GTX One-Time-Password (OTP)
HTTP API Manual

Revision: 5
Revision Date: 8/14/19 3:23:00 PM
Author: Oliver Zabel

Table of Contents

Introduction

The One-Time-Password (OTP) Interface is used to perform a mobile authentication or to build the second path in a Two-Factor-Authentication (2FA) environment.

With the OTP Interface 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:

1. Request a SMS PIN and send it to the Customer's end-user
2. Verify the PIN that was entered by the end-user

The SMS message, the SMS PIN type and the limit of validation counts are fully customizable via the API Call.

This manual will describe the API in detail and provide some examples on how to use this interface. If you have further questions regarding this interface, please contact your account manager or file a trouble ticket to support@gtx-messaging.com.

OTP API end points

a) Request a PIN

In order to **request** an SMS PIN to end-user the following endpoints have to be used. The OTP API returns values in TEXT/PLAIN as default. Please note that only SSL/TLS connections will be accepted on server port 443. If you would like to have return values in JSON format please use the JSON target endpoint:

Target for TEXT/PLAIN

You can reach the OTP request function under the following URL:

```
https://otp.gtx-messaging.net:443/smspin/request
```

Target for JSON

For return values in JSON format, please use the following endpoint:

```
https://otp.gtx-messaging.net:443/smspin/request.json
```

HTTP Request

The following HTTP-GET or HTTP-POST parameters can be set:

Field	Mandatory	Type	Description	Example
user	yes	String	API User (v1)	"123456789012345" "company_otp01"
pass	yes	String	API Pass (v1)	"topsecret"
from	yes	String	The TPOA / originator of the message. Allowed is alphanumeric up to 11 chars, shortcode, local longcode or international number (E.164, E.212 or E.214)	"Company" "+49171000000" "01729000000" "55888"
to	yes	String	The recipient of the message, international format, with leading "+" (E.164, E.212 or E.214)	"+49171000000"
text	yes	String	Content of the message including the placeholder **PIN** which will be replaced by a PIN generated by GTX. Allowed characters: GSM 03.38	"Your PIN is: PIN"
pin_type	no	String	Use the following values to define the format of the PIN: • numeric • alpha • alphanumeric **Default: "numeric"**	"numeric" for "12345" "alpha" for "abcDE" "alphanumeric" for "a1b2C3Z"
pin_length	no	Number	The length of the PIN. **Default: 5** for five digits	8
max_amount	no	Number	Maximum amount of validation tries. **Default: 3**	5

Response

The Gateway will return a HTTP Status "HTTP_OK" and a response containing the request **id**, which will be used to verify the entered PIN in the second step of validation.

In case of an error one of the following response codes will be returned:

Code	Description
`400 Bad Request`	HTTP Call not valid
`401 Unauthorized`	Wrong username / password
`403 Forbidden / Validation Error`	Reached User Limits
`500 Internal Server Error`	Please contact GTX
`503 Service Unavailable`	Service is currently unavailable, please try again

b) Verify a PIN

In order to **verify** a PIN entered the following endpoints have to be used. The OTP API returns values in TEXT/PLAIN as default. Please note that only SSL/TLS connections will be accepted on port 443. If you would like to have return values in JSON format please use the JSON target endpoint:

Target for TEXT/PLAIN

You can reach the OTP verify function under the following URL:

```
https://otp.gtx-messaging.net:443/smspin/verify
```

Target for JSON

For return values in JSON format, please use the following endpoint:

```
https://otp.gtx-messaging.net:443/smspin/verify.json
```

HTTP Request

The following HTTP-GET or HTTP-POST parameters can be set:

Field	Mandatory	Type	Description	Example
`user`	yes	String	API User (v1)	"123456789012345" "company_otp01"
`pass`	yes	String	API Pass (v1)	"topsecret"
`id`	yes	String	The request ID from the prior requested PIN SMS	"d88115fd-0416-44eb-a50d-959a60664bce"
`pin`	yes	String	The PIN entered by the end-user	"12345" "abcDE" "a1b2C3Z"

Response

The Gateway will return a HTTP Status "HTTP_OK" and a response "Success" should the entered PIN be correct.

In case of an error one of the following HTTP-Status will be returned:

Code	Description
400 Bad Request	HTTP Call not valid
401 Unauthorized	Wrong username / password
403 Forbidden / Validation Error	Reached Validation Limits
500 Internal Server Error	Please contact GTX
503 Service Unavailable	Service is currently unavailable, please try again

For further explanation the response will contain an error reason.

Examples for JSON formatted responses

a) Request an SMS PIN

HTTP-Get Request

```
https://otp.gtx-
messaging.net:443/request.json?username=comp_gold_001&password=topsecret&
from=GTXOTP&to=%2B491729084747&text=Please+enter+the+following+PIN:+$PIN$
```

GTX Gateway response HTTP_OK

```
{"id": "d88115fd-0416-44eb-a50d-959a60664bce"}
```

GTX generated a PIN "12345" and submitted successfully the SMS with content "Please enter the following PIN: 12345" to the recipient.

b) Verify a PIN

HTTP-Get Request

```
https://otp.gtx-
messaging.net:443/verify.json?username=comp_gold_001&password=topsecret&i
d=d88115fd-0416-44eb-a50d-959a60664bce&pin=12345
```

GTX Gateway response HTTP_OK

```
{"verification": "Success"}
```

Entered PIN is correct.