Evaluating the Adoption of Federation by Open Finance and Open Insurance BR

Prepared for the Open Finance and Open Insurance Work Groups

Dated 01/09/2023

Erick Domingues – Raidiam Programme Manager

Raidiam proposes to separate the presentations of the Suggested Federation Protocol and its impacts on three different sessions

1. Introduction

- What is the OIDC Federation – Protocol
- Differences and improvements between DCR-BR and the proposed Federation-BR profile
- Introducing the Unique Client_ID requirement
- Obtaining an Entity Configuration

2. Federation Artefacts

- Entity Statement Endpoint Structure
- Fetch Endpoint Structure
- List Endpoint Structure
- Chain Walk and how Federation Ensures Trust

3. Implementation and Open Data BR Federation

- Suggested Transition Plan
- Defining the Federation Standard, Certification and Preparing the Directory
- Migrating From DCR to Federation
- Setting the Open Data Brazil Entity

We highlight that "The Federation Protocol" to be presented on the agendas will consider the premises that have been presented and approved on the Months of June and July – For Simplicity we will call this the Federation BR

Federation is a framework to establish trust between clients and servers which can be used in conjunction with an Authorization Profile, like FAPI, to allow user data to be shared

Federation Profile Definitions

What is included on the Profile

- OIDC Federation is a mechanism for establishing trust between two entities (e.g TPP and Bank) wanting to interact with each other, by using a trusted third party, known as the Trust Anchor (The Directory)

- It offers the necessary technical building blocks for creating a dynamic and distributed network of trust, called a federation.

- It is Maintained by the OIDF that can be used in conjunction with any security profiles like FAPI 1.0 Adv and FAPI 2.0

What is not included on the Profile

- It's not an Authorization Profile and should not replace any profile like FAPI, OAuth 2.0 or OIDC

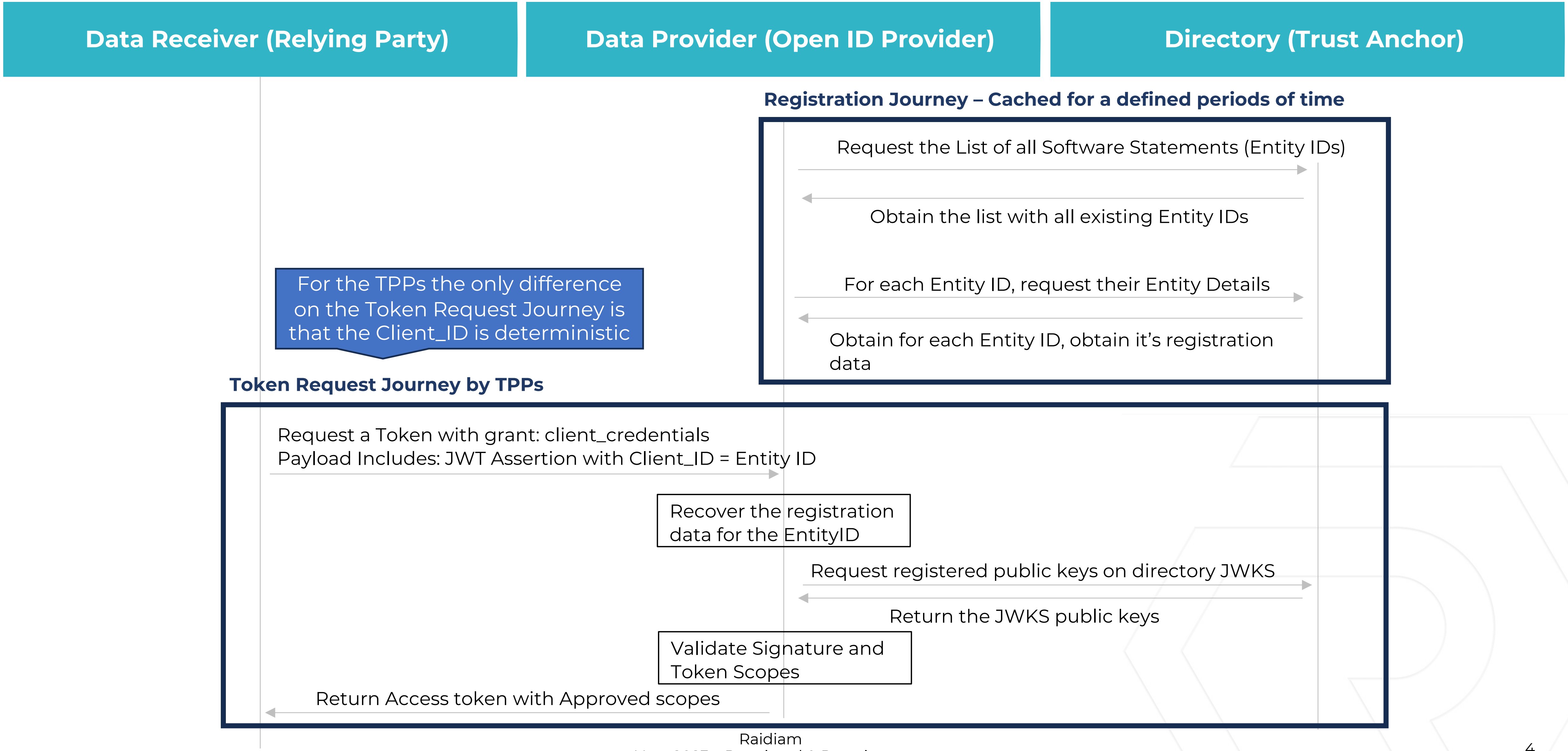
- It doesn't handle the business logic, policies, or workflows that might be necessary for the actual interactions between these entities

- It does not prescribe or mandate a specific configuration of any party – This is to be defined by the Federation Controller

Registration with the Federation BR would be done entirely between the Data Providers and the Directory, allowing for a standardized registration flow

Simplified

For Discussion



Data Receiver (Relying Party)

Data Provider (Open ID Provider)

Directory (Trust Anchor)

Registration Journey – Cached for a defined periods of time

Request the List of all Software Statements (Entity IDs)

Obtain the list with all existing Entity IDs

For each Entity ID, request their Entity Details

Obtain for each Entity ID, obtain it's registration data

For the TPPs the only difference on the Token Request Journey is that the Client_ID is deterministic

Token Request Journey by TPPs

Request a Token with grant: client_credentials
Payload Includes: JWT Assertion with Client_ID = Entity ID

Recover the registration data for the EntityID

Request registered public keys on directory JWKS

Return the JWKS public keys

Validate Signature and Token Scopes

Return Access token with Approved scopes

The Federation-BR profile can be seen as an update from the existing DCR-BR – Four diferences can be highlighted when comparing both profiles

Comparison between the current DCR-BR and the Proposed Federation-BR profile

DCR - BR	FEDERATION - BR
Registration : Performed actively by the client before the client <-> server interaction, via POST to the registration endpoint	**Registration** : Performed by the server, through proactive consultation of data in the directory, with daily updates, for example, or upon receiving a call to the token endpoint
Registration Payload: Client Defined Data + Software Statement Assertion (SSA) Obtained as a JWT signed by the directory	**Registration Payload** : Entity Statements publicized by the directory, stored in logically hierarchical endpoints
Client ID : Random string that must be unique for each client <-> server connection	**Client ID** : Unique URI for each participant directory endpoint-based client

Implementing Federation over DCR should reduce interoperability issues caused by DCR, improve access control by Governance Structure and Allow for multiple Ecosystem to communicate easier

DCR – Current Standard

Simplified Registration Mechanism :

- Performed actively by the client before the client <-> server interaction, via POST to the registration endpoint

.

