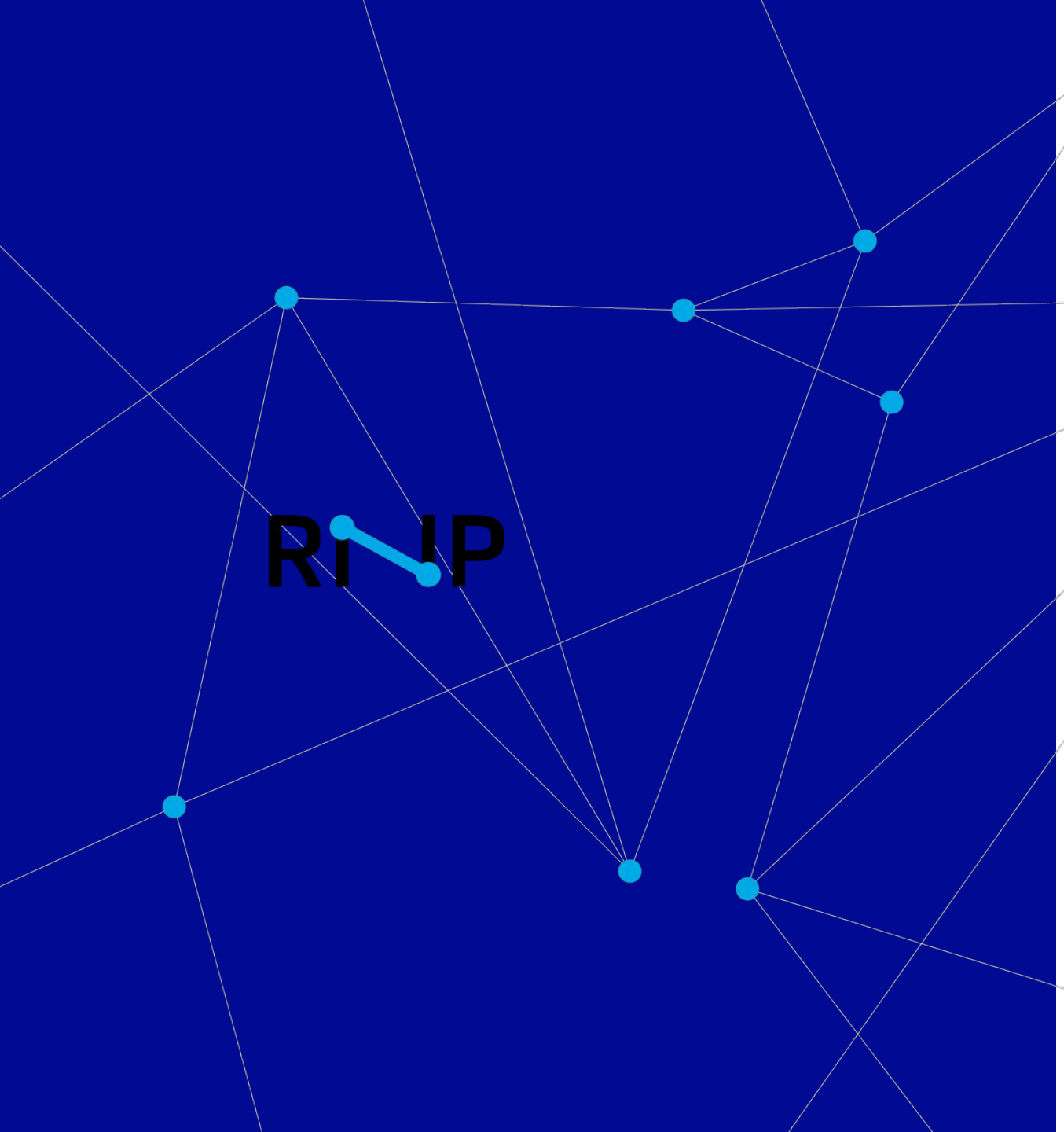


Toward the Next Generation of Academic Identity Federations: Interoperability, Trust Frameworks, and Digital Sovereignty

Prof. Frederico Schardong, PhD
UFSC

GOAL OF THIS TALK

Sharing Brazil's path from SAML to OpenID Federation

What we built · What we learned · Where we can collaborate

An experience to compare, test and improve together.

Brazilian National Research and Education Network (NREN)



RNP
ORGANIZAÇÃO SOCIAL DO MCTI

~800 Institutions
45 metropolitan networks
27 PoPs
+ 4 million users

We connect people and institutions in an environment that fosters knowledge creation and collaboration

- Network Operation
- Services & Solutions
- Research, Development & Innovation

CAFe, (kah-FEH)

Brazil's academic federation



16 years

Operated by RNP since 2010

Largest

academic federation in LATAM

Over 300

member institutions

Identity providers vs. Service providers

348
identity providers

48
service providers

9
services from outside RNP

Almost every member institution can authenticate its users, but few federated services are available to them.

Who the members are*

No dedicated IAM team

Most institutions have nobody whose job is identity.

SAML stack kept alongside

Many institutions prefer other identity technologies internally, such as Google, Microsoft or an in-house OIDC server.

~90%

of institutions need hands-on support to maintain their Shibboleth, according to CAFe operators' estimates.

~10%

run their identity provider independently.

*Based on over 60 interviews with institutional IT staff, managers, service maintainers and RNP operators, July–September 2025.

Operating SAML at each institution

Most institutions update their Shibboleth instance only with RNP assistance.

Each Shibboleth upgrade or certificate renewal takes RNP staff **several hours per institution***.

Without dedicated IAM staff, operating a SAML stack next to the main identity system is a recurring cost for institutions and for RNP*.

*Based on over 60 interviews with institutional IT staff, managers, service maintainers and RNP operators, July–September 2025.

Integrating services in other protocols

A modern service is created

It speaks OpenID Connect

CAFe

Core infrastructure is SAML; services using other protocols join through proxies

The service team

Must operate a translation proxy (e.g., SATOSA)

Every translation layer adds operational cost for the service.

Why not just switch the protocol?

For CAFe members, a switch to OIDFED means:

- A new complex protocol, run by teams that already depend on RNP to operate Shibboleth
- OIDFED key generation, rotation and signing at every institution
- The same support dependency, now with a new protocol

A protocol change alone does not address the problems in our context.

The architecture has to change as well.

SOLUTION

BAITA's proposal

[ˈbaj.tɐ] or (BYE-tuh)

A gradual transition, not a protocol switch

TODAY

SAML at the core

CAFe runs on SAML. Services in other protocols have their own proxy.

SAML

WITH BAITA

Coexistence

SAML, OAuth 2.0, OIDC and OpenID Federation work side by side. Proxies and discovery, run by RNP, connect them.

SAML OIDC OIDFed

OVER TIME

Native by default

New services join natively in OIDC or OpenID Federation, and translation.

SAML OIDC OIDFed

No abrupt migration: CAFe members keep running what they run today, while new services join in the protocol they already speak.

Trust hierarchy

Layers:

- eduGAIN trust anchor
- NREN trust anchor
- Institution trust anchors
- Intermediates
- Leaf entities



What it is:

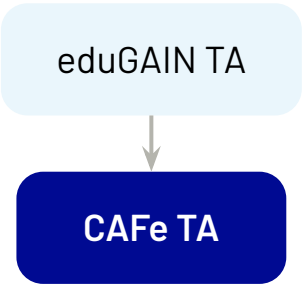
eduGAIN TA, to which NRENs must be subordinate

ARCHITECTURE 2/5

Trust hierarchy

Layers:

- eduGAIN trust anchor
- NREN trust anchor
- Institution trust anchors
- Intermediates
- Leaf entities



What it is:

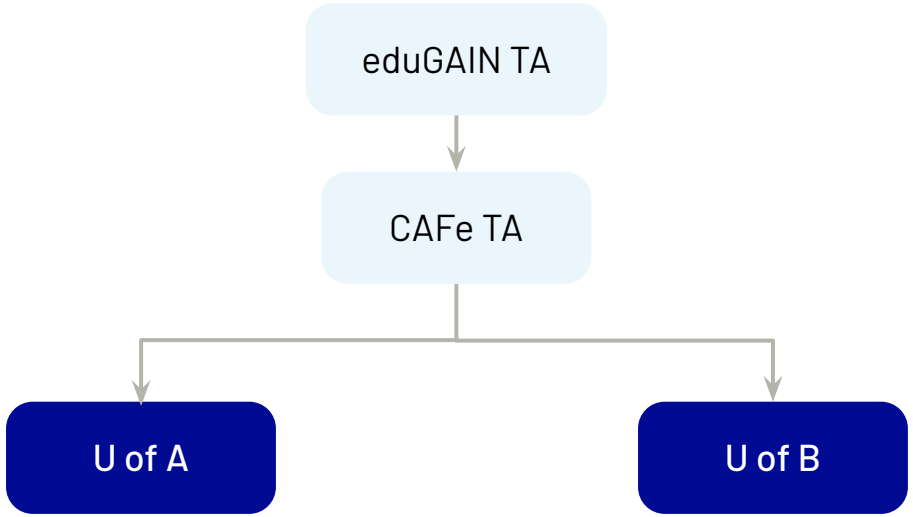
Operated by RNP, it defines federation-wide policies and resolves trust chains.

ARCHITECTURE 3/5

Trust hierarchy

Layers:

- eduGAIN trust anchor
- NREN trust anchor
- **Institution trust anchors**
- Intermediates
- Leaf entities



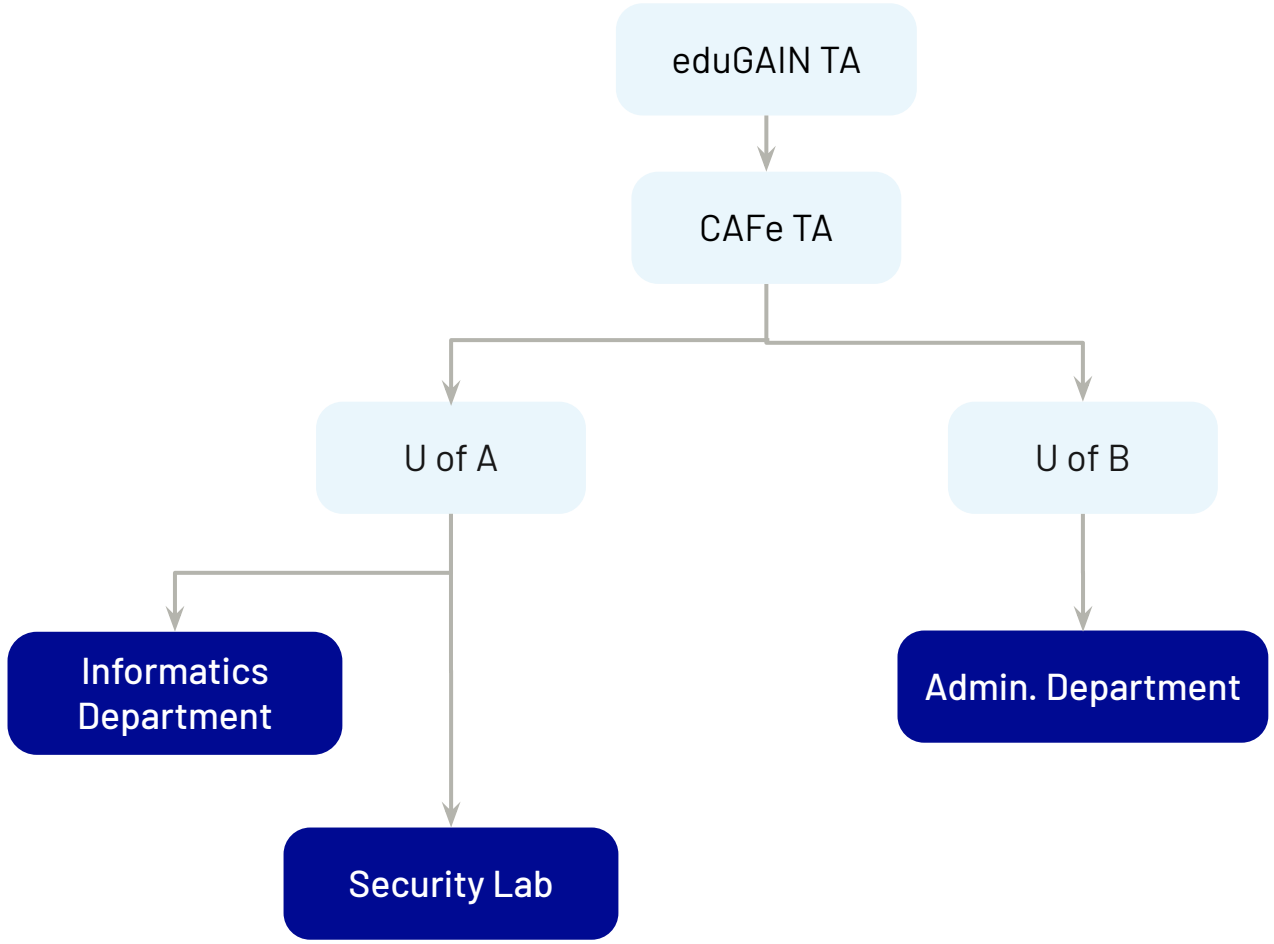
What it is:

For each member institution, directly under CAFe.

Trust hierarchy

Layers:

- eduGAIN trust anchor
- NREN trust anchor
- Institution trust anchors
- **Intermediates**
- Leaf entities



What it is:

Departments, labs, research groups.

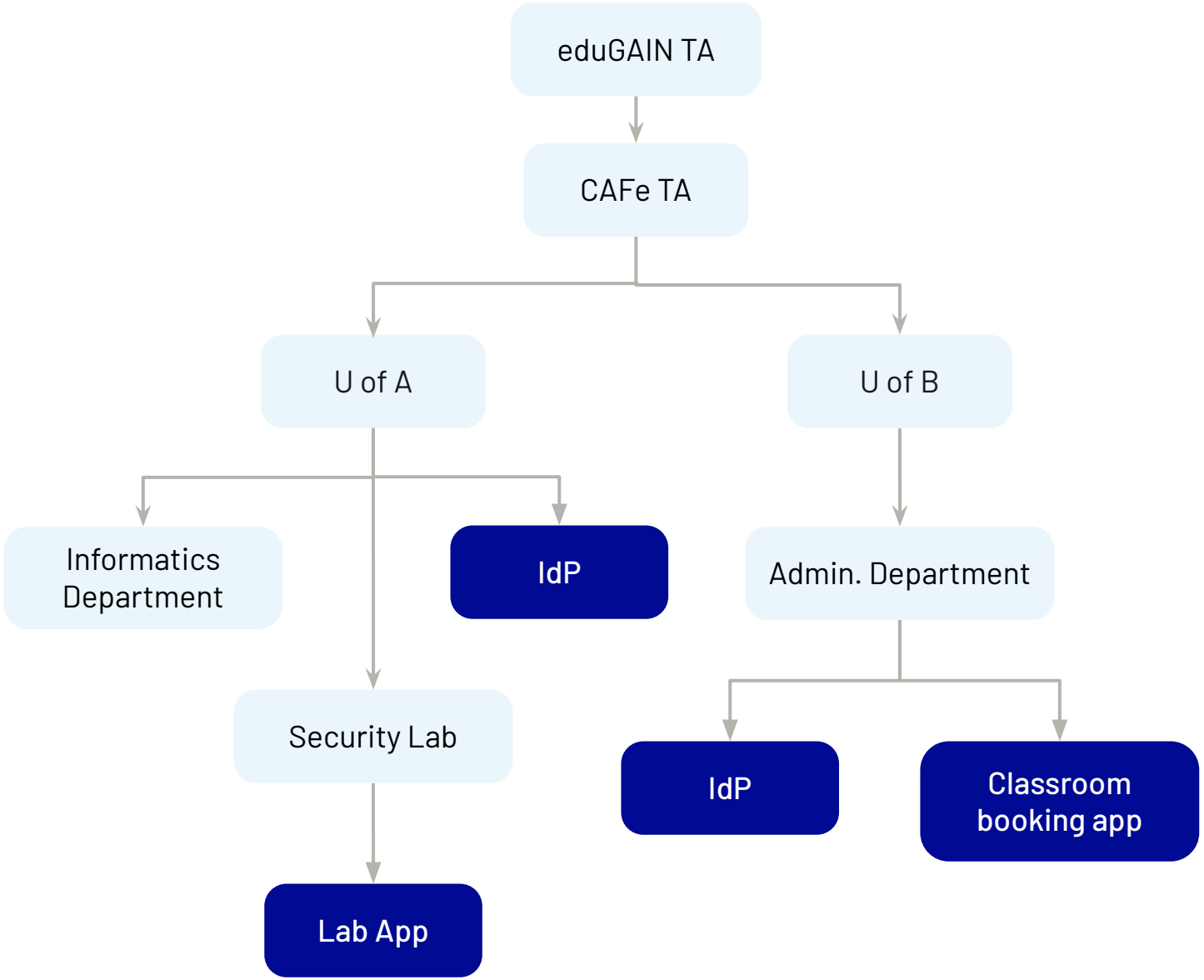
Trust hierarchy

Layers:

- eduGAIN trust anchor
- NREN trust anchor
- Institution trust anchors
- Intermediates
- ▶ **Leaf entities**

What it is:

Identity Providers, Services



SOLUTION 1/4

Four components

Management system

Registration and approval workflows, delegation and roles, key custody, audit, topology view

Discovery (WAYF)

Finds SAML and OIDC providers during the transition

Service catalog

Public list of federated services, built from the federation itself

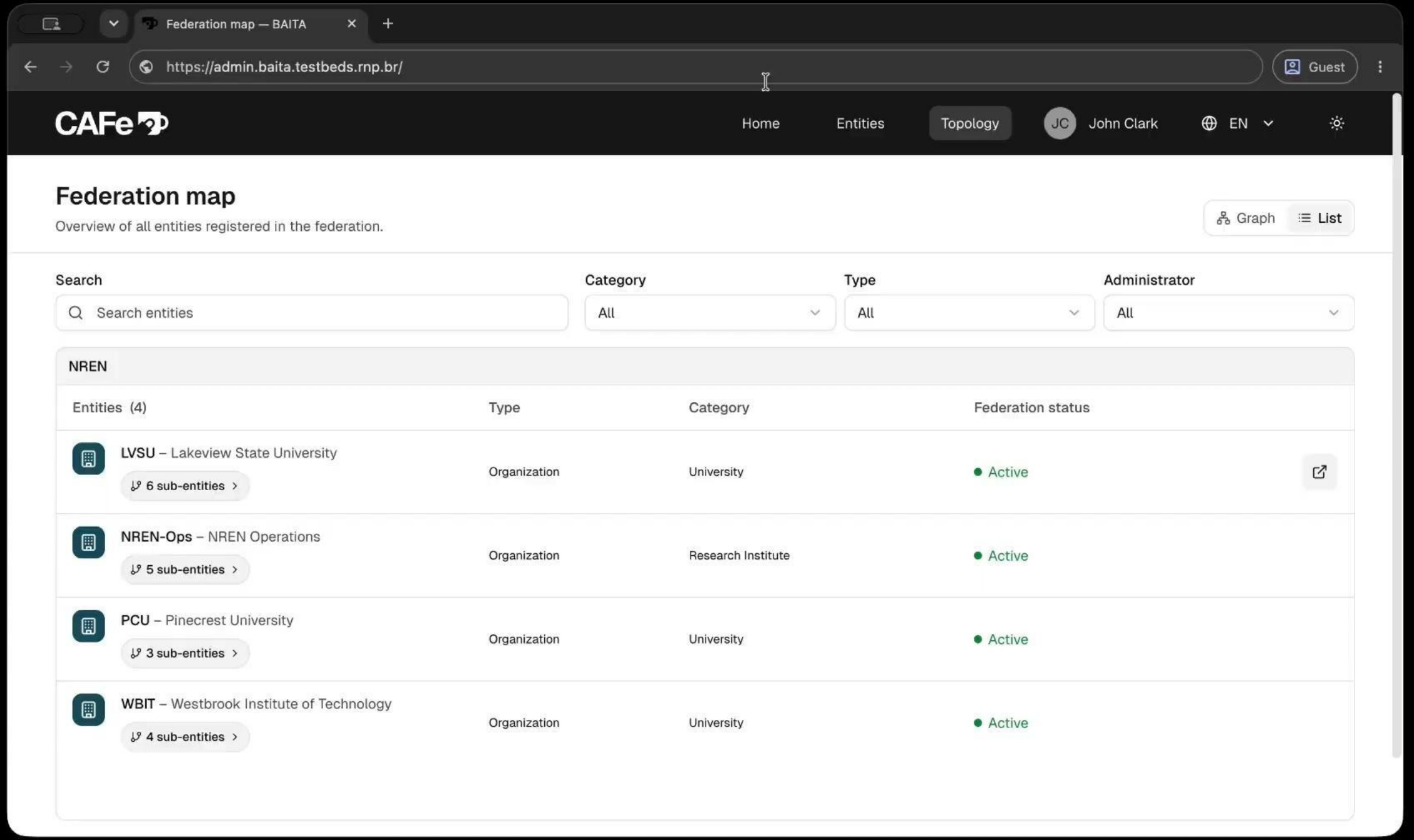
Protocol proxies

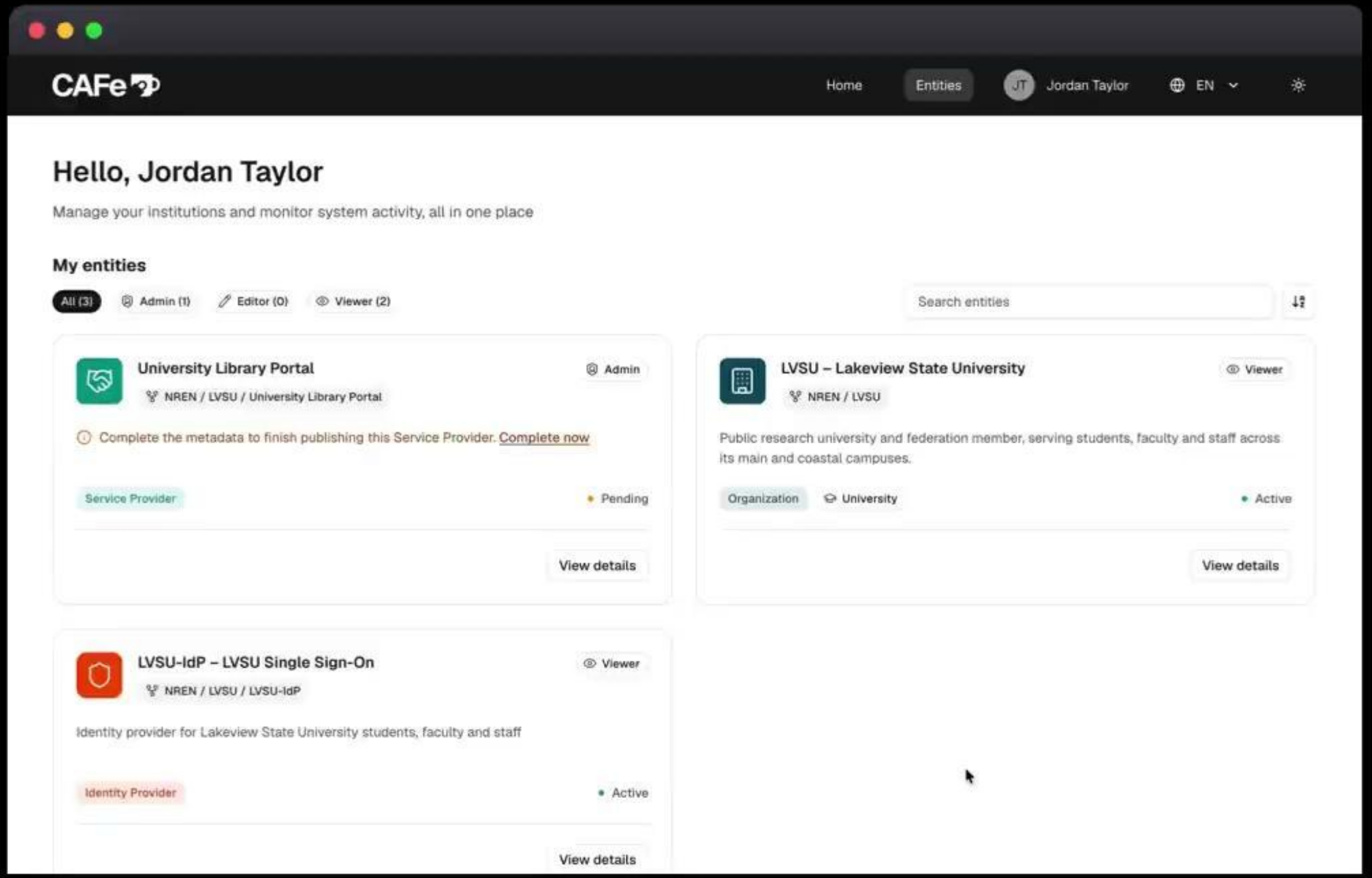
Multi-tenant SATOSA and OIDC proxies let SAML, OIDC and OpenID Federation coexist

Trust hierarchy on OpenID Federation 1.0, following the eduGAIN pilot topology.

Management system

Registration, invitation and delegation flows, roles and permissions, approval workflow, key custody and signing, audit history, topology view.


Federation map — BAITA
https://admin.baita.testbeds.rnp.br/
Guest
CAFe
Home
Entities
Topology
JC
John Clark
EN
Federation map
Overview of all entities registered in the federation.
Graph
List
Search
Search entities
Category
All
Type
All
Administrator
All
NREN
Entities (4)
Type
Category
Federation status
LVSU – Lakeview State University
6 sub-entities
Organization
University
Active
NREN-Ops – NREN Operations
5 sub-entities
Organization
Research Institute
Active
PCU – Pinecrest University
3 sub-entities
Organization
University
Active
WBIT – Westbrook Institute of Technology
4 sub-entities
Organization
University
Active

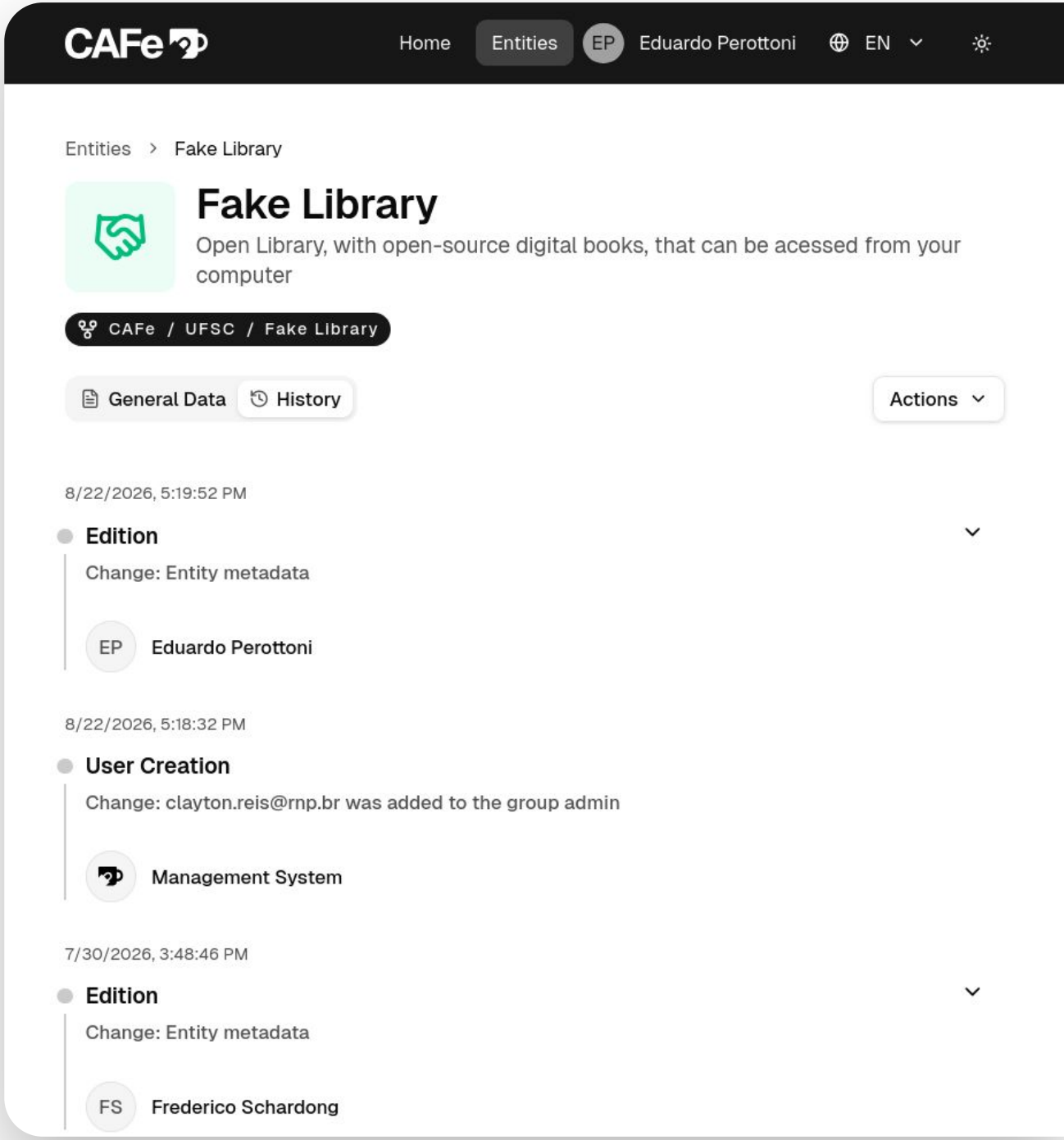

CAFe
Home
Entities
JT
Jordan Taylor
EN
Hello, Jordan Taylor
Manage your institutions and monitor system activity, all in one place
My entities
All (3)
Admin (1)
Editor (0)
Viewer (2)
Search entities
University Library Portal
Admin
NREN / LVSU / University Library Portal
Complete the metadata to finish publishing this Service Provider. Complete now
Service Provider
Pending
View details
LVSU – Lakeview State University
Viewer
NREN / LVSU
Public research university and federation member, serving students, faculty and staff across its main and coastal campuses.
Organization
University
Active
View details
LVSU-IdP – LVSU Single Sign-On
Viewer
NREN / LVSU / LVSU-IdP
Identity provider for Lakeview State University students, faculty and staff
Identity Provider
Active
View details

SOLUTION 2/4

Management system

Auditability

Managers can see the entity modification history: metadata, key rotation and permissions

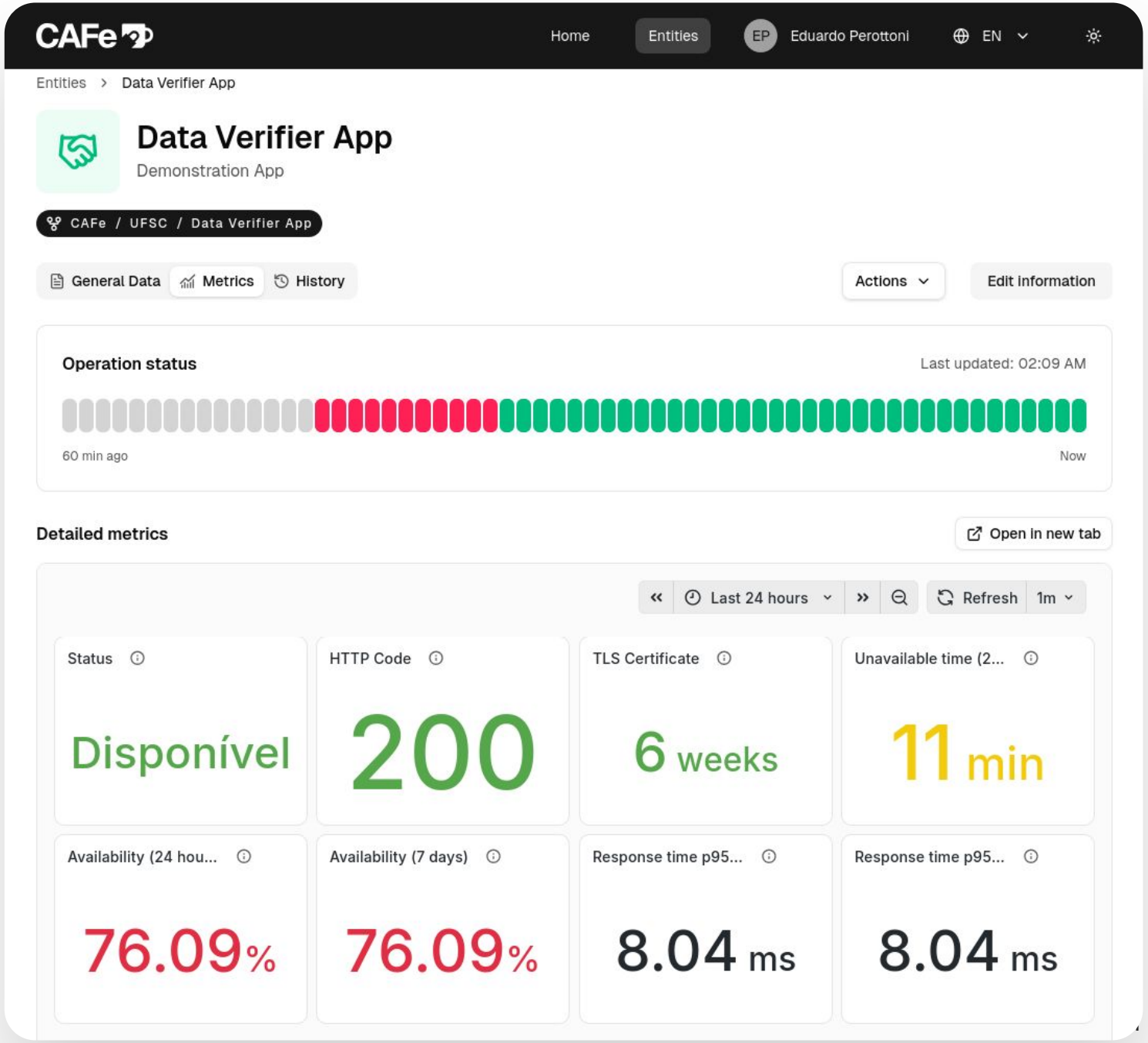


SOLUTION 2/4

Management system

Metrics and Service Analytics

Alerts about service degradation and possibility to collect user feedback for federated services

