## OAuth 2.0 Client Intermediary Metadata oauth-client-intermediary-metadata-00

Aaron Parecki

IETF 107 • Virtual Interim Meeting May 11, 2020

Secure	https://authorization-se
<b>MiBank</b>	
	Budget B
	https://example-app.co
	This application would like to:
	View your profile info
	••••• View transactions from
	Cancel By clicking "Allow", you agree to data described above wit

erver.com/oauth/authorize?response\_ty

Signed in as Aaron Parecki

#### Sunny

by ACME Corp )m

all of your accounts



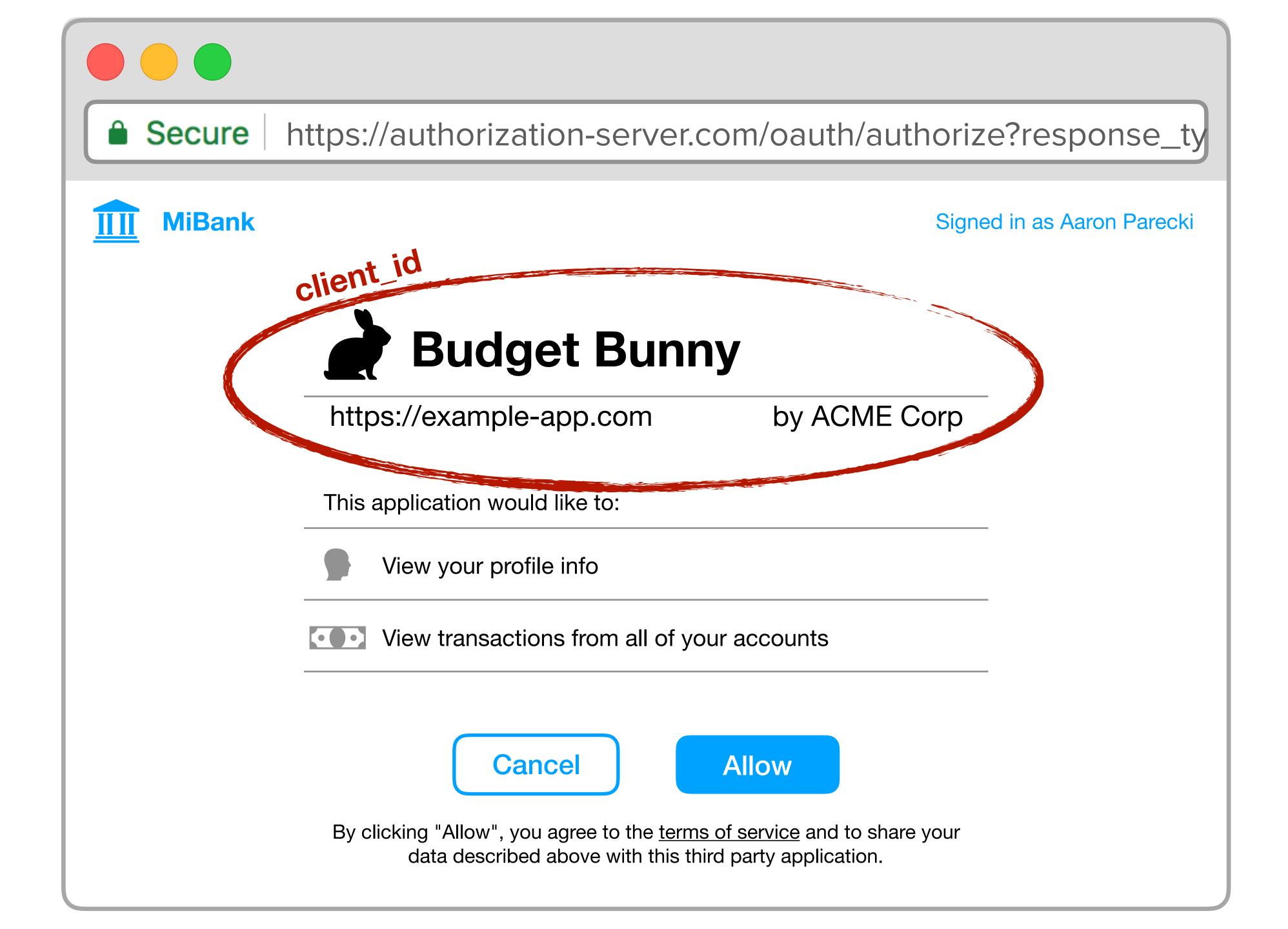
the terms of service and to share your ith this third party application.