Perceived Challenges :

- One different Registration request for each Client <-> Server interaction, leading to interoperability issues when one party does a mistake
- Registration data can often be outdated as a DCM is required for it to be updated
- Issues on registration Journey might lead to client_ids being stuck, forcing manual recovery of refresh_tokens or removal of clients
- Supporting multiple directories on registration requires multiple changes on standards

Federation – Proposed Standard

Simplified Registration Mechanism :

- Performed by the server, through proactive consultation of data in the directory, with daily updates, for example, or upon receiving a call to the token endpoint

Improvements:

- Full responsibility on Data Receivers on refreshing registration data, allowing TPPs to, Once onboarded into the Directory, to obtain data from servers directly
- Registration data is refreshed periodically allowing for fine control by Structure
- Standardized client_id and Federation Operator as the single source of truth removes any issues with lost clients
- Framework allows for easy addition of new Federations within existing Federation

FEDERATION STUDY – UNIQUE CLIENT_ID

To enable the Federation-BR profile all the existing Ecosystem client_id would need to be updated to a URI structure that would point to a URI hosted by the Federation Controller

Current ClientID

Client ID : Random string that must be unique for each client <-> server registration

Example of Client_IDs obtained for two different client <-> server interactions, from the FVP

- Bank 1:
  - Test 1: 10176094415340
  - Test 2: 10221648257854
- Bank 2:
  - Test 1: 70ee2970-038b-44d6-9300-d3af3a890154
  - Test 2: 70ee2970-038b-44d6-9300-d3af3a890154
- Bank 3:
  - Test 1: T7PPEPhV2Gt8gayR2vuPGRqI9AdtOGho
  - Test 2: HHJLltzuNXYR8MbwtDKTPKSl9PtafAzj

Some Servers set the Client_ID to be equal to the SS_ID but this is seldom the case

Proposed ClientID

Client ID : The Federation Entity ID, which would be a Unique URI for each participant directory,

Structure of proposed client_id

- The Client ID Host will point to the Federation endpoint : https://federation.directory.openbankingbrasil.org.br
- The Path will then include the SS_ID:
  - **openid_relying_party/<SS_ID>**
- **Example:** The FVP 2.0 unique Client_ID for the Federation would be :
  - **https://federation.directory.openbankingbrasil.org.br/openid_relying_party/70ee2970-038b-44d6-9300-d3af3a890154**

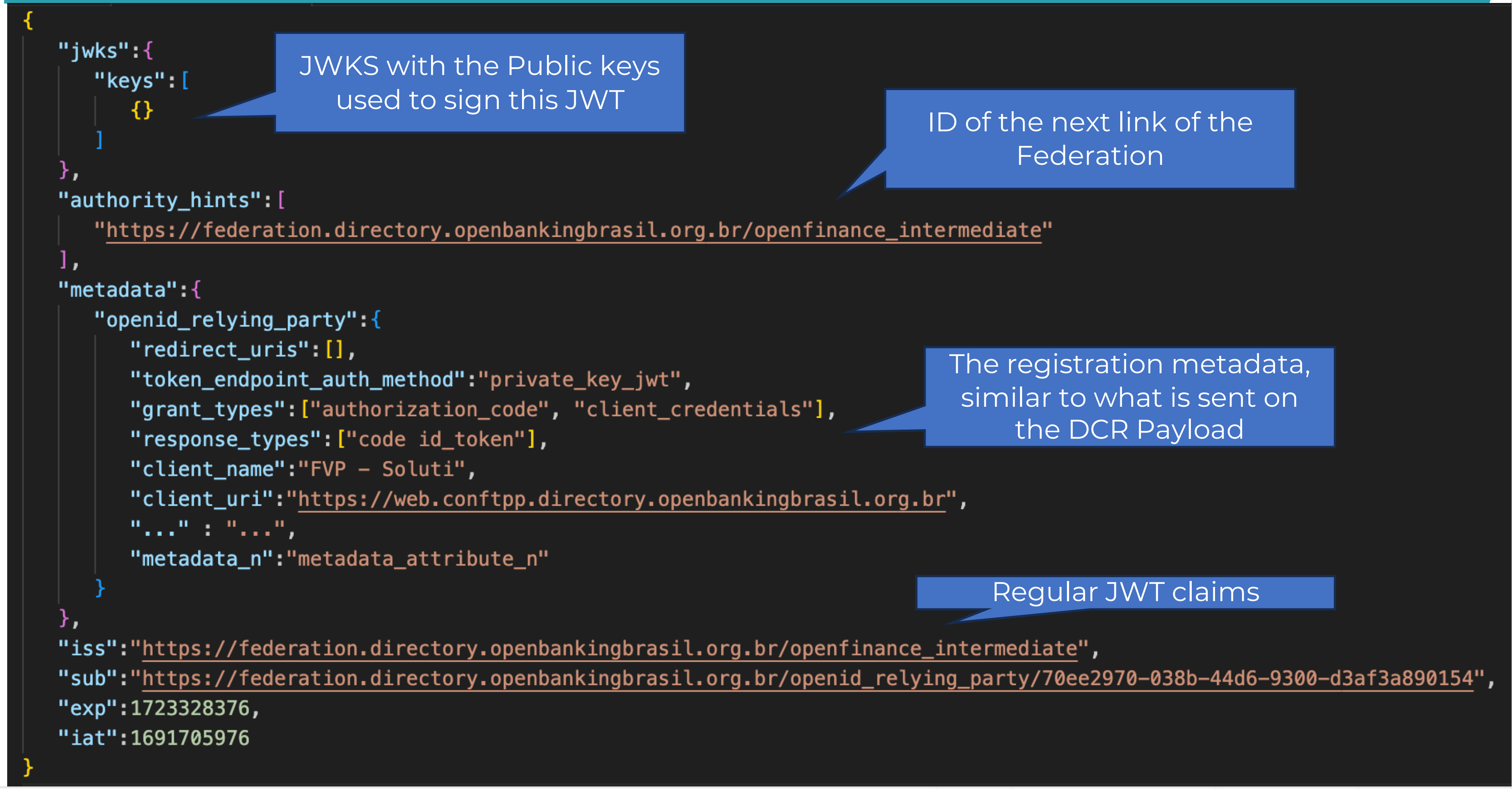
FEDERATION STUDY – UNIQUE CLIENT_ID

Having the Client_id as the Entity Identifier, which points to a URI a trusted directory endpoint, allows fast and standardized validation of the Software Statement Metadata

Federation client_id outcome

- Setting the client_id to be the Entity Identifier allows a single identification for the RP, regardless of the Federation he communicates with
- By setting the Entity Identifier to be a URI, all servers will obtain the exact same metadata (well-known) information about the RP prior to authenticating it
- Any server that do not recognize the RP can quickly evaluate its metadata verify if it belongs to a Trusted Federation, allowing the RP to be authenticated

Expected result[1] when calling : https://federation.directory.openbankingbrasil.org.br/openid_relying_party/70ee2970-038b-44d6-9300-d3af3a890154/.well-known/openid-federation



```
{
   "jwks":{
      "keys":[
         {}
      ]
   },
   "authority_hints":[
      "https://federation.directory.openbankingbrasil.org.br/openfinance_intermediate"
   ],
   "metadata":{
      "openid_relying_party":{
         "redirect_uris":[],
         "token_endpoint_auth_method":"private_key_jwt",
         "grant_types":["authorization_code", "client_credentials"],
         "response_types":["code id_token"],
         "client_name":"FVP – Soluti",
         "client_uri":"https://web.conftpp.directory.openbankingbrasil.org.br",
         "..." : "...",
         "metadata_n":"metadata_attribute_n"
      }
   },
   "iss":"https://federation.directory.openbankingbrasil.org.br/openfinance_intermediate",
   "sub":"https://federation.directory.openbankingbrasil.org.br/openid_relying_party/70ee2970-038b-44d6-9300-d3af3a890154",
   "exp":1723328376,
   "iat":1691705976
}
```

JWKS with the Public keys used to sign this JWT

ID of the next link of the Federation

The registration metadata, similar to what is sent on the DCR Payload

Regular JWT claims

[1] Example shows a JSON, however output would be a JWT for explanation

Raidiam proposes to separate the presentations of the Suggested Federation Protocol and its impacts on three different sessions

1. Introduction

- What is the OIDC Federation – Protocol
- Differences and improvements between DCR-BR and the proposed Federation-BR profile
- Introducing the Unique Client_ID requirement
- Obtaining an Entity Configuration

2. Federation Artefacts

- Entity Statement Endpoint Structure
- Fetch Endpoint Structure
- List Endpoint Structure
- Chain Walk and how Federation Ensures Trust

3. Implementation and Open Data BR Federation

- Suggested Transition Plan
- Defining the Federation Standard, Certification and Preparing the Directory
- Migrating From DCR to Federation
- Setting the Open Data Brazil Entity

We highlight that "The Federation Protocol" to be presented on the agendas will consider the premises that have been presented and approved on the Months of June and July – For Simplicity we will call this the Federation BR

There are four main basic types of Artefacts that must be published and maintained by the Federations within the Open Data BR Federation

Different Types of artefacts published in a Federation

Leaf Entity Statement

- A signed JWT (JSON Web Token) that contains the information about an Entity that participate in federation. This includes metadata about itself, and reference data related to the Federations that it belongs to.
- All the Relying Parties (Software Statements) will have one corresponding Leaf Entity Statement on the Federation, which is obtained by calling its Entity ID + /.well-known/openid-federation

