OpenFinity
www.openfinity.org

Mastering End-User Consent in Open Finance Ecosystems

August 08, 2024, 12:00 PM – 12:30PM ET

Brook Lovatt
Chief Product Officer
SecureAuth

The OpenFinity//EXPO

November 19-20, 2024

Call For Speakers

On-Line Live Free

2 Days

30+ Speakers

16 Topics

1,000+ Viewers

1. 1033 Essentials
2. Business Cases & Monetization
3. Consent management
4. Security
5. Data Governance
6. Legal & Privacy
7. Core Banking
8. Payments
9. AI
10. Krypto
11. Financial Inclusion
12. Fintech
13. Meditation & Leadership
14. Portal & Marketplace
15. DevOps
16. International Experience

https://www.openfinity.org/call-4-speakers

With the Patronage of FINANCIAL DATA EXCHANGE

OpenFinity

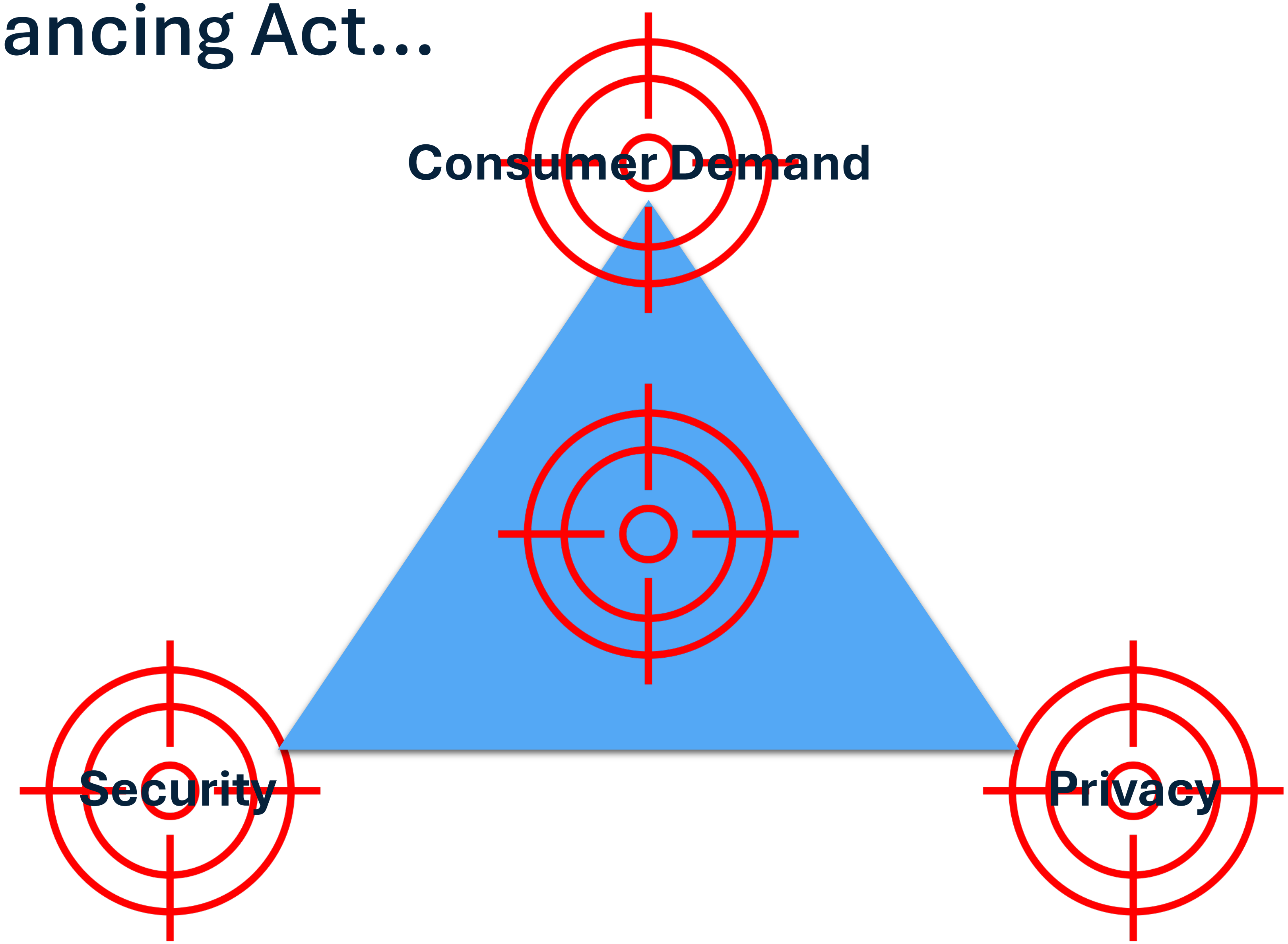
Agenda

- Balancing Security, Privacy & Consumer Demand
- Global Data Privacy Regulations
- The Key Principles of Data Protection
- Today's Open Finance Standards
- How Does Open Finance Consent Work?
- The Future of Open Finance Data Protection
- Q&A

Balancing Security, Privacy & Consumer Demand

The key to success in an open data sharing ecosystem

The Balancing Act...



A Look at Global Privacy Regulations

Understanding what has led us to this point

Global Data Privacy Regulation

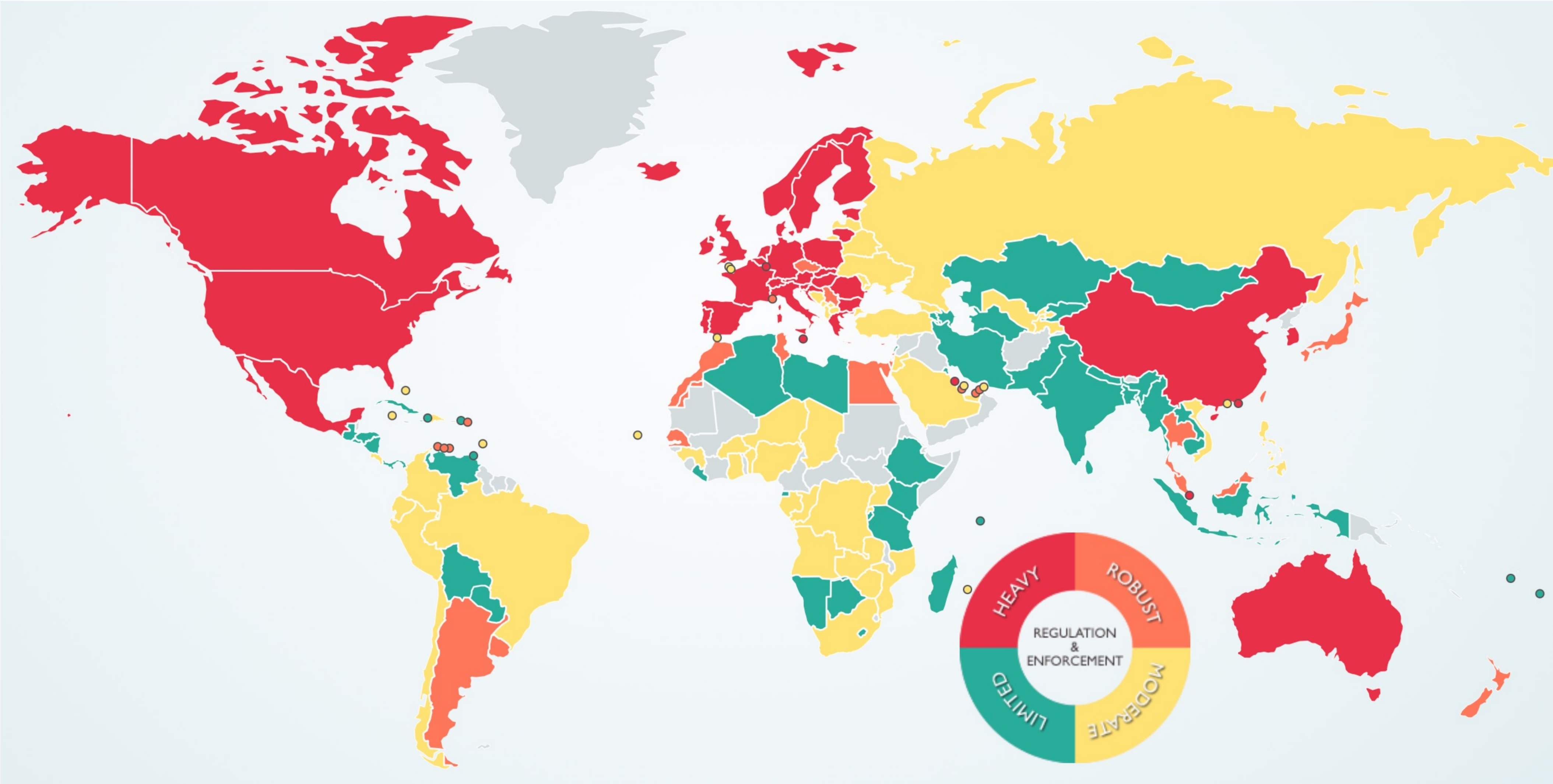


Image Source: DLA Piper "Data Protection Laws Of the World" - https://www.dlapiperdataprotection.com

Privacy Regulations

US

- Privacy Act – 1974
- GLBA – 1999
- CCPA – 2020
- Digital Identity Act(s) – 2020-2022 (Proposed)

