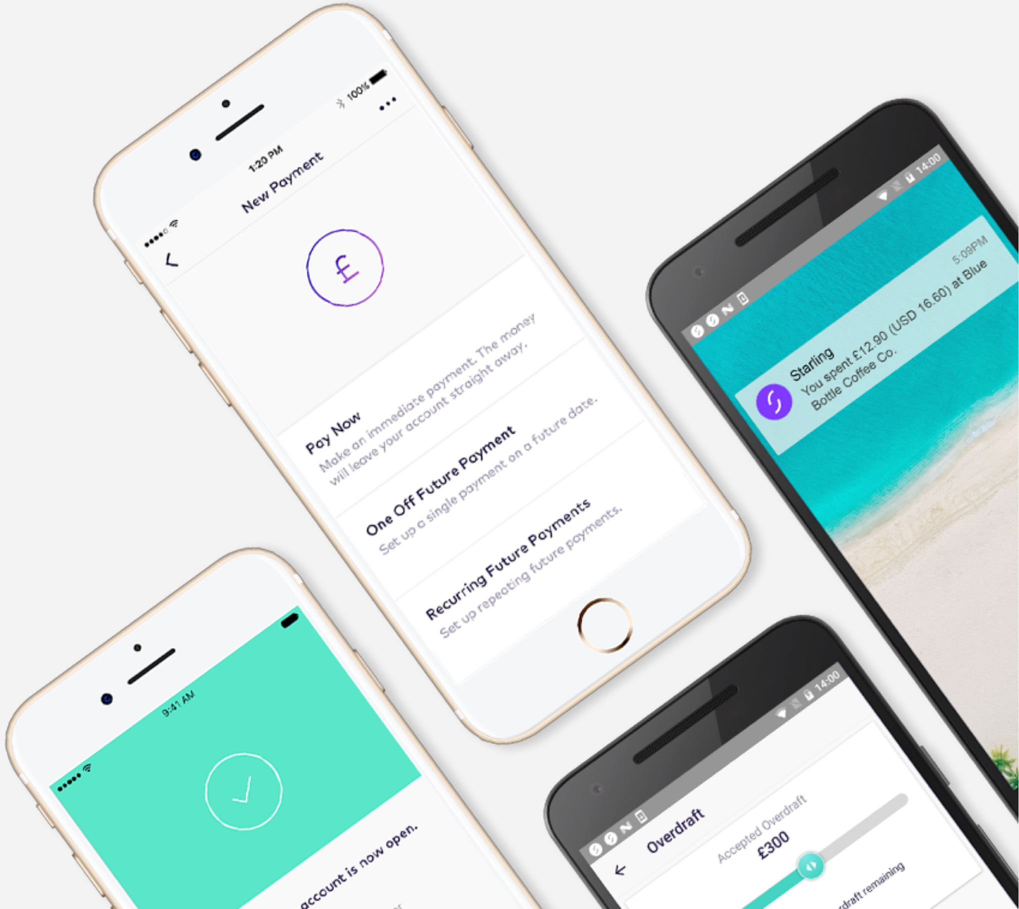
OPEN BANKING
TALES FROM THE FRONTIER

Anca Zaharia
@ancaleuca

Jason Maude
@jasonmaude

STARLING BANK


1:20 PM
100%
New Payment
£
Pay Now
Make an immediate payment. The money will leave your account straight away.
One Off Future Payment
Set up a single payment on a future date.
Recurring Future Payments
Set up repeating future payments.
14:00
Starling
You spent £12.90 (USD 16.60) at Blue Bottle Coffee Co.
5:09PM
9:41 AM
account is now open.
Overdraft
Accepted Overdraft
£300

What is open banking?

The legislation and associated technology that allow customers of financial institutions greater control of data that those institutions hold about them.

Who are Starling Bank?

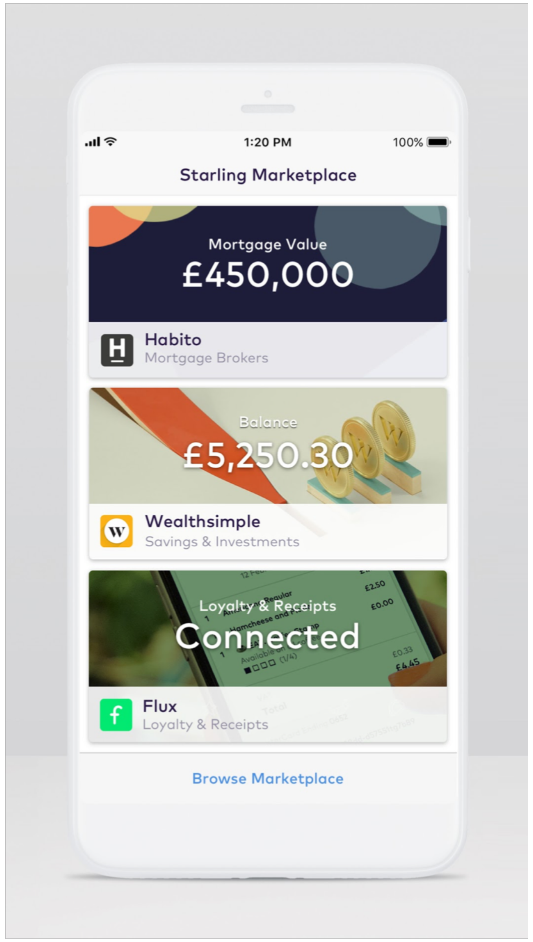
- Tech start-up with a banking licence
- ~100% cloud-based, mobile-only
- All the features that you'd expect from a current account and more
- Public APIs & developer platform

Public APIs

- Most actions that can be performed through the mobile apps are available
- Allows individuals to connect up their bank account to their own code

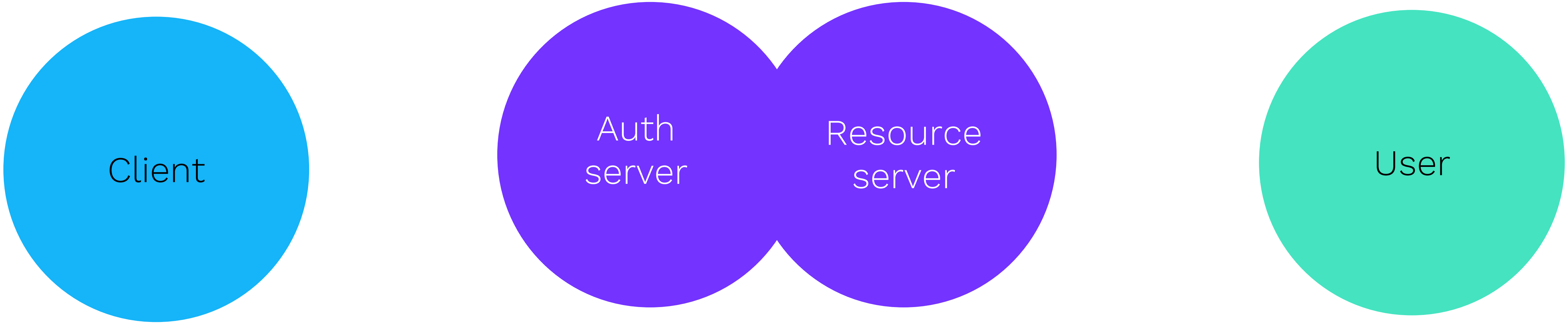
The Starling Bank marketplace

- Allows customers to securely connect to selected partners via their Starling Bank account
- Providers of mortgages, pensions, savings and investments etc



LESSON 1: UNDERSTAND OAUTH 2

OAuth 2 overview



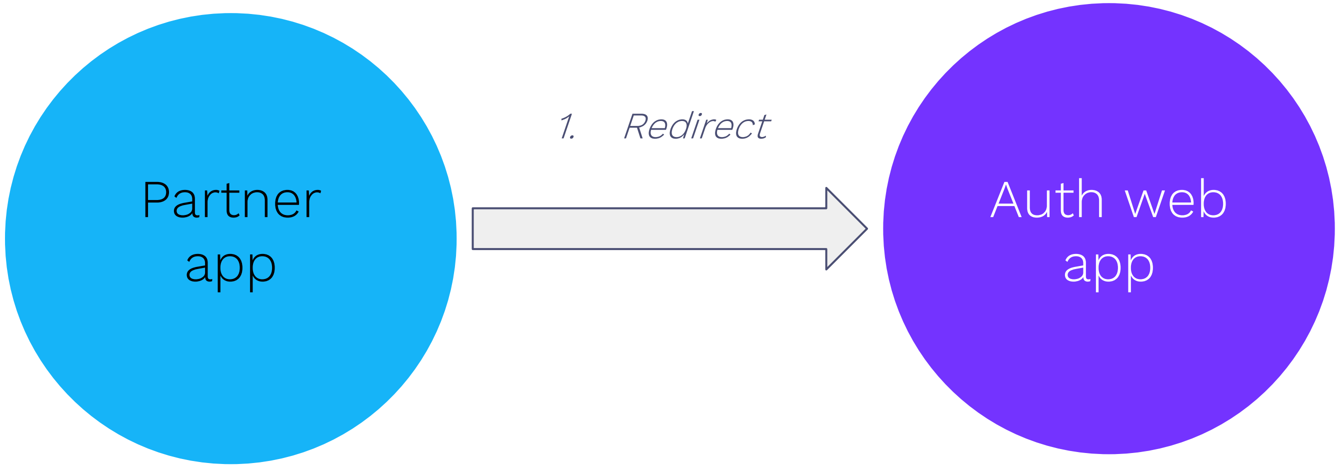
Client

Auth server

Resource server

User

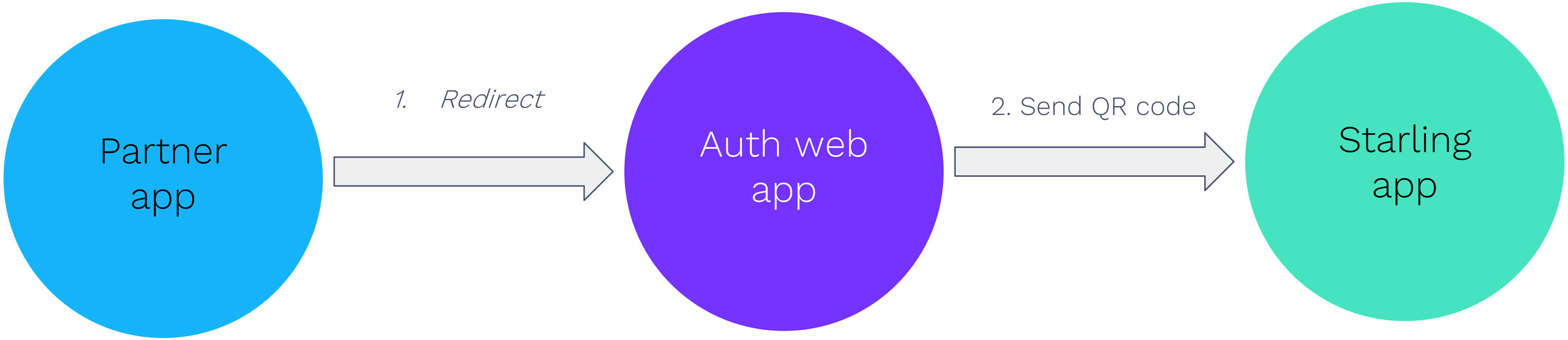
Client authentication



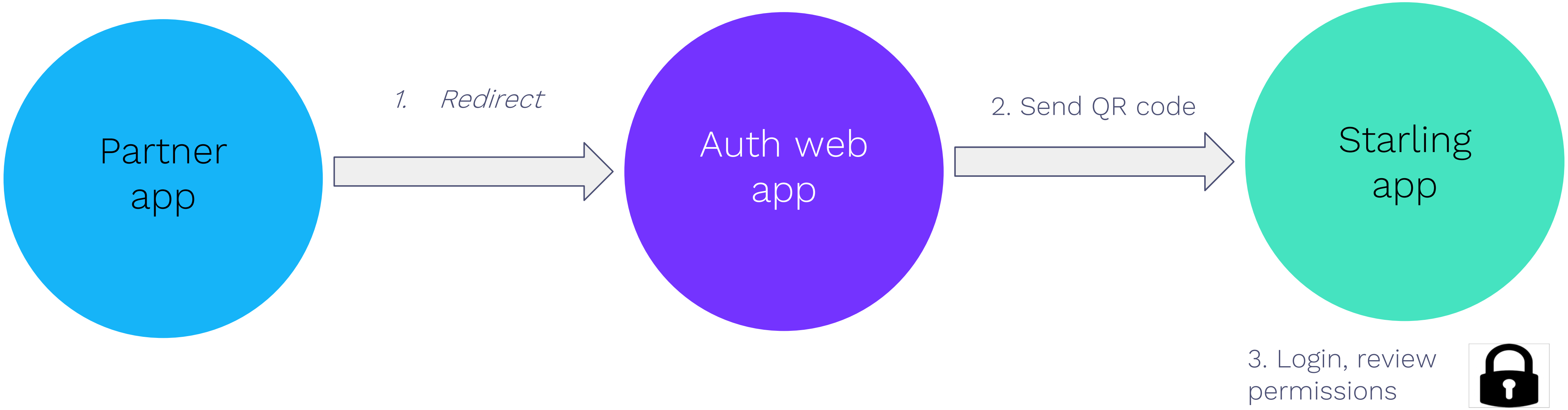
https://oauth.starlingbank.com

- **client_id**=$client_id
- **response_type**=code
- **state**=$state
- **redirect_uri**=$redirect_uri