Federation Entity Statement

- Signed JWT published by the Federation Issuer that contain metadata about itself – This include all relevant Federation Endpoints
- This Entity Statement can be used as a starting point to obtain the details about all the Entities inside the Federation as well as validate if an Entity belongs to the Federation

Federation Fetch – Entity Statement

- Signed JWT published by the Federation Issuer that can be used to retrieve Entity Statements which contain Federation Specific Policies about the Entities that existing within a Federation
- For the Open Data BR Federation, as the Leaf Entity Statements and the Fetch Entity Statements are both issued by the Directory, they will technically provide the same data, however this is not true for all Federations

Federation List Endpoint

- An endpoint at which an Entity can retrieve a list of Entity IDs that have been issued by a Federation
- For the Open Data BR Federation this will provide a list of the Relying Parties within a given Federation, for example all the Software Statements registered on the Open Banking Brazil Directory

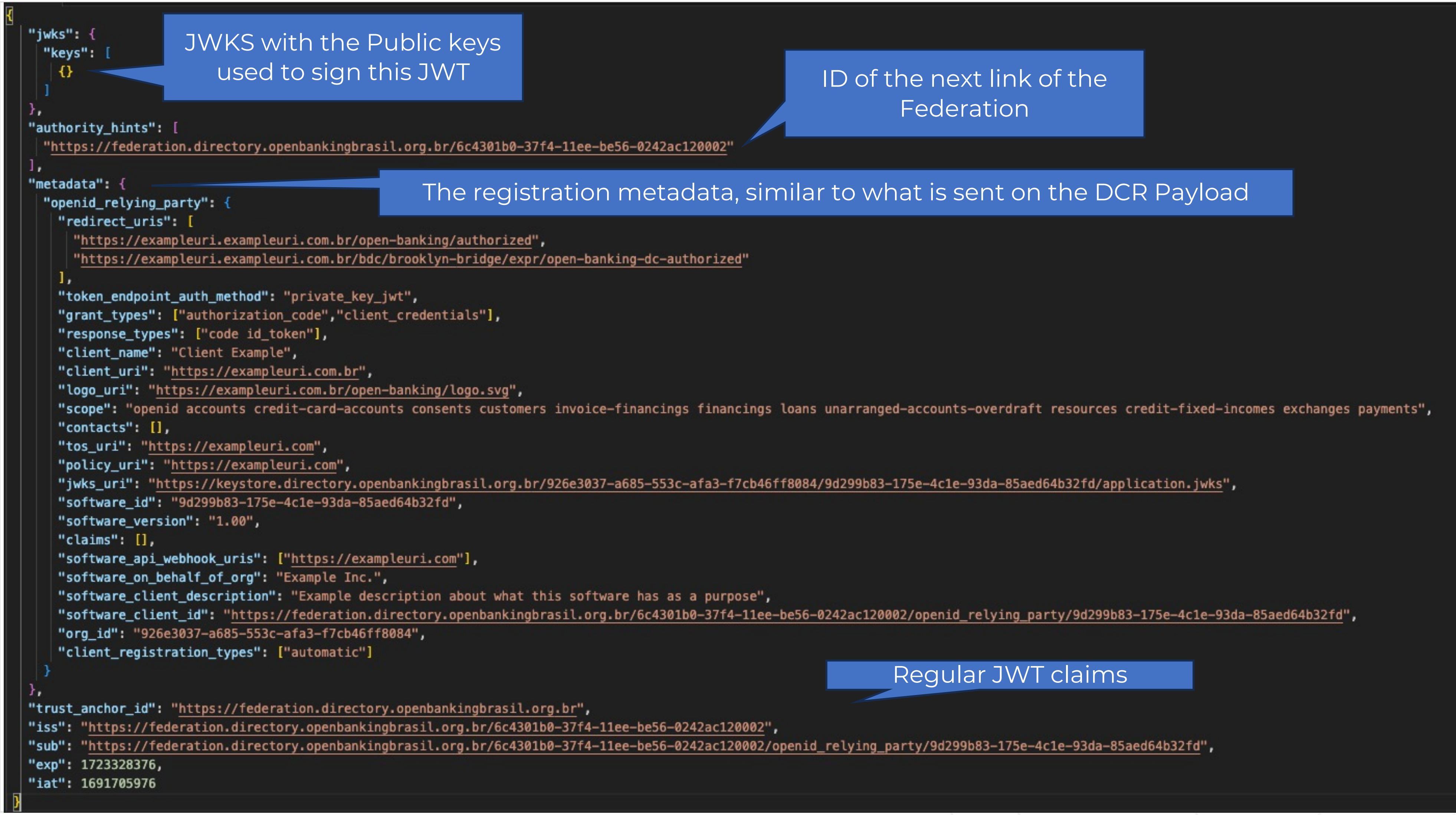
LEAF ENTITY STATEMENT ENDPOINT STRUCTURE

RAIDIAM

The Leaf Entity Statement provides the metadata registered on the Directory Software Statement required to register a client into a server

Details

- The Metatada information present on the Leaf Entity Statement contains:
    - Data registered by the institution on the directory
    - Data related to the Federation Policies
    - Scope within the Federation
- The Entity Statement also contains the authority_hints which allows to identify the Federation Entity
- Finally, on the JWKS it’s possible to evaluate the institution public keys



```
{
  "jwks": {
    "keys": [
      {}
    ]
  },
  "authority_hints": [
    "https://federation.directory.openbankingbrasil.org.br/6c4301b0-37f4-11ee-be56-0242ac120002"
  ],
  "metadata": {
    "openid_relying_party": {
      "redirect_uris": [
        "https://exampleuri.exampleuri.com.br/open-banking/authorized",
        "https://exampleuri.exampleuri.com.br/bdc/brooklyn-bridge/expr/open-banking-dc-authorized"
      ],
      "token_endpoint_auth_method": "private_key_jwt",
      "grant_types": ["authorization_code","client_credentials"],
      "response_types": ["code id_token"],
      "client_name": "Client Example",
      "client_uri": "https://exampleuri.com.br",
      "logo_uri": "https://exampleuri.com.br/open-banking/logo.svg",
      "scope": "openid accounts credit-card-accounts consents customers invoice-financings financings loans unarranged-accounts-overdraft resources credit-fixed-incomes exchanges payments",
      "contacts": [],
      "tos_uri": "https://exampleuri.com",
      "policy_uri": "https://exampleuri.com",
      "jwks_uri": "https://keystore.directory.openbankingbrasil.org.br/926e3037-a685-553c-afa3-f7cb46ff8084/9d299b83-175e-4c1e-93da-85aed64b32fd/application.jwks",
      "software_id": "9d299b83-175e-4c1e-93da-85aed64b32fd",
      "software_version": "1.00",
      "claims": [],
      "software_api_webhook_uris": ["https://exampleuri.com"],
      "software_on_behalf_of_org": "Example Inc.",
      "software_client_description": "Example description about what this software has as a purpose",
      "software_client_id": "https://federation.directory.openbankingbrasil.org.br/6c4301b0-37f4-11ee-be56-0242ac120002/openid_relying_party/9d299b83-175e-4c1e-93da-85aed64b32fd",
      "org_id": "926e3037-a685-553c-afa3-f7cb46ff8084",
      "client_registration_types": ["automatic"]
    }
  },
  "trust_anchor_id": "https://federation.directory.openbankingbrasil.org.br",
  "iss": "https://federation.directory.openbankingbrasil.org.br/6c4301b0-37f4-11ee-be56-0242ac120002",
  "sub": "https://federation.directory.openbankingbrasil.org.br/6c4301b0-37f4-11ee-be56-0242ac120002/openid_relying_party/9d299b83-175e-4c1e-93da-85aed64b32fd",
  "exp": 1723328376,
  "iat": 1691705976
}
```