	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

Aaron Pa

ന
-
g
0
g
+
Φ
2

ntermediary
Client
2.0
uth



	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

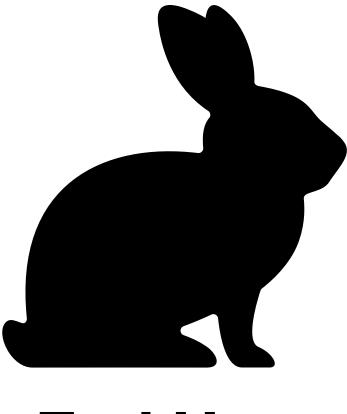
Aaron P

g
at
J
B
<u></u>
Φ
$\mathbf{C}$

С
Q
Φ
Ц Ц
Ţ
Jt
Ð
$\bigcirc$
0
$\mathcal{O}$
C
Ŧ
. <del>.</del> .

**O**A

## This works fine when the end user application registers a client\_id directly with the OAuth API



#### End User Application



#### **Bank API**

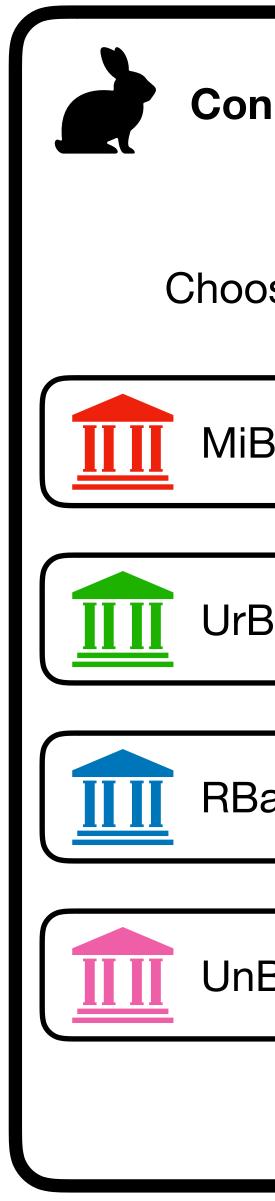
	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

Aaron Pa

ца
<u>a</u>
aC
et
$\geq$
$\geq$

g
$\overline{\mathbf{O}}$
Ū
L
()
Ť
1 L
<b>D</b>
$\cup$
$\bigcirc$
$\sim$
- <b></b>

