

OAuth 2.0 Client Intermediary Metadata

oauth-client-intermediary-metadata-00

Aaron Parecki

IETF 106 • Singapore
November 21, 2019



 **Secure** | 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

Cancel

Allow

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



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



Signed in as Aaron Parecki

client_id



Budget Bunny

https://example-app.com

by ACME Corp

This application would like to:



View your profile info



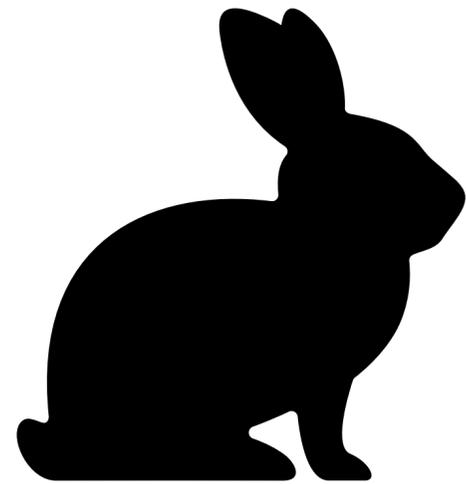
View transactions from all of your accounts

Cancel

Allow

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

This works fine when the end user application registers a `client_id` directly with the OAuth API



**End User
Application**



Bank API



Connect an Account

Choose Your Bank



MiBank



UrBank

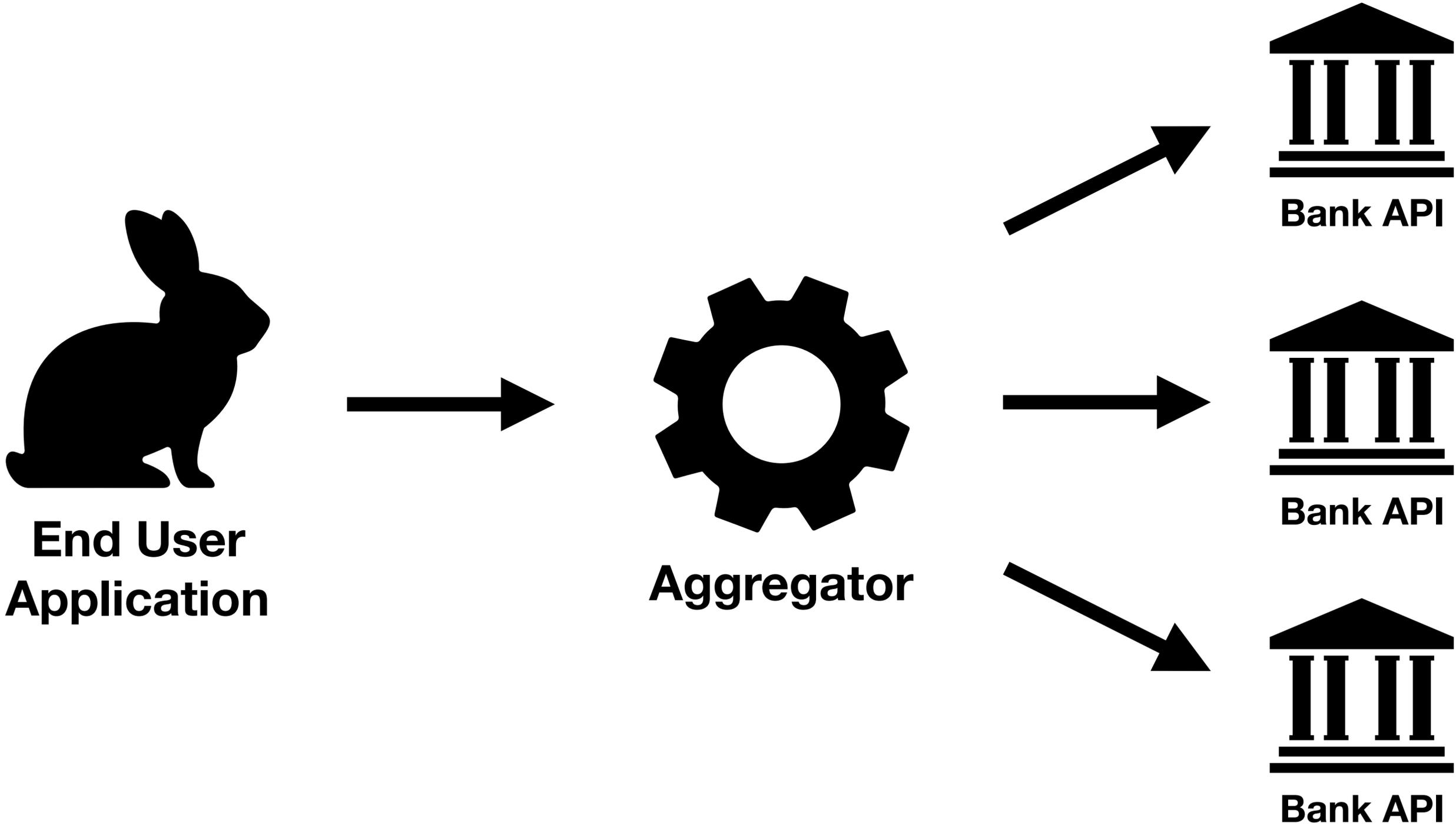


RBank

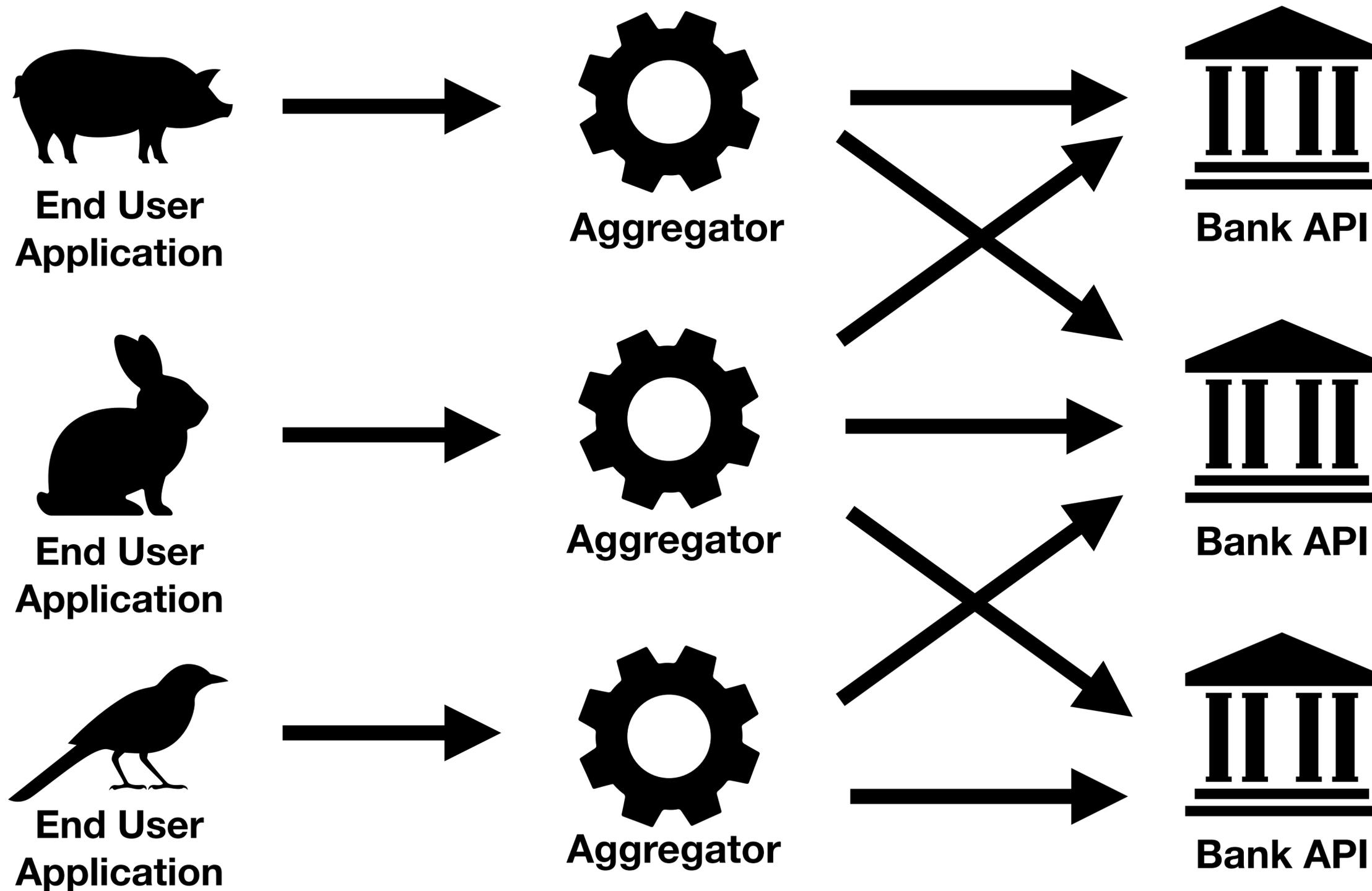


UnBank

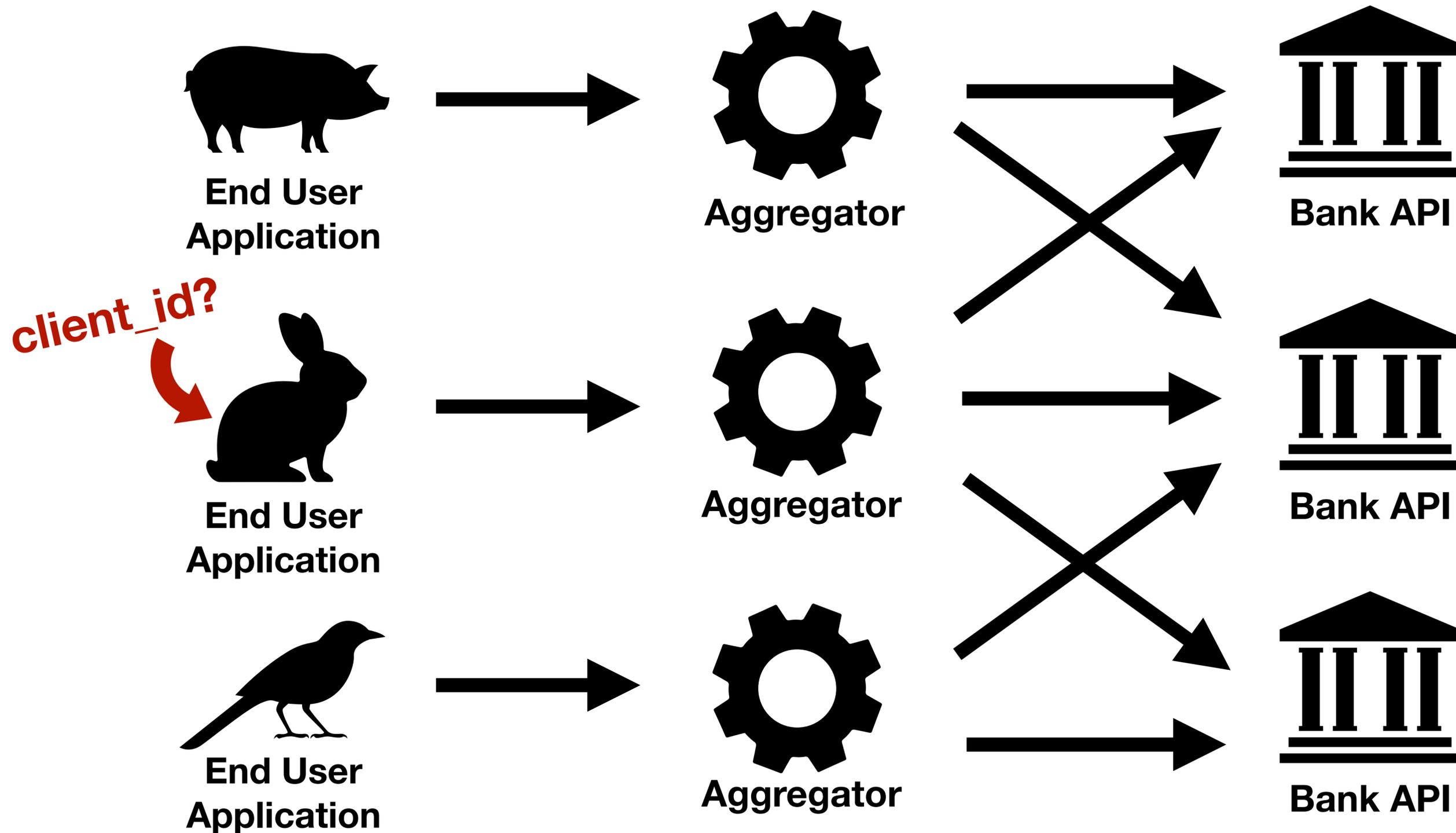
In reality, the end user application talks to a single aggregator API which has relationships with many banks



