OAuth 2.0 Client Intermediary Metadata

oauth-client-intermediary-metadata-03

Aaron Parecki

Virtual Interim Meeting
March 29, 2021

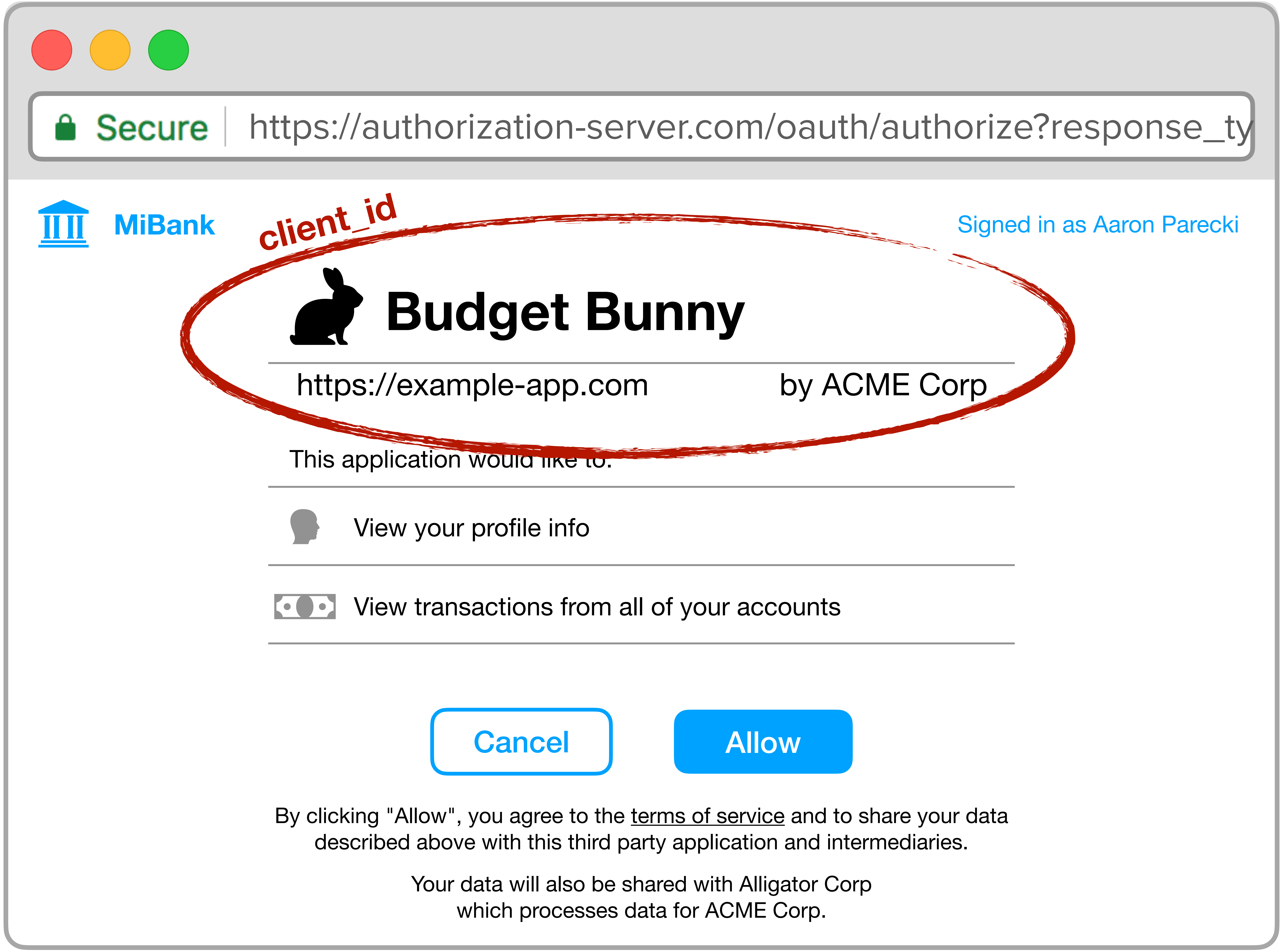
Client Intermediary Metadata

Extends **Dynamic Client Registration** to provide additional properties that describe one or more intermediaries the user's data may be shared with or through when using the client

```
POST /register
{
 ...
 "intermediaries": [{
     "name": "Partner Application",
     "uri": "https://partner.example",
     "logo_uri": "https://partner.example/logo.png"
     ...
  }]
}
```