JWKS with the Public keys used to sign this JWT

ID of the next link of the Federation

The registration metadata, similar to what is sent on the DCR Payload

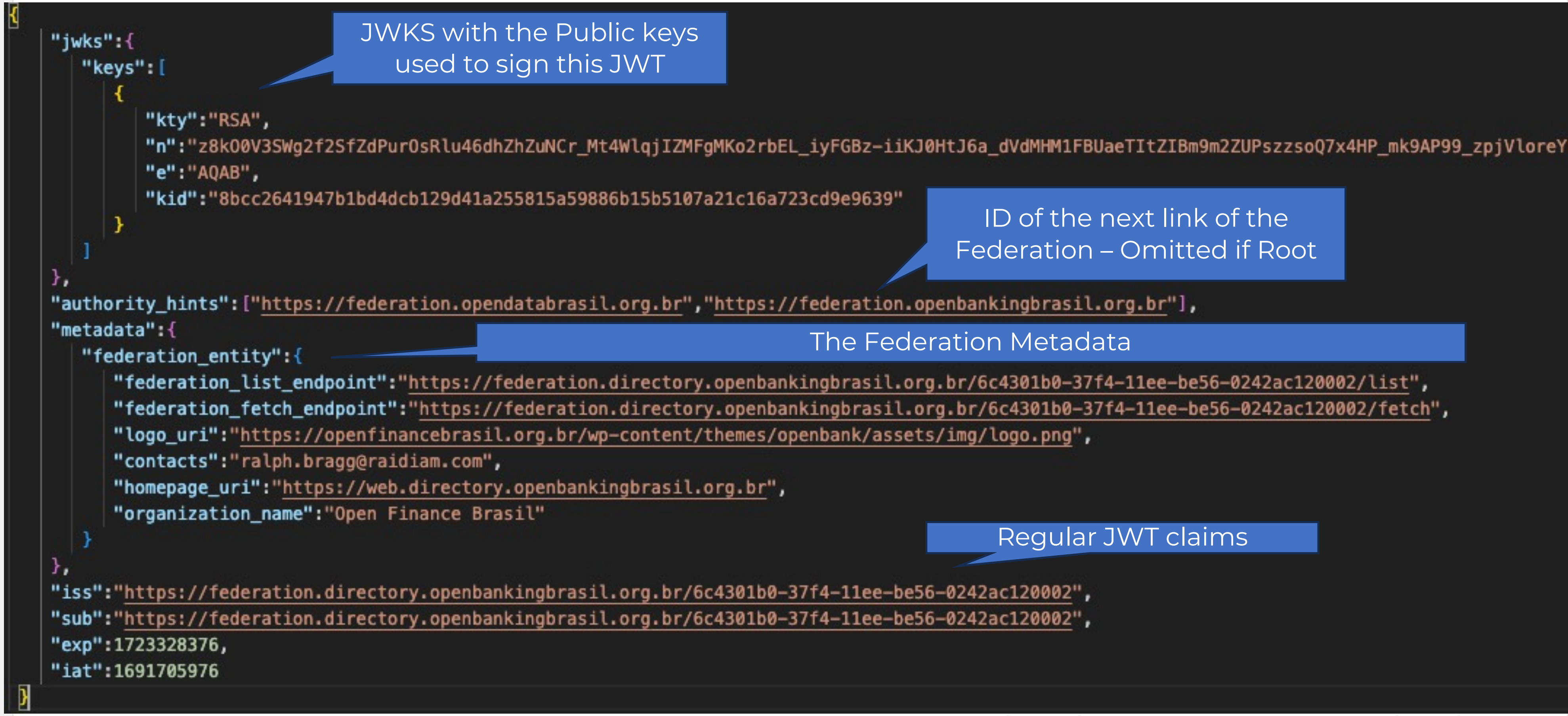
Regular JWT claims

FEDERATION ENTITY STATEMENT ENDPOINT STRUCTURE

The Federation Entity Statement contains metadata related to the Federation, which can be used identify the Federation and also obtain details about all the Entities within the Federation

Details

- The Metatada information present on the Federation Leaf Entity Statement contains:
    - The List and Fetch URI endpoints for the Federation
    - General information about the Federation
- If the Federation belongs to other Federations, it also contains the authority_hints which allows to identify those federations
- Finally, on the JWKS it's possible to evaluate the institution public keys



```
{
  "jwks":{
    "keys":[
      {
        "kty":"RSA",
        "n":"z8kO0V3SWg2f2SfZdPurOsRlu46dhZhZuNCr_Mt4WlqjIZMFgMKo2rbEL_iyFGBz-iiKJ0HtJ6a_dVdMHM1FBUaeTItZIBm9m2ZUPszzsoQ7x4HP_mk9AP99_zpjVloreY
        "e":"AQAB",
        "kid":"8bcc2641947b1bd4dcb129d41a255815a59886b15b5107a21c16a723cd9e9639"
      }
    ]
  },
  "authority_hints":["https://federation.opendatabrasil.org.br","https://federation.openbankingbrasil.org.br"],
  "metadata":{
    "federation_entity":{
      "federation_list_endpoint":"https://federation.directory.openbankingbrasil.org.br/6c4301b0-37f4-11ee-be56-0242ac120002/list",
      "federation_fetch_endpoint":"https://federation.directory.openbankingbrasil.org.br/6c4301b0-37f4-11ee-be56-0242ac120002/fetch",
      "logo_uri":"https://openfinancebrasil.org.br/wp-content/themes/openbank/assets/img/logo.png",
      "contacts":"ralph.bragg@raidiam.com",
      "homepage_uri":"https://web.directory.openbankingbrasil.org.br",
      "organization_name":"Open Finance Brasil"
    }
  },
  "iss":"https://federation.directory.openbankingbrasil.org.br/6c4301b0-37f4-11ee-be56-0242ac120002",
  "sub":"https://federation.directory.openbankingbrasil.org.br/6c4301b0-37f4-11ee-be56-0242ac120002",
  "exp":1723328376,
  "iat":1691705976
}
```

JWKS with the Public keys used to sign this JWT

ID of the next link of the Federation – Omitted if Root

The Federation Metadata

Regular JWT claims

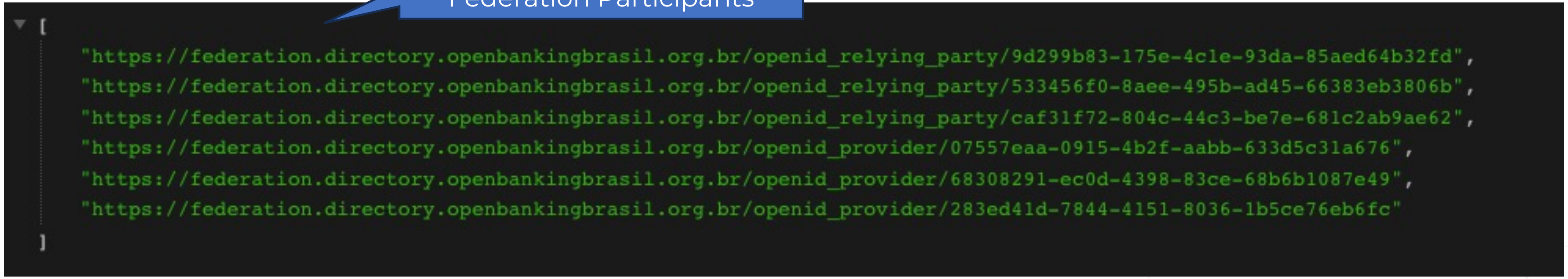
FEDERATION LIST ENDPOINT STRUCTURE

The Federation List Endpoint provides the Entity IDs of all the Entities present on the Federation

Details

- The Endpoint provides a JSON that contains a single array which contains every single Entity ID within a Federation
- For the Open Banking case this should contain one Entity Statement for each Software Statements registered within the directory
- Server Well-Knowns might also be included on this endpoint, depending on the Federation Policy

