OIDC連携実装ガイド

Digital Platformer 株式会社

2022/07/22 Ver0.2

DP社OIDC連携実装ガイドについて

- DP社の提供するDIDサーバーサービス（MyDID)では認証にOpenIDConnect（OIDC)を利用してユーザーIDや個人情報などを一元管理することができます。
- ここではID連携を利用する場合に考慮しておくべきことを簡単に説明します。
  ①ユーザーIDを作成する
  ②作成したユーザーIDをOpenID Connect利用して認証する
  について案内いたします。
  なお、ご自身のシステムに組み込むためには別途API資料と接続方式に関する資料をご覧ください。
  ✳ **＊開発途中のものであり、変更される場合があります。**

OpenID Connectで提供する機能一覧

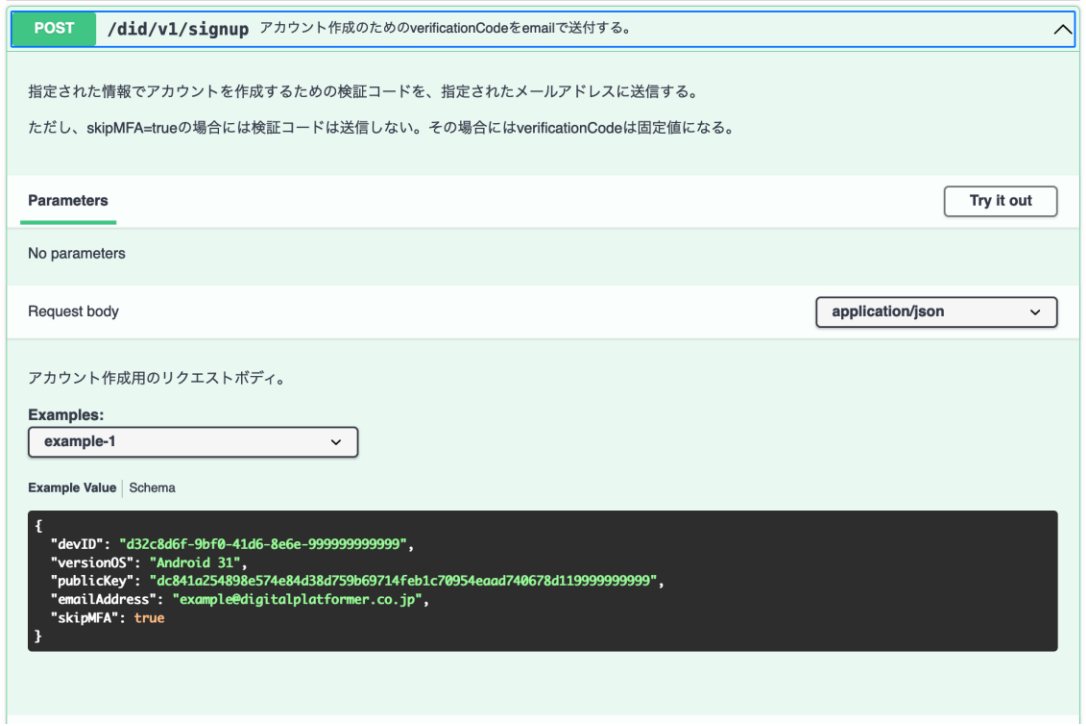
- アカウント作成とverificationCodeをemailで送付する機能
- メールアドレスの検証を行いアカウントを作成する機能とパスワード初期化
- DIDサービスへのログインとAPI認証用トークンを取得機能
- API認証用トークンを更新する機能
- パスワードリセットおよびメールアドレスリセット機能
- 認証されたユーザの個人情報を登録・更新する機能
- 登録済みユーザの個人情報を取得する機能