Client Intermediary Metadata

Authorization servers that support Client Intermediary Metadata are expected to display the intermediary information on the OAuth consent screen



https://authorization-server.com/oauth/authorize?response_ty

Signed in as Aaron Parecki

Budget Bunny

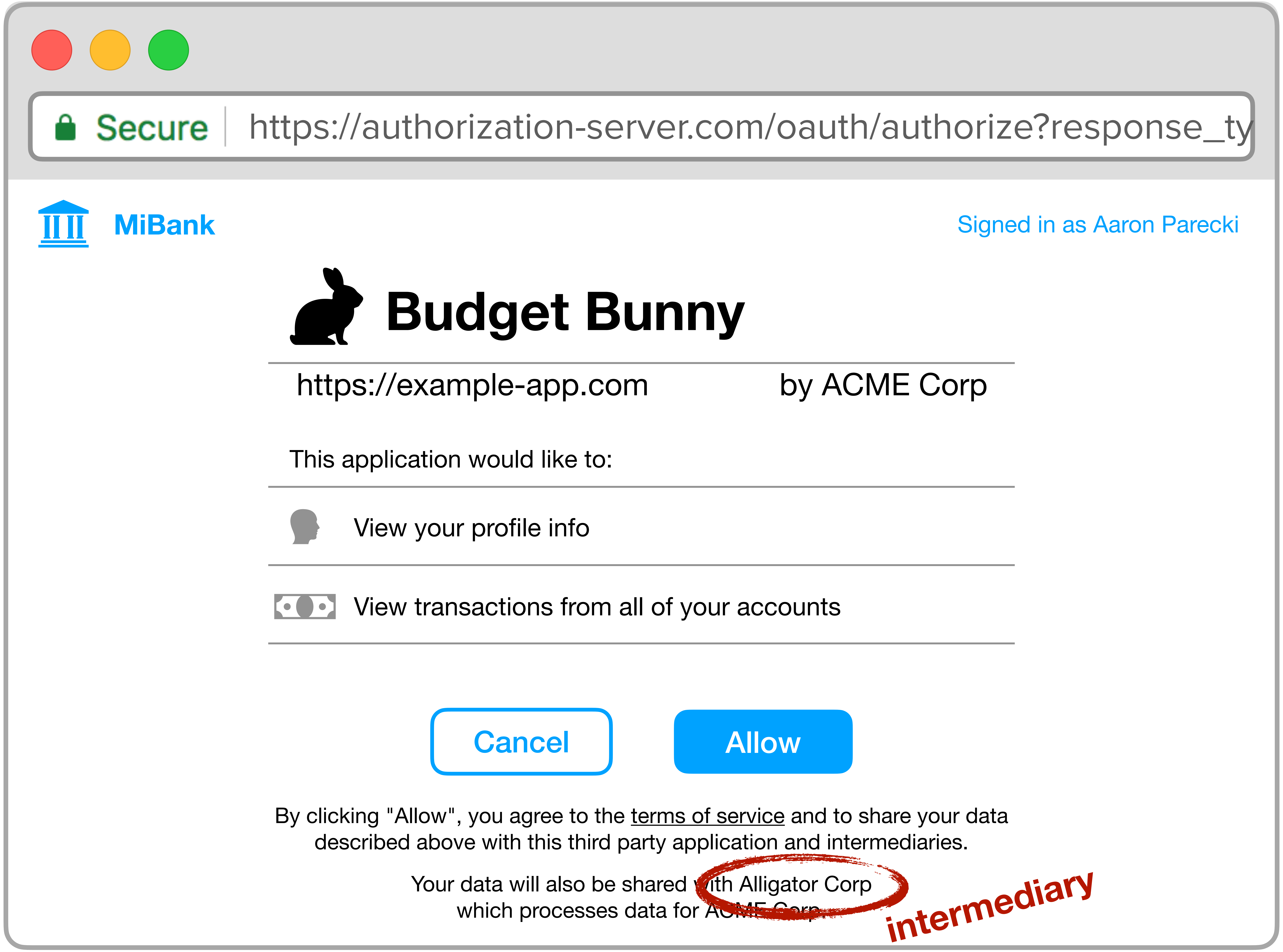
https://example-app.com by ACME Corp

This application would like to:

- View your profile info
- View transactions from all of your accounts

By clicking "Allow", you agree to the terms of service and to share your data described above with this third party application and intermediaries.

Your data will also be shared with Alligator Corp
which processes data for ACME Corp.



https://authorization-server.com/oauth/authorize?response_ty

MiBank

Signed in as Aaron Parecki

Budget Bunny

https://example-app.com by ACME Corp

This application would like to:

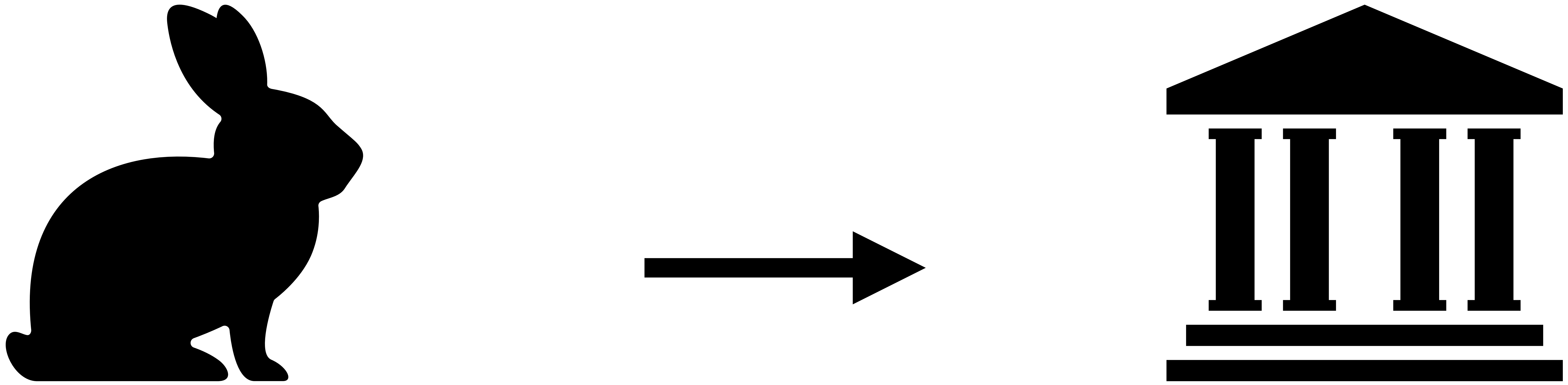
- View your profile info
- View transactions from all of your accounts

By clicking "Allow", you agree to the terms of service and to share your data described above with this third party application and intermediaries.

Your data will also be shared with Alligator Corp
which processes data for ACME Corp.