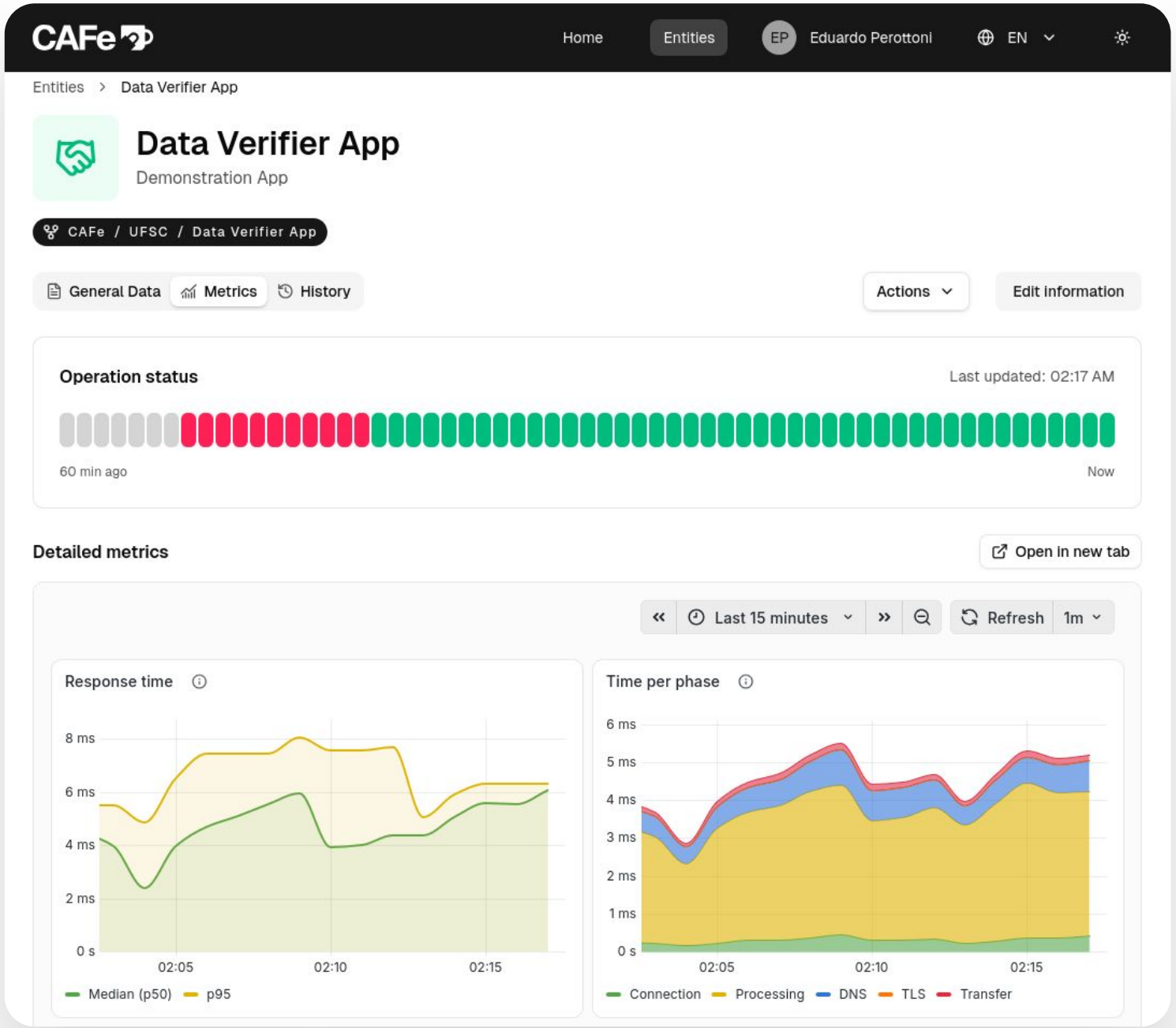


SOLUTION 2/4

Management system

Metrics and Service Analytics

Alerts about service degradation and possibility to collect user feedback for federated services

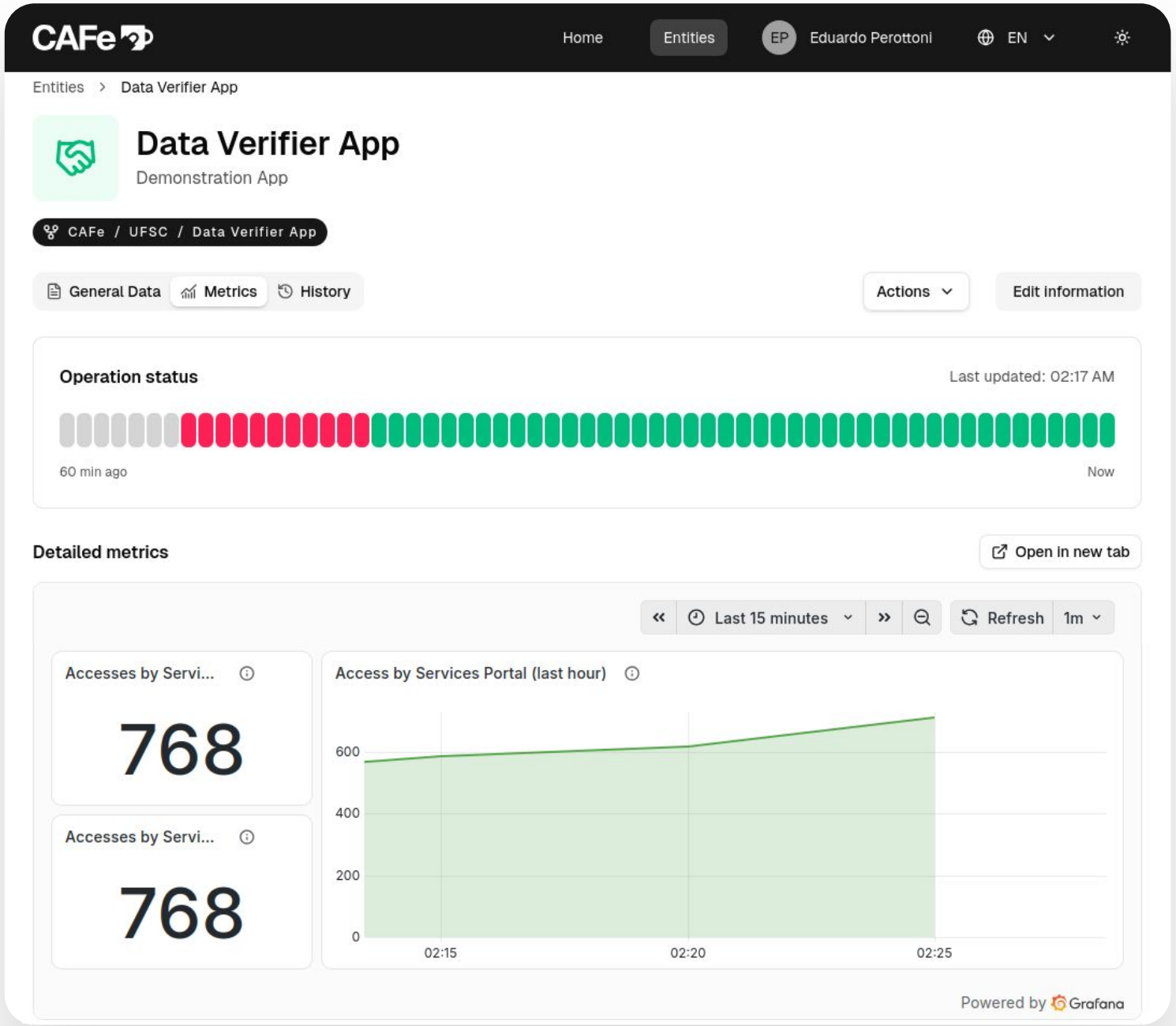


SOLUTION 2/4

Management system

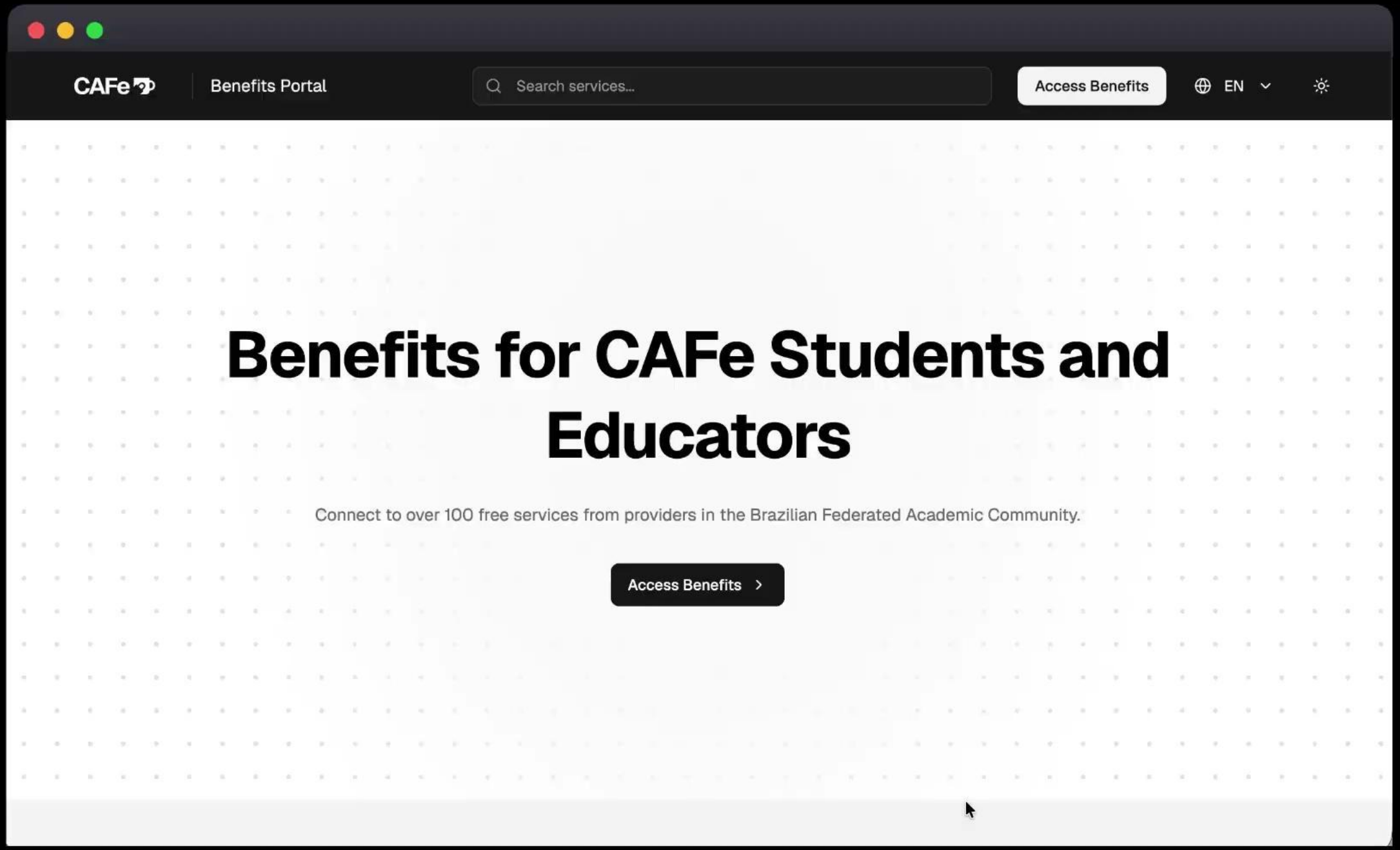
Metrics and Service Analytics

Alerts about service degradation and possibility to collect user feedback for federated services



Service catalog & WAYF

Public list of federated services, built from the federation itself; institution discovery


CAFe
Benefits Portal
Search services...
Access Benefits
EN
Benefits for CAFe Students and Educators
Connect to over 100 free services from providers in the Brazilian Federated Academic Community.
Access Benefits

SOLUTION 4/4

Protocol proxies

Both run on multi-tenant SATOSA, operated by RNP.

OIDC PROXY · for providers that speak plain OpenID Connect or OAuth

Plain OIDC or OAuth
An institution IdP, OIDC client or OAuth 2.0 service, as it runs today

OIDC

Proxy OIDC
One federation entity per provider; RNP holds its keys and signs its statements

OIDFed

OpenID Federation leaf
Resolvable under the CAFe TA like any native entity

Onboarding: register in the management system, receive a client ID, secret and endpoint, and point the OIDC configuration to it.

SAML PROXY · for the IdPs and SPs already in CAFe

CAFe SAML entities
Shibboleth IdPs and SAML SPs, unchanged

SAML

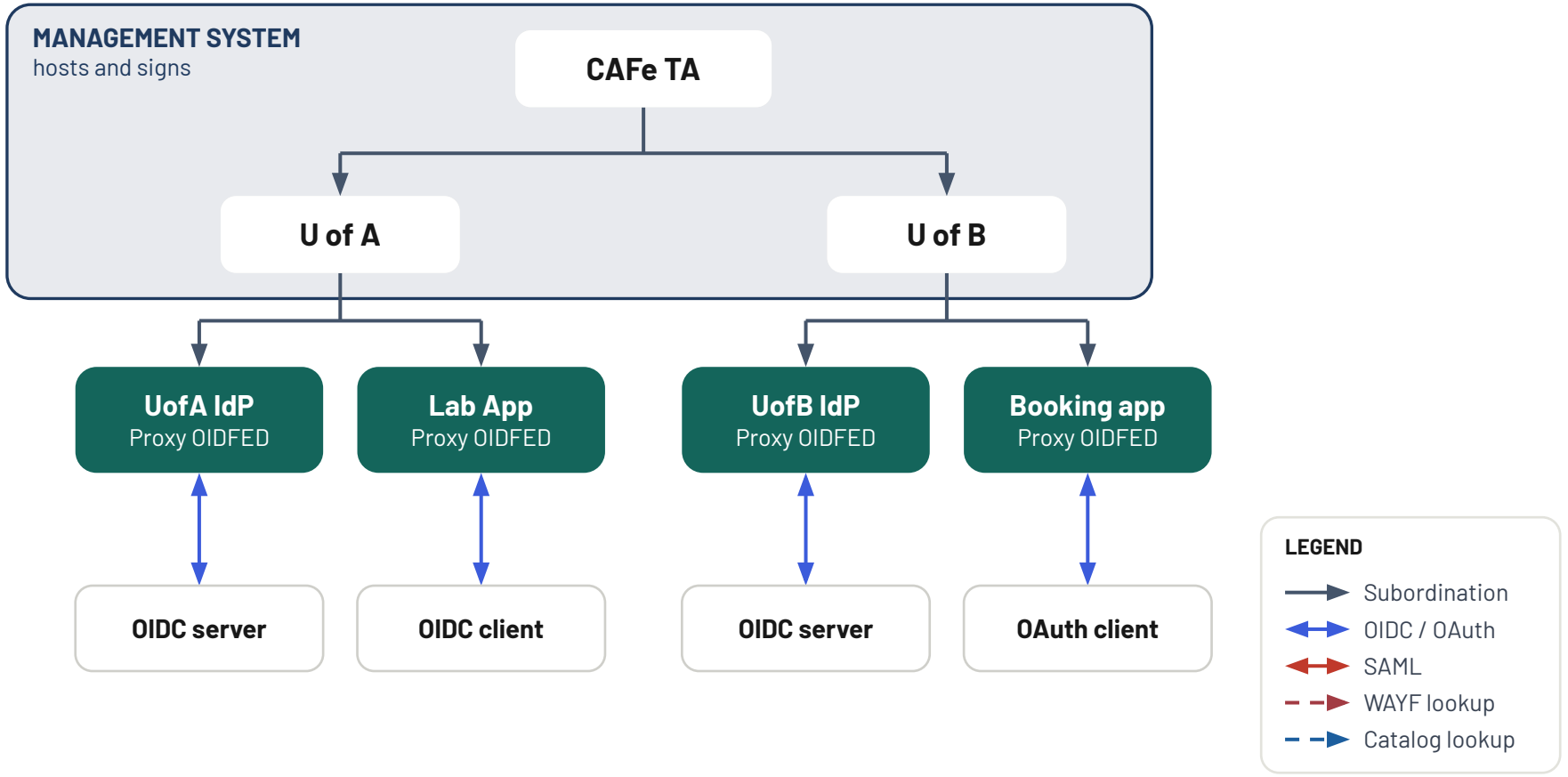
Proxy SAML
Reads CAFe metadata; acts as a SAML SP toward IdPs and as a SAML IdP toward SPs