**V** 



nect an Account	
se Your Bank	
Bank	
Bank	
ank	
Bank	

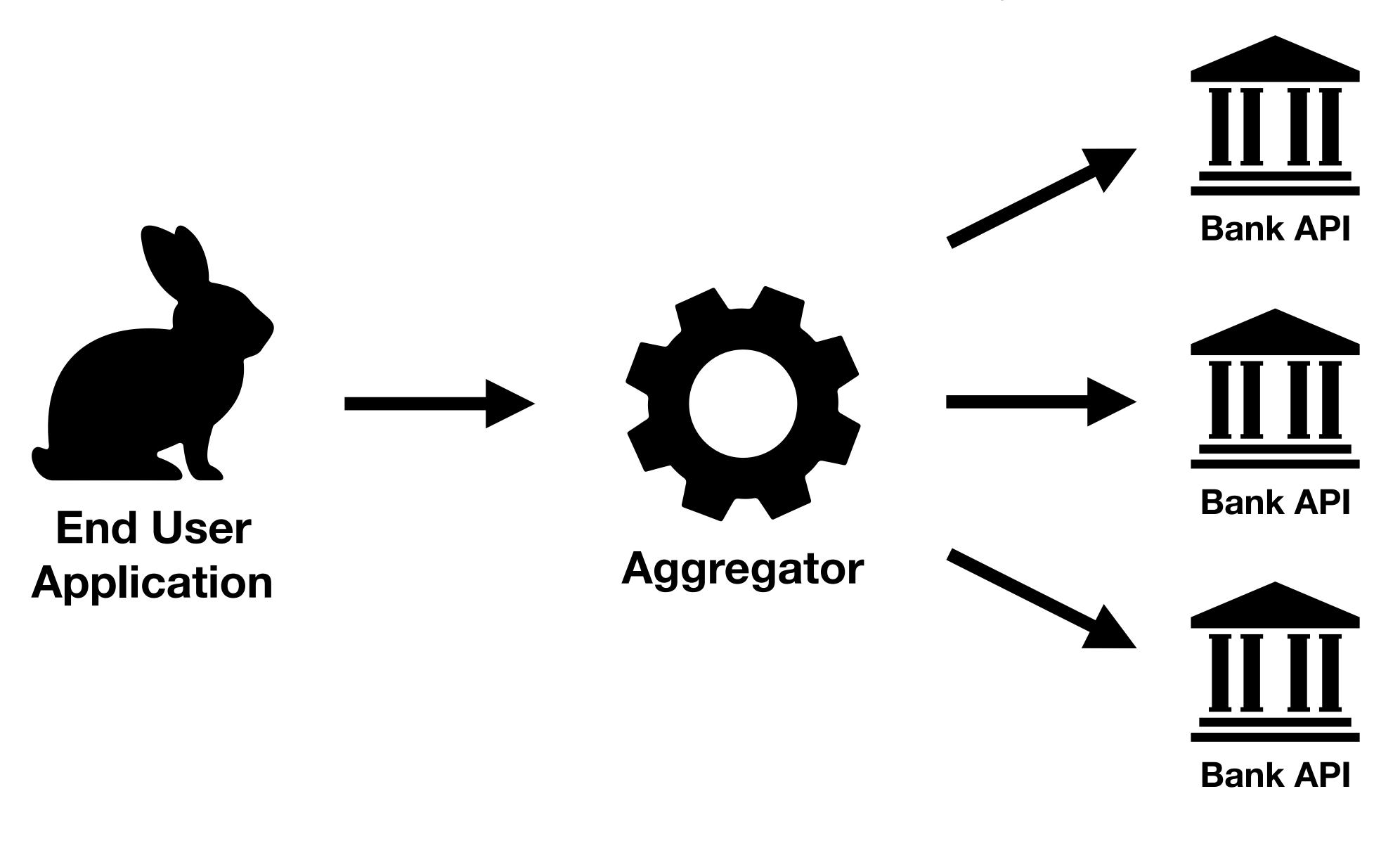
	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