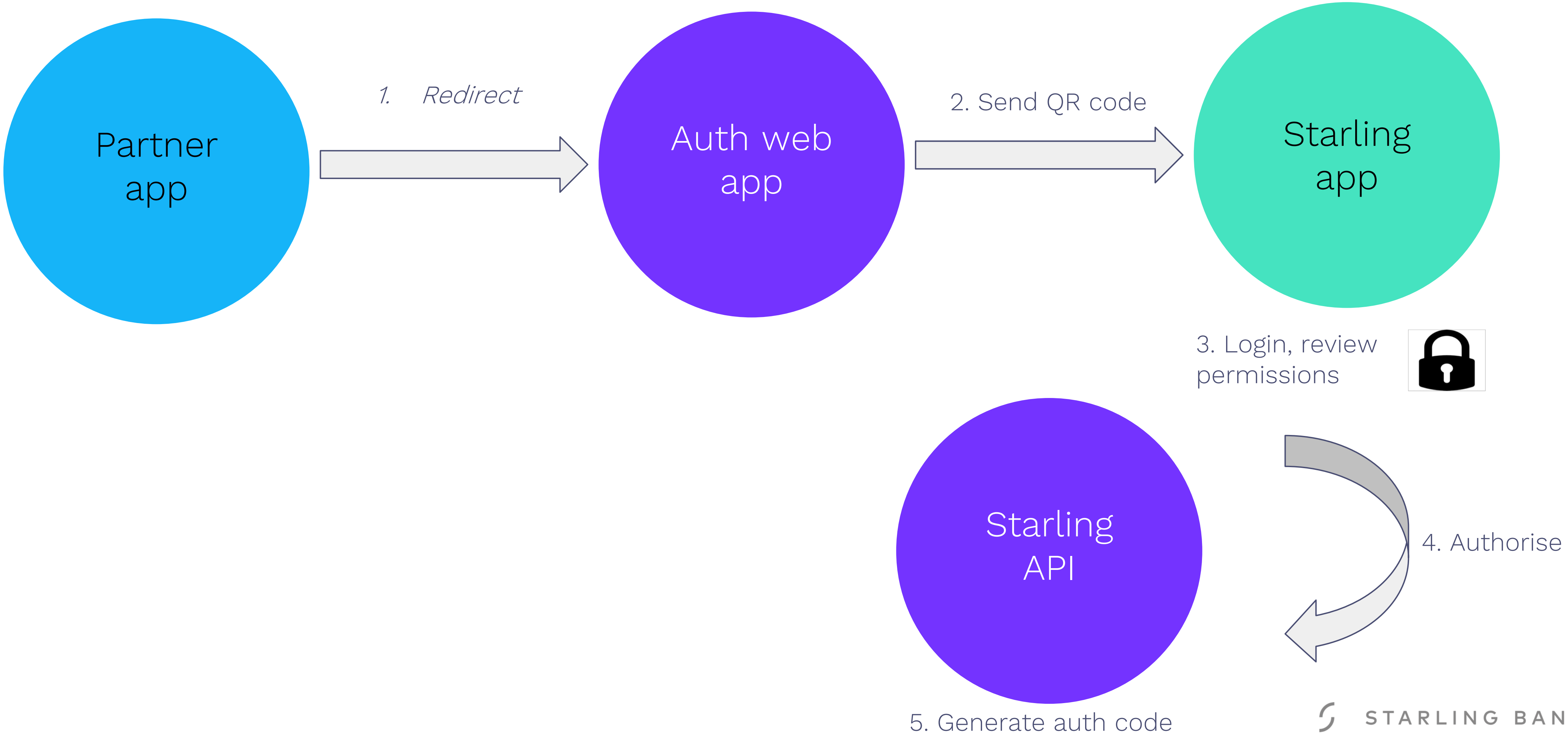
Client authentication



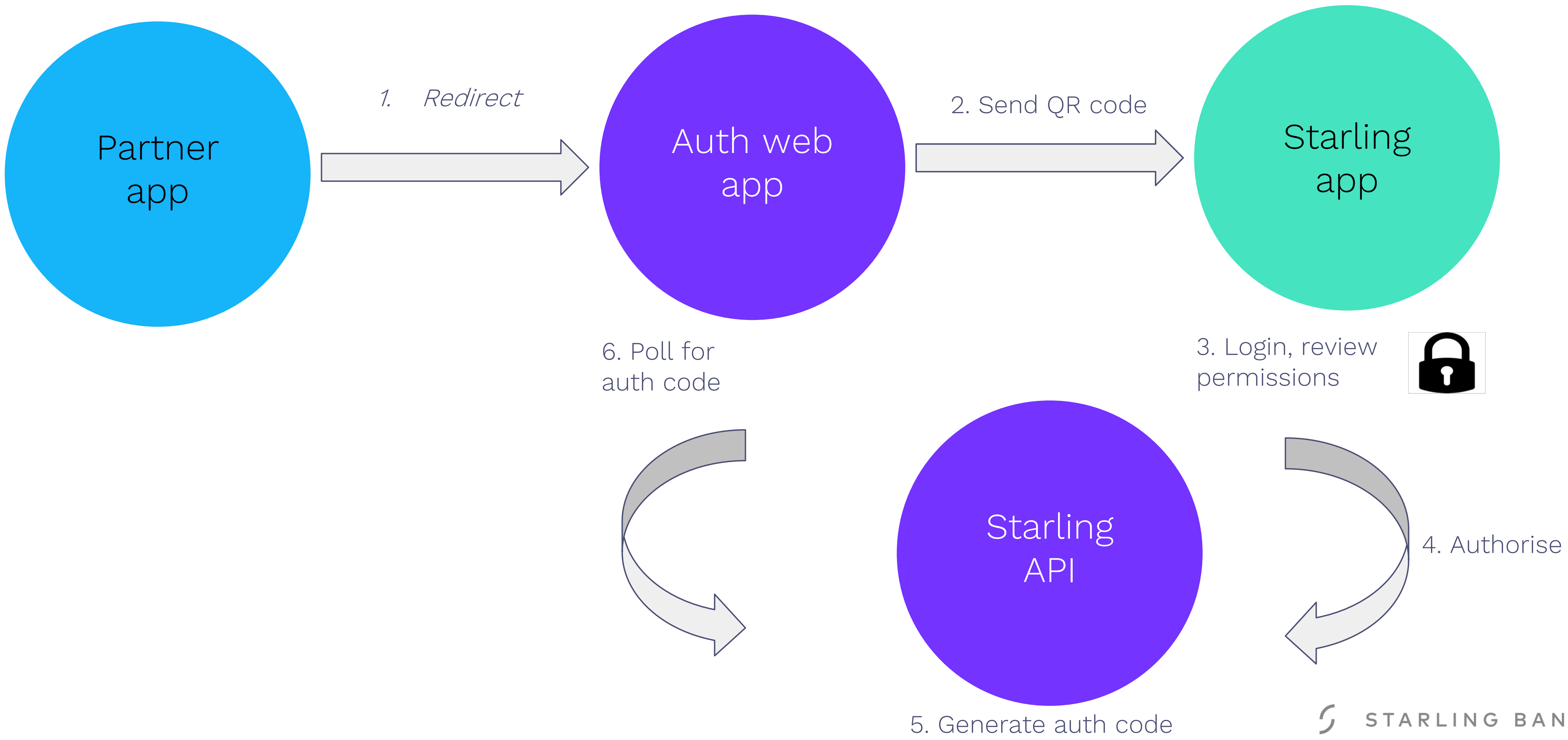
Client authorisation



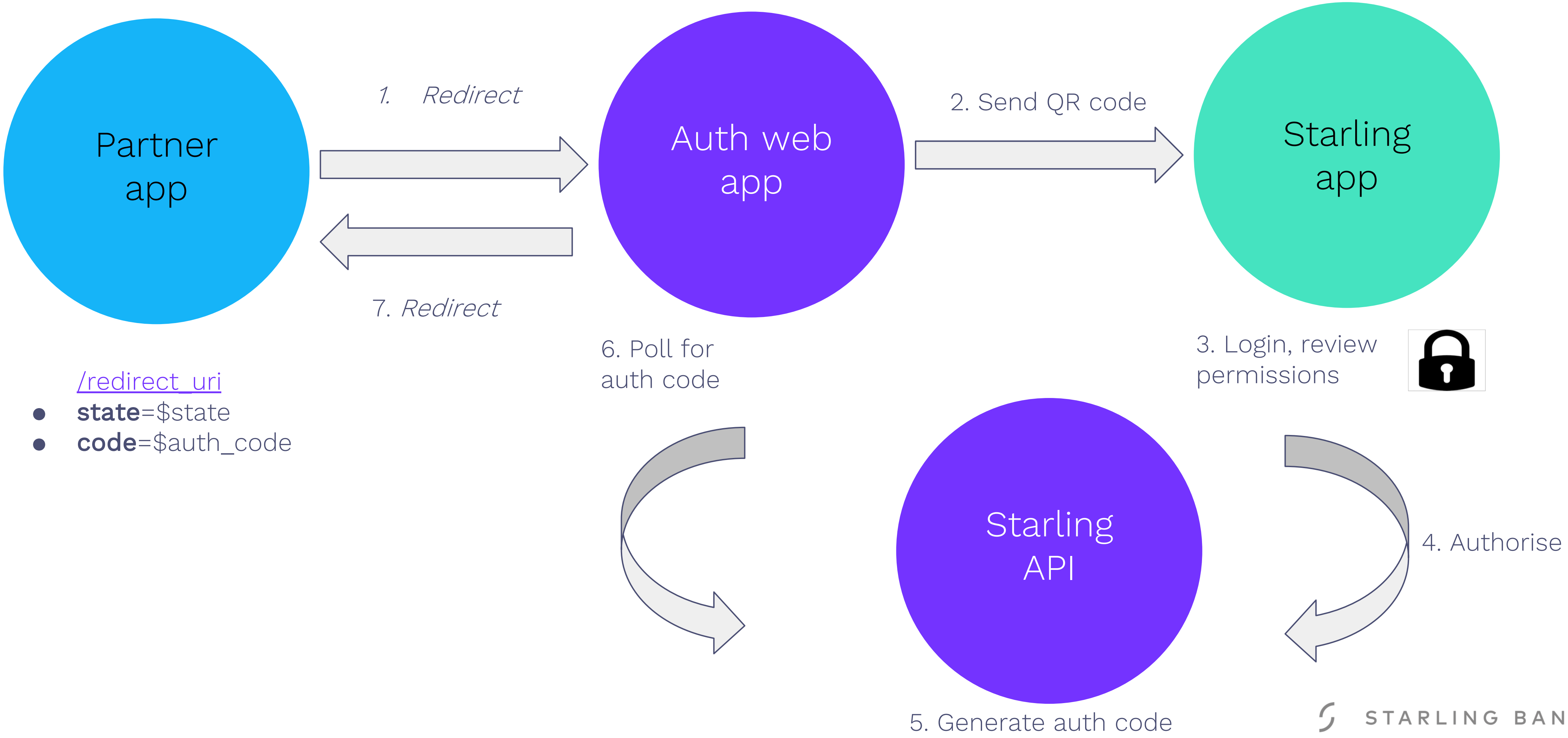
Client authorisation



Client authorisation



Client authorisation



Partner app

1. *Redirect*

Auth web app

2. Send QR code

Starling app

3. Login, review permissions

4. Authorise

Starling API

5. Generate auth code

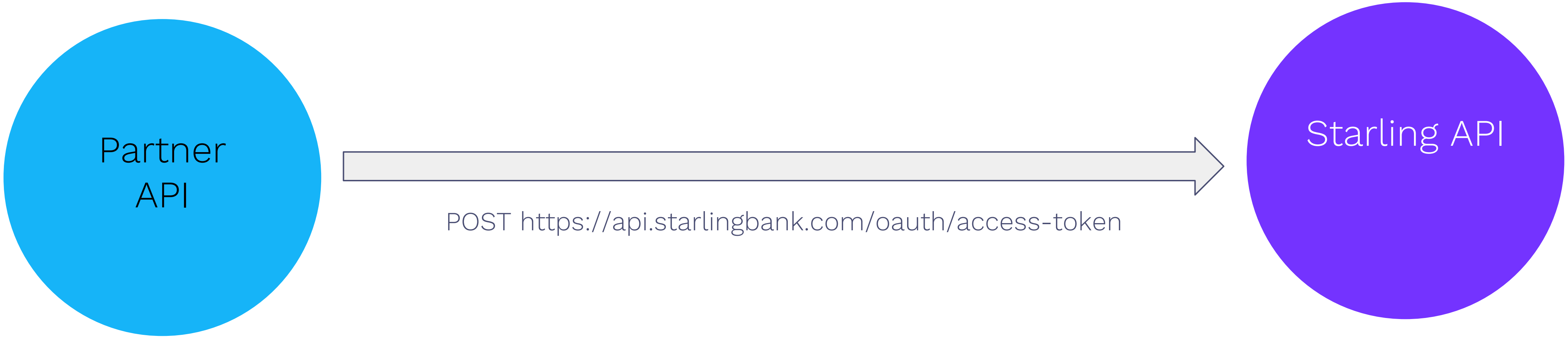
6. Poll for auth code

7. *Redirect*

/redirect_uri

- **state**=$state
- **code**=$auth_code

Exchange auth code for access token



Partner API

Starling API

POST https://api.starlingbank.com/oauth/access-token

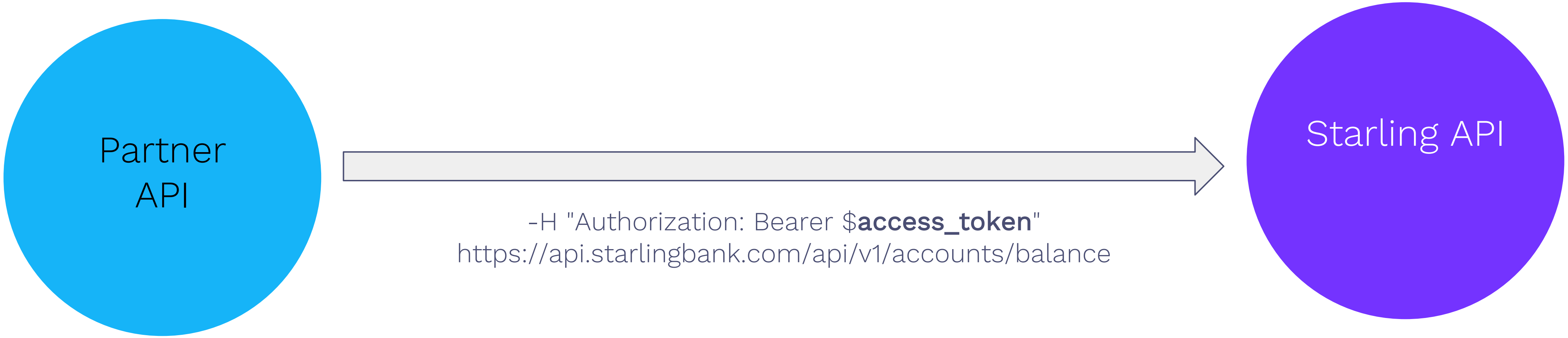
Request

- **code**=$auth_code
- **client_id**=$client_id
- **client_secret**=$client_secret
- grant_type=authorization_code
- redirect_uri=$redirect_uri

Response

- **access_token**
- **refresh_token**
- token_type=Bearer
- **expires_in**
- **scope**

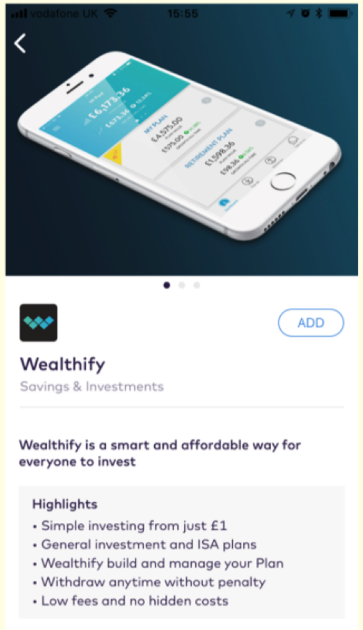
Use access token



-H "Authorization: Bearer $**access_token**"
https://api.starlingbank.com/api/v1/accounts/balance

Example screens for Wealthify using 2-way OAuth flow

1. Partner Detail