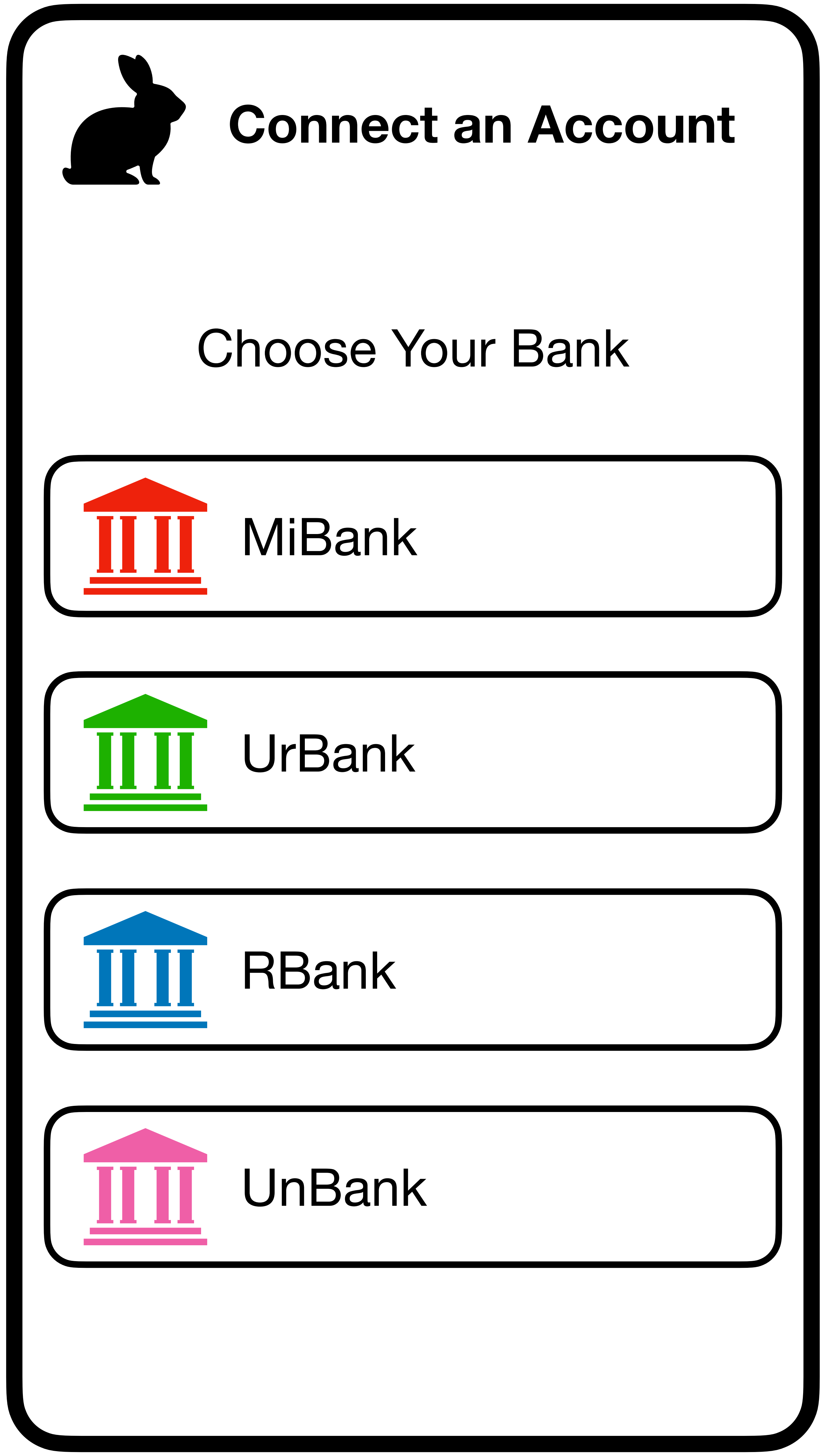
intermediary

In the traditional OAuth model, the client is represented by a `client_id` established at the OAuth authorization server