List of Entity IDs of all the Federation Participants

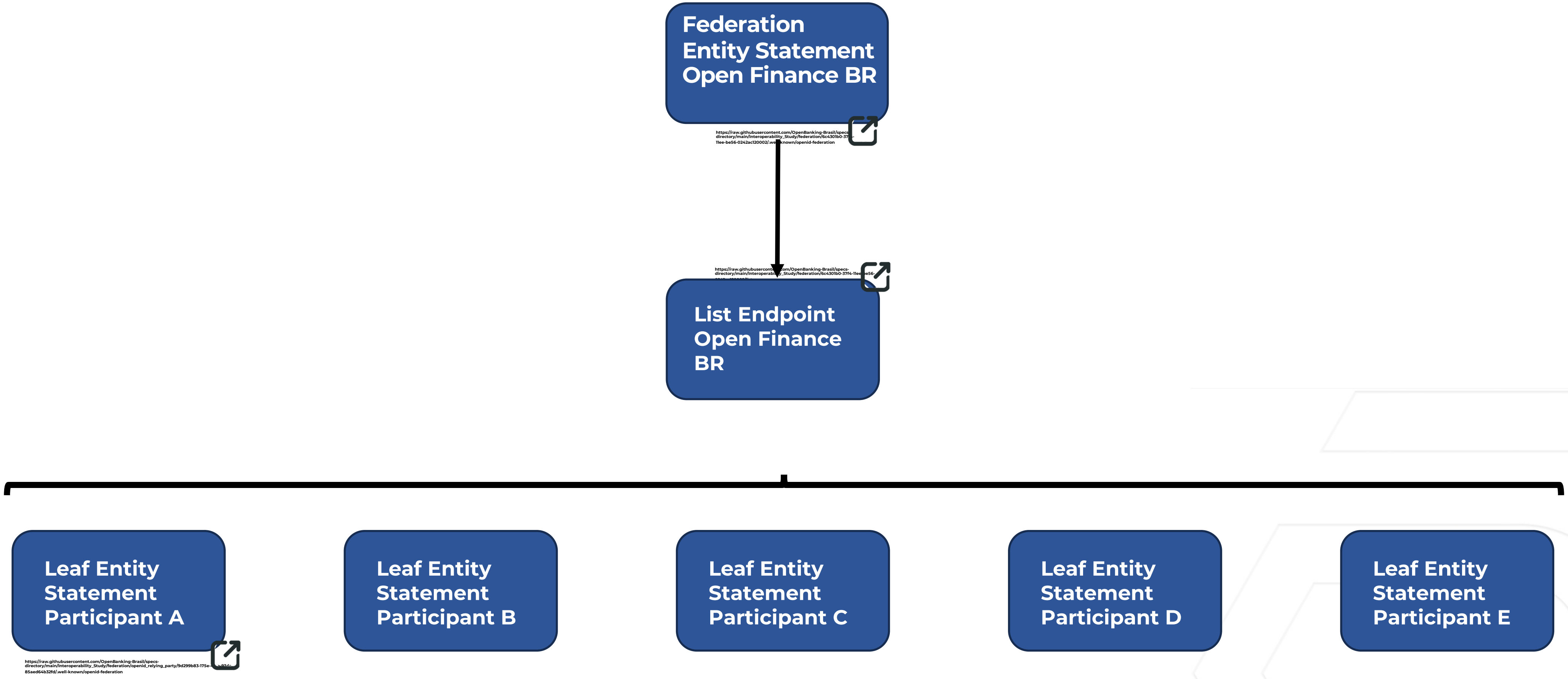


```
▼ [
      "https://federation.directory.openbankingbrasil.org.br/openid_relying_party/9d299b83-175e-4c1e-93da-85aed64b32fd",
      "https://federation.directory.openbankingbrasil.org.br/openid_relying_party/533456f0-8aee-495b-ad45-66383eb3806b",
      "https://federation.directory.openbankingbrasil.org.br/openid_relying_party/caf31f72-804c-44c3-be7e-681c2ab9ae62",
      "https://federation.directory.openbankingbrasil.org.br/openid_provider/07557eaa-0915-4b2f-aabb-633d5c31a676",
      "https://federation.directory.openbankingbrasil.org.br/openid_provider/68308291-ec0d-4398-83ce-68b6b1087e49",
      "https://federation.directory.openbankingbrasil.org.br/openid_provider/283ed41d-7844-4151-8036-1b5ce76eb6fc"
  ]
```

CHAIN WALK AND HOW FEDERATION ENSURES TRUST - PROACTIVE

Starting from the Federation Entity it’s possible to obtain all the details of the Entities that belong to the Federation – With this information Servers can pre-register all existing entities

Federation artefacts and process to obtain information about all Federation Entities


Federation Entity Statement Open Finance BR
https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/6c4301b0-37
11ee-be56-0242ac120002/.we known/openid-federation
https://raw.githubuserconte .com/OpenBanking-Brasil/specs-directory/main/Interoperabi y_Study/federation/6c4301b0-37f4-11ee e56-
List Endpoint Open Finance BR
Leaf Entity Statement Participant A
https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/openid_relying_party/9d299b83-175e-
85aed64b32fd/.well-known/openid-federation
Leaf Entity Statement Participant B
Leaf Entity Statement Participant C
Leaf Entity Statement Participant D
Leaf Entity Statement Participant E

Clients not registered within a Server can be registered by validating the trust chain up until one of the Federation issuers trusted by the Server

Example of Token Request from a Federation Participant

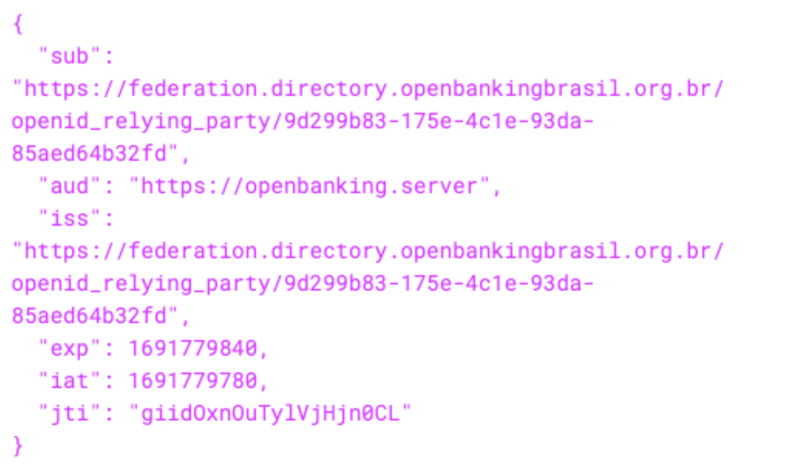
Request

POST "https://openbanking.server/token"

Request Body

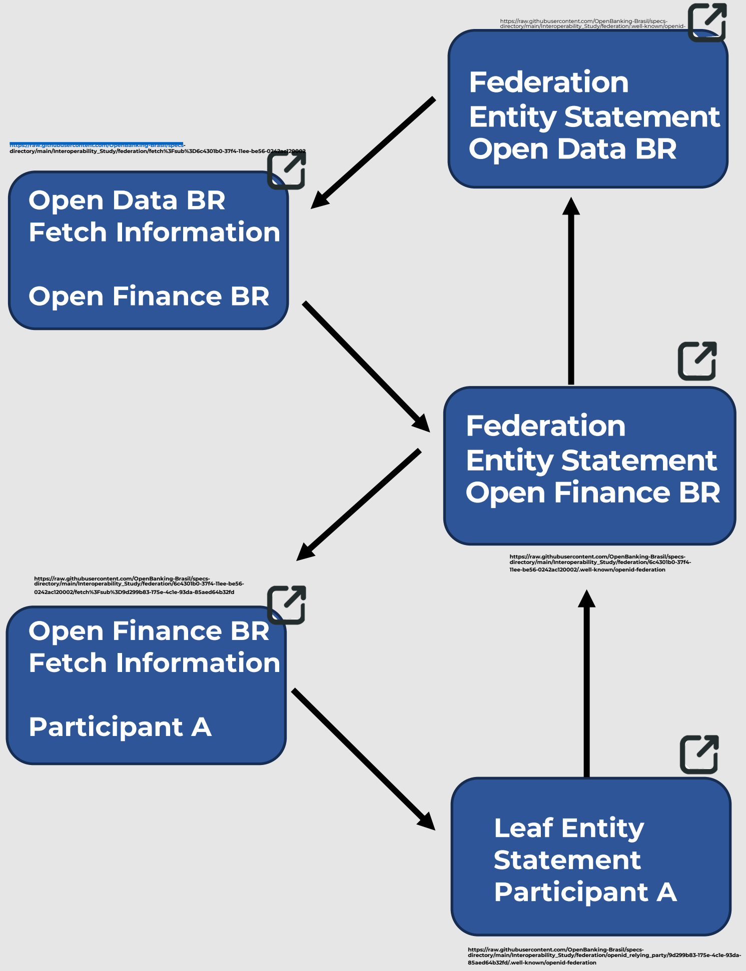
grant_type=client_credentials&scope=consents&client_assertion=XXXXXXX&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer

Decoded Assertion



```
{
  "sub":
"https://federation.directory.openbankingbrasil.org.br/
openid_relying_party/9d299b83-175e-4c1e-93da-
85aed64b32fd",
  "aud": "https://openbanking.server",
  "iss":
"https://federation.directory.openbankingbrasil.org.br/
openid_relying_party/9d299b83-175e-4c1e-93da-
85aed64b32fd",
  "exp": 1691779840,
  "iat": 1691779780,
  "jti": "giidOxnOuTylVjHjn0CL"
}
```