Wealthify

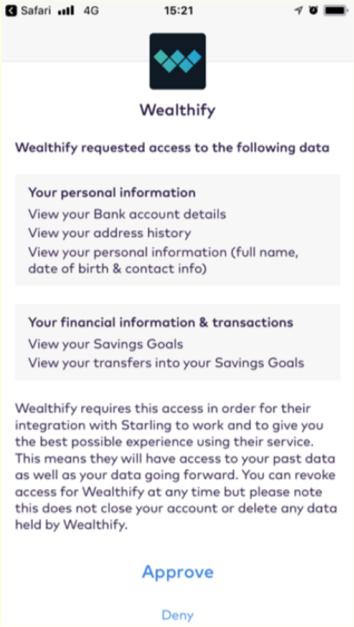
Savings & Investments

Wealthify is a smart and affordable way for everyone to invest

Highlights

- Simple investing from just £1
- General investment and ISA plans
- Wealthify build and manage your Plan
- Withdraw anytime without penalty
- Low fees and no hidden costs

2. Wealthify to access Starling



Wealthify

Wealthify requested access to the following data

Your personal information

View your Bank account details

View your address history

View your personal information (full name, date of birth & contact info)

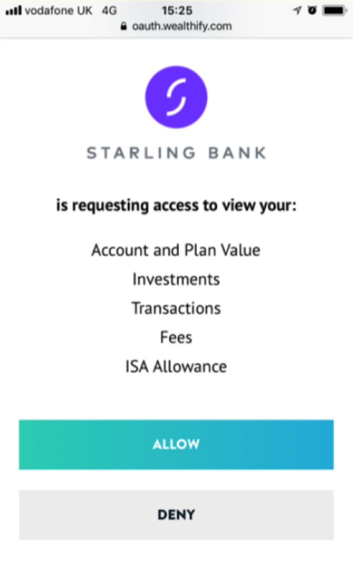
Your financial information & transactions

View your Savings Goals

View your transfers into your Savings Goals

Wealthify requires this access in order for their integration with Starling to work and to give you the best possible experience using their service. This means they will have access to your past data as well as your data going forward. You can revoke access for Wealthify at any time but please note this does not close your account or delete any data held by Wealthify.

3. Starling to access Wealthify



STARLING BANK

is requesting access to view your:

Account and Plan Value

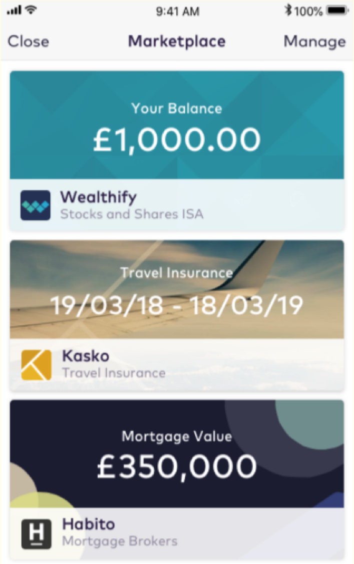
Investments

Transactions

Fees

ISA Allowance

4. Wealthify is now connected



Your Balance

£1,000.00

Wealthify

Stocks and Shares ISA

Travel Insurance

19/03/18 - 18/03/19

Kasko

Travel Insurance

Mortgage Value

£350,000

Habito

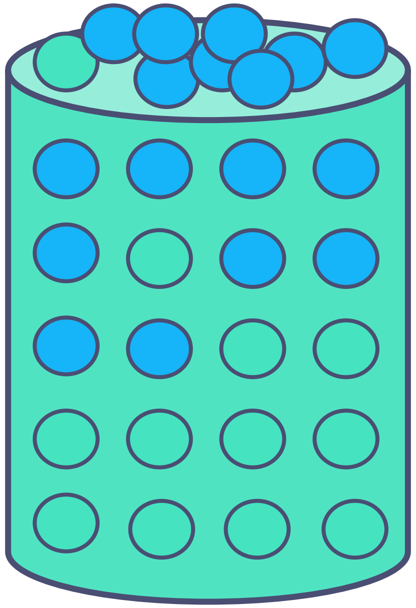
Mortgage Brokers

Additional security

- Highly sensitive requests (e.g., payment instructions) must be **signed**

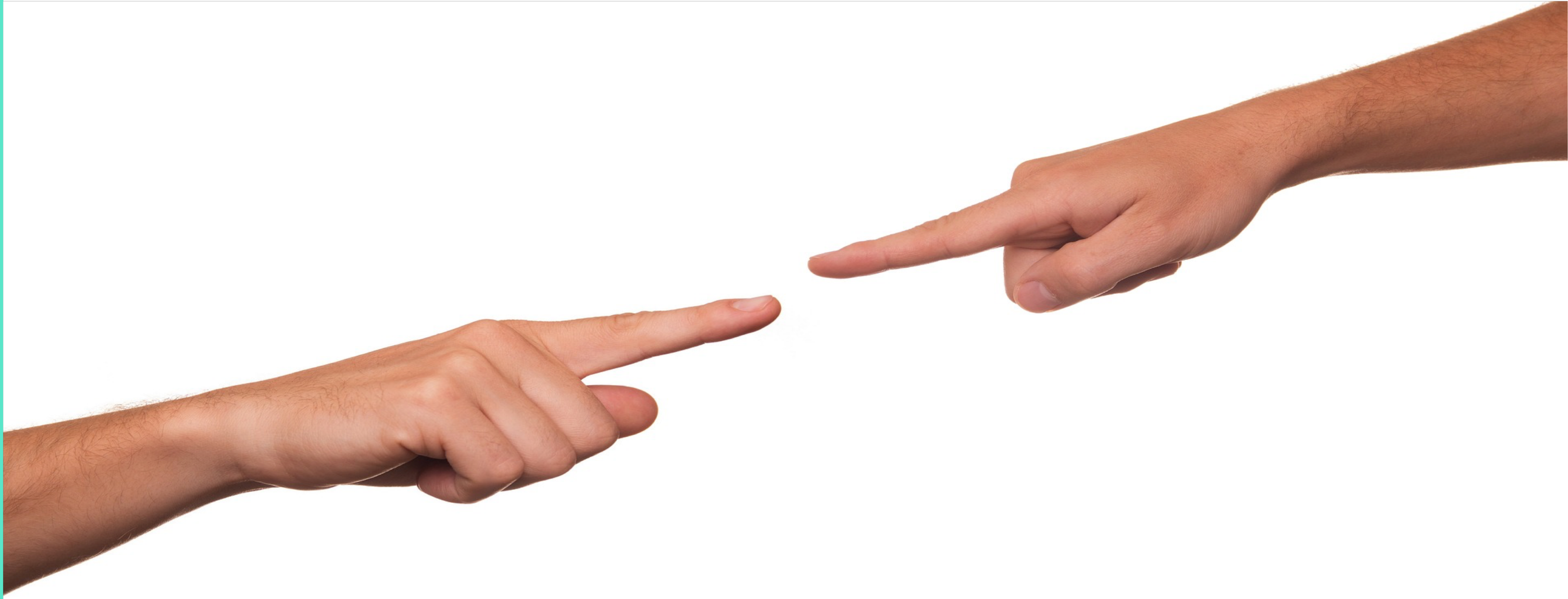
Token storage

- Don’t forget to delete expired tokens

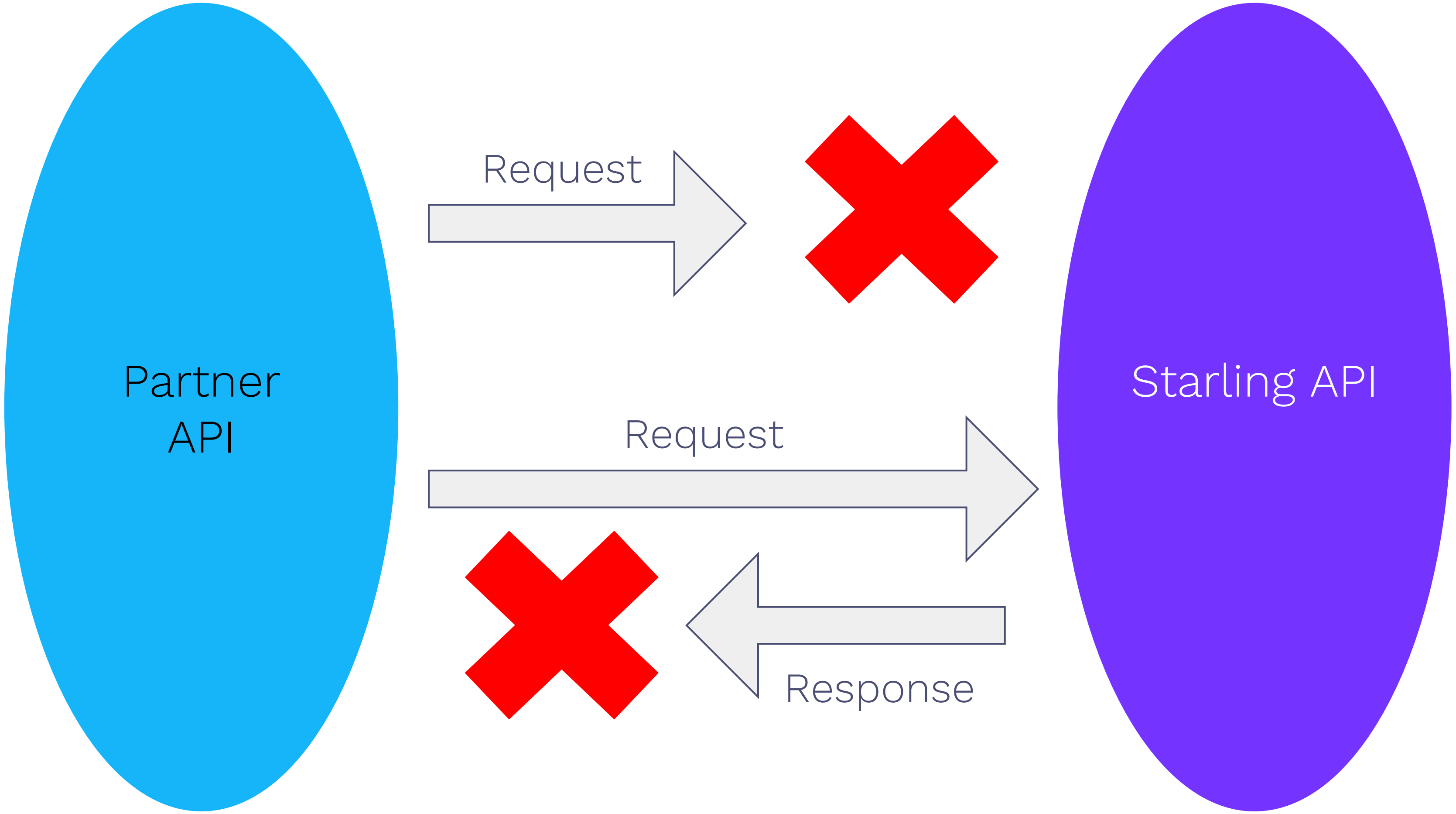


LESSON 2: YOU CAN’T ALWAYS CONNECT

Things will go wrong



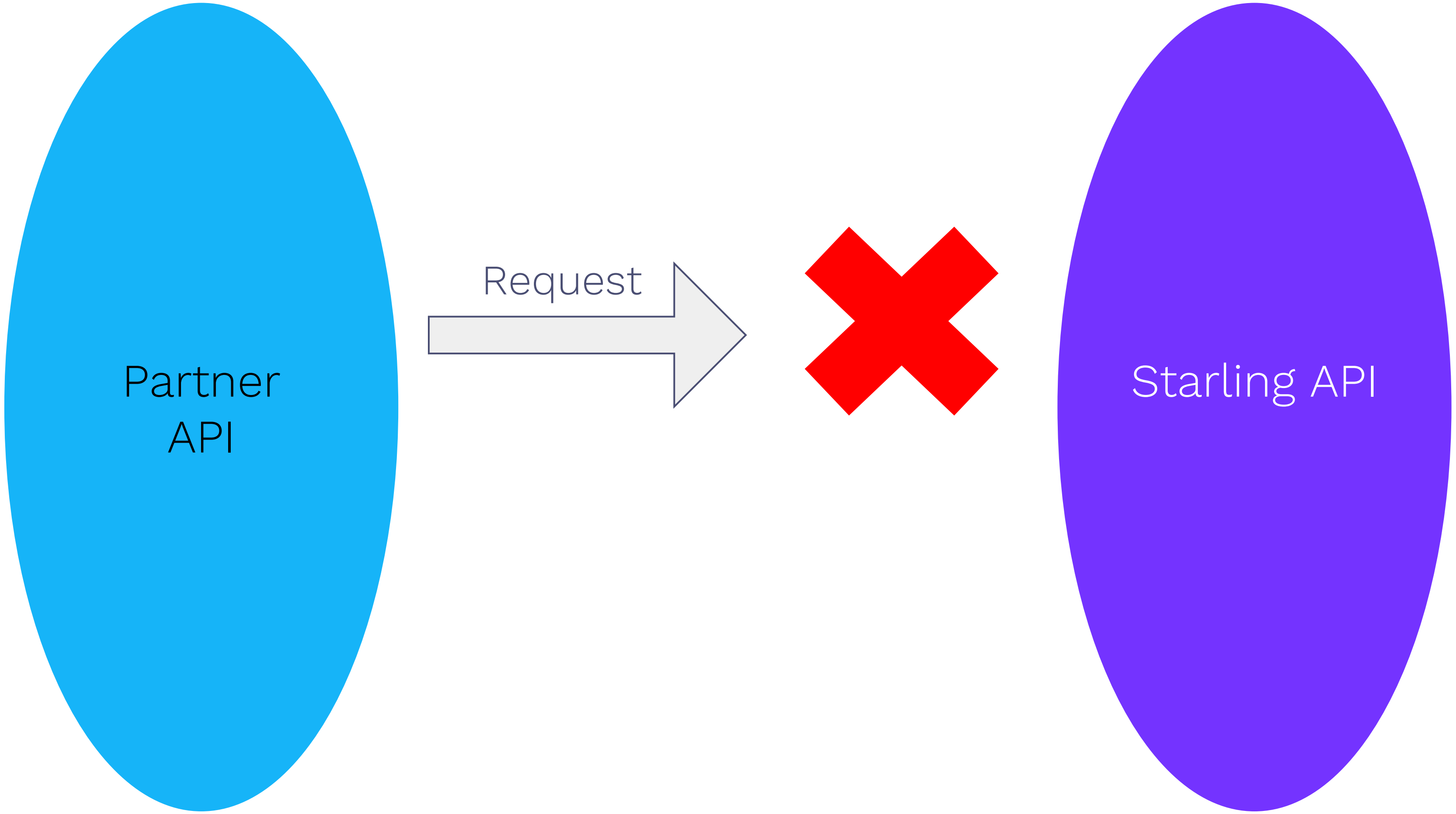
Losing requests and responses



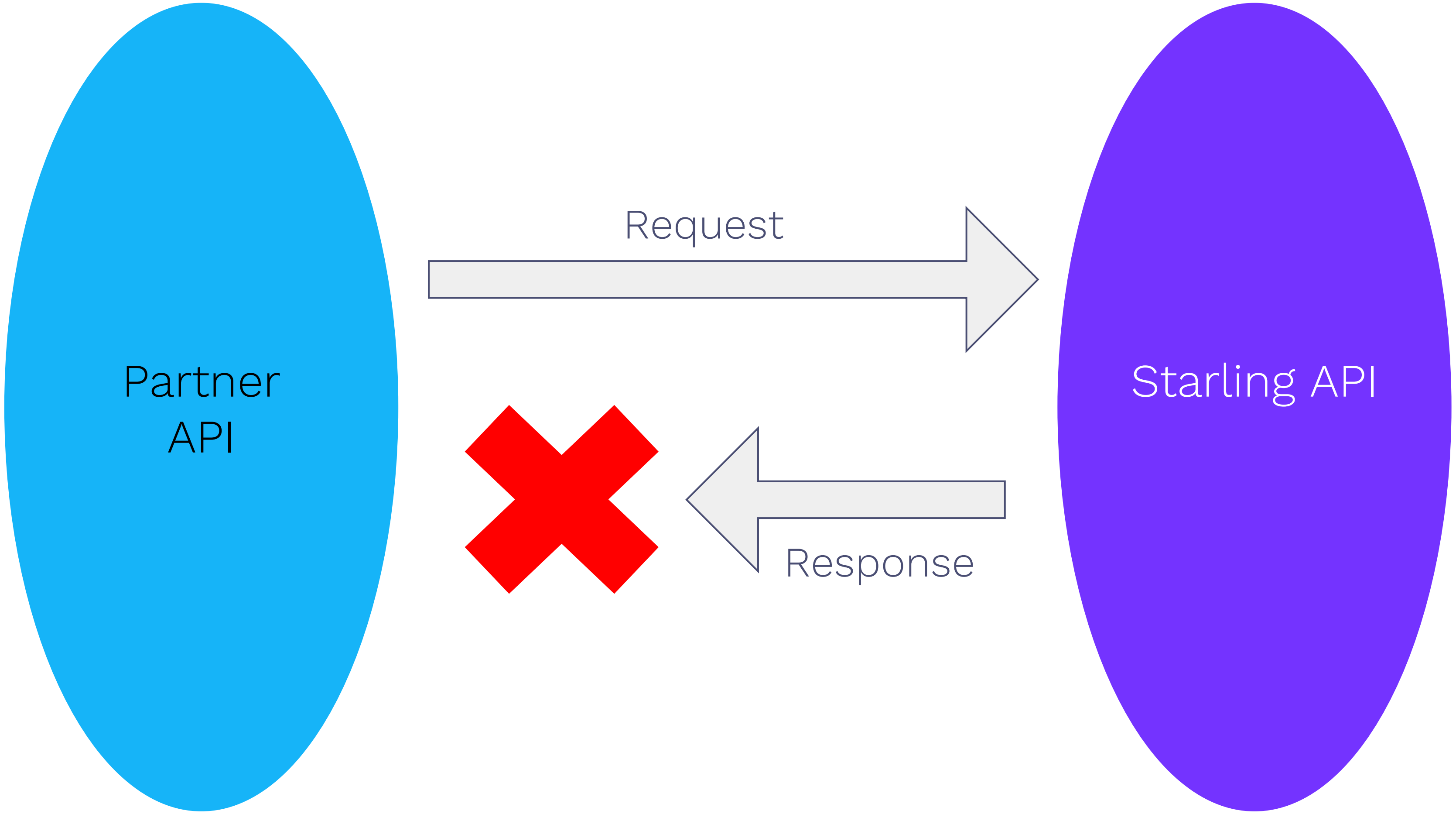
DITTO architecture

The system must ensure that every instruction from a user is actioned at least once and at most once