Canada

- Privacy Act – 1983
- PIPEDA – 2001 – 2004
- DCIA – proposed 2020 & 2022

Privacy Regulations

EU

- Data Protection Directive - 1995
  - Replaced by GDPR
- GDPR – 2018
  - Global Data Protection Regulation

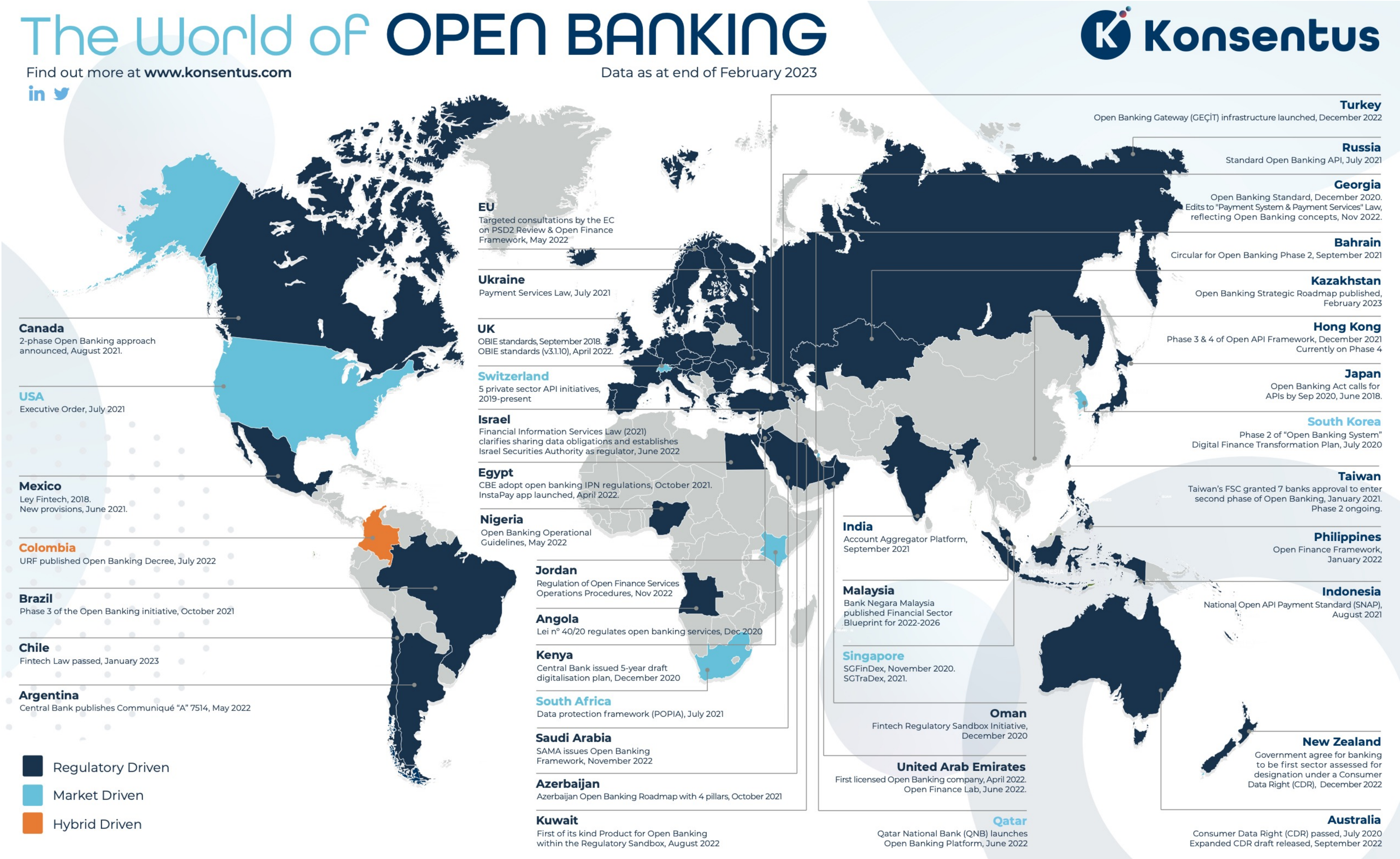
UK

- PECR – 2004 - 2018
- UK-GDPR – 2020
- Data Protection Act – 2020

Open Finance and the Key Principles of Data Protection

How does Open Finance Intersect with Privacy Regulation?

Global Open Finance Regulations



The World of OPEN BANKING

Konsentus

Find out more at **www.konsentus.com**

Data as at end of February 2023

Canada
2-phase Open Banking approach announced, August 2021.

USA
Executive Order, July 2021

Mexico
Ley Fintech, 2018.
New provisions, June 2021.

Colombia
URF published Open Banking Decree, July 2022

Brazil
Phase 3 of the Open Banking initiative, October 2021

Chile
Fintech Law passed, January 2023

Argentina
Central Bank publishes Communiqué "A" 7514, May 2022

■ Regulatory Driven

■ Market Driven

■ Hybrid Driven

EU
Targeted consultations by the EC on PSD2 Review & Open Finance Framework, May 2022

Ukraine
Payment Services Law, July 2021

UK
OBIE standards, September 2018.
OBIE standards (v3.1.10), April 2022.

Switzerland
5 private sector API initiatives, 2019-present

Israel
Financial Information Services Law (2021) clarifies sharing data obligations and establishes Israel Securities Authority as regulator, June 2022

Egypt
CBE adopt open banking IPN regulations, October 2021.
InstaPay app launched, April 2022.

Nigeria
Open Banking Operational Guidelines, May 2022

Jordan
Regulation of Open Finance Services Operations Procedures, Nov 2022

Angola
Lei nº 40/20 regulates open banking services, Dec 2020

Kenya
Central Bank issued 5-year draft digitalisation plan, December 2020

South Africa
Data protection framework (POPIA), July 2021

Saudi Arabia
SAMA issues Open Banking Framework, November 2022

Azerbaijan
Azerbaijan Open Banking Roadmap with 4 pillars, October 2021

Kuwait
First of its kind Product for Open Banking within the Regulatory Sandbox, August 2022

India
Account Aggregator Platform, September 2021

Malaysia
Bank Negara Malaysia published Financial Sector Blueprint for 2022-2026

Singapore
SGFinDex, November 2020.
SGTraDex, 2021.

Oman
Fintech Regulatory Sandbox Initiative, December 2020

United Arab Emirates
First licensed Open Banking company, April 2022.
Open Finance Lab, June 2022.

Qatar
Qatar National Bank (QNB) launches Open Banking Platform, June 2022

Turkey
Open Banking Gateway (GEÇİT) infrastructure launched, December 2022

Russia
Standard Open Banking API, July 2021

Georgia
Open Banking Standard, December 2020.
Edits to "Payment System & Payment Services" Law, reflecting Open Banking concepts, Nov 2022.

Bahrain
Circular for Open Banking Phase 2, September 2021

Kazakhstan
Open Banking Strategic Roadmap published, February 2023

Hong Kong
Phase 3 & 4 of Open API Framework, December 2021
Currently on Phase 4

Japan
Open Banking Act calls for APIs by Sep 2020, June 2018.

South Korea
Phase 2 of "Open Banking System" Digital Finance Transformation Plan, July 2020

Taiwan
Taiwan's FSC granted 7 banks approval to enter second phase of Open Banking, January 2021.
Phase 2 ongoing.

Philippines
Open Finance Framework, January 2022

Indonesia
National Open API Payment Standard (SNAP), August 2021

New Zealand
Government agree for banking to be first sector assessed for designation under a Consumer Data Right (CDR), December 2022

Australia
Consumer Data Right (CDR) passed, July 2020
Expanded CDR draft released, September 2022

Image Source: Konsentus 2024 https://www.konsentus.com/wp-content/uploads/The_World_of_Open_Banking_February_2023.pdf

Principles of Data Protection

GDPR has helped to Solidify & Clarify the key principles:

1. Lawfulness, Fairness & Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Integrity & Confidentiality

Consent Related Topics Covered in Today's specs

Area of Future Exploration for Open Finance

General Data Security that can/should be covered by Open Finance Specs

SECUREAUTH

The Power & Flexibility of Today’s Open Finance Standards

What can we do now within the available open standards?