OAuth Client

Bank API



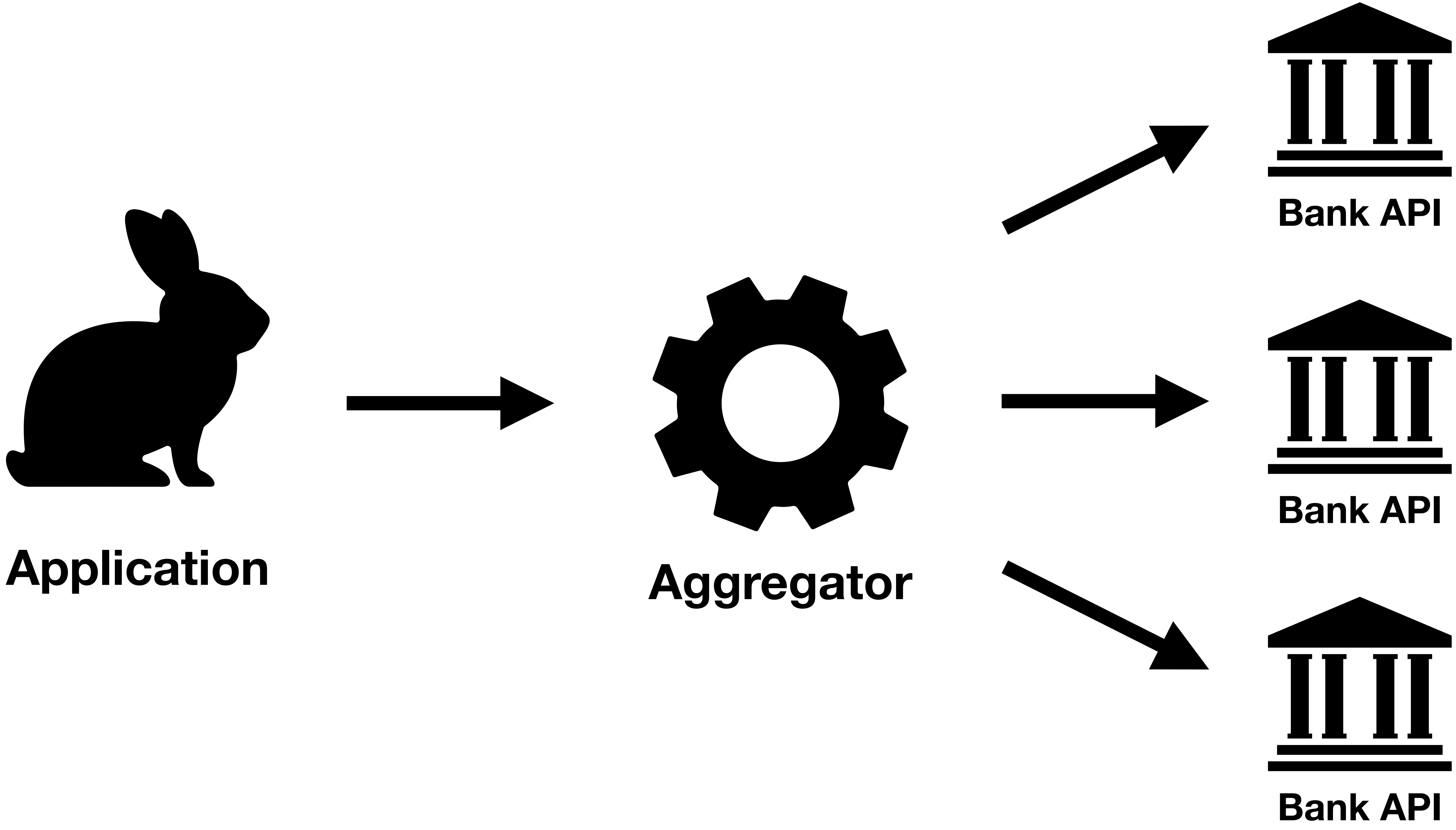
Connect an Account

Choose Your Bank

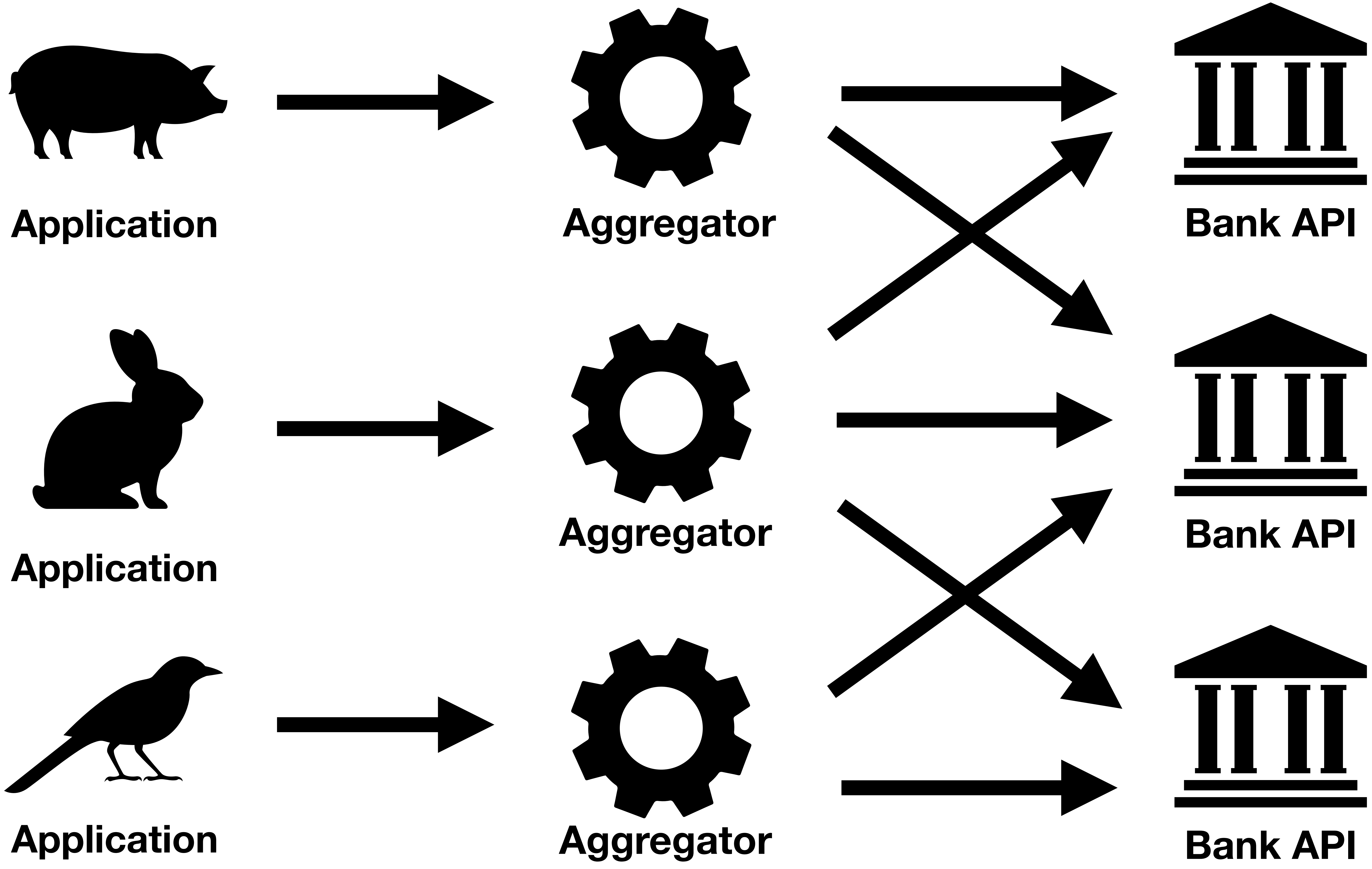
- MiBank
- UrBank
- RBank
- UnBank

In the financial world, the client may be talking to many different banks, each with their own authorization server

