C, register	1: accepted T&C

Table 1: authorize API request parameters

3.1 SP/Client sends sign-in request to MC server

Below is an example of SP/client sends request to MC server using GET method

Sample request

```
HTTP GET /app/authorize?msisdn=60131234567&response_type=code
&client_id=APP_1
&scope=openid%20mc_authz%20phone
&redirect_uri=https%3A%2F%2Fclient.serviceprovider.com.my
&version=2.2
&state=af0oth123
&acr_values=2
&client_name=APP
&binding_message=REF1134&mode=1
```

3.2 SP/Client gets authorization response from MC server

Checking MSISDN determines whether this is existing MC user.

- Existing user: MC attempts to send OTP via SMS to user handset and return response
- New user: MC responds user status, Client/SP App to display accordingly

Response returned in JSON format. Parameter ‘code” indicates result of request API

Parameter	Required	Type (max length)	Description	Value
code	Mandatory	Numeric	Response code	See section 3.3
state	Mandatory	String (50)	Taken from request parameter	Must be same as state submitted in request. If the state does not match the value presented in the initial request, the SP should reject the response
client_id	Mandatory	String (50)	Taken from request parameter	Must be same as client_id submitted in request. If different from the initial request SP should reject response

exists	Mandatory	Numeric	User has registered and login to MC before	0: new user 1: existing user
message	Mandatory	String(500)	Human readable message	Human readable message

Table 2: Authorize response parameters

Sample response

```
HTTP 200 OK
{
  "code": 0,
  "state": "af0oth123",
  "client_id": "APP_1",
  "exists": 1,
  "message": " Delivered to Network"
}
```

3.3 Authorization response code

3.3.1 Existing user

Existing user, OTP was generated and sent via SMS. The apigateMint Exchange responds success with HTTP code **201**-Created. MC responds HTTP code **200 OK** with response body

Parameter	Required	Description	Value
code	Mandatory	OTP was sent successfuly	0
state	Mandatory	Taken from request parameter	Same value as in request body
client_id	Mandatory	Taken from request parameter	Same value as in request body
exists	Mandatory	Existing MC user	1
message	Mandatory	Human readable message	apigateMint Exchange "**deliveryStatus**" message

```
HTTP 200 OK
{
  "code": 0,
  "state": "af0oth123",
  "client_id": "APP_1",
  "exists": 1,
  "message": "Delivered to Network"
}
```

In the event apigateMint Exchange responds with error other than HTTP 201 when OTP is sent. MC responds HTTP status code **400** with response body

Parameter	Required	Description	Value
code	Mandatory	SMS sent via the apigateMint Exchange	75

		failed	
state	Mandatory	Taken from request parameter	Same value as in request body
client_id	Mandatory	Taken from request parameter	Same value as in request body
exists	Mandatory	Existing MC user	1
message	Mandatory	Human readable message	apigateMint Exchange "**deliveryStatus**" message

```
HTTP 400
{
  "code": 75,
  "state": "af0oth123",
  "client_id": "APP_1",
  "exists": 1,
  "message": "Error while sending SMS"
}
```

3.3.2 New Mobile Connect user

New user, OTP not sent MC responds HTTP code **200** with response body below. Celcom App shows user registration screen.

Parameter	Required	Description	Value
code	Mandatory	New MC user	0
state	Mandatory	Taken from request parameter	Same value as in request body
client_id	Mandatory	Taken from request parameter	Same value as in request body
exists	Mandatory	Existing MC user	0
message	Mandatory	Human readable message	e.g. New Mobile Connect user

```
HTTP 200
{
  "code": 0,
  "state": "af0oth123",
  "client_id": "APP_1",
  "exists": 0,
  "message": "New Mobile Connect user"
}
```

3.3.3 Other errors

In case of errors, MC shall respond with HTTP status 400.

Parameter “code”	Description

70	Invalid client Invalid client_id is given
71	Invalid request Request is missing a parameter, contains an invalid parameter
75	Error when sending OTP to the apigateMint Exchange SMS gateway.
76	Invalid msisdn MSISDN is not numeric format, contain invalid character

Table 3: Authorization error parameters

Sample of error response

```
HTTP 400 Bad request
{
  "code": 71,
  "state": "af0oth123",
  "client_id": "APP_1",
  "exists": 0,
  "message": "Invalid requests"
}
```

3.4 Client/SP App sends authorize API request after new user accepts T&C

Once user has accepted T&C and agreed to login Mobile Connect, Client/SP App generates and sends **new** authorize API request with **`accept_tc`** value set to 1.

Below is an example of SP/client sends request to MC server using GET method

Sample request

HTTP GET `/app/authorize?msisdn=60131234567&response_type=code`
`&client_id=APP_1`
`&scope=openid%20mc_authz%20phone`
`&redirect_uri=https%3A%2F%2Fclient.serviceprovider.com.my`
`&version=2.2`
`&state=`**`af0oth456`**
`&acr_values=2`
`&client_name=APP`
`&binding_message=REF1134&mode=1&`**`accept_tc=1`**

4. OTP validation endpoint

Client/SP App e.g. Celcom App accepts OTP 4-digit number from user input and sends API request to validate it.

Endpoint:
`/app/authenthicate/ack/`**`<client_id>?`**`state=`**`<state>`**`&otp=<`**`OTP_value`**`>`

Method: GET

`client-id:` same value as in authorize API request

`state`: same value as in authorize API request (**of success response**)

Header

```
Content-Type:application/json
```

Sample of OTP validation request

HTTP GET `/app/authenticate/ack/`**`APP_1?`**`state`**`=af0oth123&`**`otp=`**`9809`**

Header

```
Content-Type: application/json
```

Mobile Connect validates OTP and returns response

Parameter	Required	Type (max length)	Description
code	Mandatory	Numeric	Response code
message	Mandatory	String (500)	Human readable message

If OTP is valid, MC responds HTTP **200** with body

```
{
  "code": 0,
  "message": "Valid OTP"
}
```

If OTP is invalid or expired, MC responds HTTP **400** with body

```
{
  "code": 77,
  "message": "Invalid OTP"
}
```

If OTP is expired, MC responds HTTP **400** with body

```
{
  "code": 78,
  "message": "Expired OTP"
}
```