Consent: Purpose Limitation

Informed Consent & Opt-In for Sharing

- Precise UX Guidelines
- Scope is displayed by both DR & DP
- Granular limitation of purpose & access
- Single consent object per recipient/user/data set

Multiple Consent Grant Models

- Time Limited
- One-Time
- Periodic
- Permanent

Central Management & Delegation

- Consent Receipts & Notifications
- End-to-End revocation

Intermediaries are Now Included

- Modern Specs call for delegation and full transparency of consent across multiple layers of service

Consent: Data Minimization

Active Task Forces focused on:

- Best Practices for Data Minimization
- Sensitive Data Exposure

Data Protection is Addressed in Specs:

- Minimizing Initial Consumer Data Disclosure
- Controlling Scope of Subsequent Disclosures

Working Groups Acknowledge that:

- The data sharing landscape is multi-party, so…
- Regulated or not, the weakest link in the chain will ALWAYS be the core issue

Security: Data Integrity & Confidentiality

Addressed by Security Specifications:

- *Integrity* => Digital Signature
- *Confidentiality* = Digital Encryption
- Communications using open standards will enable seamless integration

Market Driven Ecosystems tend not to:

- Dictate how data is protected
- Dictate how Communications are secured

Adoption of Strong Security Standards will

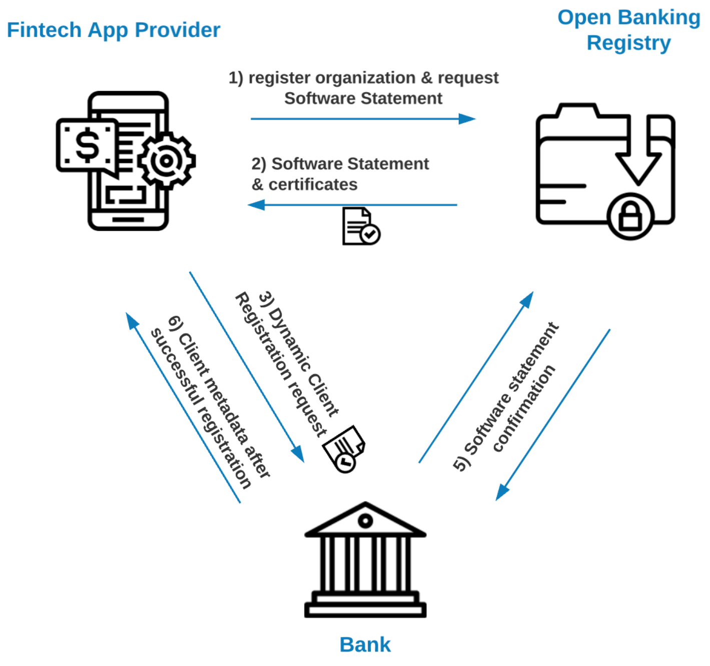
- Offer a proven security profile
- Regulated or not, the weakest link in the chain will ALWAYS be the core issue

How Does Open Finance Consent Actually Work?

Working through the common misconceptions & knowledge gaps

Open Finance

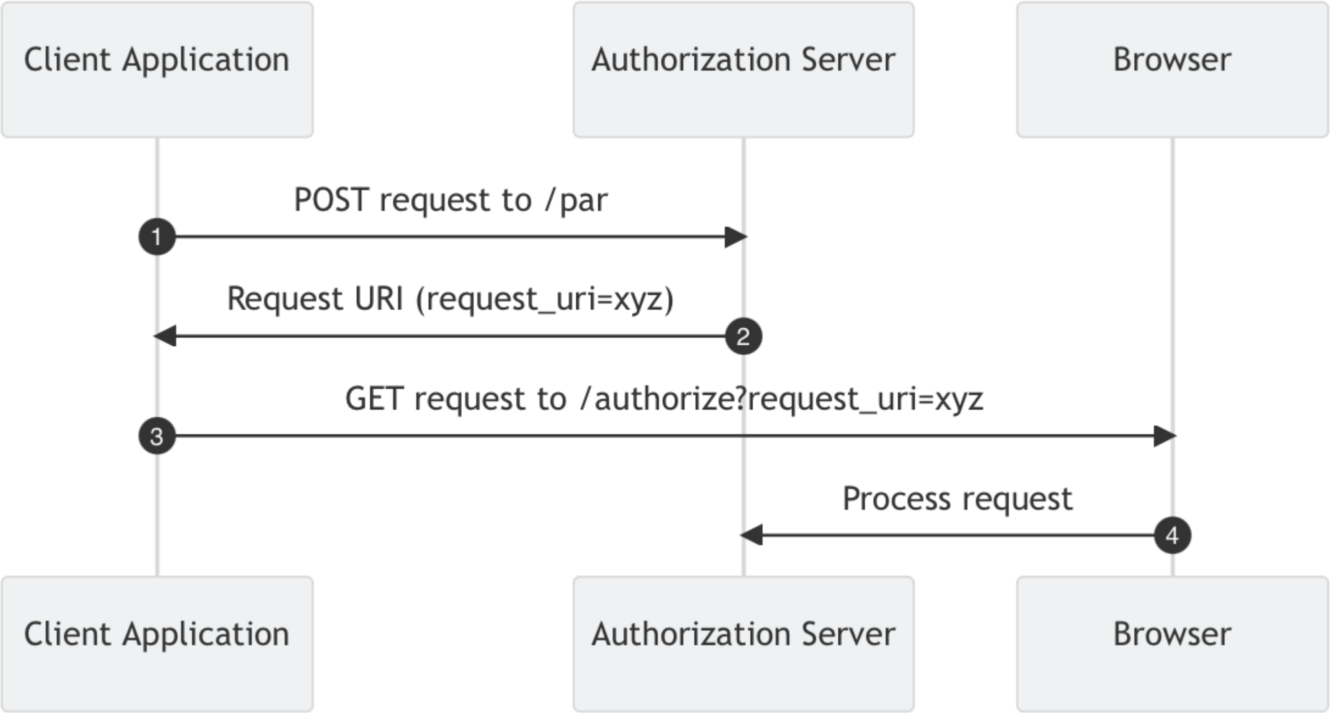
3rd Party Data Sharing


Fintech App Provider
Open Banking Registry
1) register organization & request Software Statement
2) Software Statement & certificates
3) Dynamic Client Registration request
5) Software statement confirmation
6) Client metadata after successful registration
Bank

Establish Trust

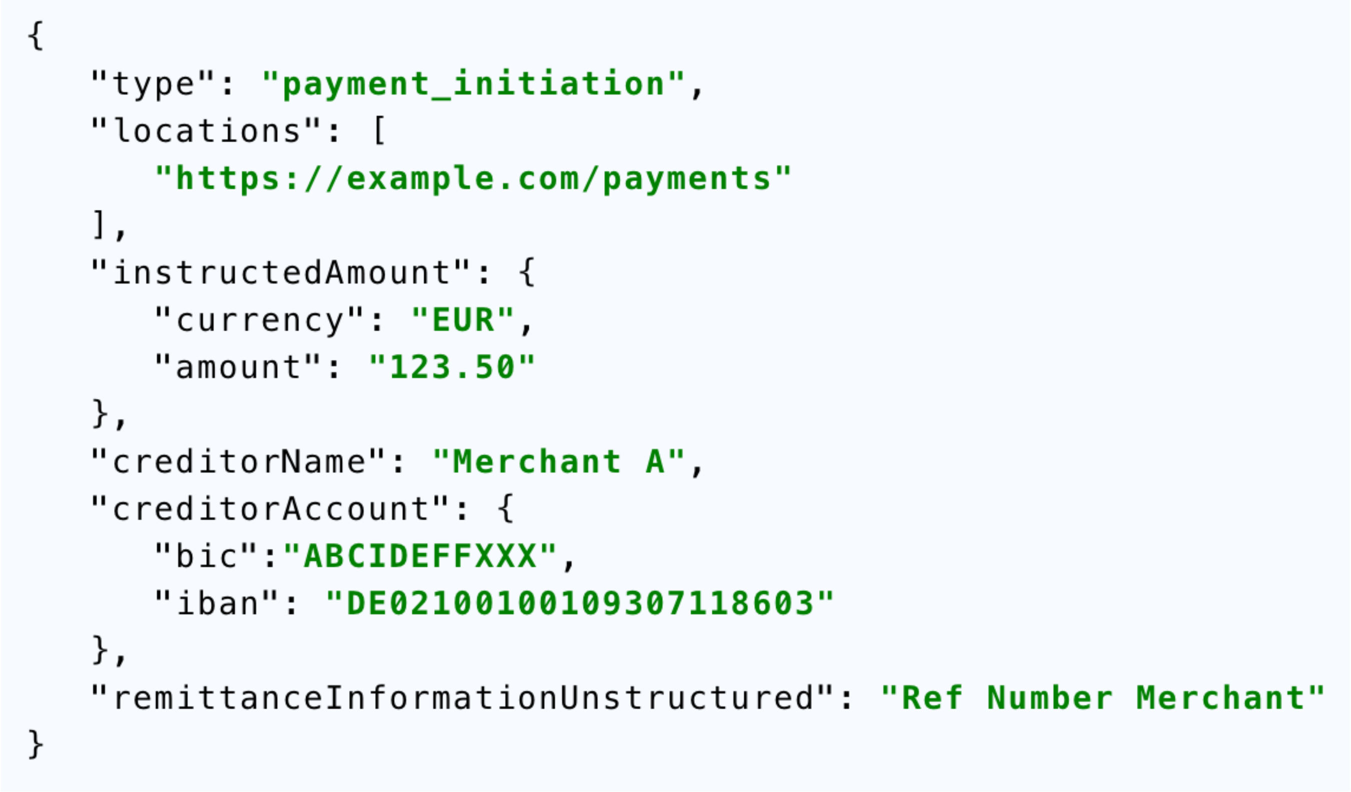
Advanced OAuth 2 Concepts: PAR

- Push Authorization Requests (PAR)
  - Client pushes authorization request payload directly to authorization server (rather than via redirect query string payload)
  - Client receives a URI reference that is relayed via query string payload