Process to validate a given Entity Statement that participants in a Federation



https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/.well-known/openid-
Federation Entity Statement Open Data BR
https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/fetch%3Fsub%3D6c4301b0-37f4-11ee-be56-0242ac120002
Open Data BR Fetch Information
Open Finance BR
Federation Entity Statement Open Finance BR
https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/6c4301b0-37f4-11ee-be56-0242ac120002/.well-known/openid-federation
https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/6c4301b0-37f4-11ee-be56-0242ac120002/fetch%3Fsub%3D9d299b83-175e-4c1e-93da-85aed64b32fd
Open Finance BR Fetch Information
Participant A
Leaf Entity Statement Participant A
https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/openid_relying_party/9d299b83-175e-4c1e-93da-85aed64b32fd/.well-known/openid-federation

Raidiam proposes to separate the presentations of the Suggested Federation Protocol and its impacts on three different sessions

1. Introduction

- What is the OIDC Federation – Protocol
- Differences and improvements between DCR-BR and the proposed Federation-BR profile
- Introducing the Unique Client_ID requirement
- Obtaining an Entity Configuration

2. Federation Artefacts

- Entity Statement Endpoint Structure
- Fetch Endpoint Structure
- List Endpoint Structure
- Chain Walk and how Federation Ensures Trust

3. Implementation and Open Data BR Federation

- Suggested Transition Plan
- Defining the Federation Standard, Certification and Preparing the Directory
- Migrating From DCR to Federation
- Setting the Open Data Brazil Entity

We highlight that “The Federation Protocol” to be presented on the agendas will consider the premises that have been presented and approved on the Months of June and July – For Simplicity we will call this the Federation BR

Raidiam suggests three separated Phases when rolling over the Federation Framework to the Brazilian Ecosystem

Phase 1: **Standards and Infra**

The Objective of the First Phase is to lay over the foundation required for Federation to be implemented

- Implement all Federation Endpoints on the Directory
- Create the Draft Version of the Federation Specification
- Have External Body do external Security Analysis on Standard
- Ecosystems to Agree on the Federation Specification
- Ecosystems to Agree on the Data Sharing Policy

Phase 2: **Technical Migration**

Both Ecosystems Separately to migrate and align to the Federation Standard

- Each Ecosystem to define timelines to adopt the Federation Standard
- Institutions to Certify to the Federation Standards
- Open Finance and Open Insurance to migrate from DCR to Federation

Phase 3: **Open Data Federation**

Setting an External Body Tasked with aligning Federation Policies and ensuring Interoperability

- Maintain the Open Data Brazil Federation Artefacts and Onboard new Federations
- Ensure Common Policies and Standards for all Intermediate Federations
- Evaluate new use cases for the Brazil Ecosystem – E.G. Verifiable Credentials

For the Standard Definition Phase objectives would be to Agree on a Federation Specification Document and to have the Directory to support the Required Artefacts

Main Deliverables of the First Phase 1

Directory Implementation

Raidiam is currently working on rolling over the Federation Standard – Once Implemented this could be configured to support the Federation Brazil Standard

- Raidiam Expects the Standard to be implemented and tested by the end of 2023 / beginning of 2024
- Framework will be initially deployed to the Australian National ID Program – ConnectID
- Once Ready the Framework could be adopted to the Federation Specification
- No Changes would be expected on the Existing Directory SSA, implying that the DCR Standard would continue working in parallel with Federation

Federation Specification

Based on the Premises discussed and the existing DCR and FAPI Brazil Specifications, the first draft Federation Specification Can be set.

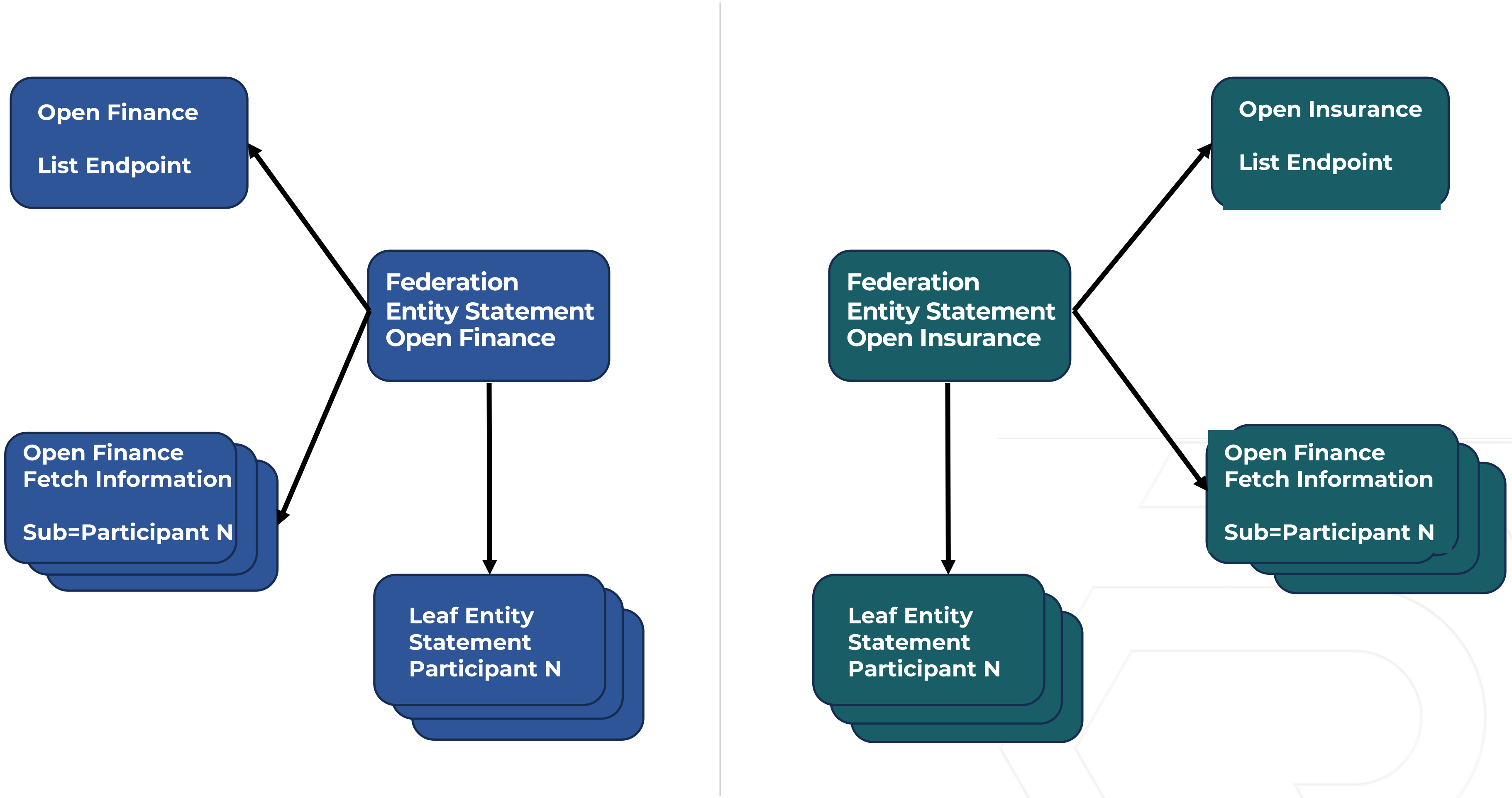
- First Draft Should Include technical details on :
  - Details about supported Endpoints
  - Expected Metadata present on the Entity Statements
  - Refresh Policy – Raidiam suggests a 7-day expiration on JWT, to be refreshed daily
- Raidiam is available to write first Draft once implementation plan is set – Draft to be reviewed and iterated by both Security WGs and External Parties
- OIDF signaled that they would be willing to set the Certification, in line with what was done with DCR-Brazil

Federation can be implemented separately by both Ecosystems each maintaining their own Security Standards and Policies – During this period, certification and a transition from DCR would be expected

