

Allied Payment Multi-factor Authentication

Allied Payment Network

Version 1.0

**Abstract**

The purpose of this document is to provide a high level overview of FlexPay/MobilePay integration using our Multi-Factor Authentication API interface to receive and verify authorization codes.

Table of Contents

[PURPOSE 1](#_Toc469390838)

[SCOPE 1](#_Toc469390839)

[FlexPay/Picturepay® integration Using Multi-Factor Authentication 1](#_Toc469390840)

[API Design 1](#_Toc469390841)

[Authentication 1](#_Toc469390842)

[Security 1](#_Toc469390843)

[API calls 2](#_Toc469390844)

[Request Code 3](#_Toc469390845)

[Verify Code 4](#_Toc469390846)

|  |  |  |
| --- | --- | --- |
| Version | Date | Change |
| 1.0 | 12/13/2016 | Initial version |

# PURPOSE

The purpose of this document is to provide a high level overview of FlexPay/MobilePay integration using our Multi-Factor Authentication API interface to receive and verify authorization codes.

# SCOPE

This guidance is limited in scope and does not necessarily provide all information necessary to complete an implementation.

# FlexPay/Picturepay® integration Using Multi-Factor Authentication

## API Design

The API is designed in a RESTful style. It uses HTTP verbs GET, PUT, and POST to retrieve resources at a URL. The resources can be serialized in either JSON or XML.

### Authentication

The API is authenticated through the AUTHORIZATION header. Each call is authenticated independently.

The Authentication line, in general, looks like this:

*Authorization: TIMESTAMP domain=ALLIED;timestamp=Tue, 16 Sep 2014 13:59:25 GMT;signature=JT3JfEO43LptmKUN2lPUiFkpZrs=;publicKey=12345*

The signature is a BASE64 encoding of a HMACSHA1 hash. The private key is issued to the vendor. The payload for the hash, in this case, is url + “/r/n” + timestamp + “/r/n”

You may use other authentication payloads which include the entire http body.

There is no need for Allied to maintain a credential store on behalf of the users.

### Security

All calls are made over HTTPS/SSL.

Calls are secured using a public / private key pair.

You may choose to sign the entire payload, or just the URL and timestamp.

API key pairs may be issued by vendor or by financial institution.

## API calls

The following API call is required to perform an integration where the User information is passed to our billpay application.

* Request Code
* Verify Code

**The following are sample HTTP requests and responses. The placeholders shown need to be replaced with actual values.**

### Request Code

This API function allows the developer to request a code be sent via the specified channel to a given target.

Valid method parameters include (SMS, VOICE, EMAIL)

Valid target parameter values include a valid phone number for SMS & VOICE methods or a valid email address when using the EMAIL method.

#### REQUEST

|  |  |
| --- | --- |
| **Method** | **URL** |
| GET | https://api.alliedpayment.com/multifactor/requestCode?method={METHOD} &target={TARGET} |
| **EXAMPLE** | |
| GET https://api.alliedpayment.com/multifactor/requestCode?method={METHOD} &target={TARGET} HTTP/1.1  Host: localhost  Authorization: TIMESTAMP username={username};domain={domain};timestamp={timestamp};signature={signature};publicKey={publickey}  Content-Type: application/json | |

#### RESPONSE

|  |
| --- |
| **EXAMPLE** |
| HTTP/1.1 204 No Content  Access-Control-Allow-Headers: Content-Type, Accept, Authorization  Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS, PATCH  Access-Control-Allow-Origin: \*  Cache-Control: private  Date: Tue, 13 Dec 2016 15:54:29 GMT  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/  X-Performance: 1000.0004 ms  X-RequestId: d577bf72-81d1-476d-9df8-a3d7756e72da  X-Robots-Tag: none  Connection: keep-alive |

### Verify Code

This API function allows the developer to verify a code that was previously requested.

#### REQUEST

|  |  |
| --- | --- |
| **Method** | **URL** |
| GET | https://api.alliedpayment.com/multifactor/verifyCode?code={CODE} &wasSentTo={TARGET} |
| **EXAMPLE** | |
| GET https://api.alliedpayment.com/multifactor/verifyCode?code={CODE} &wasSentTo={TARGET}HTTP/1.1  Host: localhost  Authorization: TIMESTAMP username={username};domain={domain};timestamp={timestamp};signature={signature};publicKey={publickey}  Content-Type: application/json  Content-Length: length | |

#### RESPONSE

|  |
| --- |
| **EXAMPLE** |
| HTTP/1.1 200 OK  Access-Control-Allow-Headers: Content-Type, Accept, Authorization  Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS, PATCH  Access-Control-Allow-Origin: \*  Cache-Control: private  Date: Tue, 13 Dec 2016 15:54:46 GMT  Set-Cookie: SERVERID=; Expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/  X-Performance: 656.2623 ms  X-RequestId: 974230bf-4e58-4b1e-a61a-51f6bfad0126  X-Robots-Tag: none  Content-Length: 0  Connection: keep-alive |