Aaron Pa

ന
-
g
0
g
+
Φ
2

$\geq$
Intermediary
Client
2.0
uth

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



	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

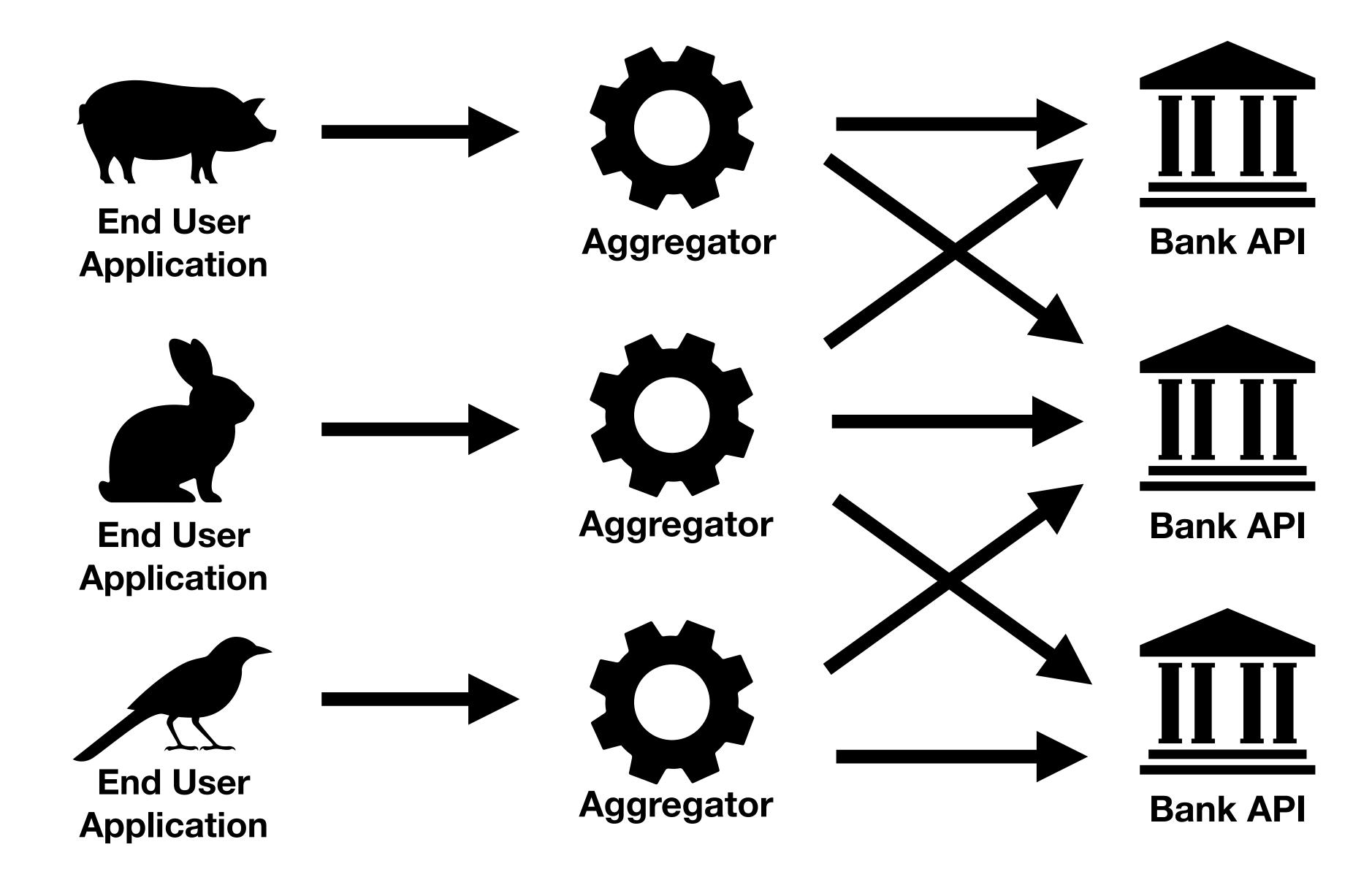
Aaron Pa

ന
-
g
0
g
+
Φ
2

2
$\geq$
C'
T
Q
Ð
Ē
Ш
Ψ
Jte
1
(1)
()
$\bigcirc$
$\sim$
Ţ
<u> </u>

**N** 

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



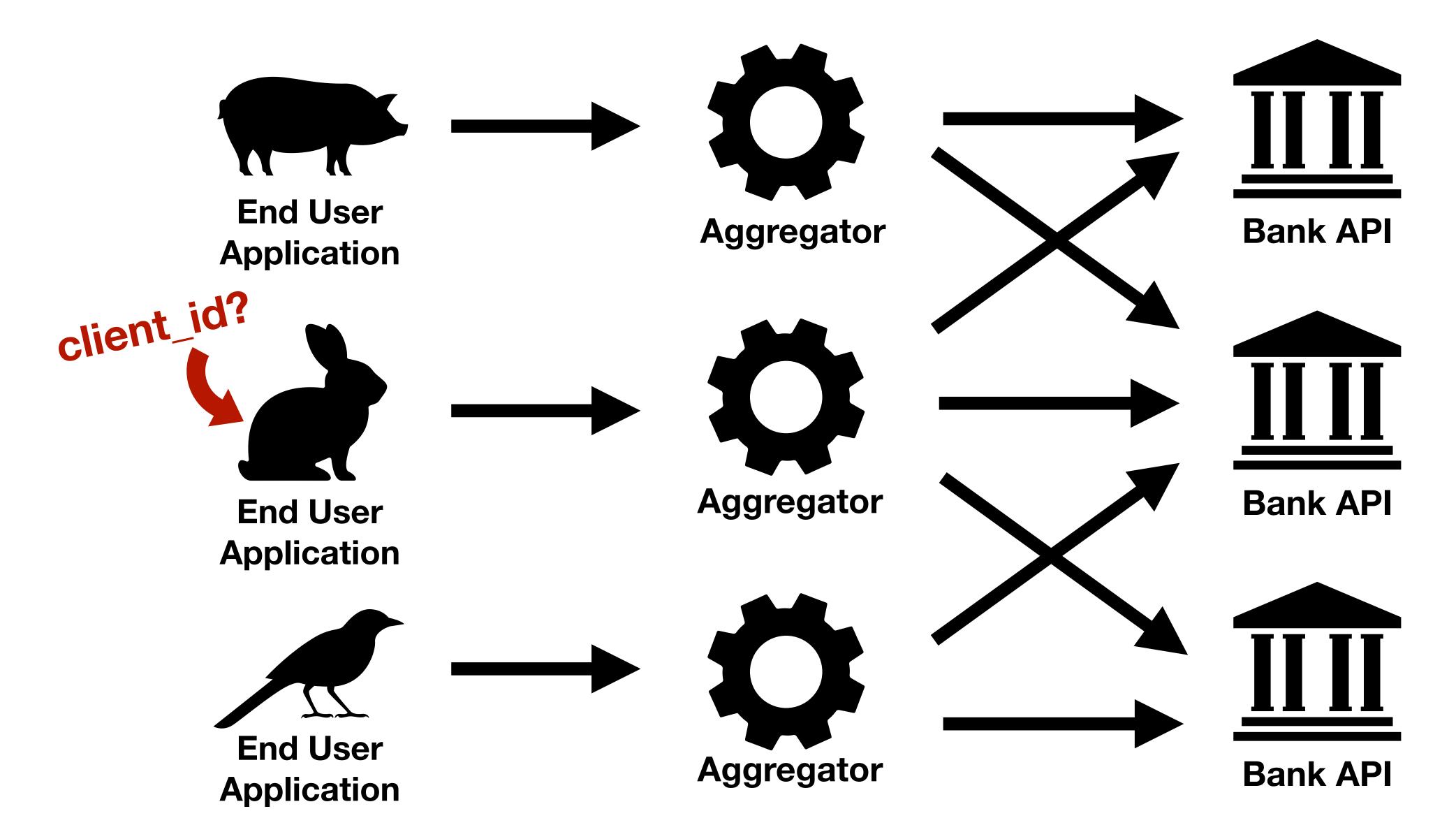
	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

Aaron P

ita
σ
J
g
<b>+</b>
Φ
2
$\geq$

	Σ		
	C	C	5
	_		
	C		5
	d	ľ	)
	2		
	2		
	Ļ		-
	Q	Ľ	)
-	H	-	J
	C		
			i.
-	+		J
	Ω		
	0	Ľ	)
	_		_
(			)
C			)
C		(	l
1		1	
	C		
	į.		,
			5
	-		

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



	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

Aaron P

ita
σ
J
g
<b>+</b>
Φ
2
$\geq$

	Σ		
	C	C	5
	_		
	C		5
	d	ľ	)
	2		
	2		
	Ļ		-
	Q	Ľ	)
-	H	-	J
	C		
			i.
-	+		J
	Ω		
	0	Ľ	)
	_		_
(			)
C			)
C		(	l
1		1	
	C		
	į.		,
			5
	-		

