Precise One-Time-Password (OTP)

API Documentation

Version	Date	Last updated
1	25-May-2021	Initial draft

INDEX

1. INTRODUCTION

This document is a guide to generate One-Time-Password (OTP) for your web/stand-alone applications to perform mobile authentication or Two-Factor-Authentication (2FA) without needing to maintain a database. The document will describe the OTP API in detail and provide some examples on how to use this.

The API is RESTful with JSON response format.

API URL: https://restapi.tobeprecisesms.com/api/otp

2. API ENDPOINTS

With the OTP API Endpoints the Customer can easily submit one time passwords to their end-users and verify their responses without needing to maintain a database. The OTP API works in two steps:

a. Request a SMS PIN and send it to the Customer's end-user

b. Verify the PIN that was entered by the end-user

2.1 Request a PIN

This method is used to generate and send OTP PIN to end user.

POST URL: request/?Username={Username}&Password={Password}

URL e.g.: https://restapi.tobeprecisesms.com/api/otp/request/?Username=xxx&Password=xxxx

Request Format Body

```
{
    "MobileNo": "971501234567",
    "RefNo"   : "Your_Reference_No"
}
```

Parameter Name	JSON Type	Mandatory	Description
MobileNo	String	YES	Mobile number must be in the international format eg: "971501234567"
RefNo	String	NO	Client's Unique Reference Number which can be used to verify the OTP Pin.
Message	String	NO	Content of the message including the placeholder $$PIN$$ which will be replaced by a PIN generated.

			Eg: "Your PIN is: $$PIN$$" If the message is not provided, the default pre-defined message will be sent to end user.
SenderName	String	NO	Sender name that will be used to send OTP SMS to end users. Only sender names that are allocated on your account can be used in this field. If the sender name is not passed, then one of the sender names available on your account will be used to send sms.
PinLength	Number	NO	The length of the PIN. Default: 4 (four digits) Allowed value is 4, 5 and 6
PinValidity	Number	NO	The time duration OTP is valid. Default is 20
PinMaxAttempt	Number	NO	Maximum OTP validation attempts/tries by end user. Default: No limit – User can try any number of attempts.

Response

Response will be a JSON object mentioning if the transaction was successful or not. See below for a sample response.

Status	Response

200


```
{
 "status": "OK",
 "data": [
  {
   "msgId": 6010523144740000001,
   "mobileNo": "971501234567",
   "status": "OK",
   "details": "Message Sent",
   "creditsUsed": "0.060000"
  }
 ]
}
```

200	{
	"status": "OK",
	"data": [
	{
	"status": "Error",
	"details": "Invalid Mobile Number"
	}
	]
	}

200	{
	"status": "ERROR",
	"errorDescription": " Invalid login id and/or password."
	}

500	{
	"status": "ERROR",
	"errorDescription": "Something went wrong. Please try again later."
	}

Request e.g. 1 - with all the Parameters

```
{
        "MobileNo":"971501234567",
        "RefNo":"123456",
        "Message":"Welcome! Use the verification code $$PiN$$ to login",
        "SenderName":"Your_Sender_ID",
        "PinLength":4,
        "PinValidity":10,
        "PinMaxAttempt":3
}
```

Request e.g. 2 - with only Mandatory Parameter

```
{
        "MobileNo":"971501234567"
}
```

2.2 Verify a PIN

This method is used to verify the OTP PIN entered by end user.

POST URL : verify/?Username={Username}&Password={Password}

URL Ex. : https://restapi.tobeprecisesms.com/api/otp/verify/?Username=xxx&Password=xxxx

Request Format Body

```
{
        "MobileNo": "971501234567",
        "OTPPin":"2135",
        "MsgID":"6010523144740000001",
        "RefNo": "1234qse"
}
```

Parameter Name	JSON Type	Mandatory	Description
MobileNo	String	YES	Mobile number must be in the international format eg: "971501234567"
OTPPin	String	YES	The OTP Pin entered by the end user.
RefNo	String	NO	Client's Unique Reference Number that was used to request the OTP.
MsgID	String	NO	Gateway MSG ID which was returned as response to the OTP request.

Response

Response will be a JSON object mentioning if the verification was successful or not. See below for a sample response.

Status	Response

200	{
	"status": "OK",
	"data": {
	"Status": "OK",
	"Details": "Successfully Verified",
	"MsgId": 6010523144740000001,
	"RefNo": "1234qse ",
	"MobileNo": "971501234567"
	}
	}

200	{
	{
	"status": "OK",
	"data": {
	"Status": "Error",
	"Details": "No matching details found!",
	"MobileNo": "971501234567"
	}
	}

200	{
	"status": "OK",
	"data": {
	"Status": "Error",
	"Details": "Max attempts exceeded!",
	"MobileNo": "971501234567"

<table>
<tr><td></td><td>

```
  }
}
```

</td></tr>
<tr><td>200</td><td>

```
 {
  "status": "ERROR",
  "errorDescription": " Invalid login id and/or password."
}
```

</td></tr>
<tr><td>500</td><td>

```
{
 "status": "ERROR",
 "errorDescription": "Something went wrong. Please try again later."
}
```

</td></tr>
</table>

Request e.g. 1 - with all the Parameters

```
{
        "MobileNo": "971501234567",
        "OTPPin":"2135",
        "MsgID":"6010523144740000001",
        "RefNo": "1234qse"
}
```

Request e.g. 2 - with only Mandatory Parameters

```
{
        "MobileNo":"971501234567",
        "OTPPin":"2135"
}
```

3. AUTHORIZATION:

There are 2 methods that can be used to perform authorization,

a. Pass the Username & Password in the Query string as plain text.

E.g. APIURL?Username=xxx&Password=xxxx

b. Using the request header to pass the Basic authorization values. Use Base64 encoding to encode the *Username:Password* in header authorization. A sample header is as shown below,

Authorization: Basic cHJlY2lzZTpwcmVjaXNl

4. GLOSSARY

Conventions

- All the possible responses are listed under 'Responses' for each method. Only one of them is issued per request server.
- All responses are in JSON format.
- For every request user name & password is mandatory for authorization purpose.

Status Codes

All status codes are standard HTTP status codes. The below ones are used in this API.

200 - Success of some kind

4XX - Error occurred in client's part

5XX - Error occurred in server's part

Status Code	Description
200	OK
400	Bad request
401	Authentication failure
403	Forbidden

404	Resource not found
405	Method Not Allowed
409	Conflict
412	Precondition Failed
413	Request Entity Too Large
500	Internal Server Error
501	Not Implemented
503	Service Unavailable

5. SUPPORT DETAILS

Should you require any clarification or support related to the OTP API please feel free to write to support@tobeprecisesms.com