Second Phase Details

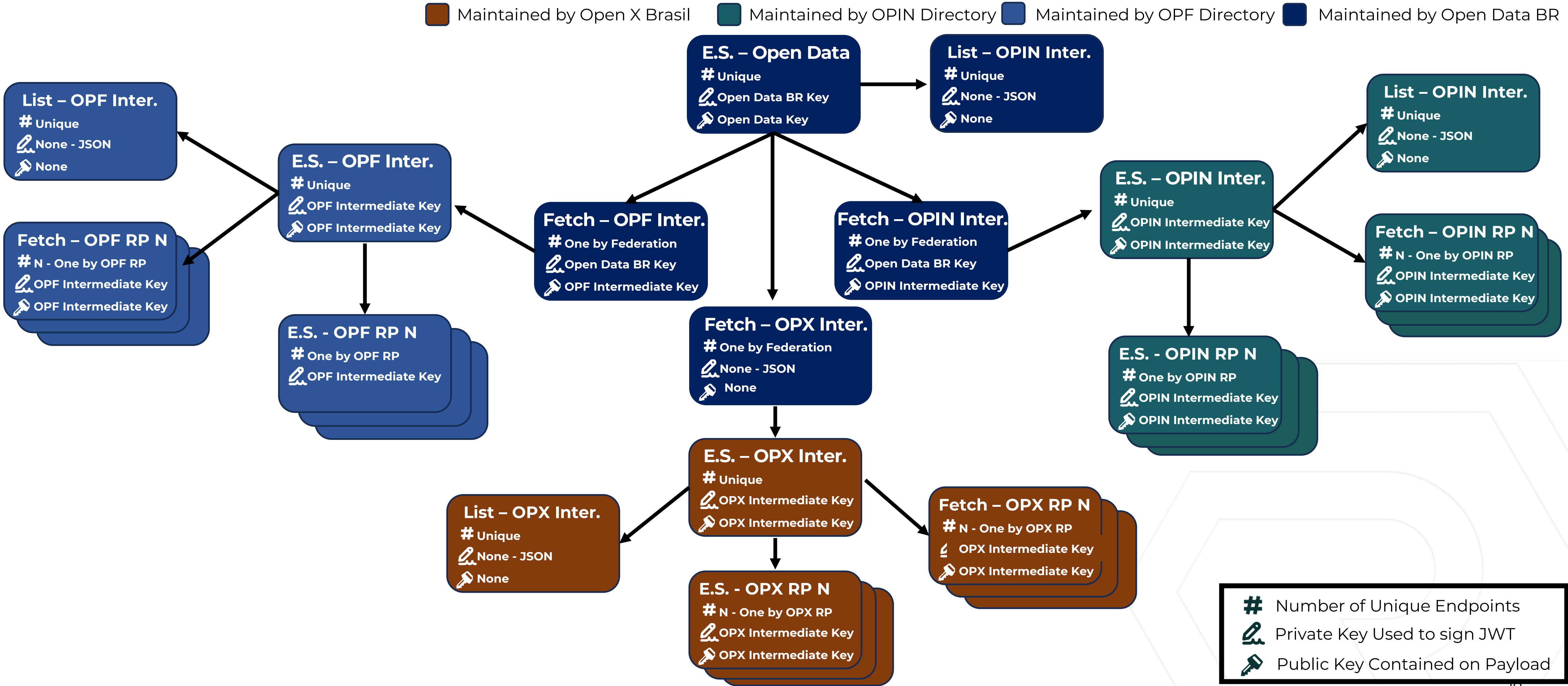
- Both Ecosystem would have the Directory providing their own Federation Endpoints
- Data Receivers would be able to configure their Metadata on the Software Statement
- Structures would agree on a transition timeline, which should include:
  - Servers to Certify to the new Policy on the OIDF
  - Client_IDs to be migrated to the Federation Model
  - Transition from DCR to Federation
- Interoperability could be enabled by having each Federation the other Federation on their Security Model

Suggested Initial Artefacts of Separated Federations


Open Finance
List Endpoint
Federation Entity Statement Open Finance
Open Finance Fetch Information
Sub=Participant N
Leaf Entity Statement Participant N
Open Insurance
List Endpoint
Federation Entity Statement Open Insurance
Open Finance Fetch Information
Sub=Participant N
Leaf Entity Statement Participant N

For the Third Phase a Separated Open Data Brazil Federation entity would be set acting as the Federation Root, which would also enable the addition of other Federations

Open Data Brasil Structure with 3 Intermediate Federations



🟫 Maintained by Open X Brasil 🟩 Maintained by OPIN Directory 🟦 Maintained by OPF Directory ■ Maintained by Open Data BR

E.S. – Open Data
Unique
✍ Open Data BR Key
🖋 Open Data Key

List – OPIN Inter.
Unique
✍ None - JSON
🖋 None

List – OPF Inter.
Unique
✍ None - JSON
🖋 None

E.S. – OPF Inter.
Unique
✍ OPF Intermediate Key
🖋 OPF Intermediate Key

Fetch – OPF RP N
N - One by OPF RP
✍ OPF Intermediate Key
🖋 OPF Intermediate Key

E.S. - OPF RP N
One by OPF RP
✍ OPF Intermediate Key

Fetch – OPF Inter.
One by Federation
✍ Open Data BR Key
🖋 OPF Intermediate Key

Fetch – OPIN Inter.
One by Federation
✍ Open Data BR Key
🖋 OPIN Intermediate Key

E.S. – OPIN Inter.
Unique
✍ OPIN Intermediate Key
🖋 OPIN Intermediate Key

List – OPIN Inter.
Unique
✍ None - JSON
🖋 None

Fetch – OPIN RP N
N - One by OPIN RP
✍ OPIN Intermediate Key
🖋 OPIN Intermediate Key

E.S. - OPIN RP N
One by OPIN RP
✍ OPIN Intermediate Key
🖋 OPIN Intermediate Key

Fetch – OPX Inter.
One by Federation
✍ None - JSON
🖋 None

E.S. – OPX Inter.
Unique
✍ OPX Intermediate Key
🖋 OPX Intermediate Key

List – OPX Inter.
Unique
✍ None - JSON
🖋 None

Fetch – OPX RP N
N - One by OPX RP
✍ OPX Intermediate Key
🖋 OPX Intermediate Key

E.S. - OPX RP N
N - One by OPX RP
✍ OPX Intermediate Key
🖋 OPX Intermediate Key

Number of Unique Endpoints
✍ Private Key Used to sign JWT
🖋 Public Key Contained on Payload

In Addition to maintain the Open Data Brazil Federation, we suggest that this entity could also be tasked on maintaining the Ecosystem Common Policies and to expand to other use cases in Brazil

1 - Maintain the Federation Artefacts

- The Open Data BR Federation Artefacts, which define all the Intermediate Federations, would be maintained by this External Party – Ideally those endpoints would have a very long duration (> 6 months)

- Body Responsible for Onboarding new Brazilian Open X Ecosystems and validating that they comply with the required policies

2 - Ensure Common Policies

- Entity Responsible for defining the Security and Registration Profile for all the member Federations – This should be unified across all participants to enable interoperability

- Rules around which Data Scopes can be accredited to each Federation to also be defined by this body, based on common Ecosystem Regulations
  - Which and what Scopes will be common?
  - How can a common scope be accredited?

3 - Advance Use Cases

- Focus of Entity to also evaluate other use cases for Brazil, enabled by the Ecosystem Open ID and Data Sharing Standards

- Example of additional use cases:

  - Open ID Verifiable Credentials –
    - OIDC4V Specifications

  - Brazilian Digital ID

Para o início do estudo referente ao impacto na adoção do Protocolo Federation para o "Open Data Brasil" foram levantados premissas referentes as definições da Federação e Protocolo (1/3)

Federação Open Data Brasil - Premissas referentes a configuração do protocolo

Metodo de Registro

- Será adotado o metodo de registro automatico definido na sessão "10.1. Automatic Registration"
- Por Consequencia, Apos plena adoção do Federation, o protocolo DCR não deverá mais ser utilizado para registro de aplicações visto que processo será realizado de forma automatica

Client_ID

- Para viabilizar o ponto acima, referente ao registro automático, um client_id único por Software Statement em formato de URI
- Todos os client_id do ecossistema deverão adotar um formato padronizado que, ao ser concatenado com /.well-known/openid-federation, permitirá à obtenção do Entity Configuration fornecido pelo diretório
- Esse formato deve ser determinístico tendo como única variação entre participantes o Software Statement ID

Para o início do estudo referente ao impacto na adoção do Protocolo Federation para o “Open Data Brasil” foram levantados premissas referentes as definições da Federação e Protocolo (2/3)

Federação Open Data Brasil - Premissas referentes ao escopo das Entity Statements e Trust Anchors

Trust Anchor Open Data Brasil

- O papel de Federation Operator da Trust Anchor Open Data Brasil deverá ser assumido por entidade independente
- A entidade independente será responsável a acreditação de Federações Intermediarias, as quais incluem o OPF e OPIN
- Até incorporação desta entidade independente a Federação poderá ser hospedada por um dos diretorios