#### **End User Applications**



















https://www.businesswire.com/news/home/20200416005151/en/Charles-Schwab-Reinforces-Commitment-Customer-Data-Protection https://www.prnewswire.com/news-releases/microbilt-joins-financial-data-exchange-301003933.html

https://www.fidelity.com/bin-public/060\_www\_fidelity\_com/documents/press-release/akoya-independent-company-022020.pdf

https://newsroom.wf.com/press-release/innovation-and-technology/wells-fargo-and-plaid-sign-data-exchange-agreement

https://www.finicity.com/usbank-direct-data-announcement/

https://www.prnewswire.com/news-releases/envestnet--yodlee-and-jpmorgan-chase-sign-data-agreement-to-enhance-consumer-data-protections-bolster-overall-data-connectivity-and-reliability-300969708.html https://www.usbank.com/newsroom/stories/us-bank-and-fiserv-sign-agreement-to-simplify-data-exchange-between-customers-and-applications.html

#### Aggregators

#### **Banks**

## Yodlee

# Finicity

## PLAID

#### S NINTH WAVE"



## CHASE ( **Usbank**®





**BANK OF AMERICA** 



*charles* SCHWAB

# **IETF 107 Virtual Interim**

Aaron Parecki

g
<u>a</u>
ad
et e
Š

## 0 Client Intermediary I $\sim$ OAuth



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

	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

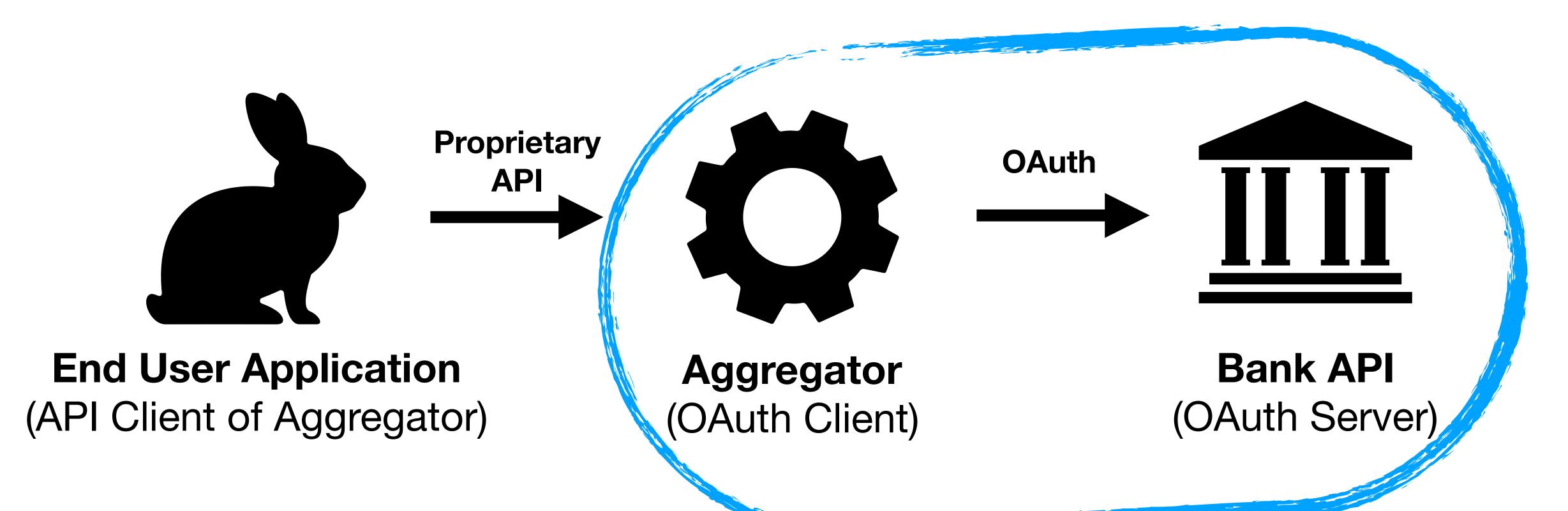
Aaron Pa

ന
-
g
0
g
+
Φ
2

>
$\sim$
(U)
$\overline{\mathbf{O}}$
Ň
Ψ
<u> </u>
Û
Ц.
<u> </u>
_
(1)
()
$\bigcirc$
$\bigcirc$
<u> </u>
$\overline{\mathbf{n}}$
L L

**AO** 

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



# **IETF 107 Virtual Interim** Aaron Parecki •

ന
<u></u>
g
σ
g
<b></b>
Ð
~

# 0 Client Intermediary N OAuth 2

Secure	https://authorization-se
<b>MiBank</b>	
	Budget B
	https://example-app.cc
	This application would like to:
	View your profile info