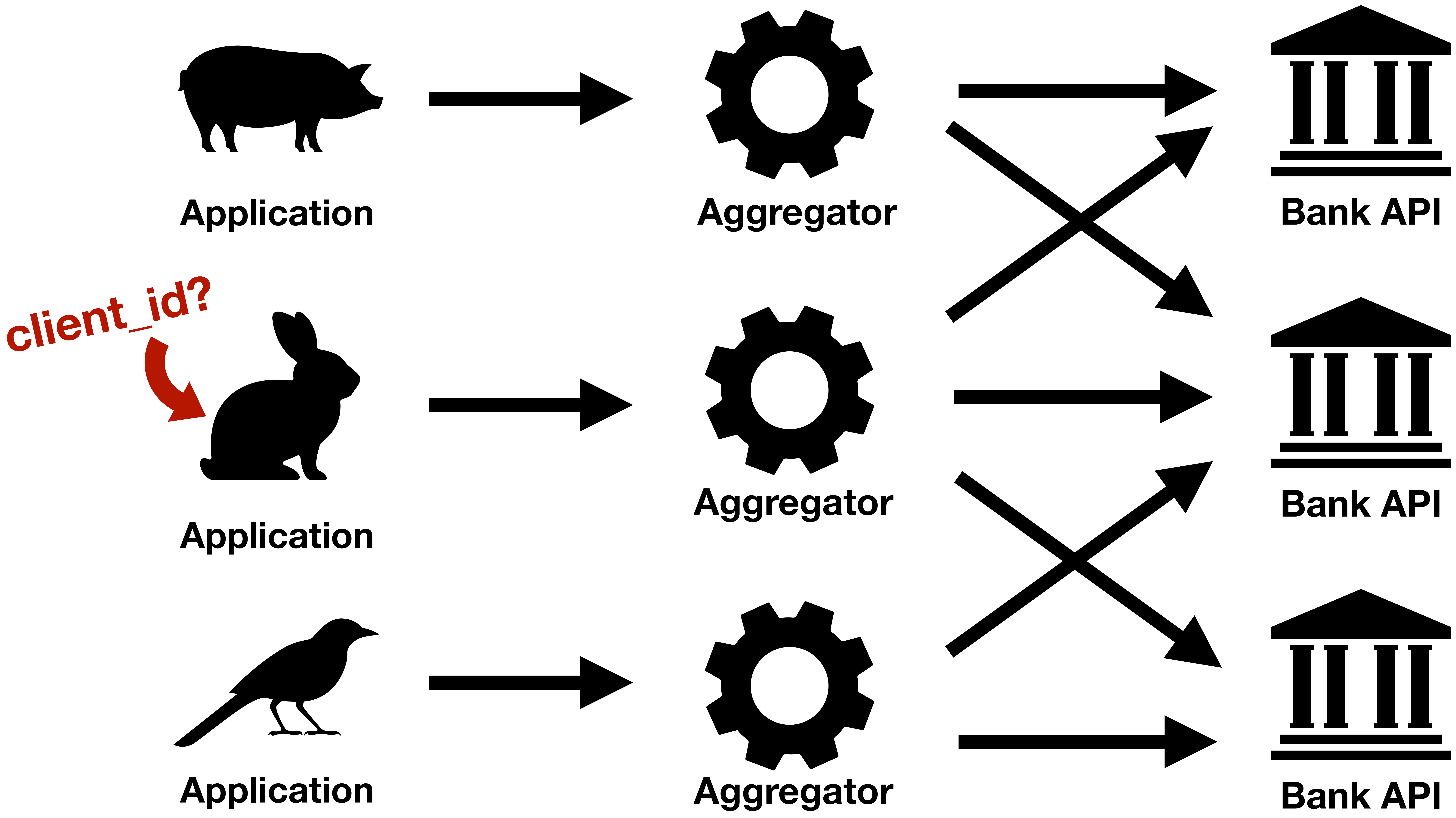
In practice, the application talks to a single aggregator API which has relationships with many banks