Advanced OAuth 2 Concepts: RAR

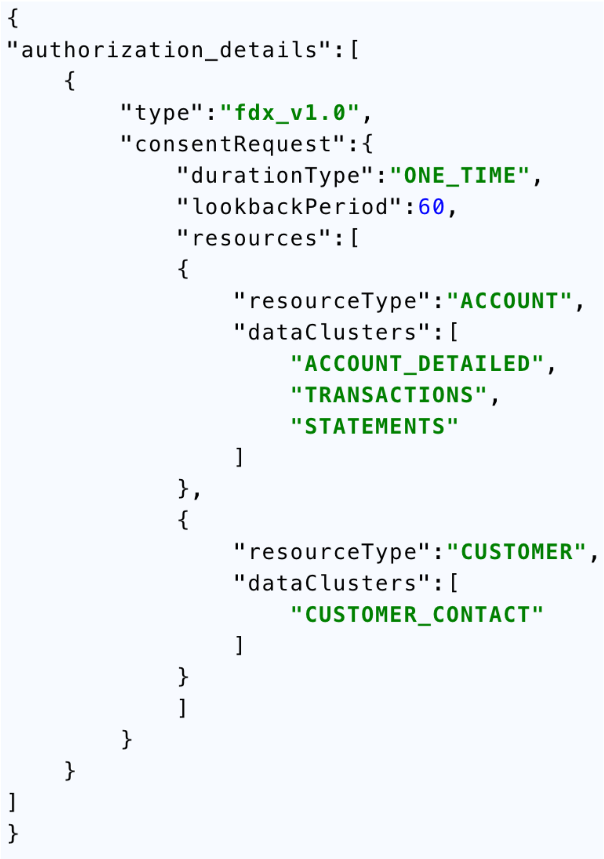
- Rich Authorization Requests (RAR)
  - Client application extends the payload of the authorization request via `authorization_details`
  - This parameter provides more granular authorization capabilities than the standard mechanism: `scope`



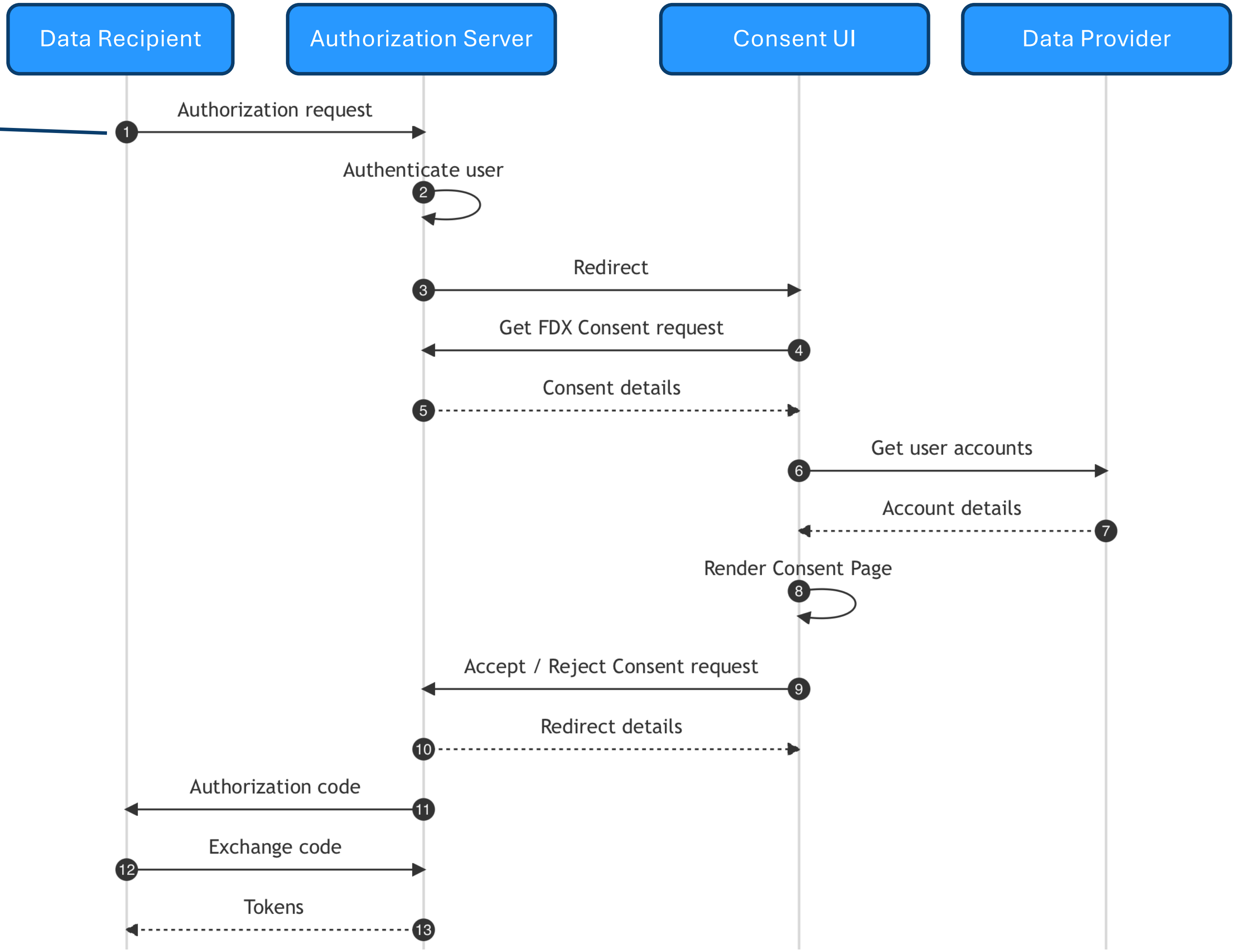
```
{
   "type": "payment_initiation",
   "locations": [
      "https://example.com/payments"
   ],
   "instructedAmount": {
      "currency": "EUR",
      "amount": "123.50"
   },
   "creditorName": "Merchant A",
   "creditorAccount": {
      "bic":"ABCIDEFFXXX",
      "iban": "DE02100100109307118603"
   },
   "remittanceInformationUnstructured": "Ref Number Merchant"
}
```

Example: FDX Consent Flow

Push Authorization Request (PAR) performed using Rich Authorization Request (RAR) format



```
{
"authorization_details":[
    {
        "type":"fdx_v1.0",
        "consentRequest":{
            "durationType":"ONE_TIME",
            "lookbackPeriod":60,
            "resources":[
            {
                "resourceType":"ACCOUNT",
                "dataClusters":[
                    "ACCOUNT_DETAILED",
                    "TRANSACTIONS",
                    "STATEMENTS"
                ]
            },
            {
                "resourceType":"CUSTOMER",
                "dataClusters":[
                    "CUSTOMER_CONTACT"
                ]
            }
            ]
        }
    }
]
}
```