OIDFed

OpenID Federation leaves
Each CAFe entity is published as a leaf, with no new registration

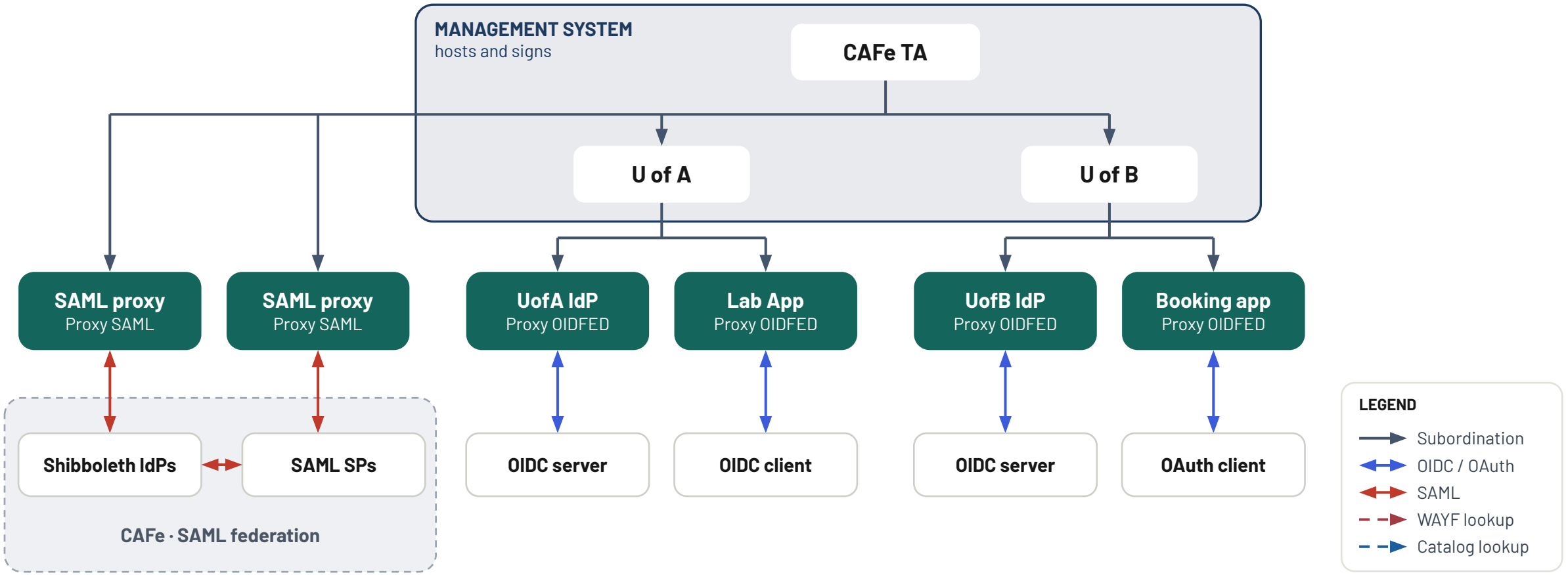
New OIDC services log users in at existing Shibboleth IdPs. Letting existing SAML services accept new OIDC IdPs is in progress.

The components on the federation tree



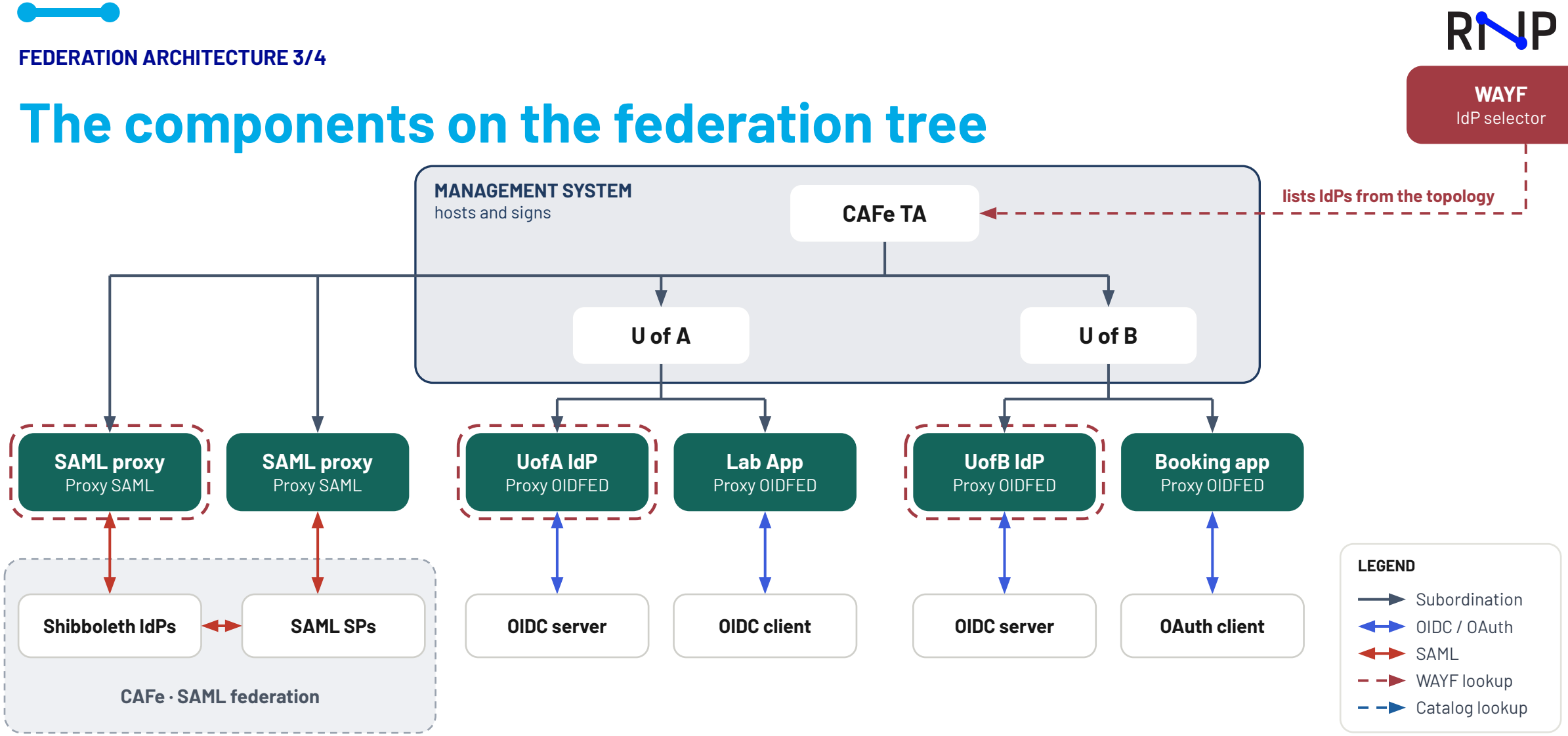
Each OIDC or OAuth leaf is an **Proxy OIDFED instance**; the server behind it only speaks plain OIDC.

The components on the federation tree



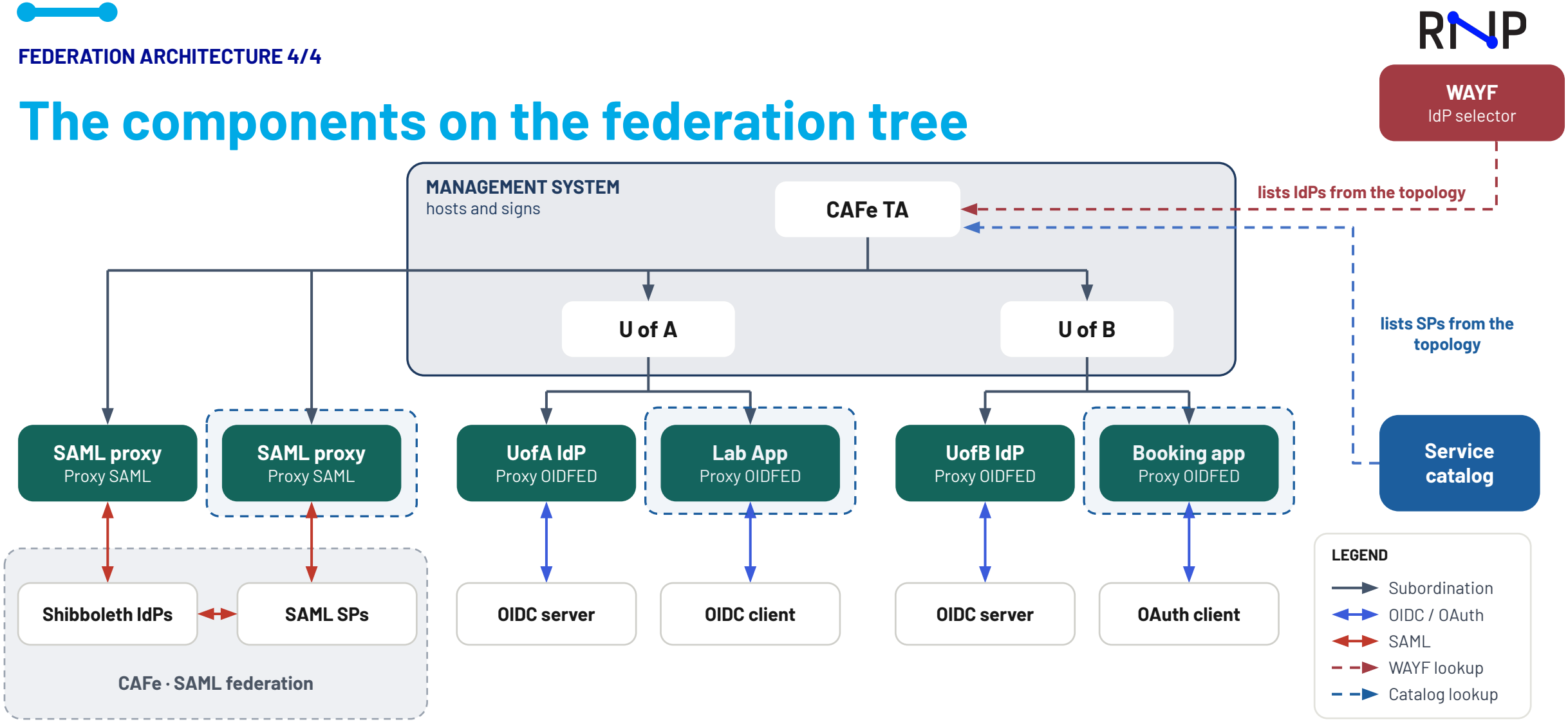
CAFe stays on SAML. **A SATOSA proxy instance** exposes its IdPs and SPs as OIDFed leaf entities.

The components on the federation tree



The WAYF reads the tree to list every IdP; the user picks one.

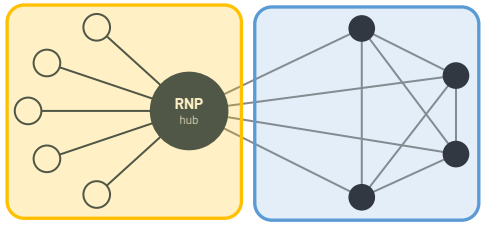
The components on the federation tree



The service catalog reads the leaf entities' metadata to list every service.

THE HYBRID MODEL 1/2

Mesh & hub-and-spoke



RUN BY RNP

MANAGEMENT SYSTEM
hosts and signs

CAFe TA

U of A

U of B

WAYF
IdP selector

Discovers IdPs under the CAFe TA

Discovers SPs under the CAFe TA

Service catalog

SAML proxy
Proxy SAML

SAML proxy
Proxy SAML

UofA IdP
Proxy OIDFED

Lab App
Proxy OIDFED

UofB IdP
Proxy OIDFED

Booking app
Proxy OIDFED

Shibboleth IdPs

SAML SPs

CAFe · SAML federation

OIDC server

OIDC client

OIDC server

OAuth client

RUN BY THE INSTITUTION

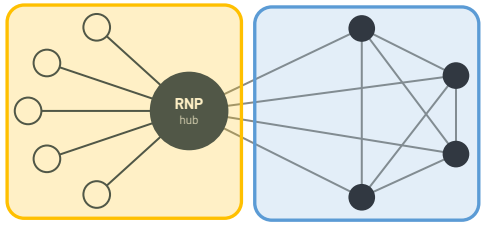
LEGEND

- Subordination
- OIDC / OAuth
- SAML
- WAYF lookup
- Catalog lookup

Hosted (default): RNP runs the hub; the institution runs only its IdP and services.

THE HYBRID MODEL 2/2

Mesh & hub-and-spoke



RUN BY RNP

MANAGEMENT SYSTEM
hosts and signs

CAFe TA

U of A

U of B

WAYF
IdP selector

Discovers IdPs under the CAFe TA

Discovers SPs under the CAFe TA

Service catalog

SAML proxy
Proxy SAML

SAML proxy
Proxy SAML

UofA IdP
Proxy OIDFED

Lab App
Proxy OIDFED

UofB IdP
OIDFED

Booking app
OIDFED

Shibboleth IdPs

SAML SPs

CAFe · SAML federation

OIDC server

OIDC client

RUN BY THE INSTITUTION

LEGEND

- Subordination
- OIDC / OAuth
- SAML
- WAYF lookup
- Catalog lookup
- Direct OIDFed

Self-managed (optional): U of B runs its own branch and joins the mesh, next to the hub.