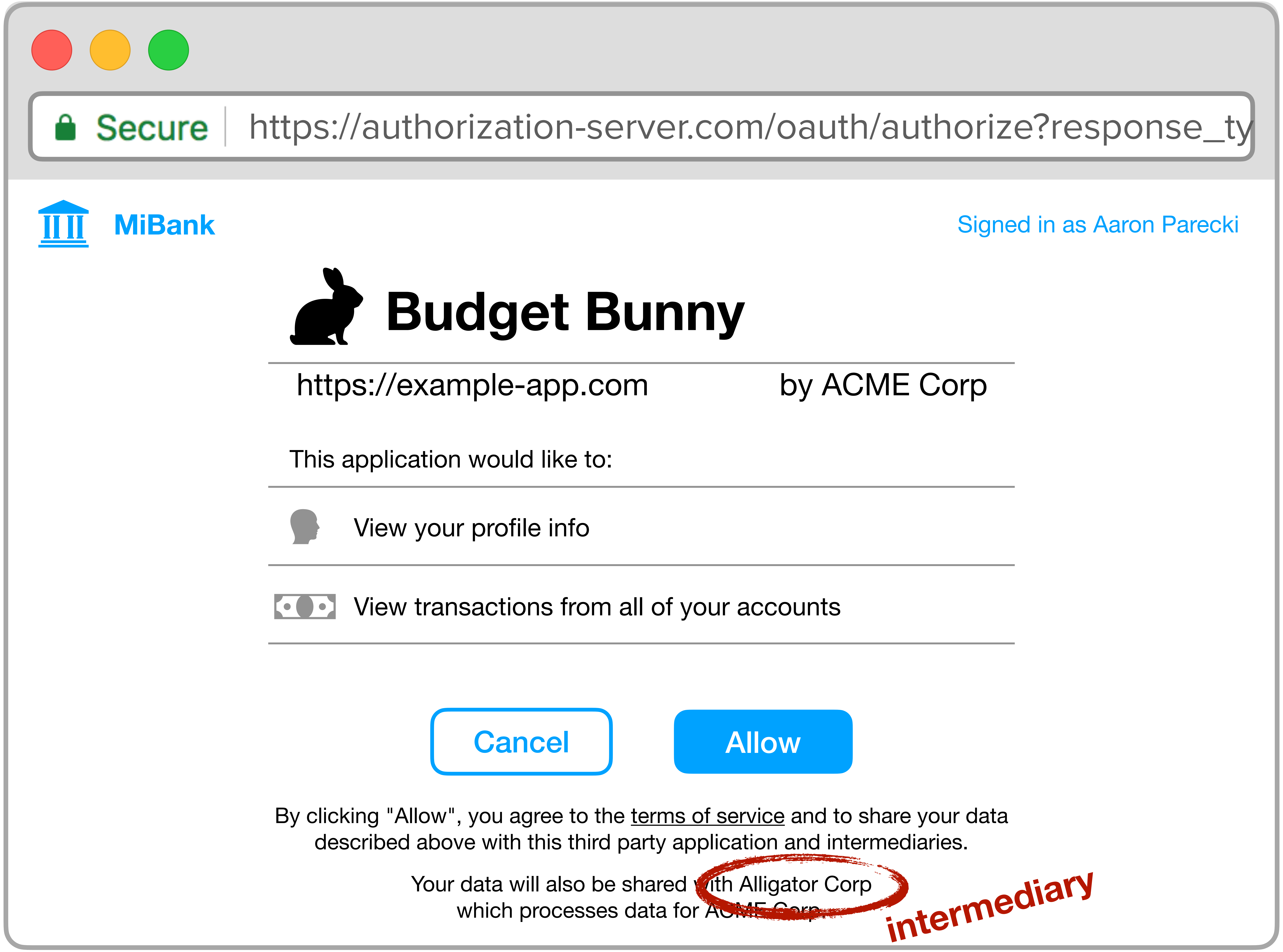
The banks sign contracts with aggregator companies, and the banks don't actually have a relationship with the application directly



The banks sign contracts with aggregator companies, and the banks don't actually have a relationship with the application directly



Banks want to ensure the user is informed and has agreed to share their data with the end user application as well as any intermediaries that may be processing their data



https://authorization-server.com/oauth/authorize?response_ty

MiBank

Signed in as Aaron Parecki

Budget Bunny

https://example-app.com by ACME Corp

This application would like to:

- View your profile info
- View transactions from all of your accounts

By clicking "Allow", you agree to the terms of service and to share your data described above with this third party application and intermediaries.

Your data will also be shared with Alligator Corp
which processes data for ACME Corp.

A single Dynamic Client Registration request establishes the end user application as well as the list of intermediaries that will have access to the user's data by using this application

FINANCIAL™
DATA EXCHANGE

The Financial Data Exchange (FDX) is a nonprofit organization that is dedicated to unifying the financial industry around a common, interoperable and royalty-free standard for the secure access of user permissioned financial data.

financialdataexchange.org

FINANCIAL™
DATA EXCHANGE

FDX builds on OAuth and FAPI, adding extensions when needed

financialdataexchange.org

Client Intermediary Metadata

https://tools.ietf.org/html/draft-parecki-oauth-client-intermediary-metadata-03