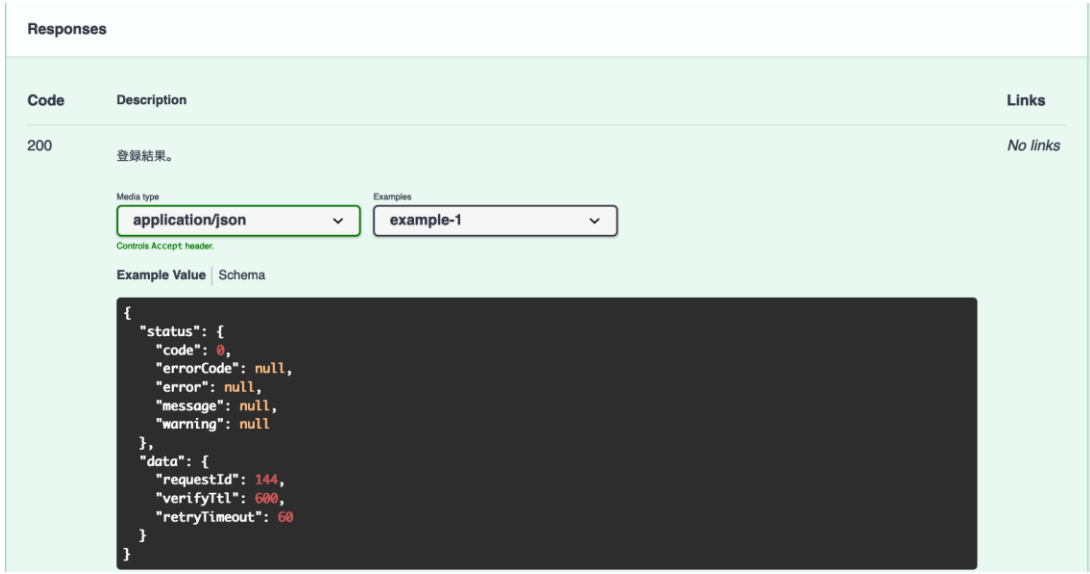
ユーザーIDの作成

- ユーザーIDを作成するには
  利用したいアプリケーションからOIDCエンドポイントに対して
  httpsによるPOST通信を行います。Content-typeは
  application/jsonとし、POST Bodyに
  - "devID": "string",
  - "versionOS": "string",
  - "publicKey": "string",
  - "emailAddress": "user@example.com",
  - "skipMFA": true

を指定します。
ただしユーザーID作成処理に関しては当社が「ユーザーID作成用MyDIDクライアントアプリ（Android/iOS用)仮称」を用意いたしますので、実際には組み込む必要はありません。