Contributions to standards and implementations

OpenID Federation 1.0

Published February 2026

OpenID Federation for Wallet Architectures 1.0

Published February 2026

OpenID Connect Relying Party Metadata Choices 1.0

Published March 2026

Developers Italia

OpenID Federation related implementations

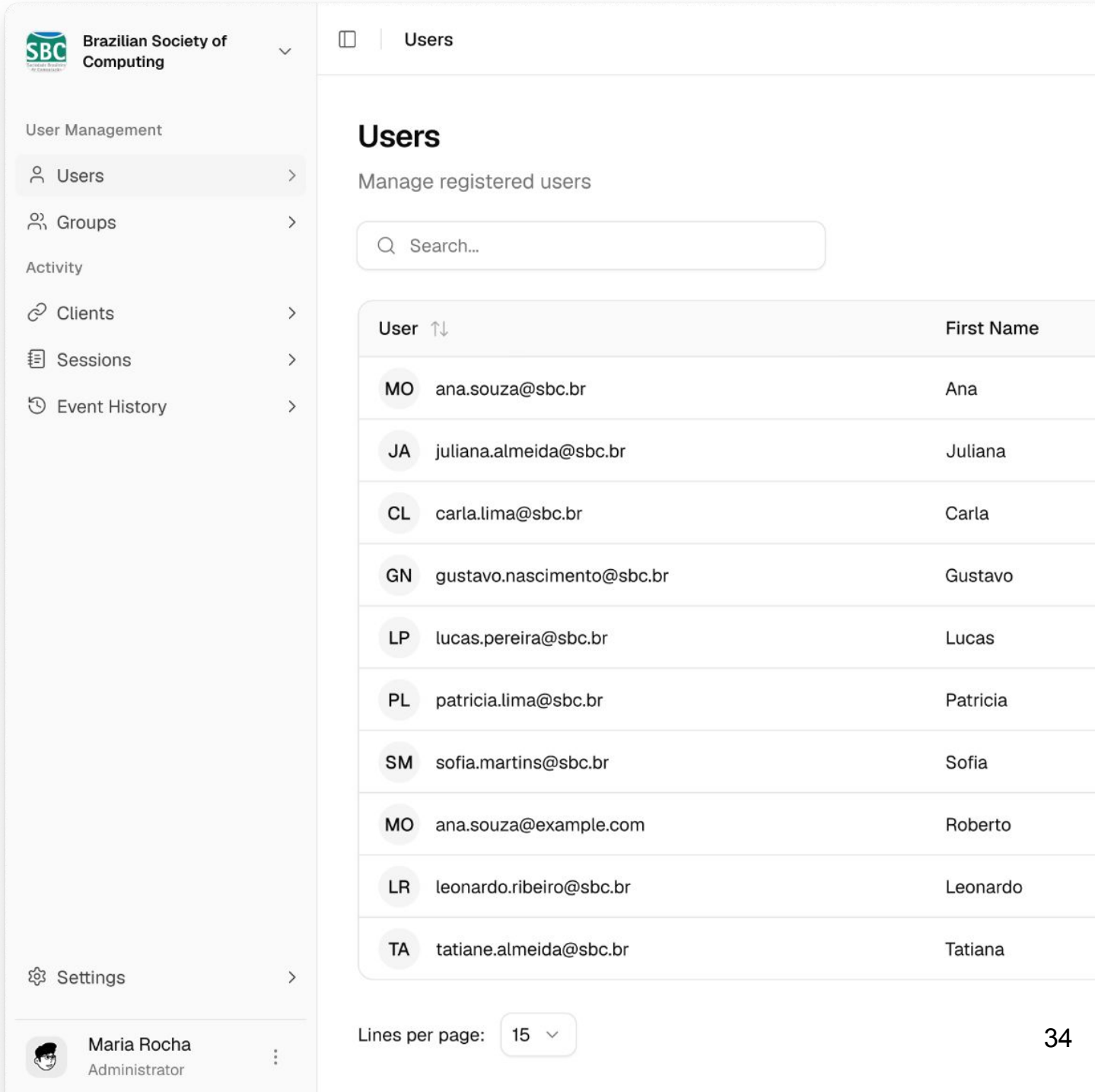
- SATOSA implementation
- django implementation

WORK IN PROGRESS 1/3

Next steps

IdP as a Service

Bridging the gap of identity and access management inside the federated institutions

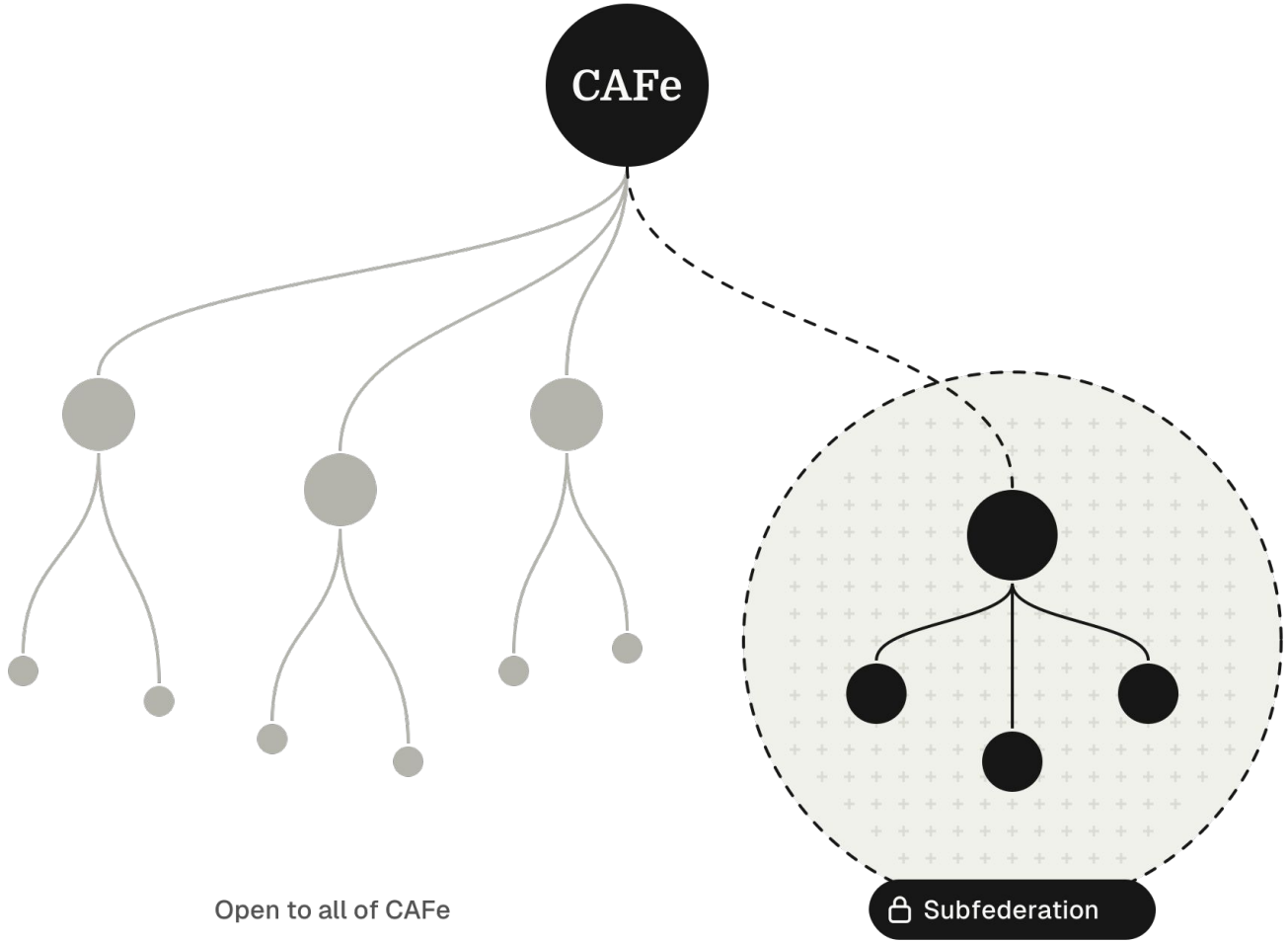


Next steps

Subfederations

Private spaces inside CAFe.

Groups of institutions can share services with their own members only, while still following the federation's common rules.



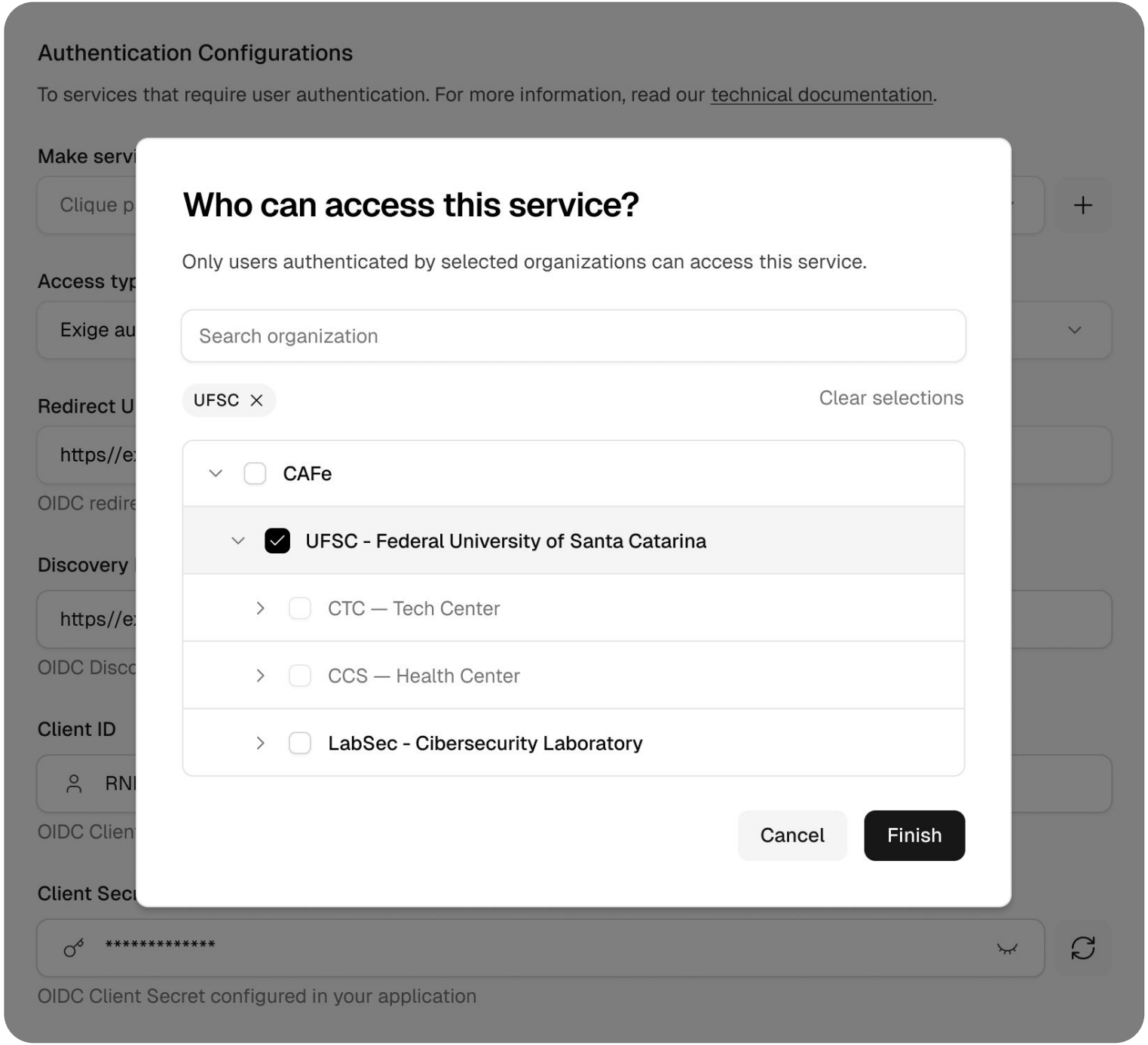
WORK IN PROGRESS 2/3

Next steps

Subfederations

Private spaces inside CAFe.

Groups of institutions can share services with their own members only, while still following the federation's common rules.



Next steps

Partial

- Attribute normalization
- MFA enforcement
- Request/receive eduGAIN trust mark
- Smart(er) service catalog

Planned

- Support for metadata policies
- Service catalog personalization
- Pentesting

NEXT STEPS 2/2

Phase 2: from MVP to experimental operation

Early adopters

Select interested institutions and put the components into experimental operation

Validation and integration

Validate with users and institutions; integrate progressively into CAFe

International alignment

Follow eduGAIN's OpenID Federation pilots and work with US and European communities

Beyond login

Verifiable credentials; RNP's future federated HPC and AI infrastructure (OIDC)

Technology changes go together with a review of federation policies.

CALL TO ACTION

Where we could work together

Opportunity: InCommon's PORE (Profiling OpenID Federation for R&E) calls for implementation evidence.

Interoperability without a forced migration

Test BAITA's OIDC and SAML proxies with new services and existing campus identity providers.

Less operational work for campuses

Evaluate BAITA's hosted management model for registration, key handling and auditability.

More visible federated services

Test BAITA's service catalog and discovery for simpler access to research services.

Evidence for shared trust requirements

Test BAITA trust chains against InCommon policies and the emerging R&E profile.

Opportunity: a joint technical workshop with Internet2/InCommon, eduGAIN and partner NRENs.

If you or your institution are facing similar scenarios to what we described, feel free to contact us!

We are always looking for different use cases that could strengthen our solution.

https://gt-baita.ifrs.edu.br/

THE TEAM



PRINCIPAL INVESTIGATOR

Frederico Schardong, PhD



INNOVATION ASSISTANT

Eduardo Perottoni



INNOVATION ASSISTANT

Brendon Vicente



INNOVATION ASSISTANT

Giulia Manno



DEVELOPER

Leonardo Passos



DEVELOPER

Rayane Melo



DEVELOPER

Raissa Lima



DEVELOPER

Charlie Terra



DEVELOPER

Álison Batista

WG-BAITA

Thank you!

Prof. Frederico Schardong, PhD
UFSC

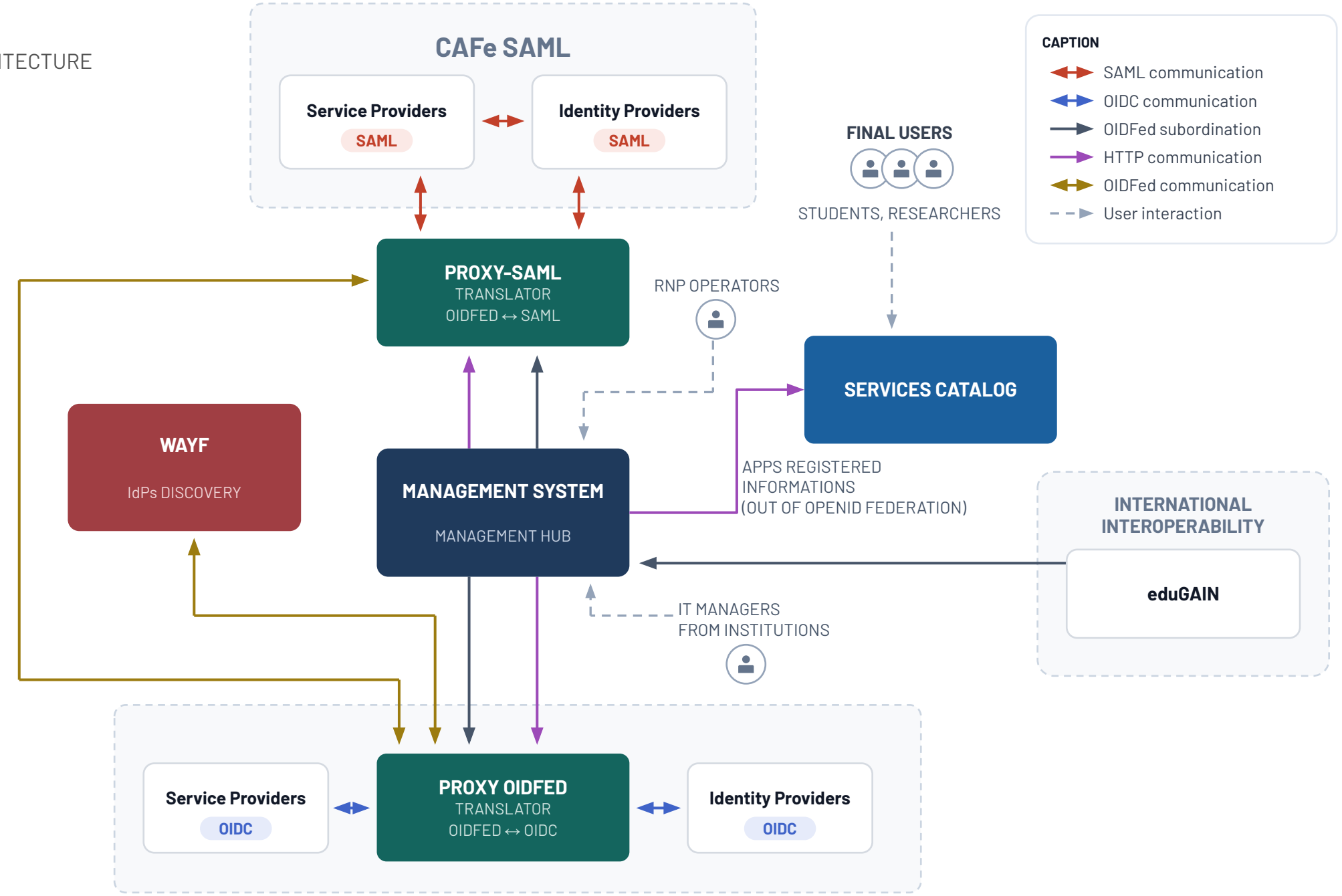
https://admin.baita.testbeds.rnp.br/

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Extra material

Educação, Pesquisa
e Inovação em Rede

THE ARCHITECTURE



PROXY 1/2

OIDC proxy

For services and identity providers that speak plain OpenID Connect.

To the federation

An OpenID Federation entity

To the provider

A standard OIDC server or client

Who uses it

Both services and identity providers

Onboarding

The provider registers in the management system and receives a client ID, a secret and an endpoint. Pointing its OIDC configuration to that endpoint is the only change on the provider's side.

PROXY 2/2

SAML proxy

CAFe stays on SAML; the proxy exposes each CAFe entity as an OpenID Federation leaf.

CAFe · SAML FEDERATION
keeps running as it is today

CAFe SAML metadata
every IdP and SP in CAFe

Shibboleth IdPs
existing CAFe identity providers

SAML SPs
existing CAFe services

PROXY 2/2

SAML proxy

CAFe stays on SAML; the proxy exposes each CAFe entity as an OpenID Federation leaf.

CAFe · SAML FEDERATION
keeps running as it is today

- **CAFe SAML metadata**
  every IdP and SP in CAFe
- **Shibboleth IdPs**
  existing CAFe identity providers
- **SAML SPs**
  existing CAFe services

OPENID FEDERATION
BAITA

- **CAFe TA/Intermediates**
  OIDFed entities
- **New SPs**
  onboarded on BAITA
- **New IdPs**
  onboarded on BAITA

PROXY 2/2

SAML proxy

CAFe stays on SAML; the proxy exposes each CAFe entity as an OpenID Federation leaf.