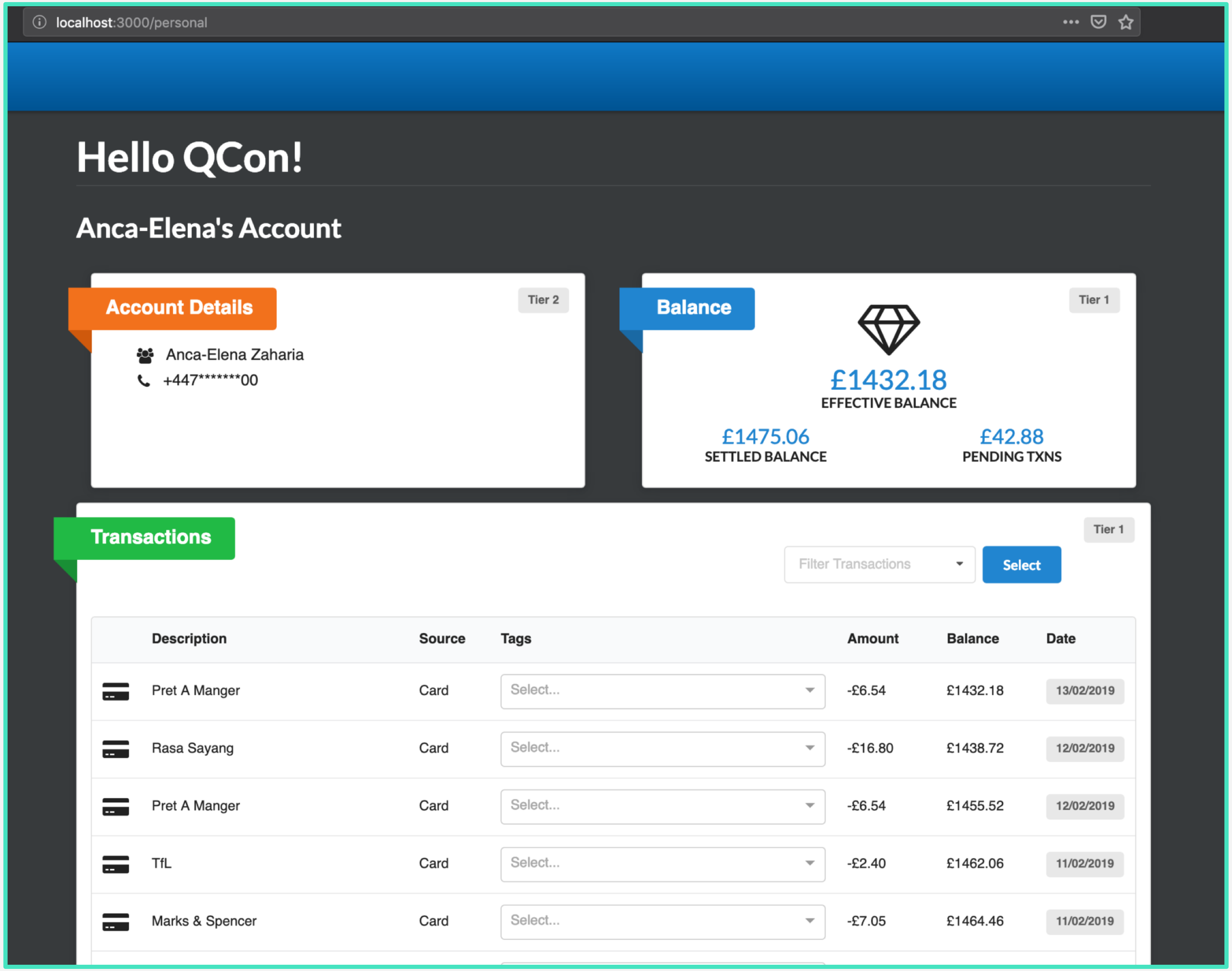
Losing requests - at least once



Losing responses - at most once



LESSON 3: MAKE TESTING EASY



localhost:3000/personal

Hello QCon!

Anca-Elena's Account

Account Details Tier 2

Anca-Elena Zaharia

☎ +447*******00

Balance Tier 1

£1432.18
EFFECTIVE BALANCE

£1475.06
SETTLED BALANCE

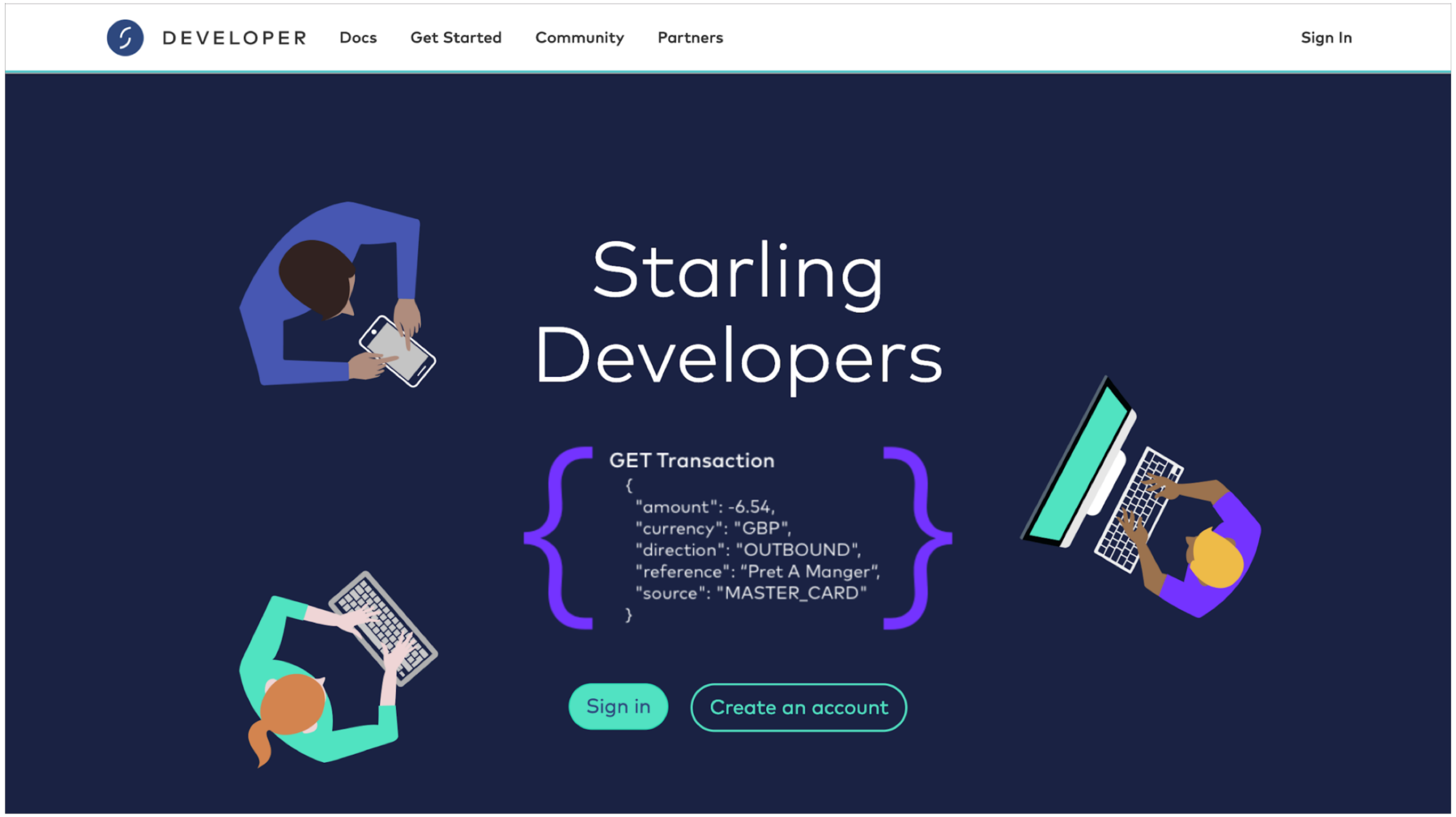
£42.88
PENDING TXNS

Transactions Tier 1

Filter Transactions ▾ Select

	Description	Source	Tags	Amount	Balance	Date
	Pret A Manger	Card	Select... ▾	-£6.54	£1432.18	13/02/2019
	Rasa Sayang	Card	Select... ▾	-£16.80	£1438.72	12/02/2019
	Pret A Manger	Card	Select... ▾	-£6.54	£1455.52	12/02/2019
	TfL	Card	Select... ▾	-£2.40	£1462.06	11/02/2019
	Marks & Spencer	Card	Select... ▾	-£7.05	£1464.46	11/02/2019

Personal access



DEVELOPER Docs Get Started Community Partners Sign In

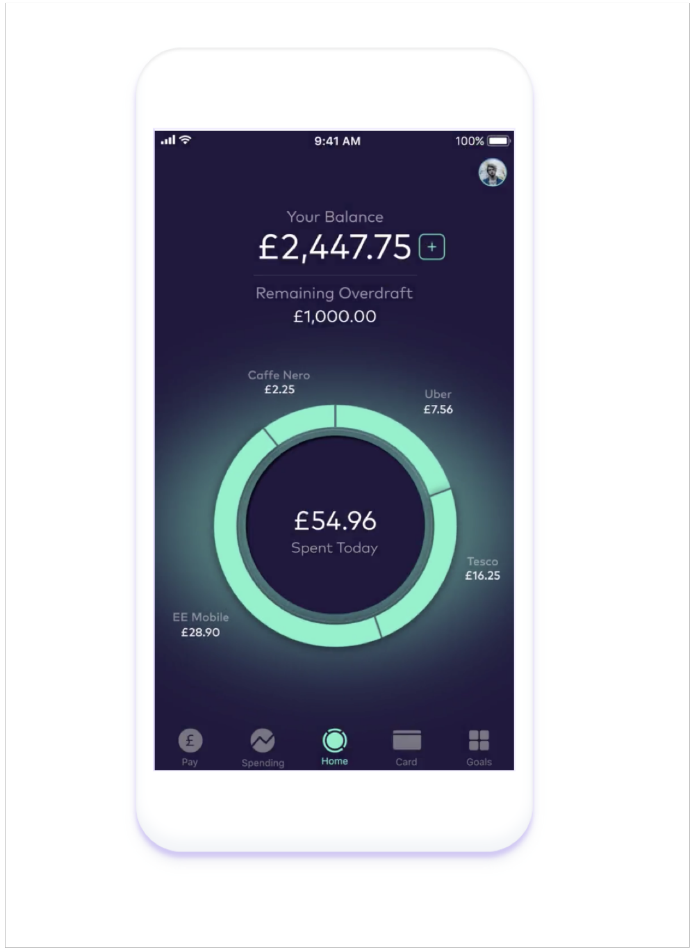
Starling Developers

GET Transaction

```
{
  "amount": -6.54,
  "currency": "GBP",
  "direction": "OUTBOUND",
  "reference": "Pret A Manger",
  "source": "MASTER_CARD"
}
```