ユーザーID作成リクエストAPIとレスポンス例



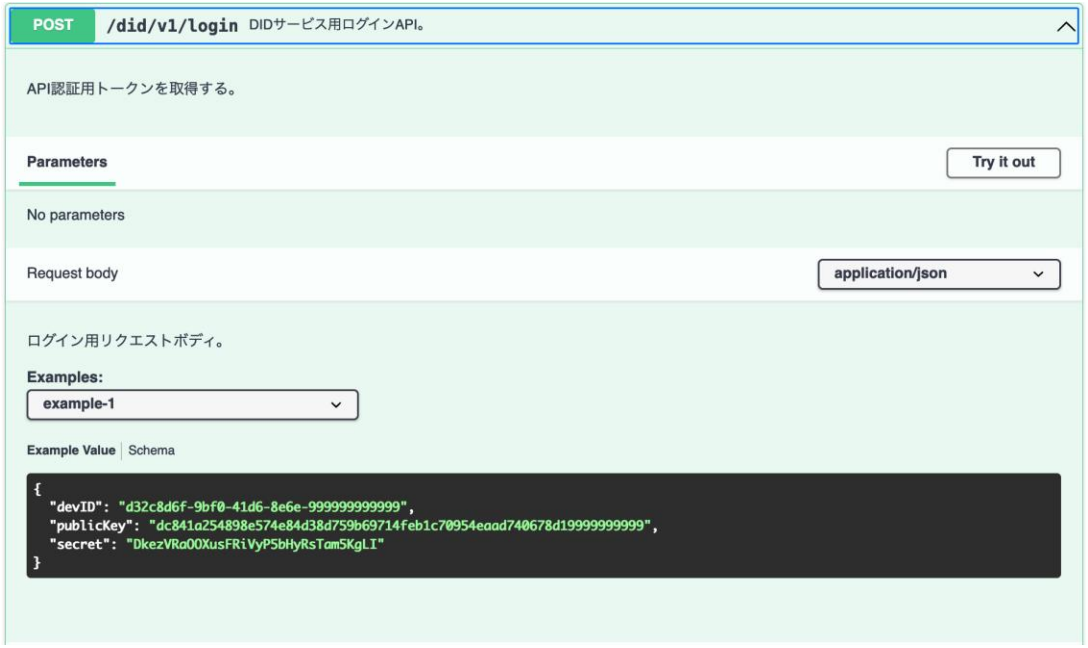


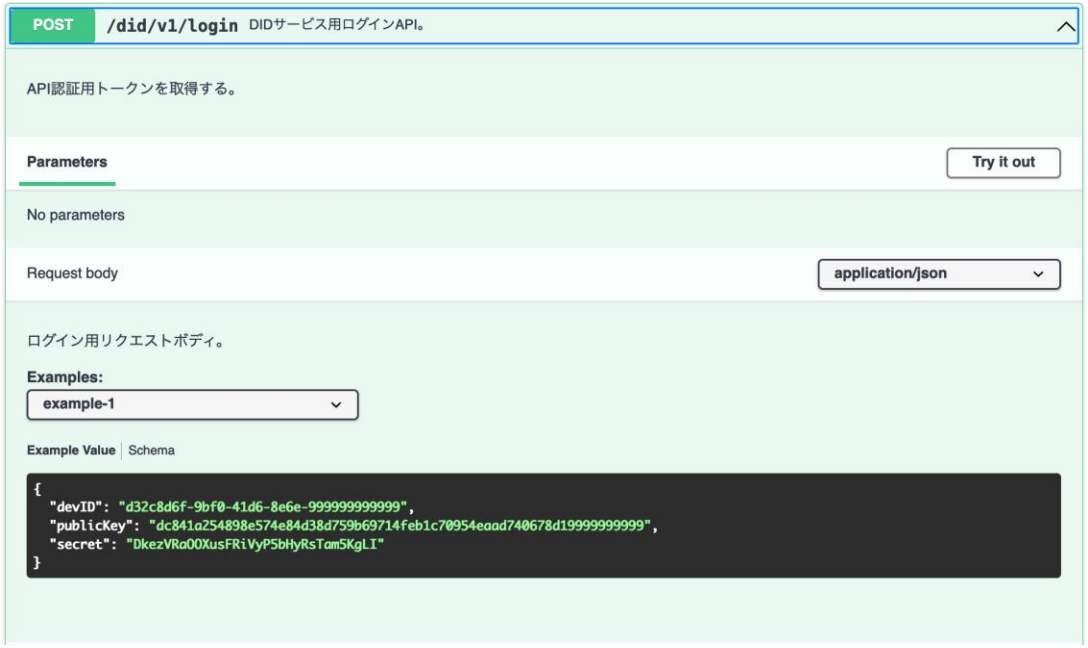
作成したユーザーIDをOpenID Connect利用してアプリで認証する

- MyDIDから受け取ったトークンを利用して認証や個人情報の取得などを行います。

1. MyDID側で用意するログイン用のエンドポイント(Web URL)を利用したいアプリ・サービスで表示させて、ユーザーID作成時に登録したユーザーIDとパスワードの入力し実行してください
2. ログイン失敗時は「ユーザーIDまたはパスワードが異なっている」旨の結果が得られますので、再入力などを促してください
    1. もしユーザー登録がまだの場合はユーザー登録用アプリのダウンロードと実行を促してください
3. 成功すると①AccessToken（認証情報）、②IDToken（個人情報）、③RefreshToken（有効期限を超えた場合に利用する）を受け取ることができますので、①AccessToken（認証情報）を利用して認証処理を行います
4. 受け取った①AccessToken（認証情報）をMyDIDで用意するエンドポイント（Web URL）に送信すれば、正しいAccessTokenでユーザーIDが正しい情報かを判別し認証を行います
5. 認証の成功後は利用中のログインセッション管理機構を利用して有効なログイン中であるか検証の上アプリ上での処理を継続ください

ログインリクエストAPIとレスポンス例





その他API

- 本ドキュメントではMyDIDで用意しているOpenIDConnectでのユーザーIDの作成とログイン認証について簡単に記述しましたが、その他のAPIに関しては後日提供いたします。
- また本APIに関しては開発中のものとなっていますので変更が発生する場合があります。

追加参考情報

OIDC**とは？**ID Federation　2021/11/22
OpenID Connect**による**ID**連携**
https://www.alpha.co.jp/blog/202111_02

IDトークンとは？アクセストークンとは？どのタイミングでとのような内容のやり取りがされるか？
https://qiita.com/TakahikoKawasaki/items/498ca08bbfcc341691fe

リフレッシュトークンとは？御社の場合どのタイミングでとのような内容のやり取りがされるか？
https://qiita.com/TakahikoKawasaki/items/185d34814eb9f7ac7ef3

OIDC標準のユーザー属性クレーム群
https://qiita.com/TakahikoKawasaki/items/8f0e422c7edd2d220e06

- DP社オリジナルの拡張クレーム名に関しては最新情報をDP社へご確認ください。