Vendor: DWOLLA

Website Link: https://docs.dwolla.com/#introduction

API Description:

This API will give you the ability to connect your software to banking infrastructure to move money, store funds, validate customer identities, and verify bank accounts.

Important Information:

Making requests

All requests should supply the `Accept: application/vnd.dwolla.v1.hal+json` header. `POST` requests must specify the `Content-Type: application/vnd.dwolla.v1.hal+json` header. Request and response bodies are JSON encoded.

Requests must be made over HTTPS. Any non-secure requests are met with a redirect (HTTP 302) to the HTTPS equivalent URI.

Authorization

All requests require either an OAuth access token or a `client_id` and `client_secret`. OAuth access tokens are passed via the `Authorization` HTTP header:

`Authorization: Bearer {access_token_here}`

API Host

Production: `https://api.dwolla.com`

Sandbox: `https://api-sandbox.dwolla.com`

Idempotency key

To prevent an operation from being performed more than once, Dwolla supports passing in an `Idempotency-Key` header with a unique key as the value. Multiple `POSTs` with the same idempotency key won't result in multiple resources being created. It is recommended to use a random value for the idempotency key, like a UUID (i.e. - `Idempotency-Key: d2adcbab-4e4e-430b-9181-ac9346be723a`).

Copyright 2019 - Michigan Health Information Network Shared Services

For example, if a request to initiate a transfer fails due to a network connection issue, you can reattempt the request with the same idempotency key to guarantee that only a single transfer is created.

If you reattempt a POST request with the same value for the Idempotency-Key, rather than creating new or potentially duplicate resources, you will receive a 201 Created, with the original response of the created resource. If the Dwolla server is still processing the original POST request, you will receive a 409 Conflict error response on the subsequent request. Idempotency keys are intended to prevent conflicts over a short period of time, therefore keys will expire after 24 hours.

DISCLAIMER: In addition to our Terms of Service, third parties' terms may apply to your participation in the Connectathon, such as Github's Terms of Use. Please be aware that while our Terms are our full agreement with you, other parties' terms govern their relationship with you. These may include acceptable use policies, rights to use content, API terms and intellectual property.

MiHIN and our licensors, vendors, agents, and/or our content providers retain ownership of all intellectual property rights of any kind related to our site and service. We reserve all rights that are not expressly granted to you under our Terms of Service or by law. You may not duplicate, copy, or reuse any portion of the HTML/CSS, Javascript, or visual design elements or concepts without express written permission from MiHIN. If you'd like to use MiHIN's trademarks, you must follow all of our trademark guidelines.

MiHIN respects the intellectual property rights of others. We are providing links to open application programming interface (API) resources for your convenience. We do not have control over that content and any use will be at your own risk. Please read all terms and conditions prior to accepting and using the API.

Copyright 2019 - Michigan Health Information Network Shared Services