Sign in | Create an account

Developer Portal account



9:41 AM 100%

Your Balance
£2,447.75 +

Remaining Overdraft
£1,000.00

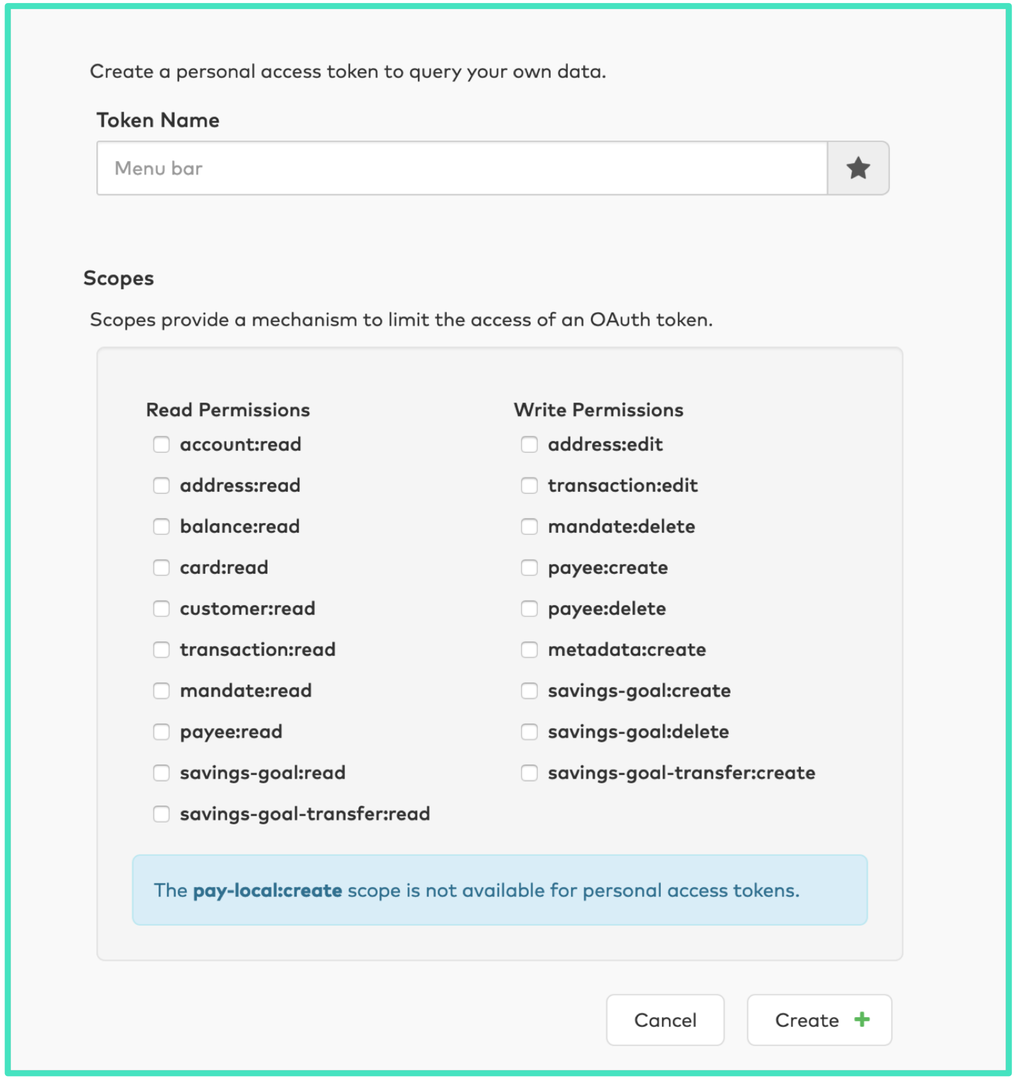
Caffe Nero £2.25
Uber £7.56
Tesco £16.25
EE Mobile £28.90

£54.96
Spent Today

Pay Spending Home Card Goals

Starling Bank account

Personal access



Create a personal access token to query your own data.

Token Name

Menu bar

Scopes

Scopes provide a mechanism to limit the access of an OAuth token.

Read Permissions

- □ account:read
- □ address:read
- □ balance:read
- □ card:read
- □ customer:read
- □ transaction:read
- □ mandate:read
- □ payee:read
- □ savings-goal:read
- □ savings-goal-transfer:read

Write Permissions

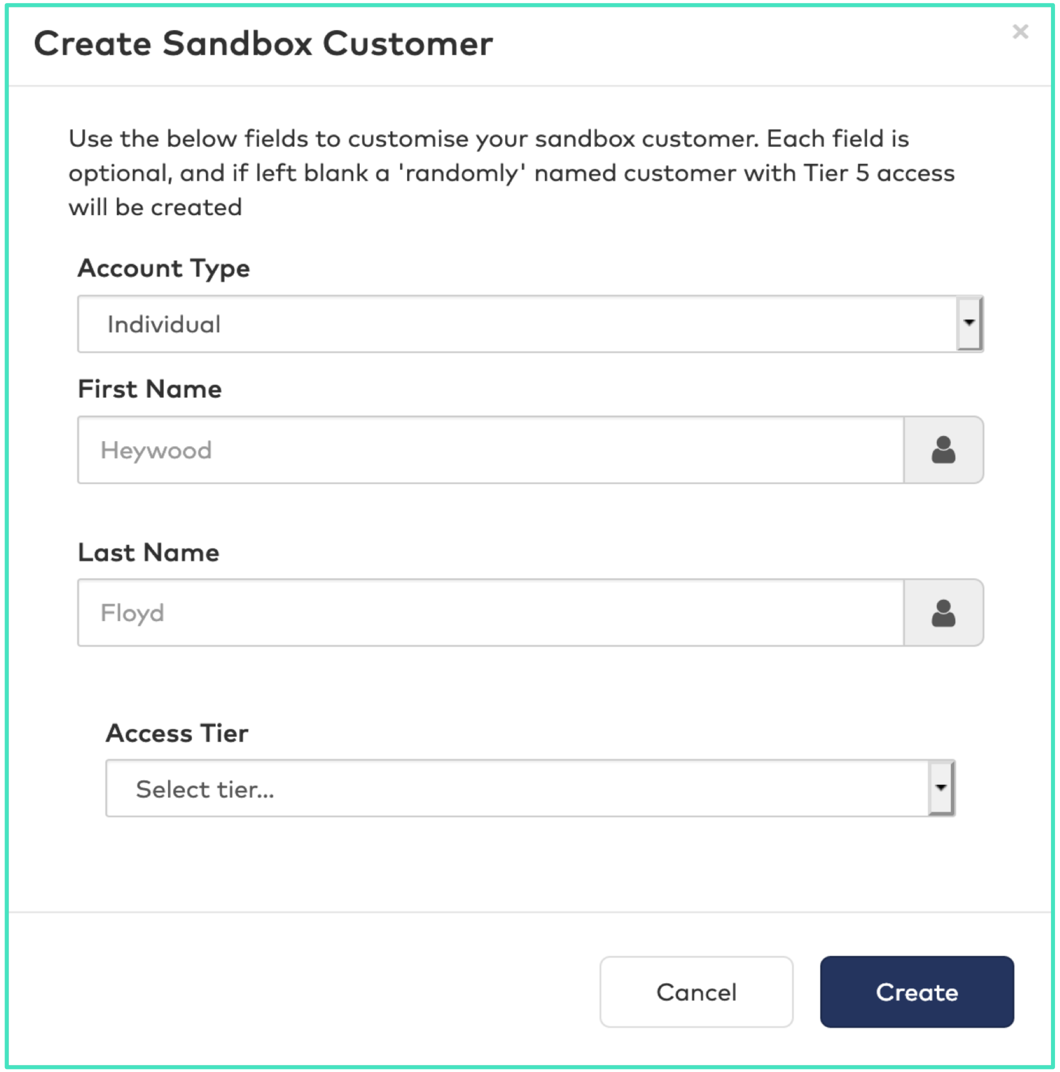
- □ address:edit
- □ transaction:edit
- □ mandate:delete
- □ payee:create
- □ payee:delete
- □ metadata:create
- □ savings-goal:create
- □ savings-goal:delete
- □ savings-goal-transfer:create

The **pay-local:create** scope is not available for personal access tokens.

```
$  curl -H “Authorization: Bearer <personal access token>” https://api.starlingbank.com/api/v1/transactions
```

What if I want more?

Play in the sandbox



Create Sandbox Customer

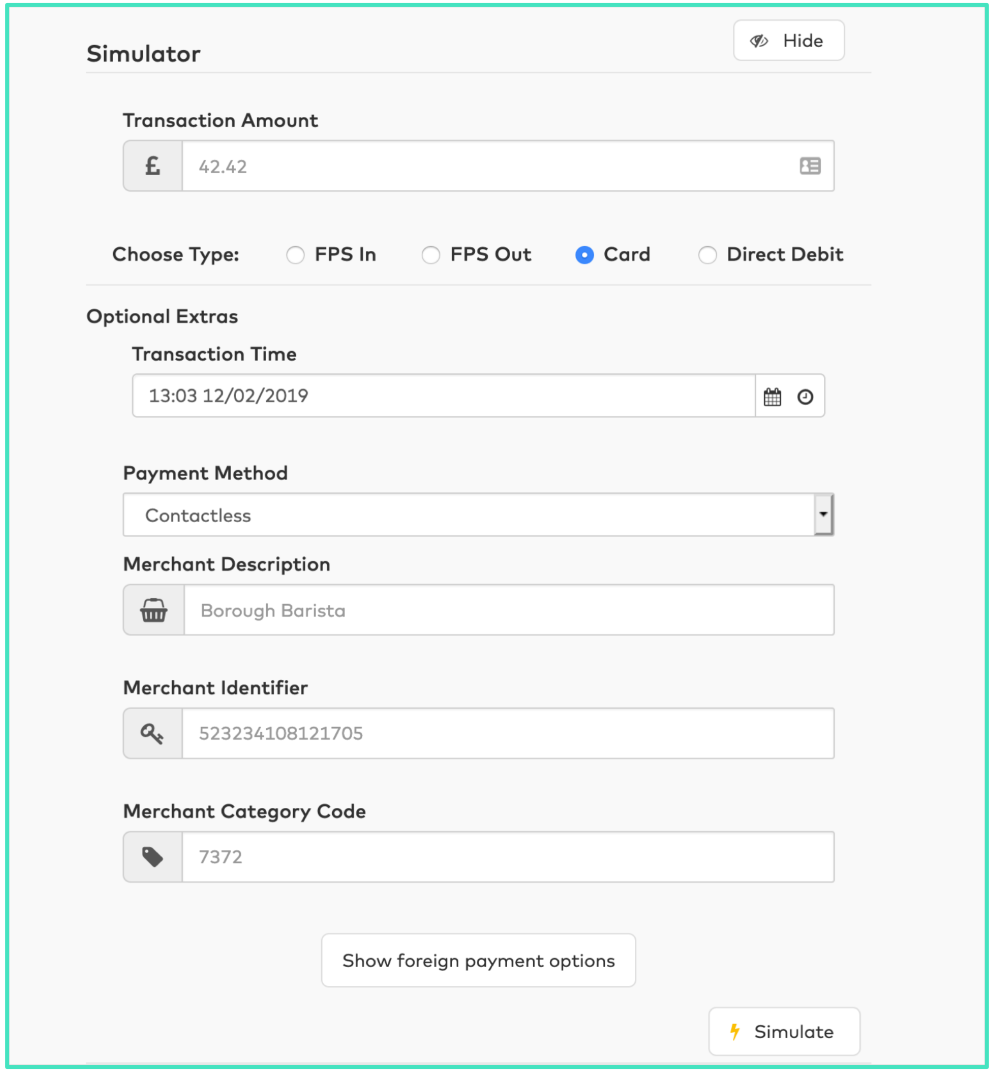
Use the below fields to customise your sandbox customer. Each field is optional, and if left blank a 'randomly' named customer with Tier 5 access will be created

Account Type: Individual

First Name: Heywood

Last Name: Floyd

Access Tier: Select tier...