CAFe · SAML FEDERATION
keeps running as it is today

- **CAFe SAML metadata**
  every IdP and SP in CAFe
- **Shibboleth IdPs**
  existing CAFe identity providers
- **SAML SPs**
  existing CAFe services

SAML PROXY · SATOSA

Publishes each CAFe entity
as an OIDFed leaf, no new registration

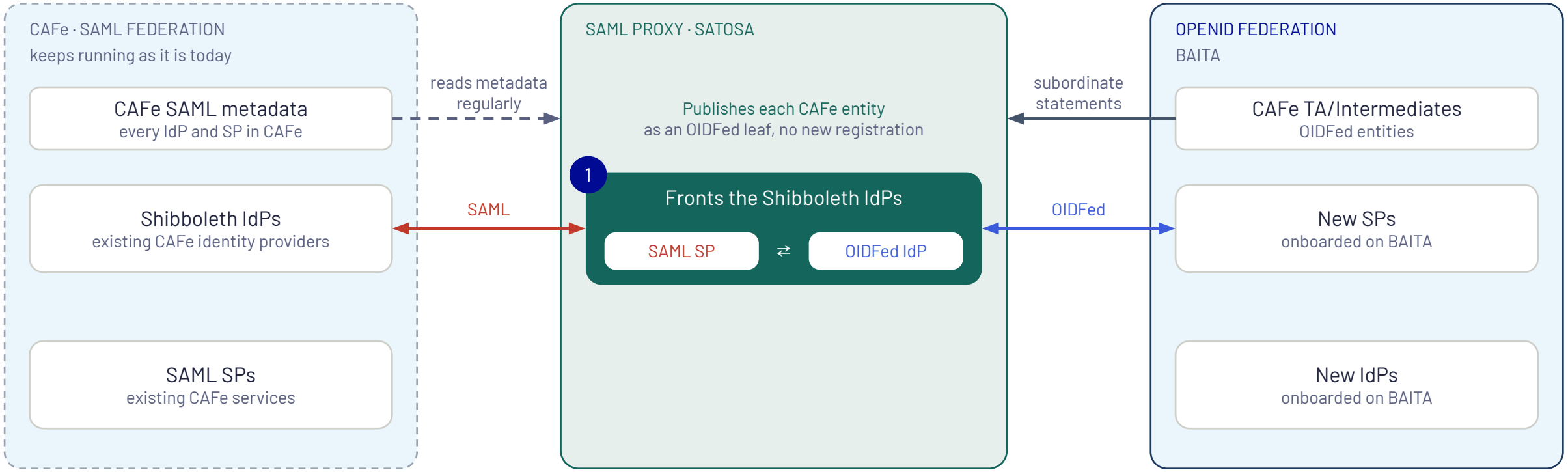
OPENID FEDERATION
BAITA

- **CAFe TA/Intermediates**
  OIDFed entities
- **New SPs**
  onboarded on BAITA
- **New IdPs**
  onboarded on BAITA

Side by side. Neither federation changes.
They meet only through the proxy.

SAML proxy

CAFe stays on SAML; the proxy exposes each CAFe entity as an OpenID Federation leaf.

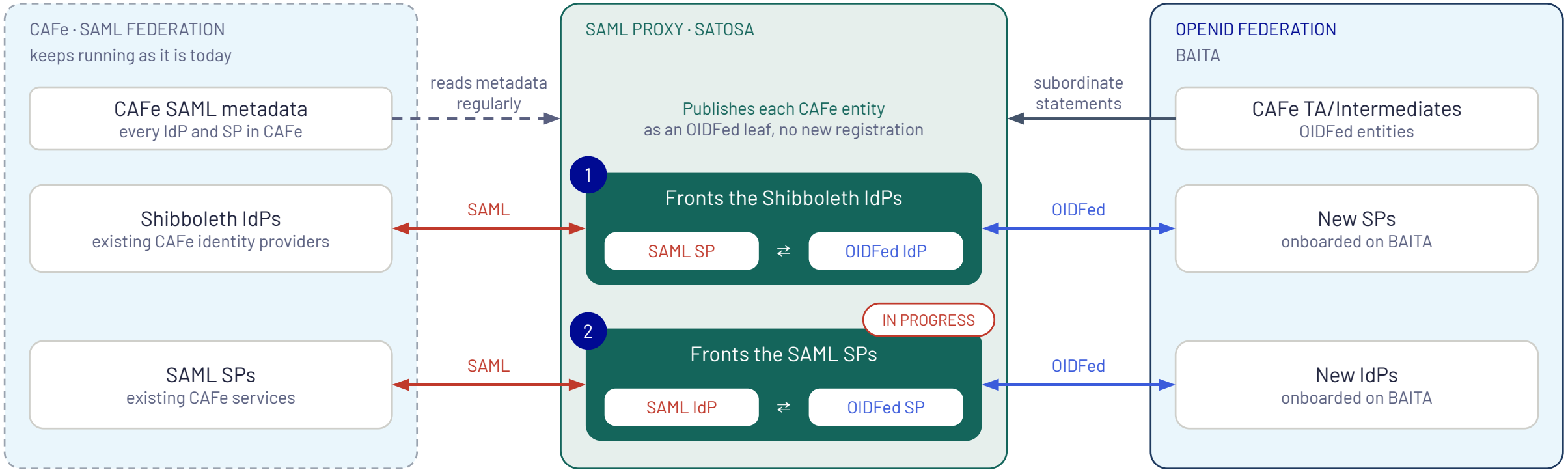


Side by side. Neither federation changes. They meet only through the proxy.

1 New OIDC services sign users in with existing Shibboleth IdPs, unchanged.

SAML proxy

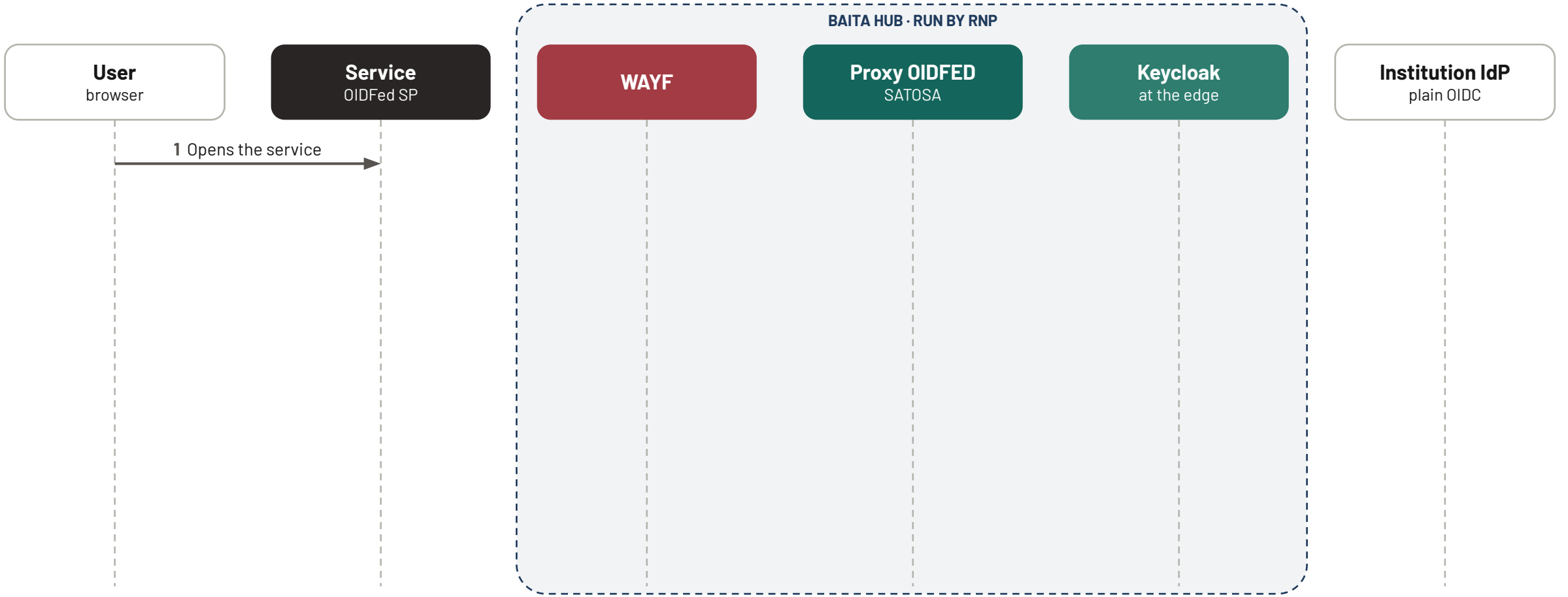
CAFe stays on SAML; the proxy exposes each CAFe entity as an OpenID Federation leaf.



Side by side. Neither federation changes. They meet only through the proxy.

1. New OIDC services sign users in with existing Shibboleth IdPs, unchanged.
2. Existing SAML services accept logins from new OIDC IdPs.

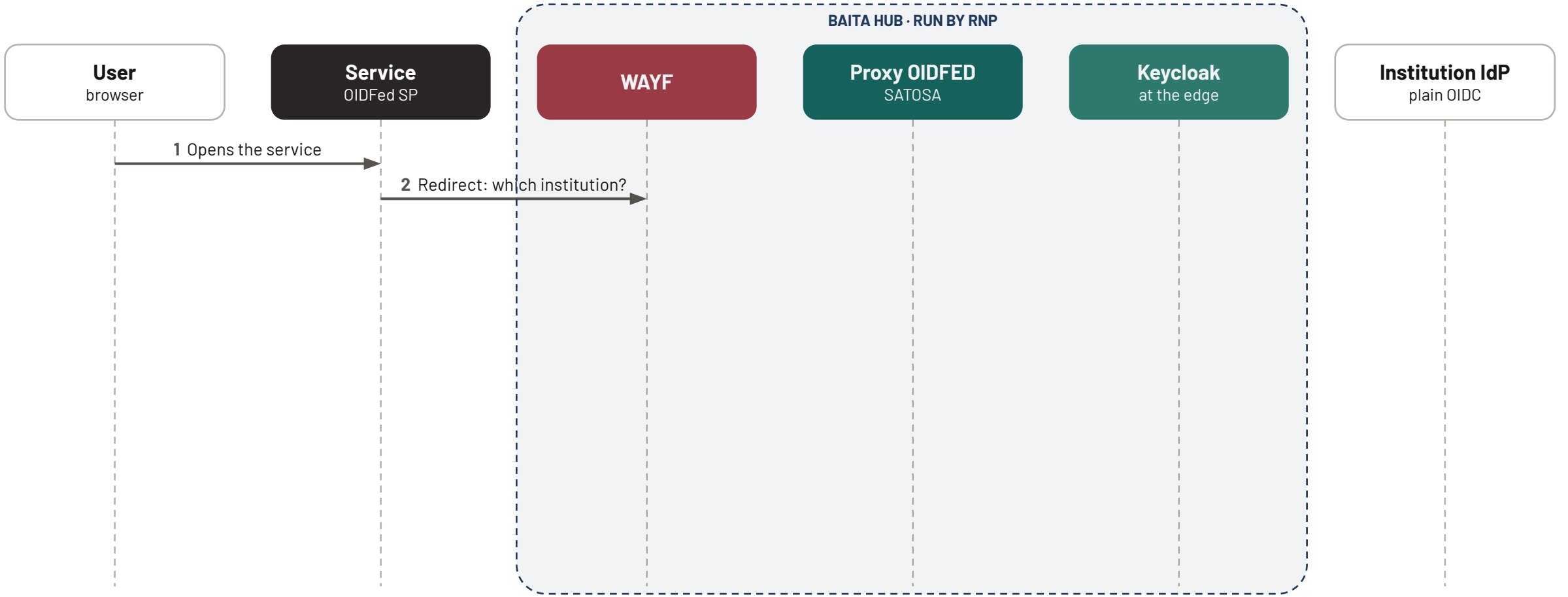
Login flow: OIDC identity provider



Discovery. The WAYF is only a hop: it lists IdPs from the topology and hands the choice back.

OpenID Federation · OIDC · SAML · Browser

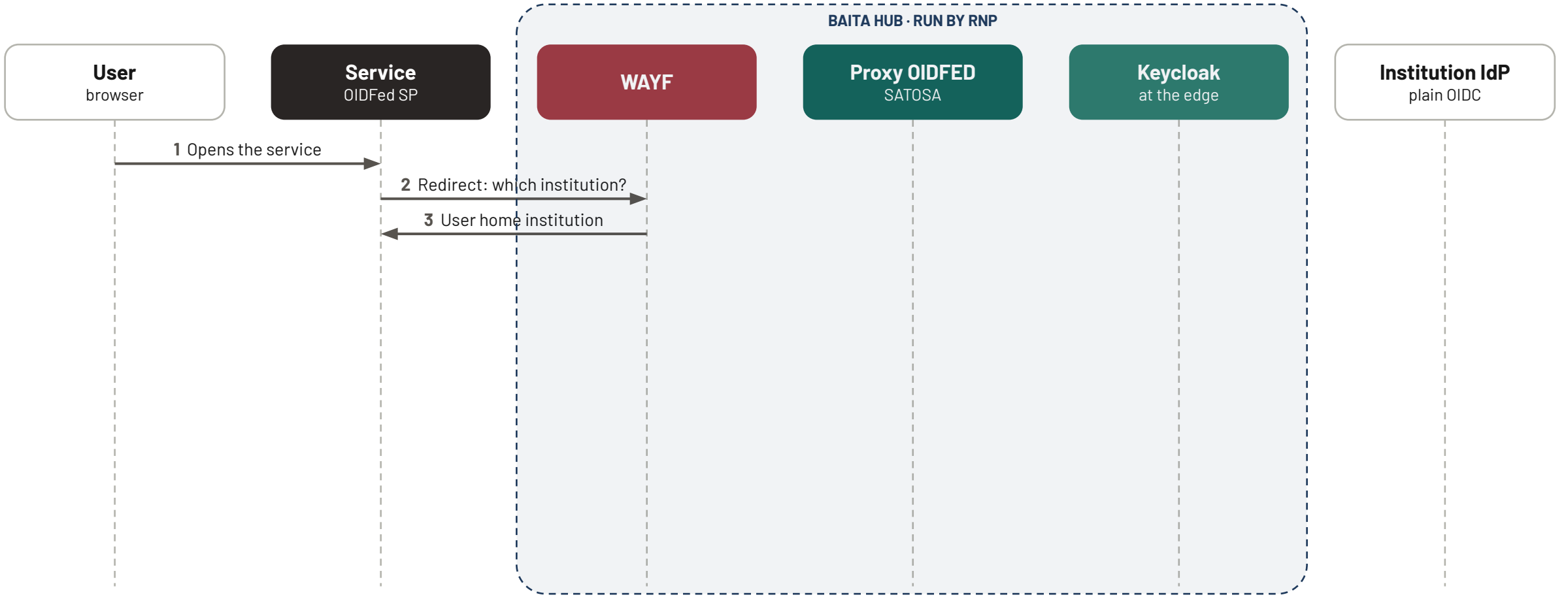
Login flow: OIDC identity provider



Discovery. The WAYF is only a hop: it lists IdPs from the topology and hands the choice back.