Trust Anchor Intermediarios

- O Diretório do OPIN irá atuar como Federation Operator da Federação Open Insurance, hospedando a Trust Anchor e todos os elementos referentes aos seus participantes – Entity Statements e Entity Configurations
- De forma semelhante o Diretório do Open Finance também irá atuar como Federation Operator da Federação Open Finance

Escopo Entity Statements

- O Diretório de cada Ecossistema irá hospedar os Entity Statements do seu respectivo Ecossistema
- Os Entity Statements/Leaf Entities serão compostos por todos os Software Statements (RPs) e Authorisation Servers (OPs)

ESTUDO FEDERATION – PREMISSAS INICIAIS

RAIDIAM

Para o início do estudo referente ao impacto na adoção do Protocolo Federation para o "Open Data Brasil" foram levantados premissas referentes as definições da Federação e Protocolo (3/3)

Federação Open Data Brasil - Premissas referentes a documentação de segurança utilizada

Perfil FAPI adotado

- As duas federações, OPF e OPIN, irão manter o mesmo metadata definido hoje na especificação de segurança comum aos dois ecossistemas, logo mesmos grants, scopes, algoritmos de assinatura
- Serão assumidos as modificações aprovadas para atualização do perfil FAPI-Brazil – private_key_jwt/PKCE/PAR/code id_token

Documentação Unificada

Carece de aprovação

- Para o futuro espera-se adotar um repositório único para a documentação de segurança do "Open Data Brasil"
- Assume-se que novos entrants irão adotar a mesma documentação unificada, sendo esta atualizada para dar suporte a estes entrantes

Escopo dos dados compartilhado

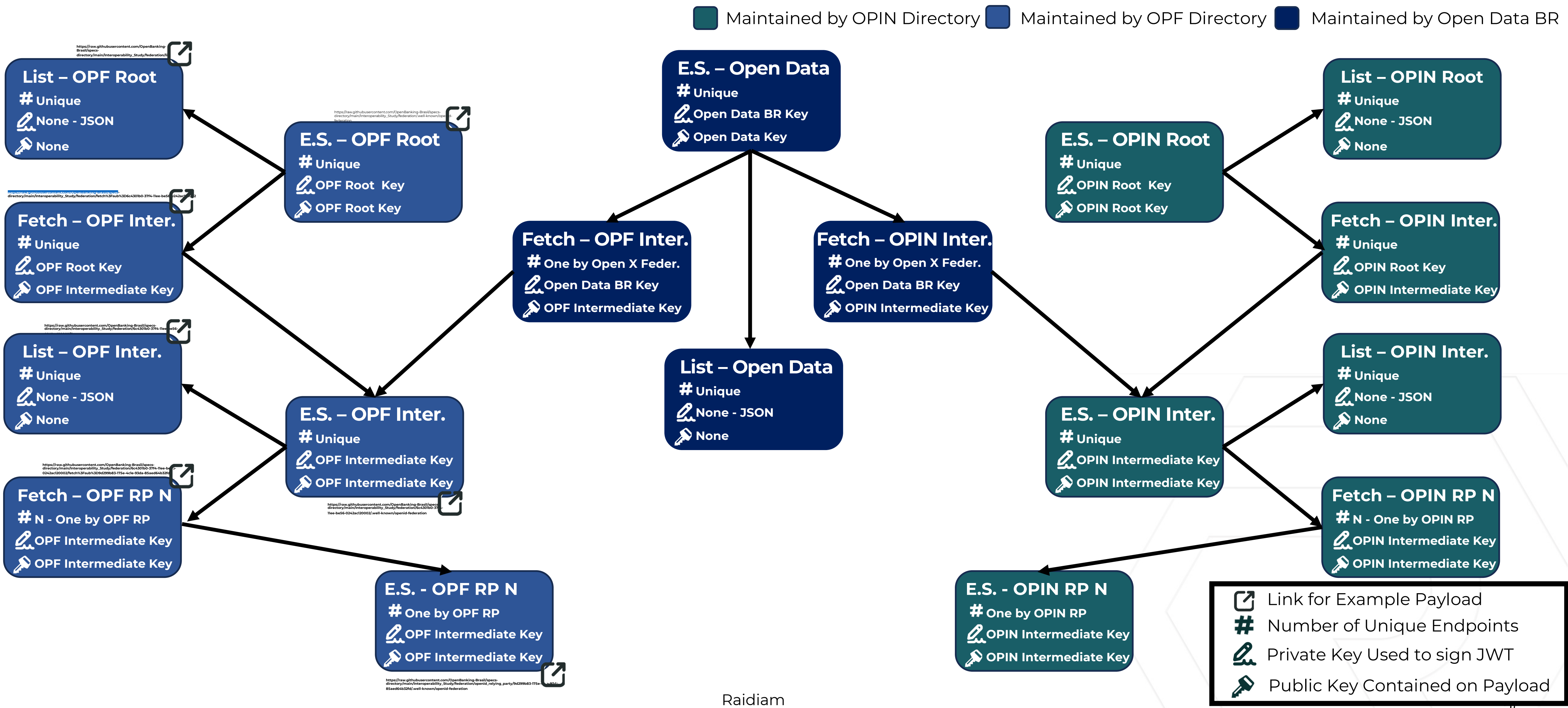
Carece de aprovação

- Assume-se que o escopo de interoperabilidade é referente a apenas os dados da Fase 2 sendo que todos os Ecossistemas da Federação Open Data Brasil terão acesso a todos os escopos existentes referentes a dados do consumidor
- Escopos de serviços não estão incluidos no escopo de compartilhamento, ficando inicialmente restritos a cada Ecossistema

Assinatura dos JWTs

- Serão mantidos as mesmas definições referentes a assinatura de JWT definida no FAPI Brasil, hoje utilizado no Open Finance
- Sem restrição quanto a origem das chaves para assinatura dos Entity Statements, desde que mantido o padrão dos ecossistemas - RSA 2048 bits

Possible Structure of the Open Data Federation and expected Artefacts - Examples



🟩 Maintained by OPIN Directory 🟦 Maintained by OPF Directory ■ Maintained by Open Data BR

E.S. – Open Data
# Unique
Open Data BR Key
Open Data Key

Fetch – OPF Inter.
# One by Open X Feder.
Open Data BR Key
OPF Intermediate Key

Fetch – OPIN Inter.
# One by Open X Feder.
Open Data BR Key
OPIN Intermediate Key

List – Open Data
# Unique
None - JSON
None

List – OPF Root
# Unique
None - JSON
None

https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/li

E.S. – OPF Root
# Unique
OPF Root Key
OPF Root Key

https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/.well-known/openid-federation

Fetch – OPF Inter.
# Unique
OPF Root Key
OPF Intermediate Key

https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/fetch%3Fsub%3D6c4301b0-37f4-11ee-be56-0242ac120002

List – OPF Inter.
# Unique
None - JSON
None

https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/6c4301b0-37f4-11ee-be56-

E.S. – OPF Inter.
# Unique
OPF Intermediate Key
OPF Intermediate Key

https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/6c4301b0-37f4-11ee-be56-0242ac120002/.well-known/openid-federation

Fetch – OPF RP N
# N - One by OPF RP
OPF Intermediate Key
OPF Intermediate Key

https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/6c4301b0-37f4-11ee-be56-0242ac120002/fetch%3Fsub%3D9d299b83-175e-4c1e-93da-85aed64b32fd

E.S. - OPF RP N
# One by OPF RP
OPF Intermediate Key
OPF Intermediate Key

https://raw.githubusercontent.com/OpenBanking-Brasil/specs-directory/main/Interoperability_Study/federation/openid_relying_party/9d299b83-175e-4c1e-93da-85aed64b32fd/.well-known/openid-federation

E.S. – OPIN Root
# Unique
OPIN Root Key
OPIN Root Key

List – OPIN Root
# Unique
None - JSON
None

Fetch – OPIN Inter.
# Unique
OPIN Root Key
OPIN Intermediate Key

List – OPIN Inter.
# Unique
None - JSON
None

E.S. – OPIN Inter.
# Unique
OPIN Intermediate Key
OPIN Intermediate Key

Fetch – OPIN RP N
# N - One by OPIN RP
OPIN Intermediate Key
OPIN Intermediate Key

E.S. - OPIN RP N
# One by OPIN RP
OPIN Intermediate Key
OPIN Intermediate Key

↗ Link for Example Payload
# Number of Unique Endpoints
✎ Private Key Used to sign JWT
🔑 Public Key Contained on Payload