Data Recipient

Authorization Server

Consent UI

Data Provider

1 Authorization request

2 Authenticate user

3 Redirect

4 Get FDX Consent request

5 Consent details

6 Get user accounts

7 Account details

8 Render Consent Page

9 Accept / Reject Consent request

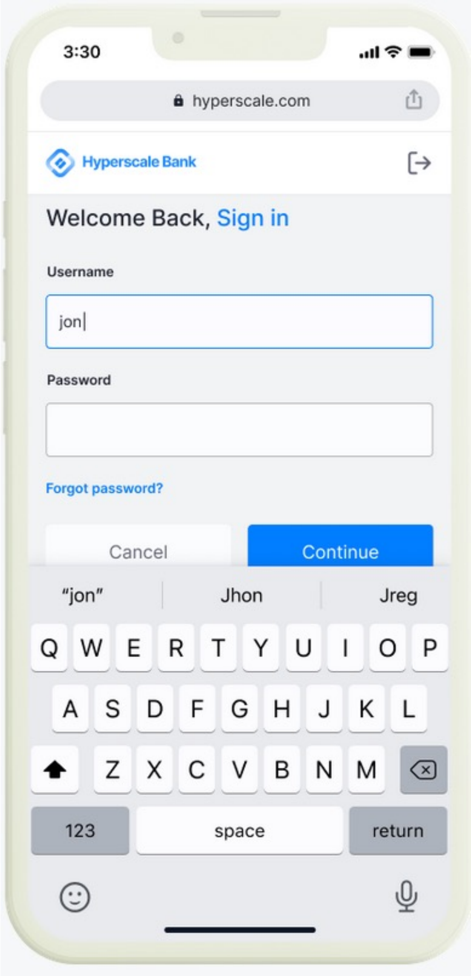
10 Redirect details

11 Authorization code

12 Exchange code

13 Tokens

Example: FDX Consent Flow



3:30

hyperscale.com

Hyperscale Bank

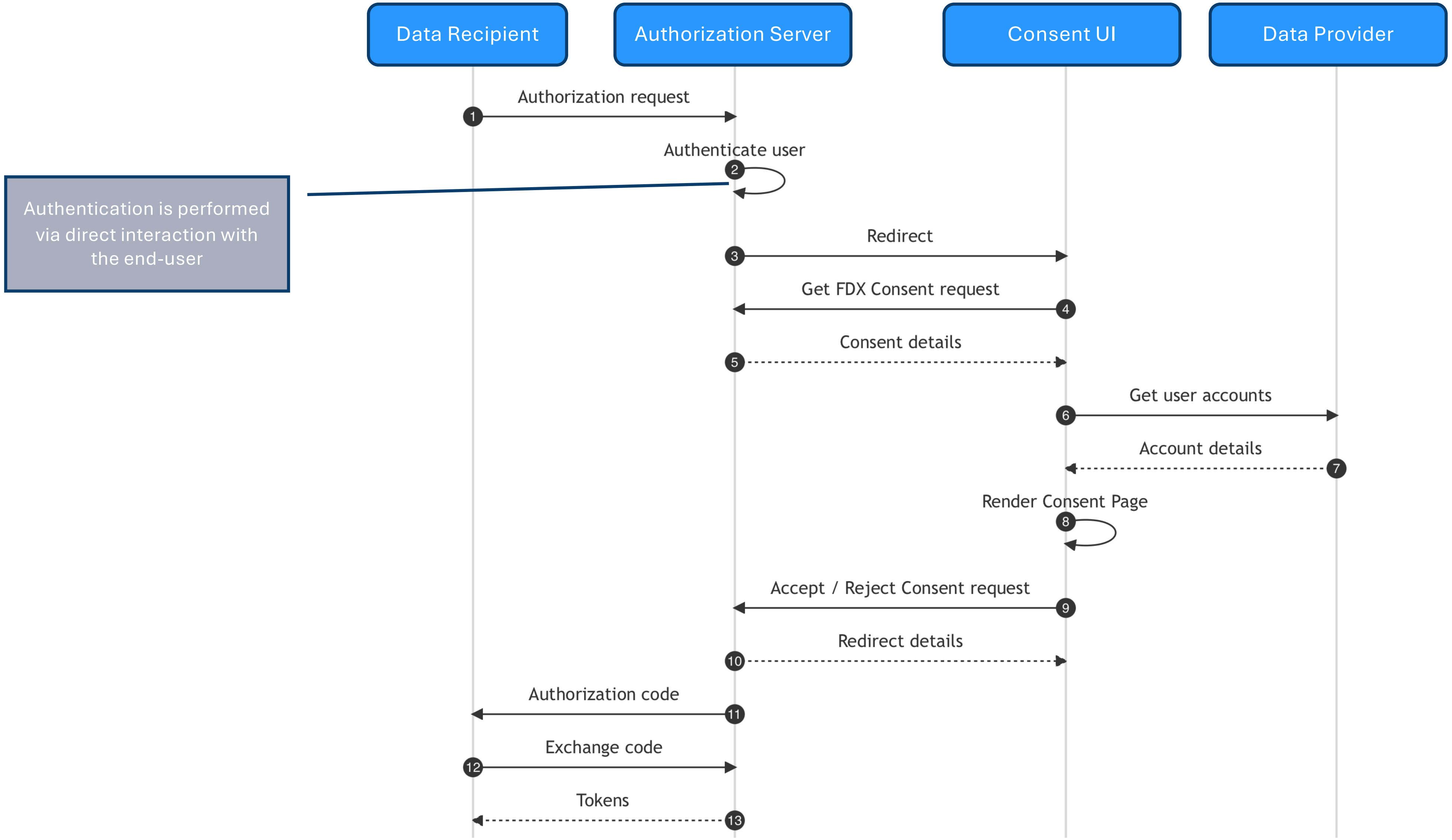
Welcome Back, Sign in

Username

jon

Password

Forgot password?



Data Recipient

Authorization Server

Consent UI

Data Provider

Authentication is performed via direct interaction with the end-user

1 Authorization request

2 Authenticate user

3 Redirect

4 Get FDX Consent request

5 Consent details

6 Get user accounts

7 Account details

8 Render Consent Page

9 Accept / Reject Consent request

10 Redirect details

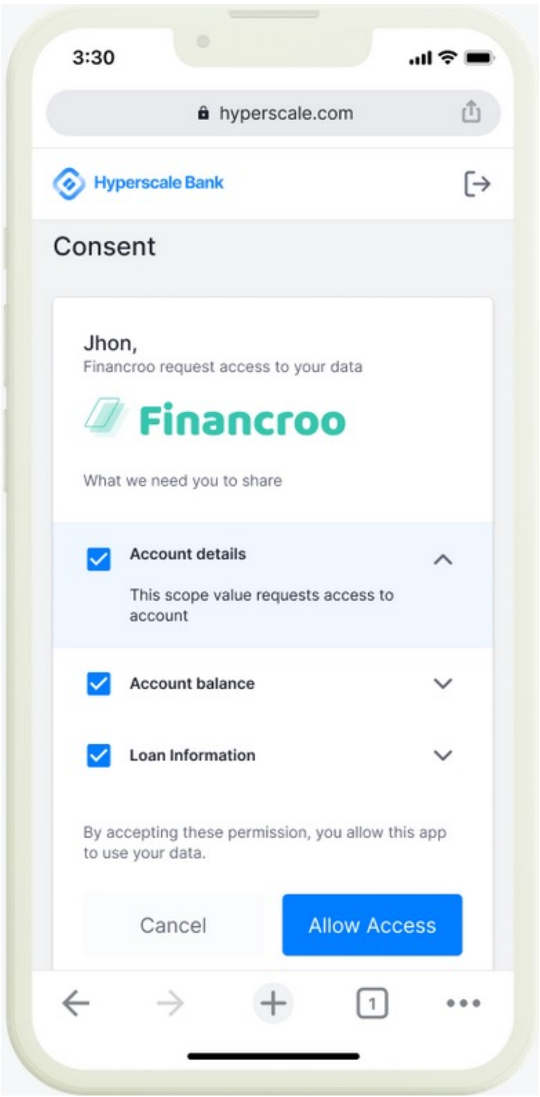
11 Authorization code

12 Exchange code

13 Tokens

SECUREAUTH

Example: FDX Consent Flow



3:30

hyperscale.com

Hyperscale Bank

Consent

Jhon,

Financroo request access to your data

Financroo

What we need you to share

☑ Account details

This scope value requests access to account

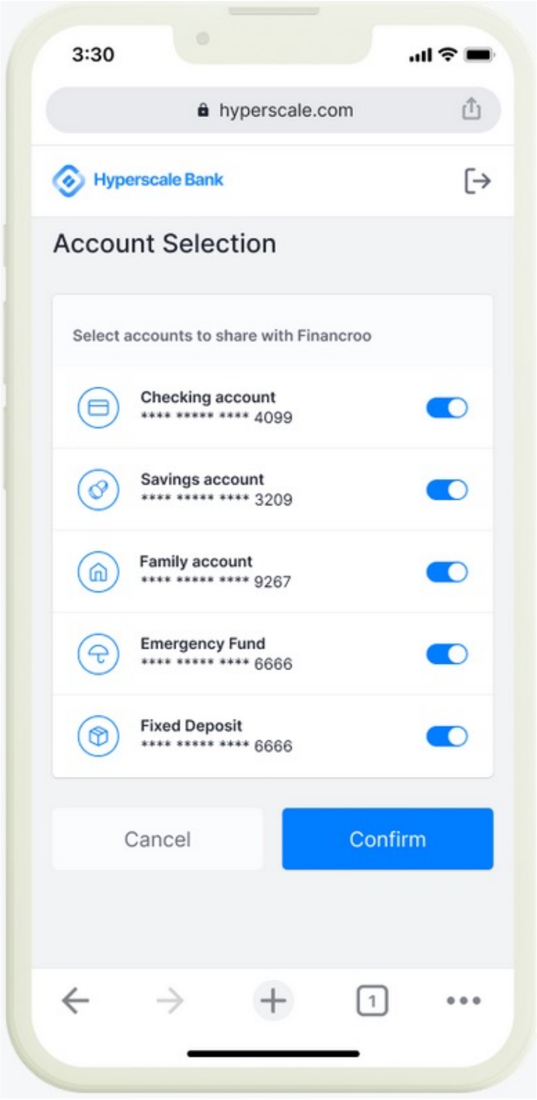
☑ Account balance

☑ Loan Information

By accepting these permission, you allow this app to use your data.