Simulator

Transaction Amount: £ 42.42

Choose Type: ○ FPS In ○ FPS Out ● Card ○ Direct Debit

Optional Extras

Transaction Time: 13:03 12/02/2019

Payment Method: Contactless

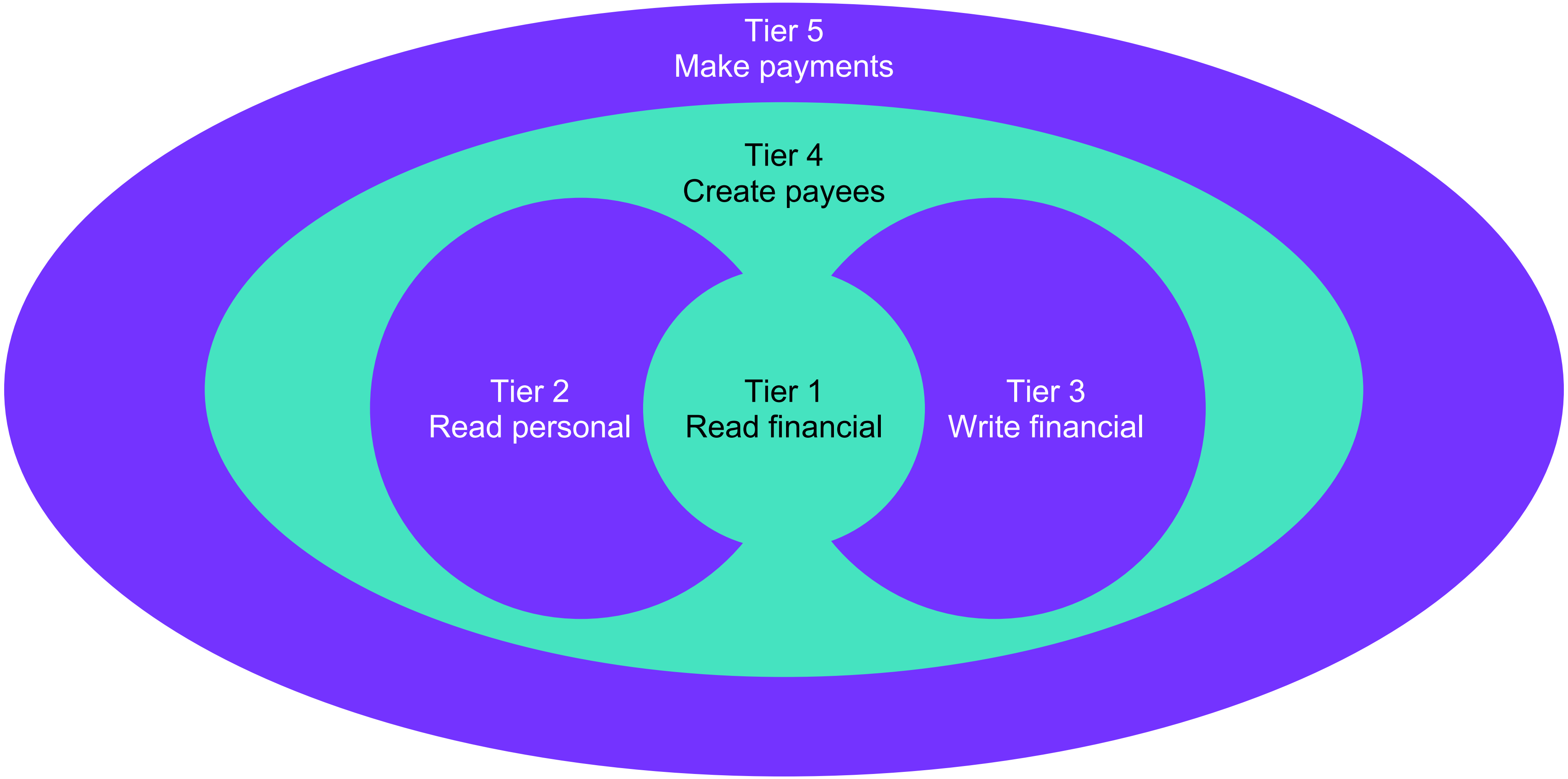
Merchant Description: Borough Barista

Merchant Identifier: 523234108121705

Merchant Category Code: 7372

LESSON 4: WORK ON YOUR PERMISSIONS MODEL

Permission model v1



Tier 5
Make payments

Tier 4
Create payees

Tier 2
Read personal

Tier 1
Read financial

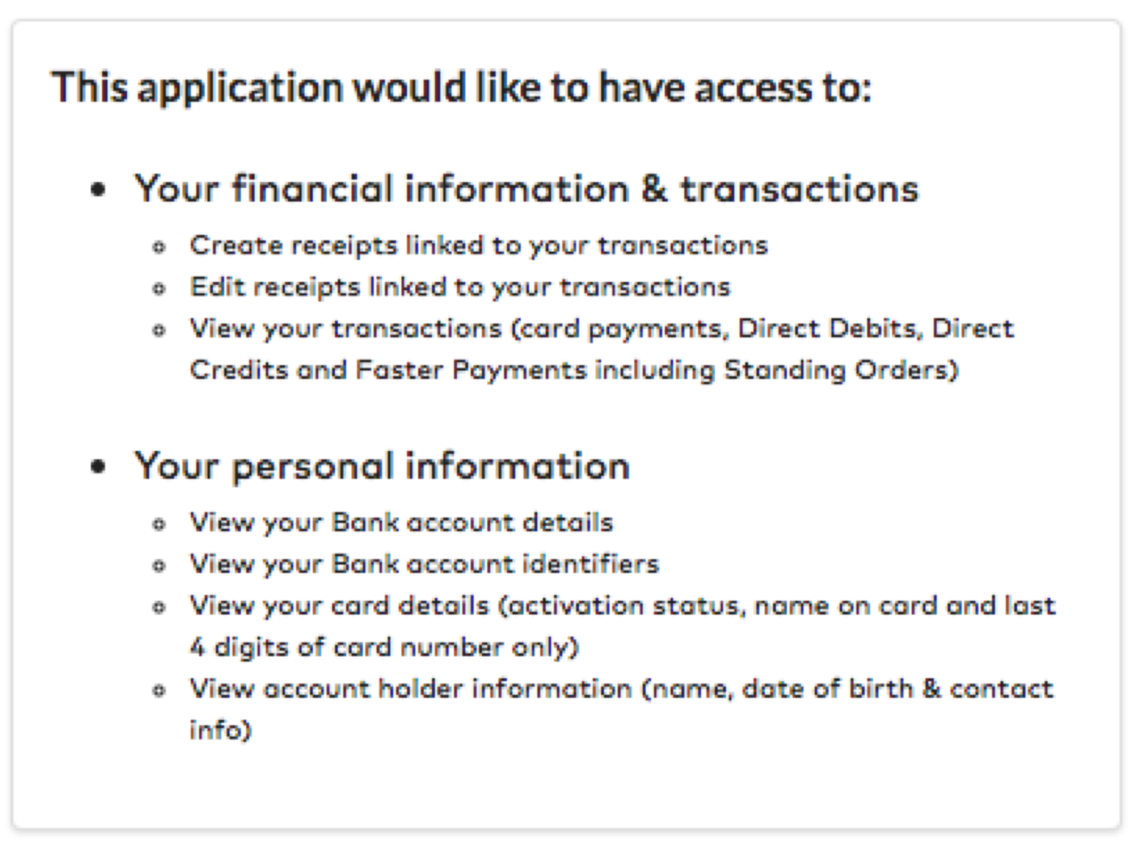
Tier 3
Write financial

STARLING BANK

Permission model v2

- Create Payees ✗
- Delete DD Mandates ✗
- Read Address ✗
- Edit Metadata ✗
- Create Savings Goal ✓
- Read Transactions ✗
- Read Balance ✓
- Create Local Payment ✗

Displaying permissions

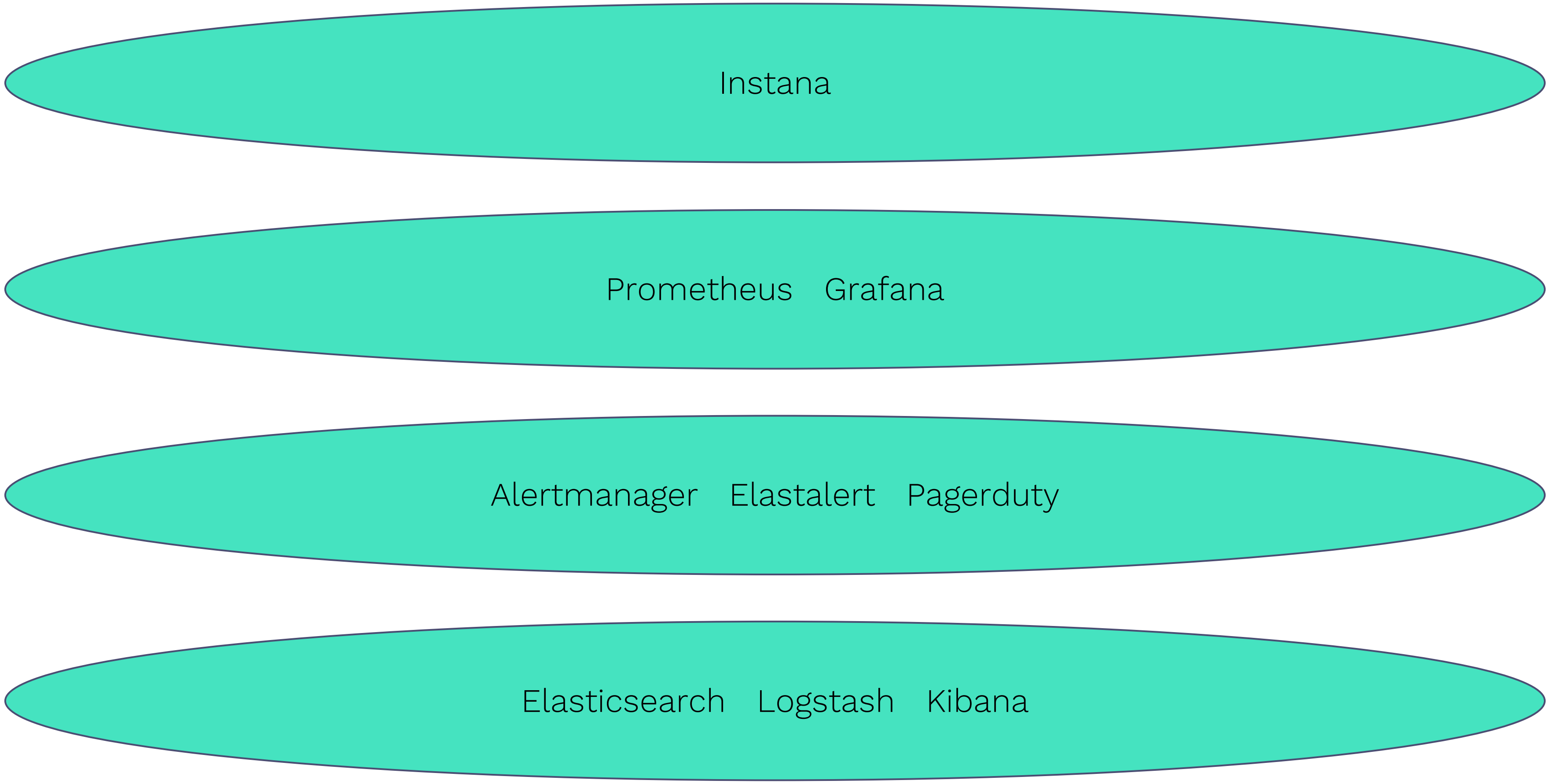


This application would like to have access to:

- Your financial information & transactions
  - Create receipts linked to your transactions
  - Edit receipts linked to your transactions
  - View your transactions (card payments, Direct Debits, Direct Credits and Faster Payments including Standing Orders)
- Your personal information
  - View your Bank account details
  - View your Bank account identifiers
  - View your card details (activation status, name on card and last 4 digits of card number only)
  - View account holder information (name, date of birth & contact info)