OpenID Federation · OIDC · SAML · Browser

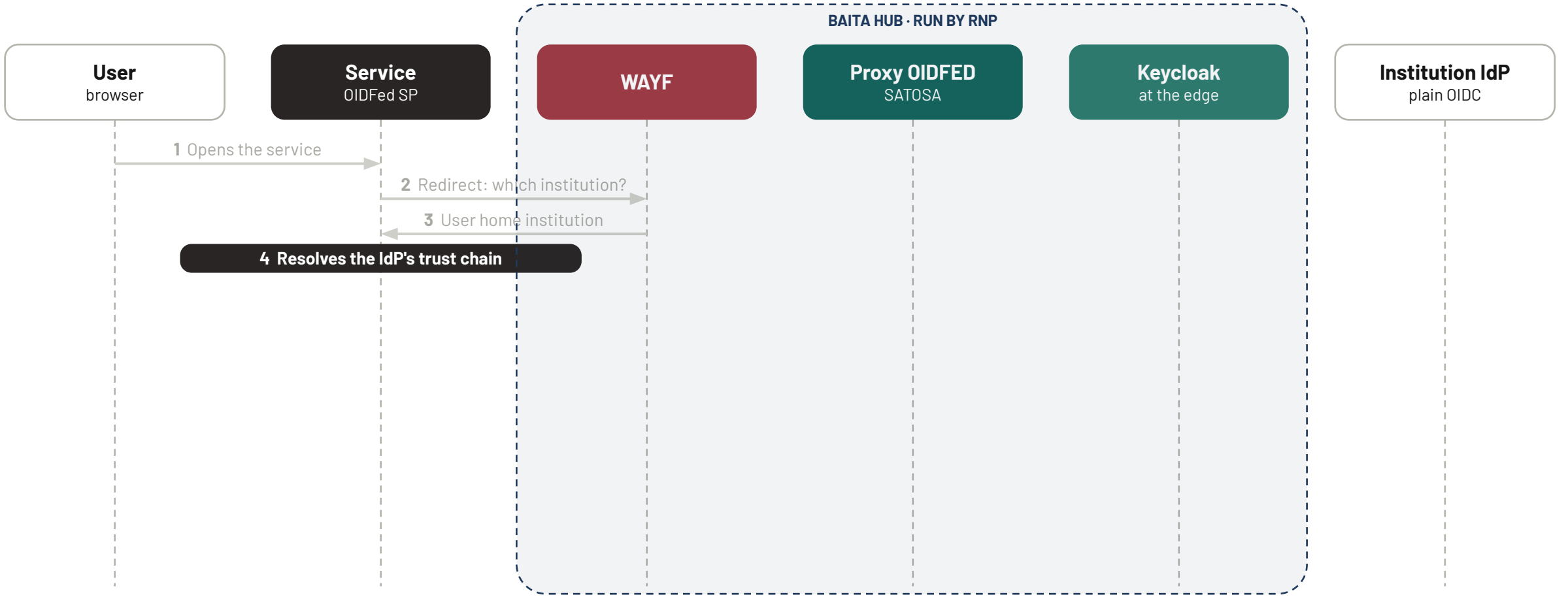
Login flow: OIDC identity provider



Discovery. The WAYF is only a hop: it lists IdPs from the topology and hands the choice back.

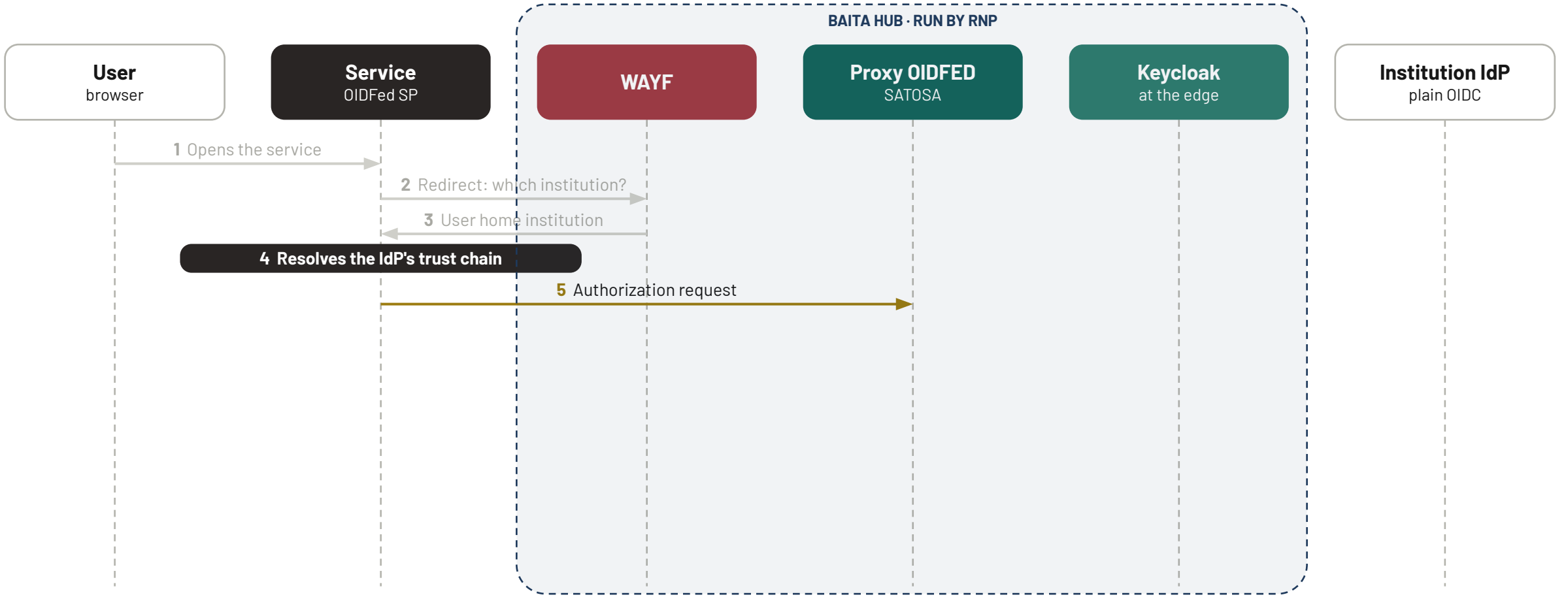
OpenID Federation · OIDC · SAML · Browser

Login flow: OIDC identity provider



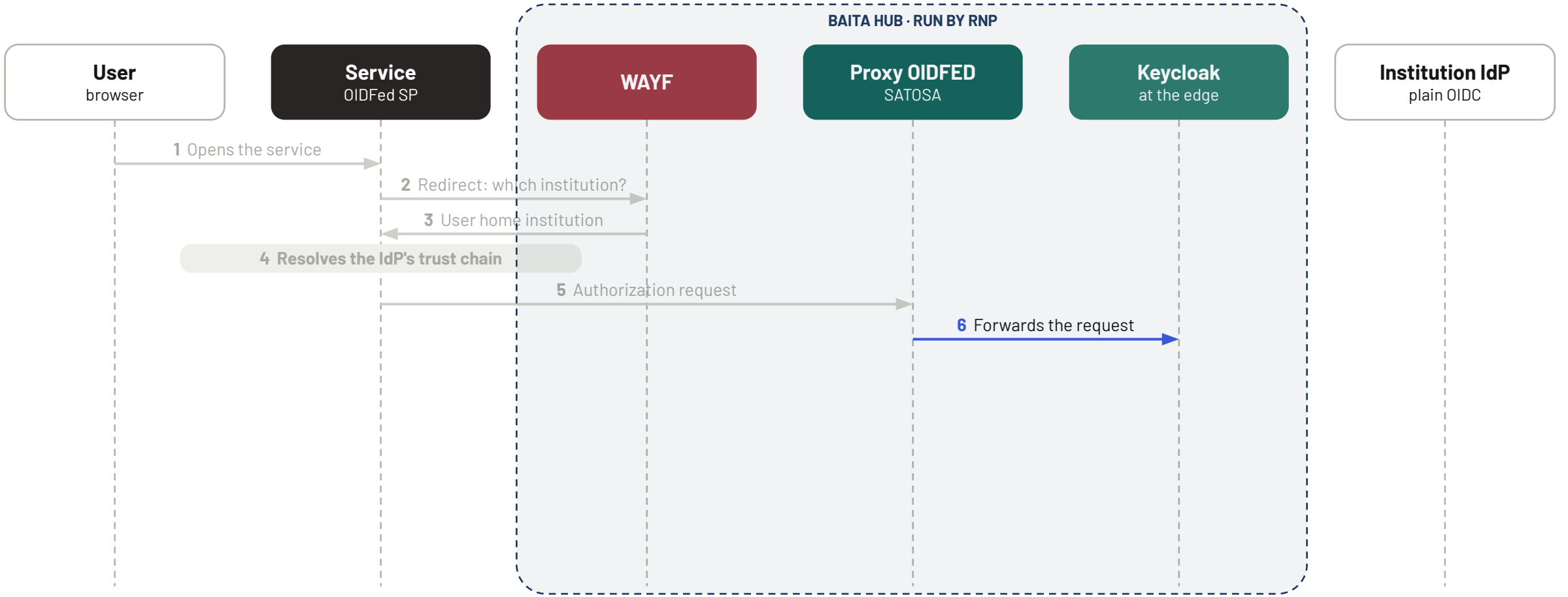
Trust. The service resolves the IdP's trust chain and sends a federation request, no prior registration.

Login flow: OIDC identity provider



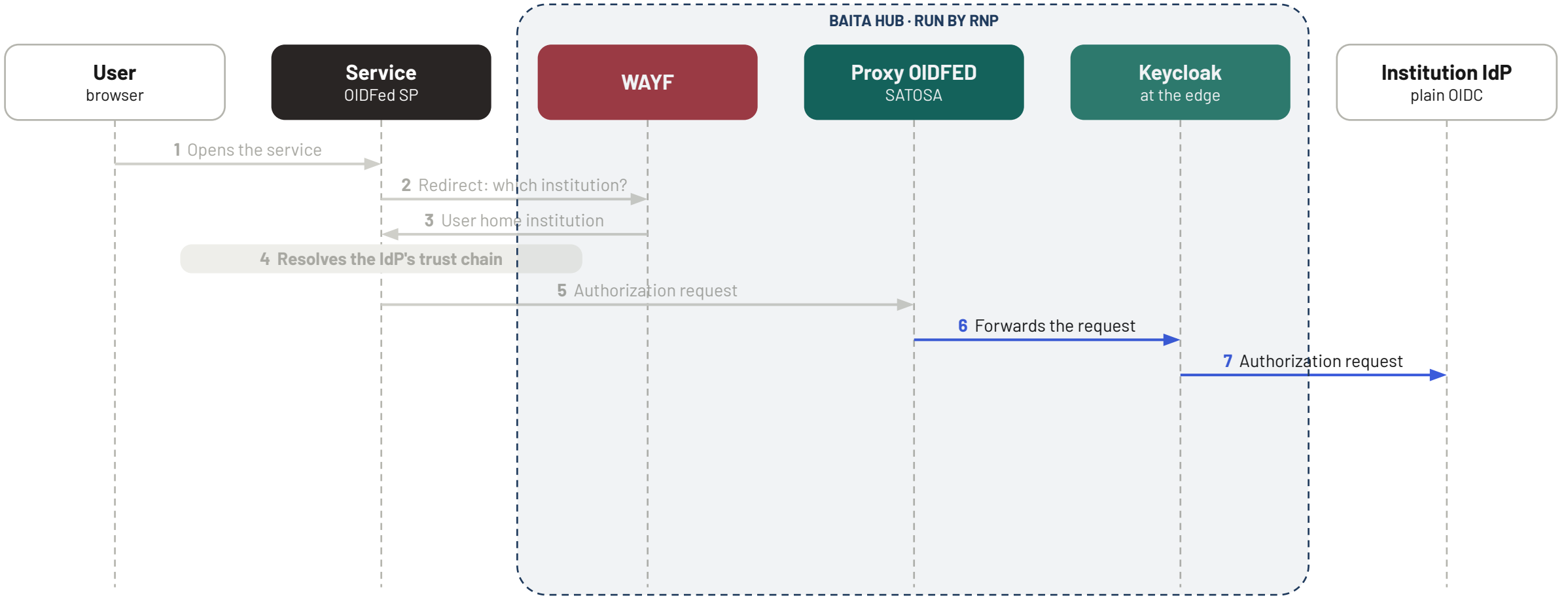
Trust. The service resolves the IdP's trust chain and sends a federation request, no prior registration.

Login flow: OIDC identity provider



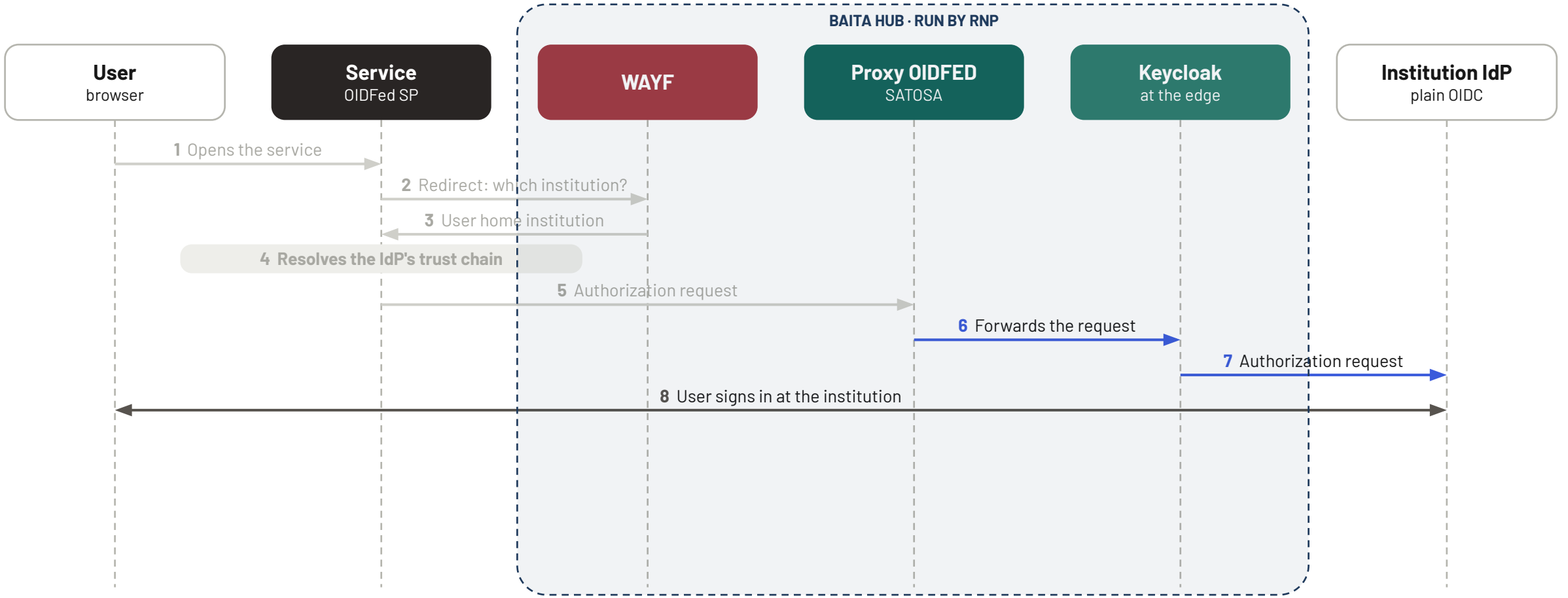
Authentication. Keycloak, at the edge, speaks plain OIDC to the institution's IdP.

Login flow: OIDC identity provider



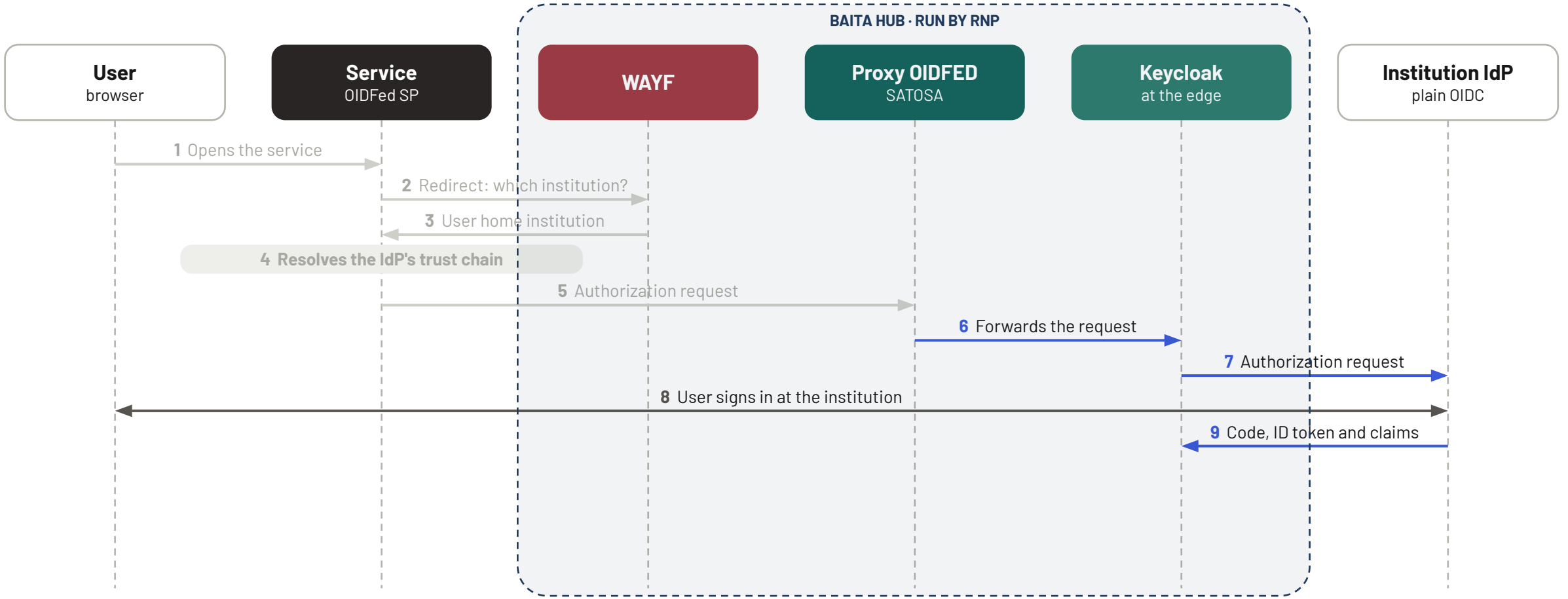
Authentication. Keycloak, at the edge, speaks plain OIDC to the institution's IdP.