Cancel

Allow Access



3:30

hyperscale.com

Hyperscale Bank

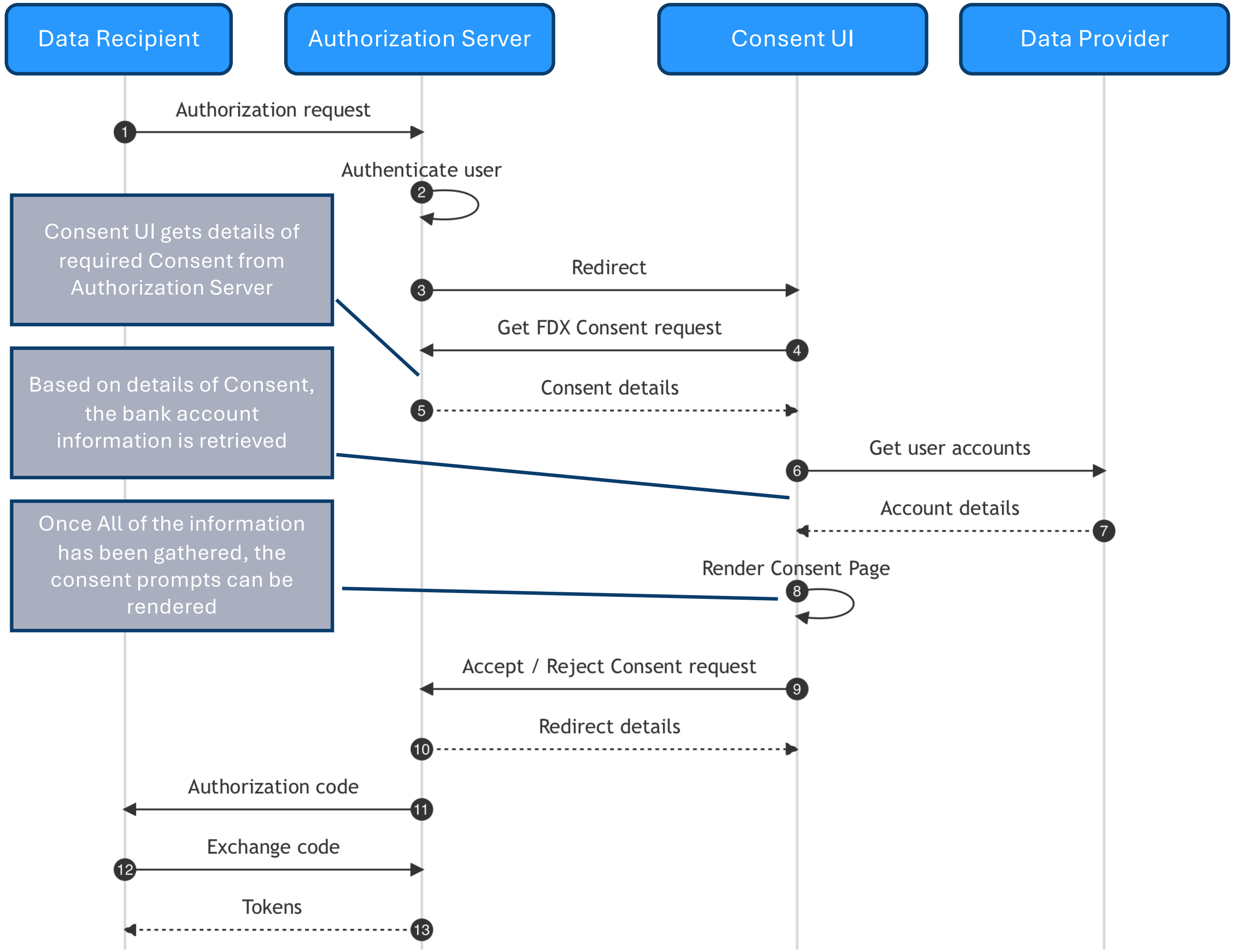
Account Selection

Select accounts to share with Financroo

Checking account **** ***** **** 4099	●
Savings account **** ***** **** 3209	●
Family account **** ***** **** 9267	●
Emergency Fund **** ***** **** 6666	●
Fixed Deposit **** ***** **** 6666	●

Cancel

Confirm



Data Recipient

Authorization Server

Consent UI

Data Provider

1 Authorization request

2 Authenticate user

3 Redirect

4 Get FDX Consent request

5 Consent details

6 Get user accounts

7 Account details

8 Render Consent Page

9 Accept / Reject Consent request

10 Redirect details

11 Authorization code

12 Exchange code

13 Tokens

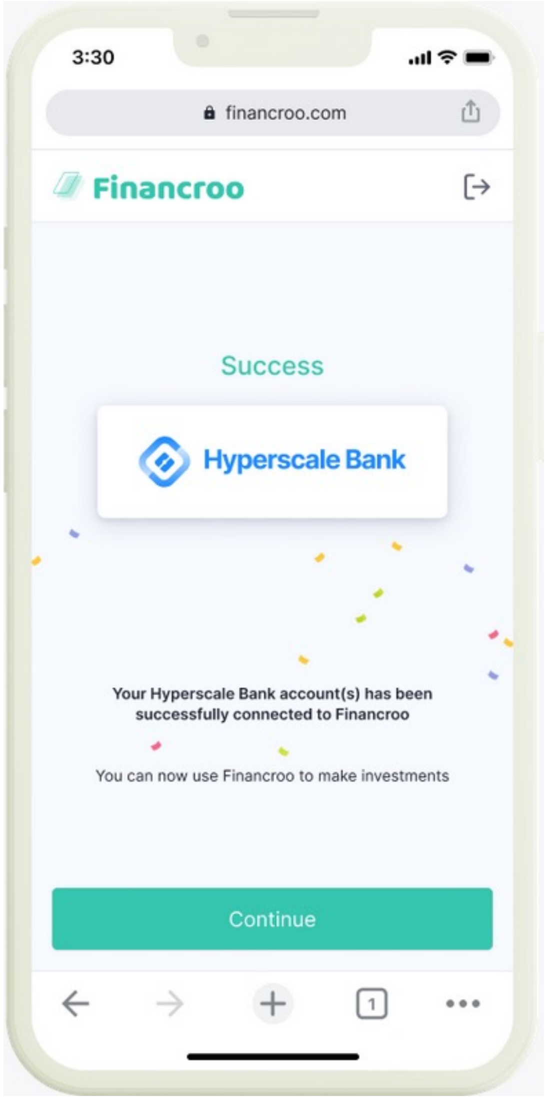
Consent UI gets details of required Consent from Authorization Server

Based on details of Consent, the bank account information is retrieved

Once All of the information has been gathered, the consent prompts can be rendered