LESSON 5: MONITOR YOUR API

Monitoring and observability stack

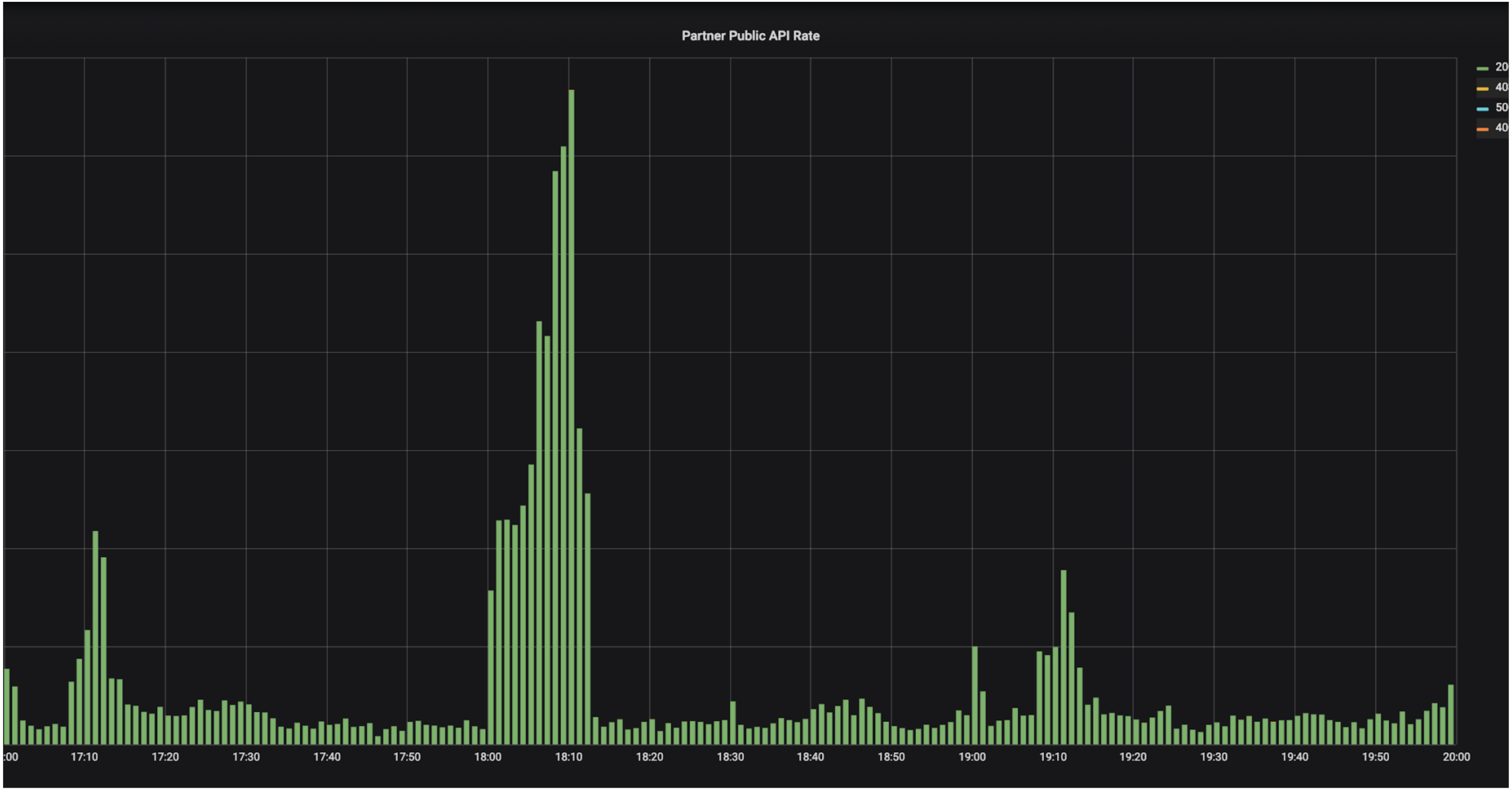


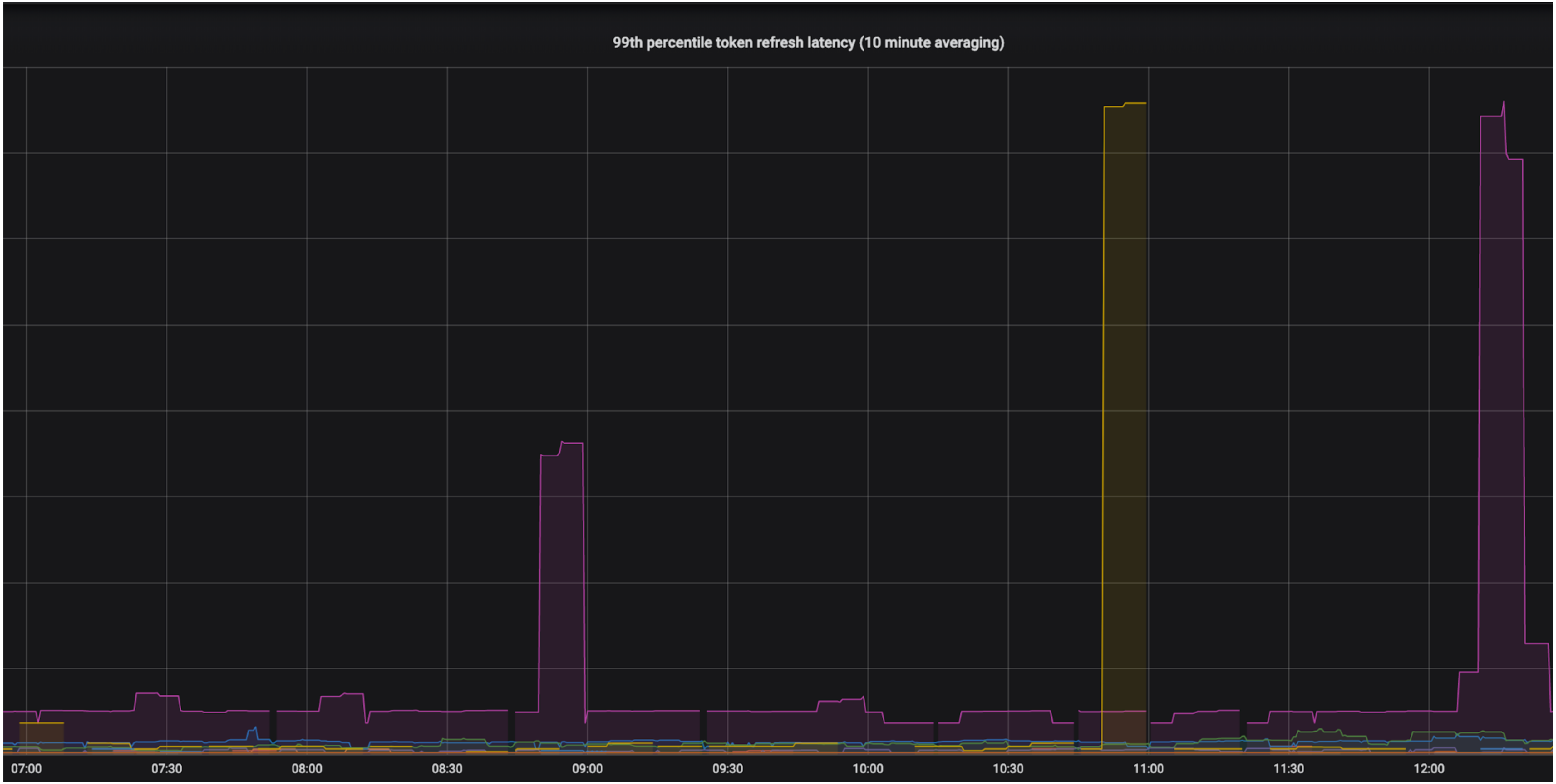
Instana

Prometheus Grafana

Alertmanager Elastalert Pagerduty

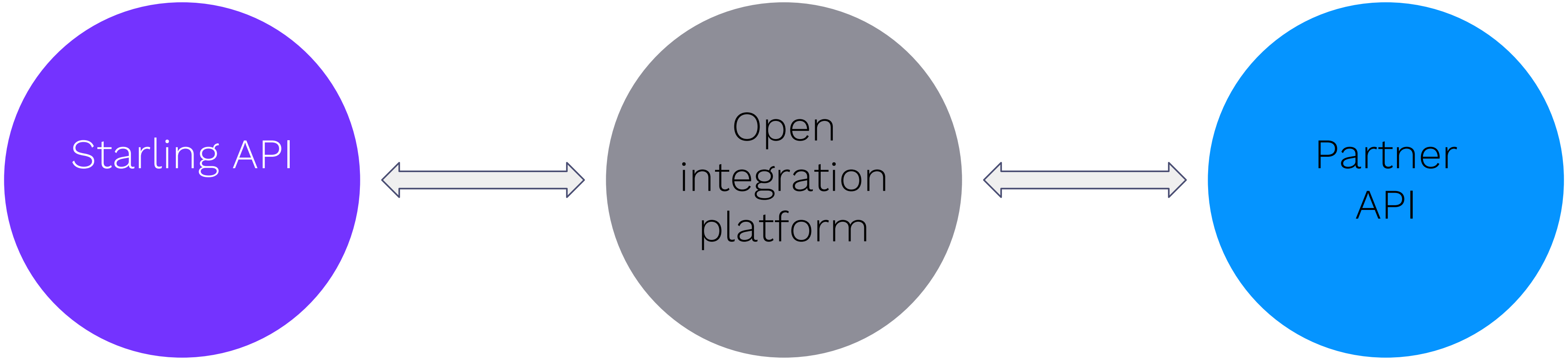
Elasticsearch Logstash Kibana


Partner Public API Rate
🟩 20
🟨 40
🟦 50
🟧 40
:00
17:10
17:20
17:30
17:40
17:50
18:00
18:10
18:20
18:30
18:40
18:50
19:00
19:10
19:20
19:30
19:40
19:50
20:00

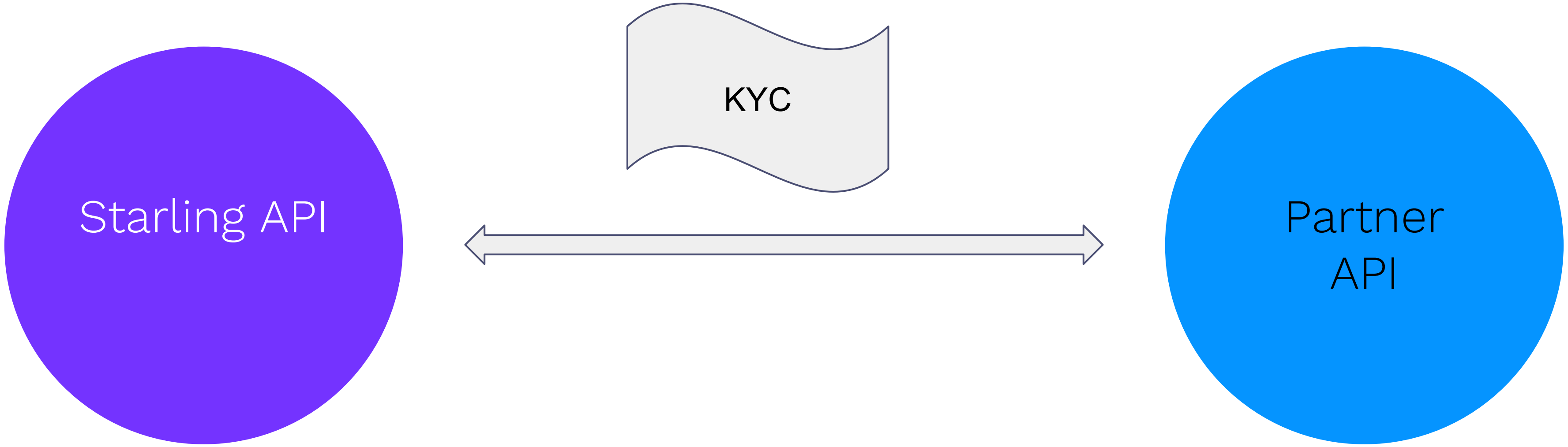

99th percentile token refresh latency (10 minute averaging)
07:00
07:30
08:00
08:30
09:00
09:30
10:00
10:30
11:00
11:30
12:00

THE FUTURE

Open integration platform

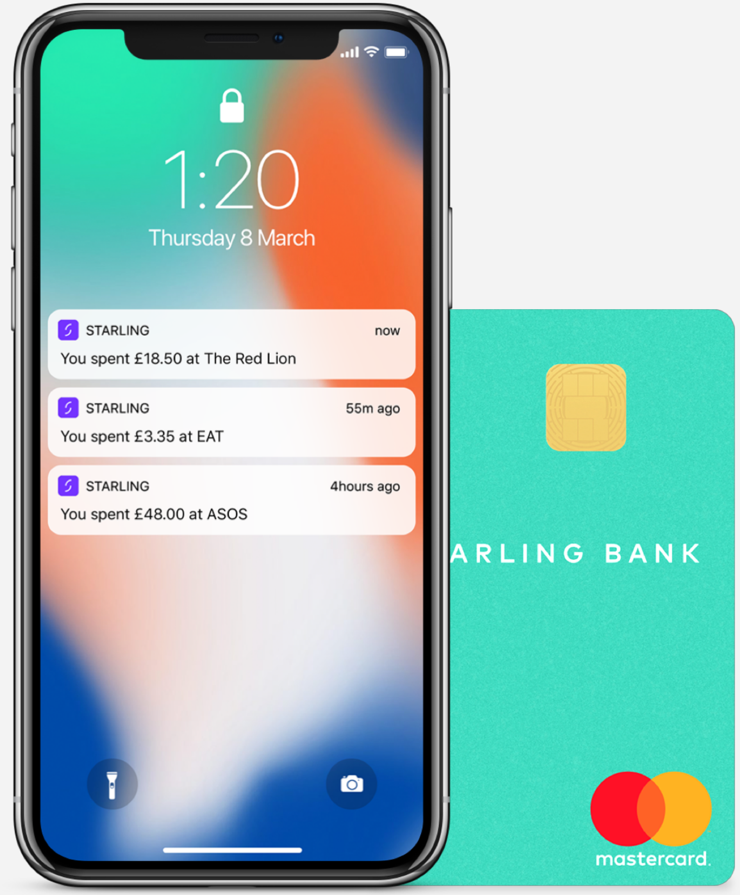


Share your identity confirmation



Key takeaways

- Lesson 1: Understand OAuth
- Lesson 2: You can’t always connect
- Lesson 3: Make testing easy
- Lesson 4: Work on your permissions model
- Lesson 5: Monitor your API



Thank you!

Check out the Starling Developer Podcast!

https://developer.starlingbank.com

@ancaleuca
@jasonmaude