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

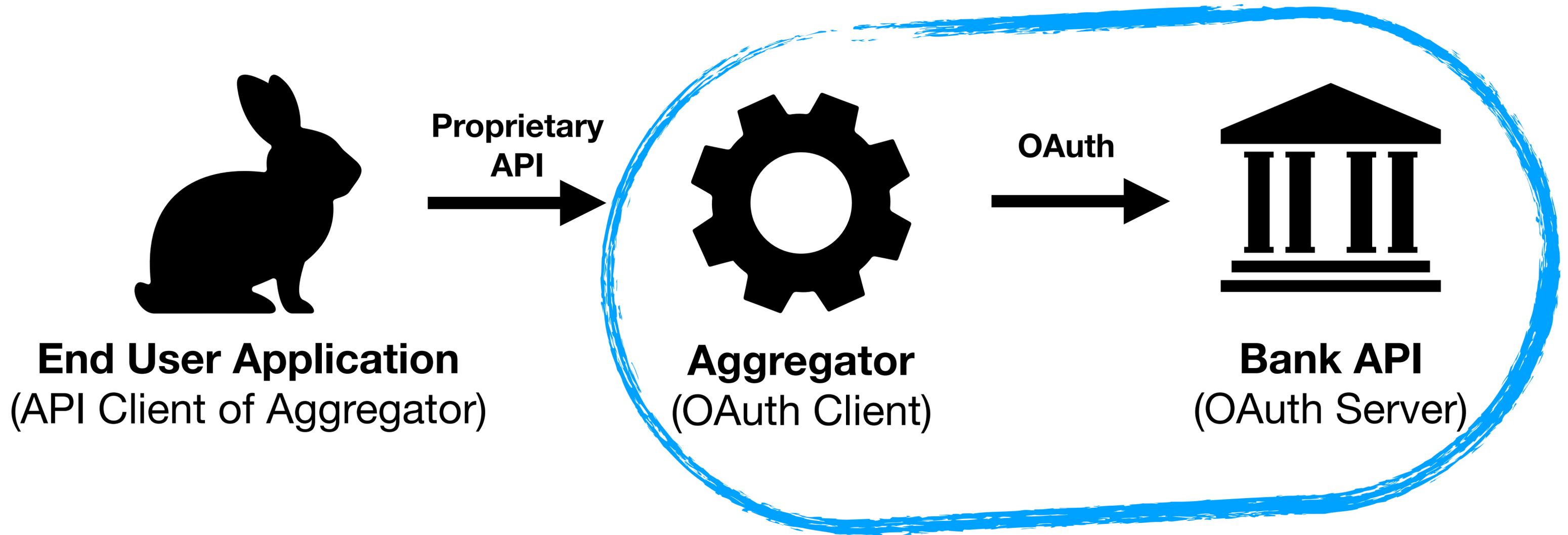


The banks sign contracts with aggregator companies, and don't actually have a relationship with the end user application



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

In practice, effectively an aggregator is acting on behalf of many end user applications





Secure | 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

Cancel

Allow

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

Client Intermediary Metadata

Extends **Dynamic Client Registration** to provide additional properties that describe one or more intermediaries acting on behalf of the client

```
POST /register
{
  ...
  "end_user_application": {
    "name": "Budget Bunny",
    "uri": "https://example-app.com/logo.png"
  },
  "intermediaries": [{
    "name": "Partner Application",
    ...
  }]
}
```

Client Intermediary Metadata

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

Client Intermediary Metadata

<https://tools.ietf.org/html/draft-parecki-oauth-client-intermediary-metadata-00>