SECUREAUTH

Example: FDX Consent Flow



3:30

financroo.com

Financroo

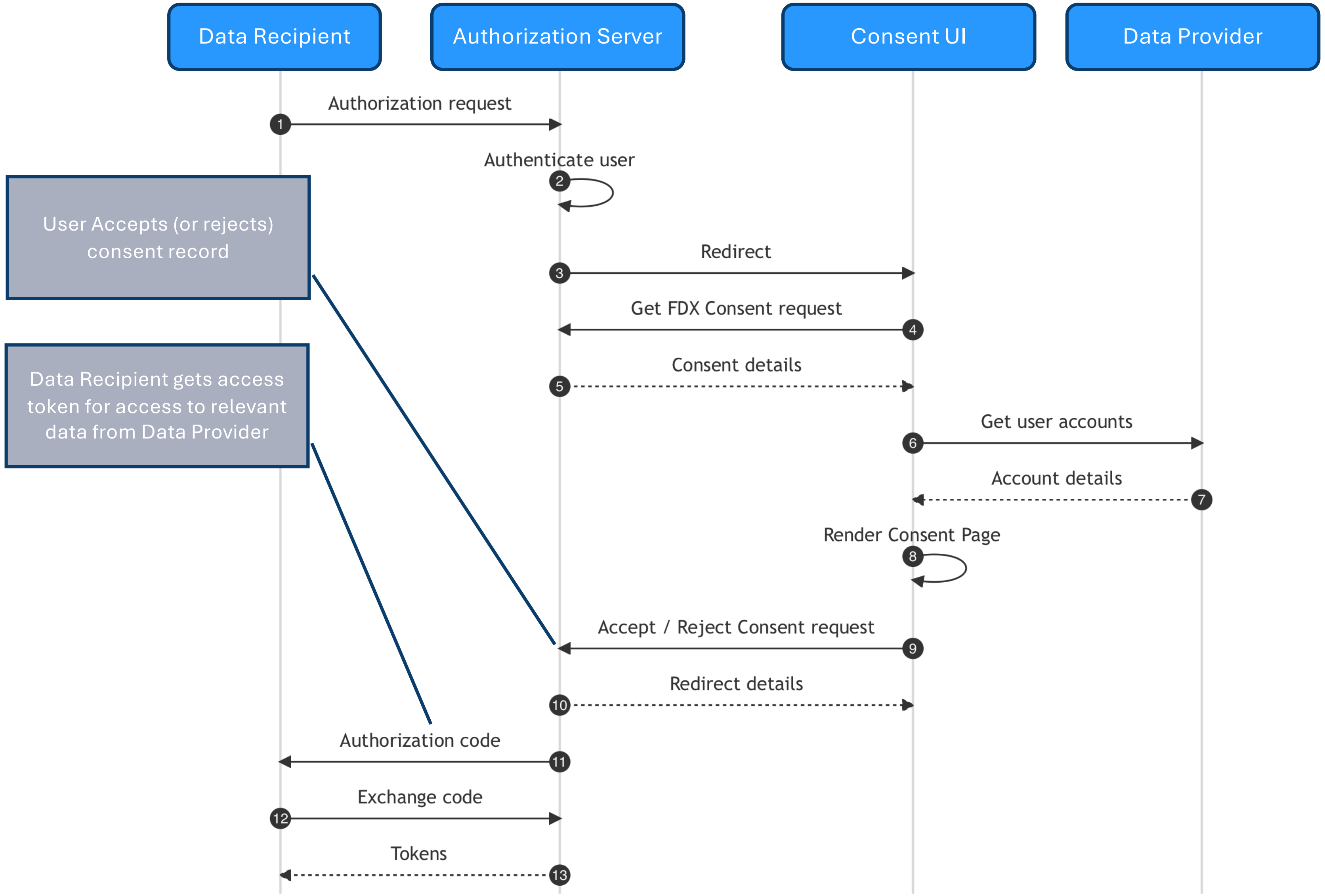
Success

Hyperscale Bank

Your Hyperscale Bank account(s) has been successfully connected to Financroo

You can now use Financroo to make investments

Continue



Data Recipient

Authorization Server

Consent UI

Data Provider

1 Authorization request

2 Authenticate user

3 Redirect

4 Get FDX Consent request

5 Consent details

6 Get user accounts

7 Account details

8 Render Consent Page

9 Accept / Reject Consent request

10 Redirect details

11 Authorization code

12 Exchange code

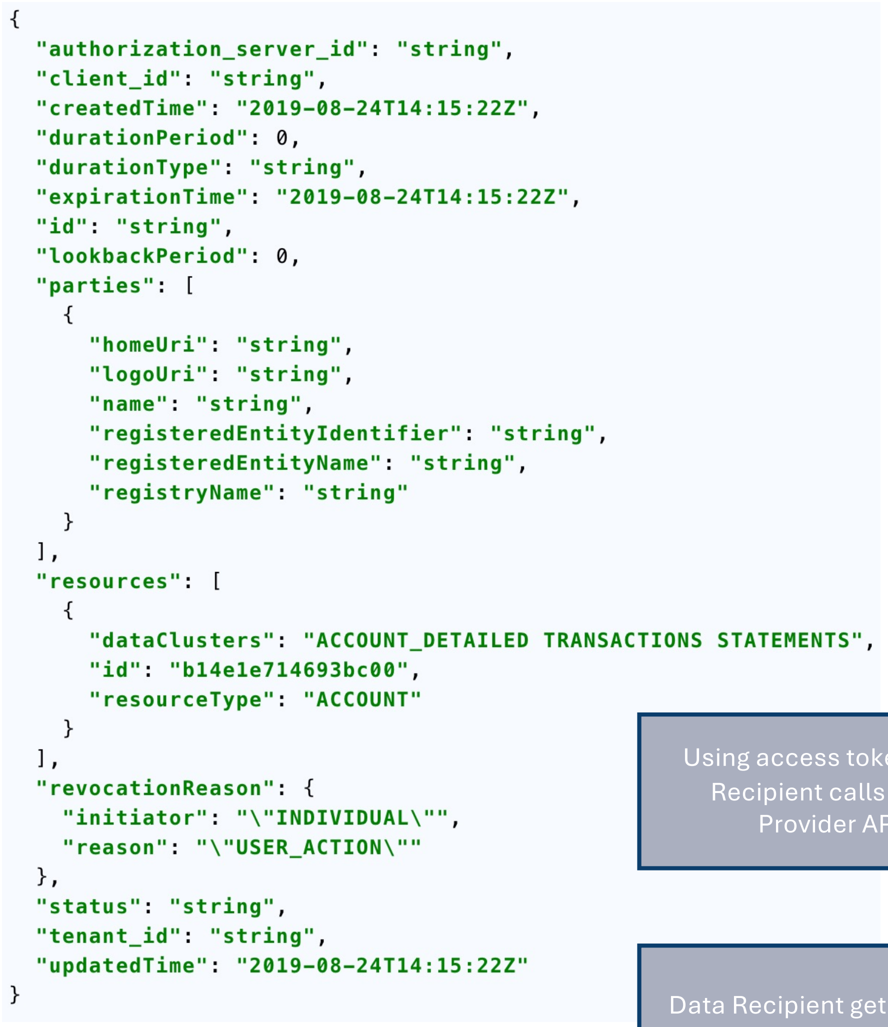
13 Tokens

User Accepts (or rejects) consent record

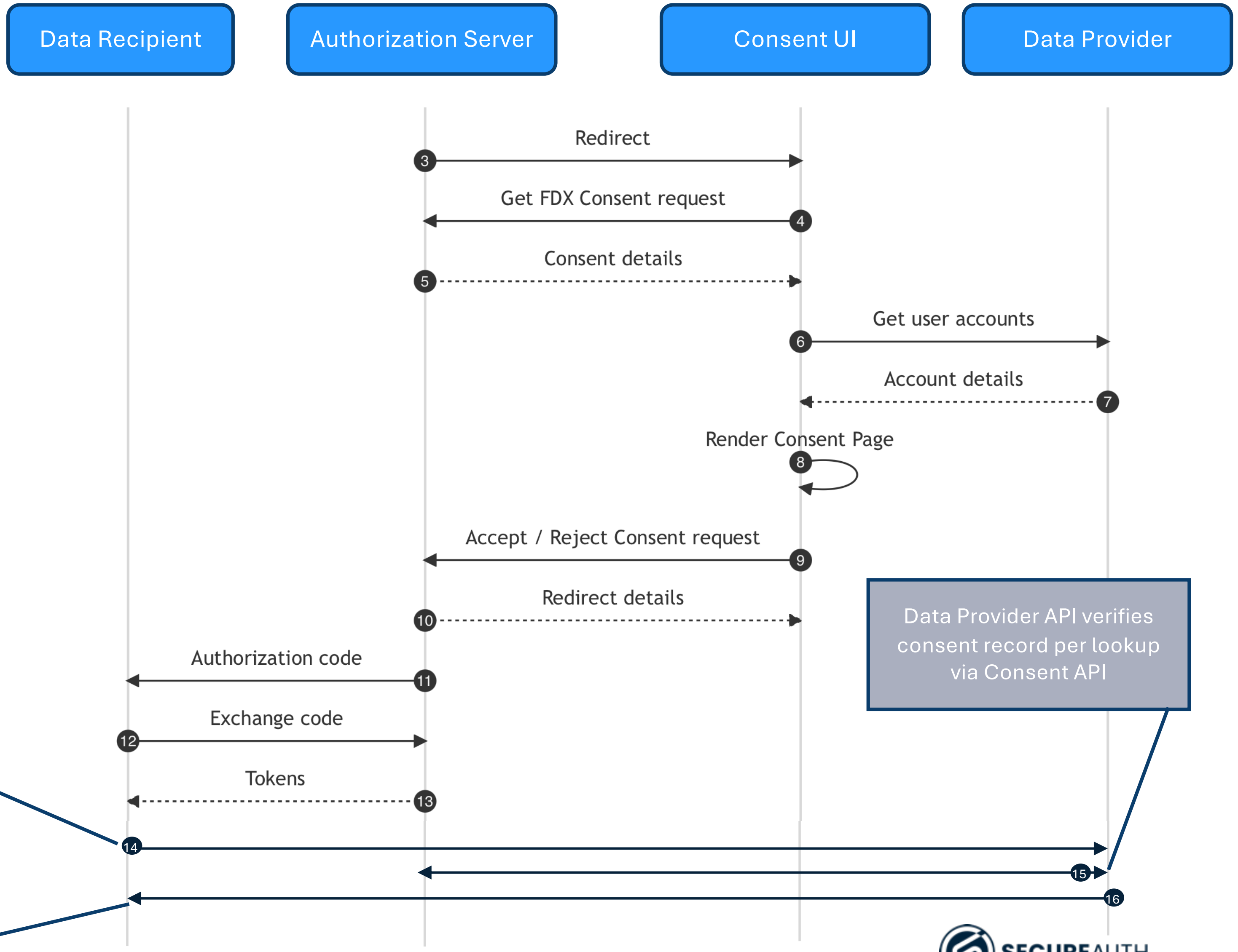
Data Recipient gets access token for access to relevant data from Data Provider

SECUREAUTH

Example: FDX Consent Flow



```
{
  "authorization_server_id": "string",
  "client_id": "string",
  "createdTime": "2019-08-24T14:15:22Z",
  "durationPeriod": 0,
  "durationType": "string",
  "expirationTime": "2019-08-24T14:15:22Z",
  "id": "string",
  "lookbackPeriod": 0,
  "parties": [
    {
      "homeUri": "string",
      "logoUri": "string",
      "name": "string",
      "registeredEntityIdentifier": "string",
      "registeredEntityName": "string",
      "registryName": "string"
    }
  ],
  "resources": [
    {
      "dataClusters": "ACCOUNT_DETAILED TRANSACTIONS STATEMENTS",
      "id": "b14e1e714693bc00",
      "resourceType": "ACCOUNT"
    }
  ],
  "revocationReason": {
    "initiator": "\"INDIVIDUAL\"",
    "reason": "\"USER_ACTION\""
  },
  "status": "string",
  "tenant_id": "string",
  "updatedTime": "2019-08-24T14:15:22Z"
}
```



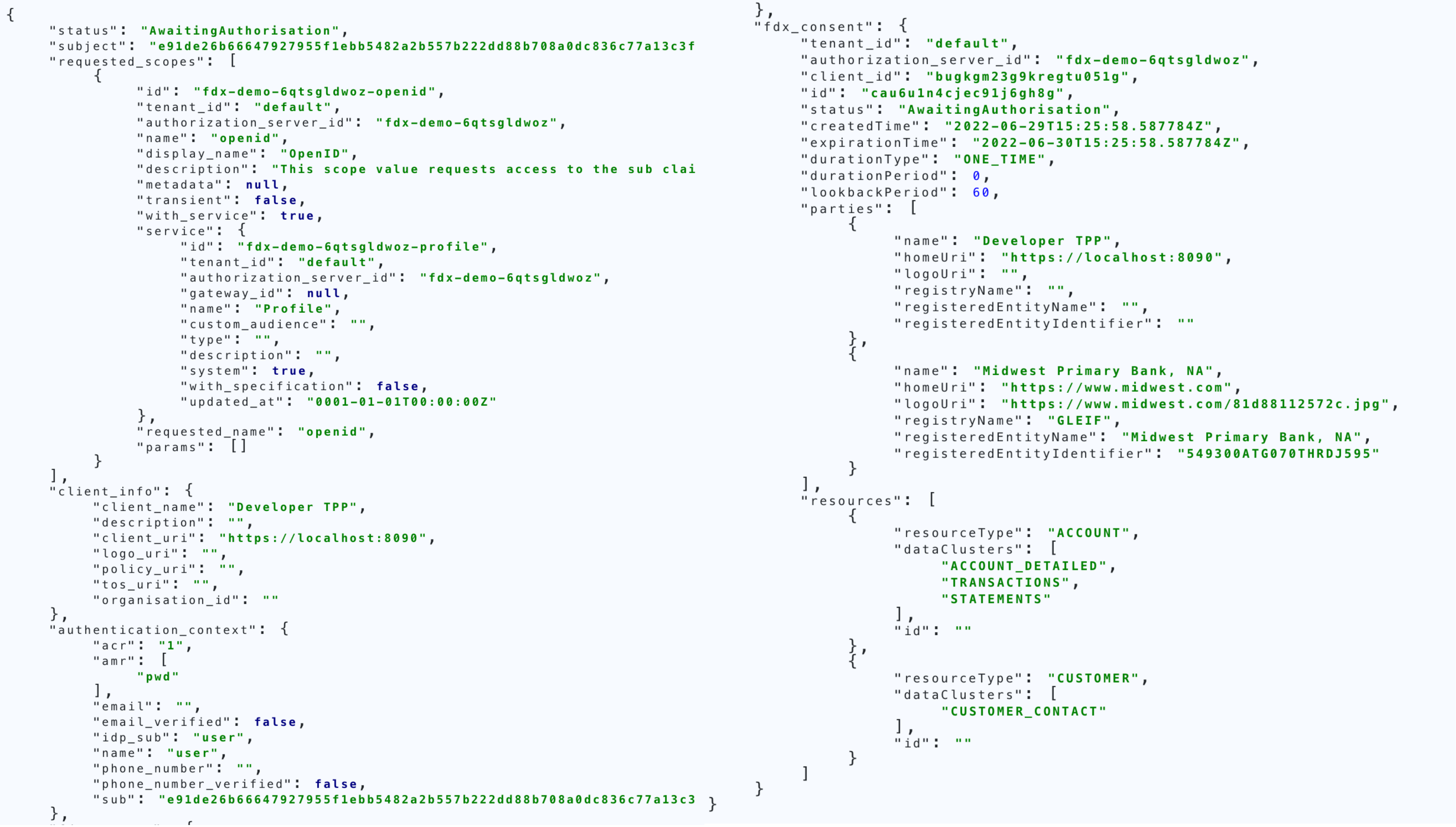
Using access token Data Recipient calls Data Provider API