	•••• View transactions from
	Cancel By clicking "Allow", you agree to the
	described above with this third Your data will also be which processes

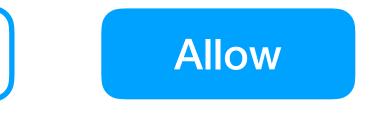
#### erver.com/oauth/authorize?response\_ty

Signed in as Aaron Parecki

### Bunny

om by ACME Corp :

n all of your accounts



ne <u>terms of service</u> and to share your data I party application and intermediaries.

e shared with Alligator Corp s data for ACME Corp Intermediary

	┢
-	
	በ
	<u> </u>
1	Ě
_	
-	
	ιU
÷	
7	>
1	
ľ	
5	
C	
1	
٦	
i.	
L	_
ĩ	
ŀ	
î.	1.1
L	ш
-	
	$\checkmark$
	$\bigcirc$
	ă
	U
	$\overline{}$
	_
	$\sigma$

Aaron Pa

ata
g
eta
Ř
$\geq$

g
$\nabla$
Φ
Φ
_
Jt
Ð
$\bigcirc$
$\frown$

OAL

## **Client Intermediary Metadata**

## 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",
  . . .
```

Extends **Dynamic Client Registration** to provide additional properties that

	_
	-
	_
	(1)
	4
1	
	$\Box$
_	
-	
	$\sigma$
	-
2	$\sim$
5	
_	>
ľ	
I.	
(	
_	
L	
ĩ	
ŀ	
î.	1.1
Ļ	_
-	
	•
-	
_	$\leq$
1	~
	$\cup$
	<b>(</b> )
	$\mathbf{x}$
	$(\mathbf{U})$

Aaron P

ന
-
g
0
g
+
Φ
2

## Client Intermediary I 0 OAuth 2

## **Client Intermediary Metadata**

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

	_
	-
	_
	(1)
	4
1	
	$\Box$
_	
-	
	$\sigma$
	-
2	$\sim$
5	
_	>
ľ	
I.	
(	
_	
L	
ĩ	
ŀ	
î.	1.1
Ļ	_
-	
	•
-	
_	$\leq$
1	~
	$\cup$
	<b>(</b> )
	$\mathbf{x}$
	$(\mathbf{U})$

Aaron Pa

ന
-
g
0
g
+
Φ
2

## 0 Client Intermediary [ OAuth 2

## **Client Intermediary Metadata**

https://tools.ietf.org/html/draft-parecki-oauth-client-intermediary-metadata-01

	_
	-
	_
	(1)
	4
1	
	$\Box$
_	
-	
	$\sigma$
	-
2	$\sim$
5	
_	>
ľ	
I.	
(	
_	
L	
ĩ	
ŀ	
î.	1.1
Ļ	_
-	
	•
-	
_	$\leq$
1	~
	$\cup$
	<b>(</b> )
	$\mathbf{x}$
	$(\mathbf{U})$

Aaron Pa

ന
-
g
0
g
+
Φ
2

## Client Intermediary I 0 OAuth 2