Data Recipient gets access to data

Data Provider API verifies consent record per lookup via Consent API

SECUREAUTH

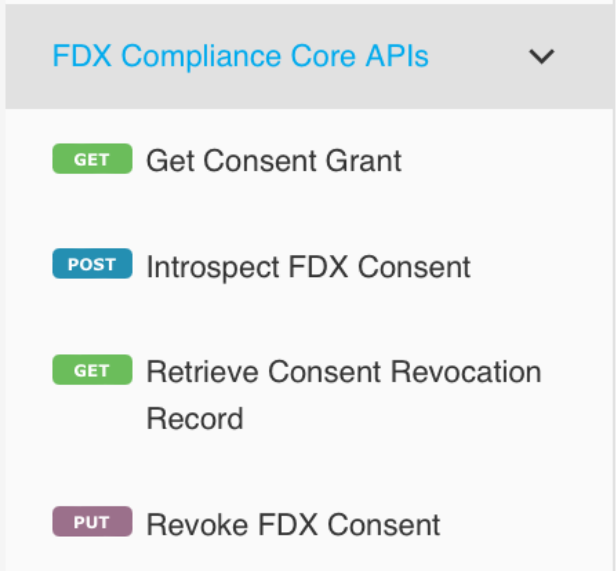
Example: FDX Consent Response



```
{
    "status": "AwaitingAuthorisation",
    "subject": "e91de26b66647927955f1ebb5482a2b557b222dd88b708a0dc836c77a13c3f
    "requested_scopes": [
        {
            "id": "fdx-demo-6qtsgldwoz-openid",
            "tenant_id": "default",
            "authorization_server_id": "fdx-demo-6qtsgldwoz",
            "name": "openid",
            "display_name": "OpenID",
            "description": "This scope value requests access to the sub clai
            "metadata": null,
            "transient": false,
            "with_service": true,
            "service": {
                "id": "fdx-demo-6qtsgldwoz-profile",
                "tenant_id": "default",
                "authorization_server_id": "fdx-demo-6qtsgldwoz",
                "gateway_id": null,
                "name": "Profile",
                "custom_audience": "",
                "type": "",
                "description": "",
                "system": true,
                "with_specification": false,
                "updated_at": "0001-01-01T00:00:00Z"
            },
            "requested_name": "openid",
            "params": []
        }
    ],
    "client_info": {
        "client_name": "Developer TPP",
        "description": "",
        "client_uri": "https://localhost:8090",
        "logo_uri": "",
        "policy_uri": "",
        "tos_uri": "",
        "organisation_id": ""
    },
    "authentication_context": {
        "acr": "1",
        "amr": [
            "pwd"
        ],
        "email": "",
        "email_verified": false,
        "idp_sub": "user",
        "name": "user",
        "phone_number": "",
        "phone_number_verified": false,
        "sub": "e91de26b66647927955f1ebb5482a2b557b222dd88b708a0dc836c77a13c3 }
    },
```

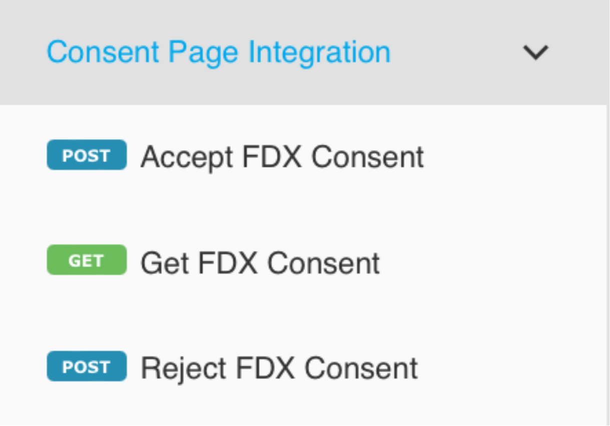
```
    },
    "fdx_consent": {
        "tenant_id": "default",
        "authorization_server_id": "fdx-demo-6qtsgldwoz",
        "client_id": "bugkgm23g9kregtu051g",
        "id": "cau6u1n4cjec91j6gh8g",
        "status": "AwaitingAuthorisation",
        "createdTime": "2022-06-29T15:25:58.587784Z",
        "expirationTime": "2022-06-30T15:25:58.587784Z",
        "durationType": "ONE_TIME",
        "durationPeriod": 0,
        "lookbackPeriod": 60,
        "parties": [
            {
                "name": "Developer TPP",
                "homeUri": "https://localhost:8090",
                "logoUri": "",
                "registryName": "",
                "registeredEntityName": "",
                "registeredEntityIdentifier": ""
            },
            {
                "name": "Midwest Primary Bank, NA",
                "homeUri": "https://www.midwest.com",
                "logoUri": "https://www.midwest.com/81d88112572c.jpg",
                "registryName": "GLEIF",
                "registeredEntityName": "Midwest Primary Bank, NA",
                "registeredEntityIdentifier": "549300ATG070THRDJ595"
            }
        ],
        "resources": [
            {
                "resourceType": "ACCOUNT",
                "dataClusters": [
                    "ACCOUNT_DETAILED",
                    "TRANSACTIONS",
                    "STATEMENTS"
                ],
                "id": ""
            },
            {
                "resourceType": "CUSTOMER",
                "dataClusters": [
                    "CUSTOMER_CONTACT"
                ],
                "id": ""
            }
        ]
    }
```

Additional FDX Consent APIs



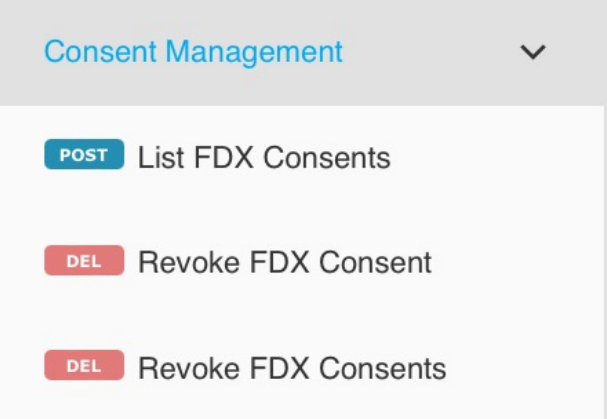
FDX Compliance Core APIs

- GET Get Consent Grant
- POST Introspect FDX Consent
- GET Retrieve Consent Revocation Record
- PUT Revoke FDX Consent



Consent Page Integration

- POST Accept FDX Consent
- GET Get FDX Consent
- POST Reject FDX Consent



Consent Management

- POST List FDX Consents
- DEL Revoke FDX Consent
- DEL Revoke FDX Consents

https://cloudentity.com/developers/api/openfinance_apis/fdx/

What Might the Future Hold for Open Finance Data Protection?

What should we be thinking about as our ecosystems mature?

What’s Next?

Moving Beyond Finance

Open Health

- What types of consent controls will we need to weave 3rd party data sharing standards into HIPAA?

Open Data

- Can we define standards that can be used for any industry?
- What about global cross-boarder transactions?

Taking control of Your Digital Identity

- Digital Identity provided by National/State Governments will bring new authorization and consent challenges – how will we deal with this?

Storage Limitation

An Area for Expansion?

- Emerging/evolving regional specifications should begin to contemplate how this might be handled

What's the issue?

- Data that is accessed once can be stored indefinitely
  - This will certainly happen inadvertently, but will also be a common privacy attack vector

How can we address this?

- Watermarking?
- Self-destructive or self-locking data?
- DRM-style content encryption?
- Legislation!

Questions?