Login flow: OIDC identity provider



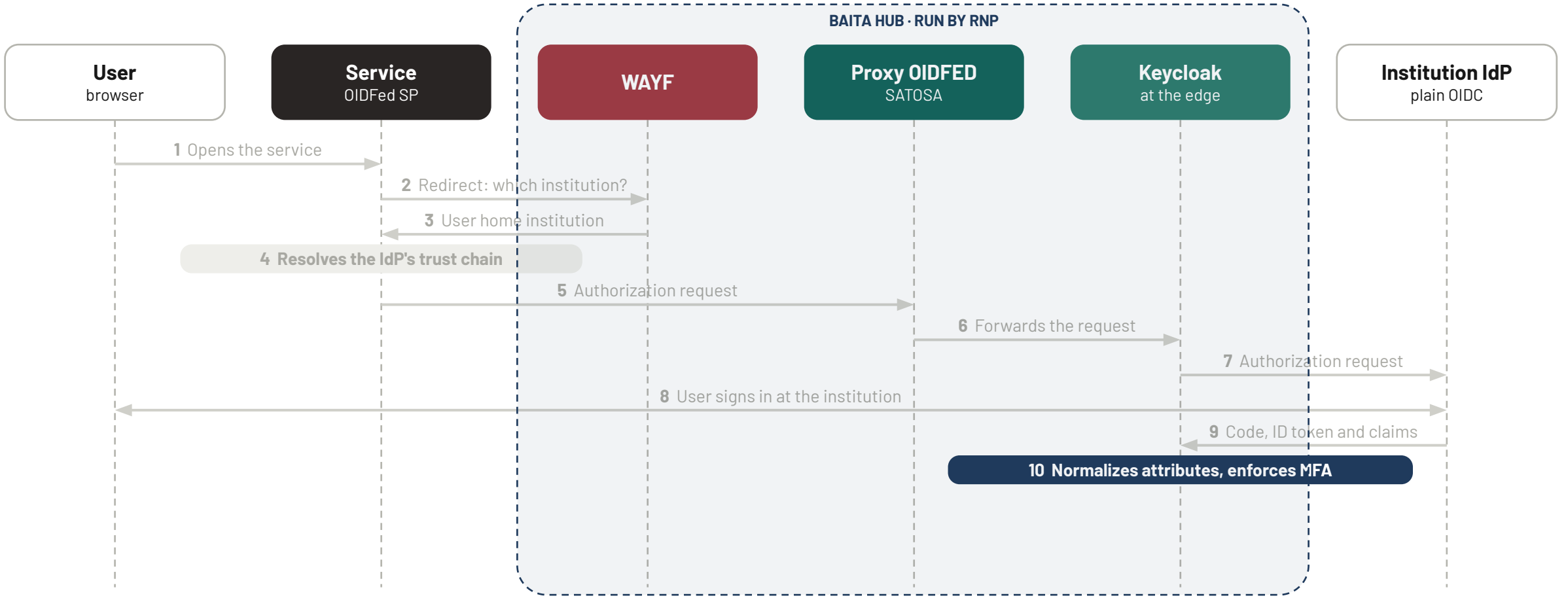
Authentication. Keycloak, at the edge, speaks plain OIDC to the institution's IdP.

Login flow: OIDC identity provider



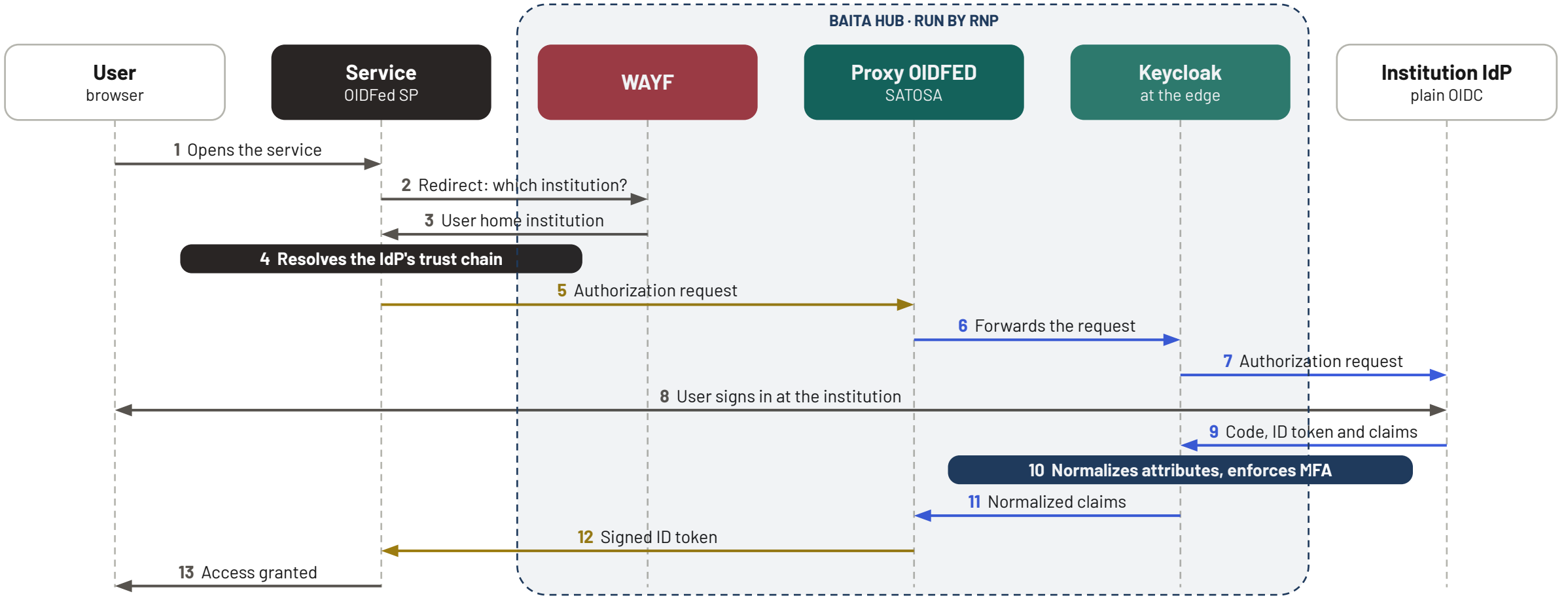
Authentication. Keycloak, at the edge, speaks plain OIDC to the institution's IdP.

Login flow: OIDC identity provider



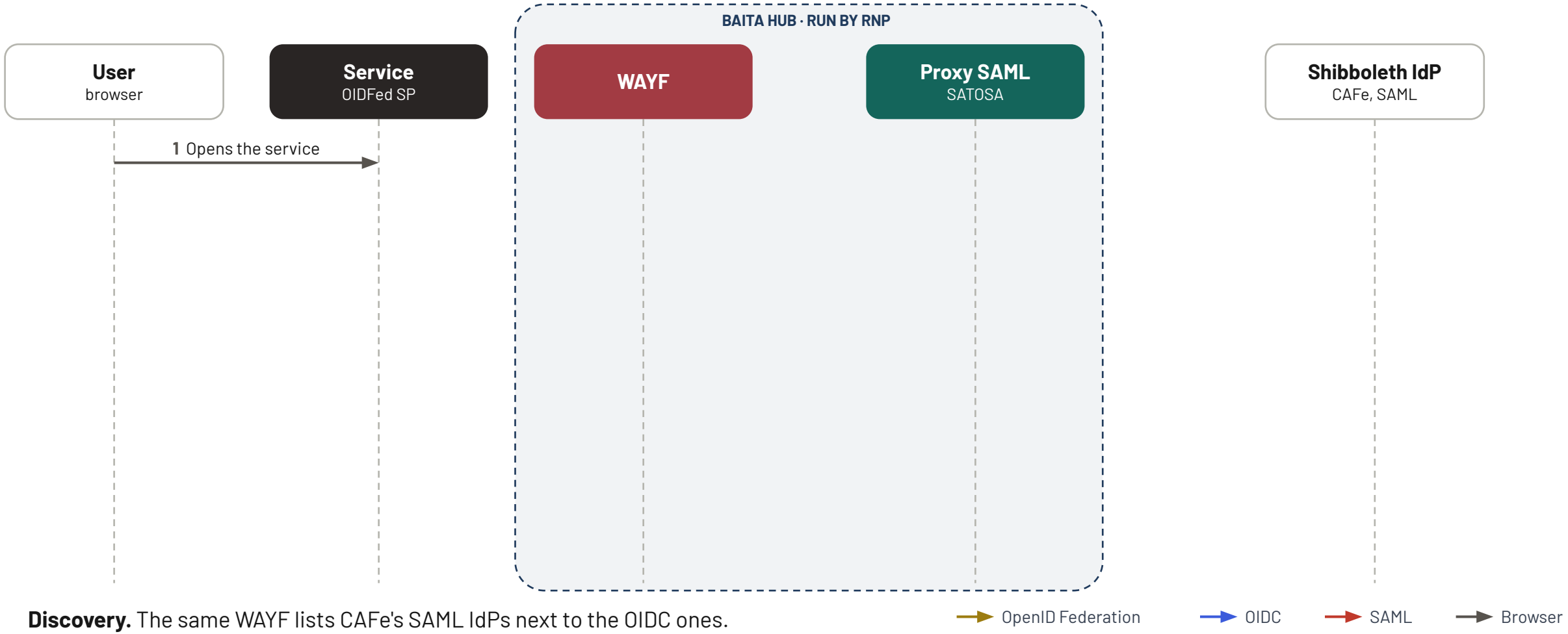
What the bus adds. Keycloak normalizes attributes and enforces MFA, not the WAYF.

Login flow: OIDC identity provider



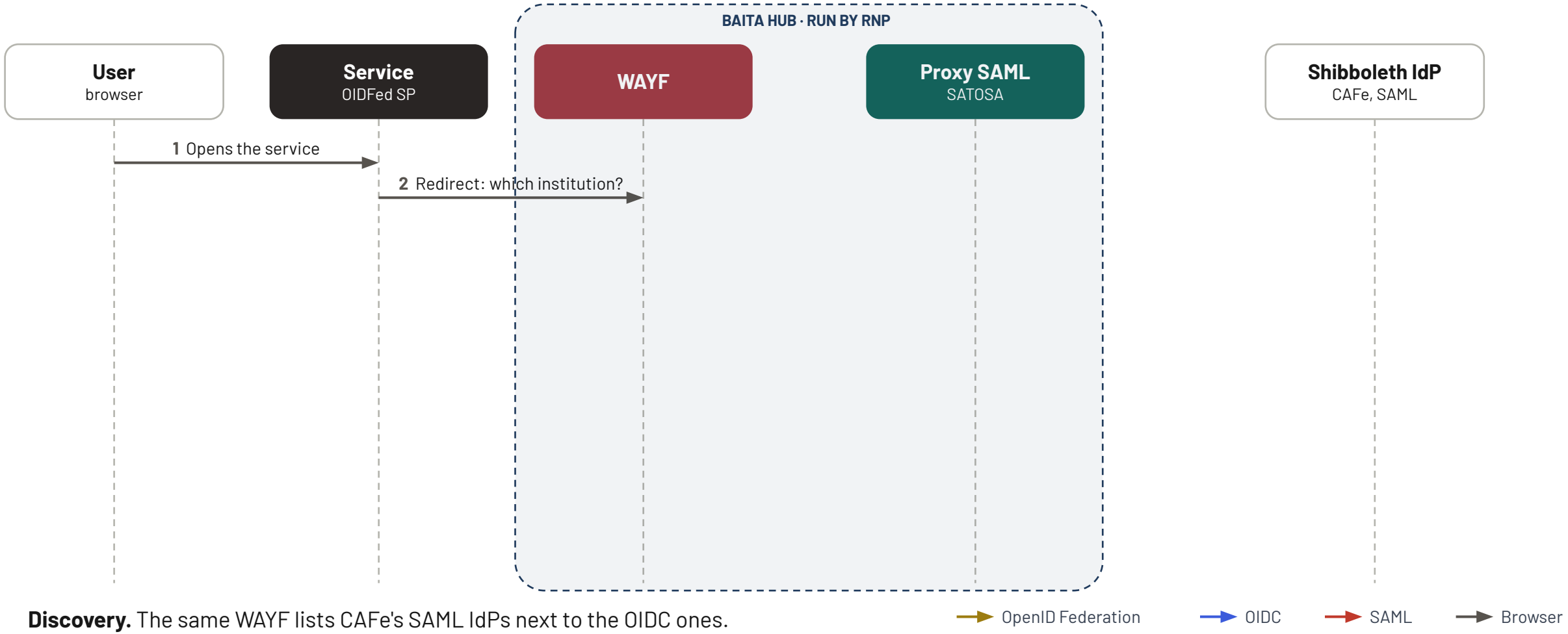
Response. The proxy returns a signed ID token to the service.

Login flow: CAFe SAML identity provider



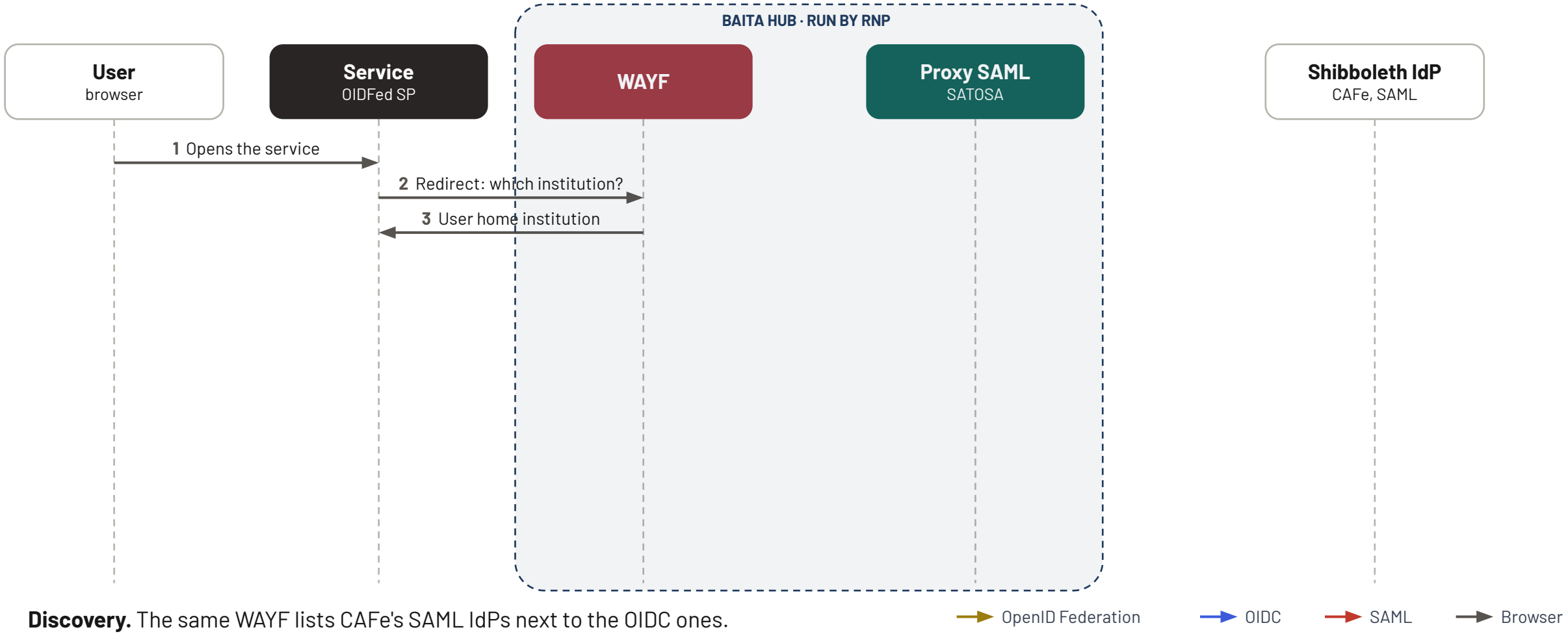
Discovery. The same WAYF lists CAFe's SAML IdPs next to the OIDC ones.

Login flow: CAFe SAML identity provider



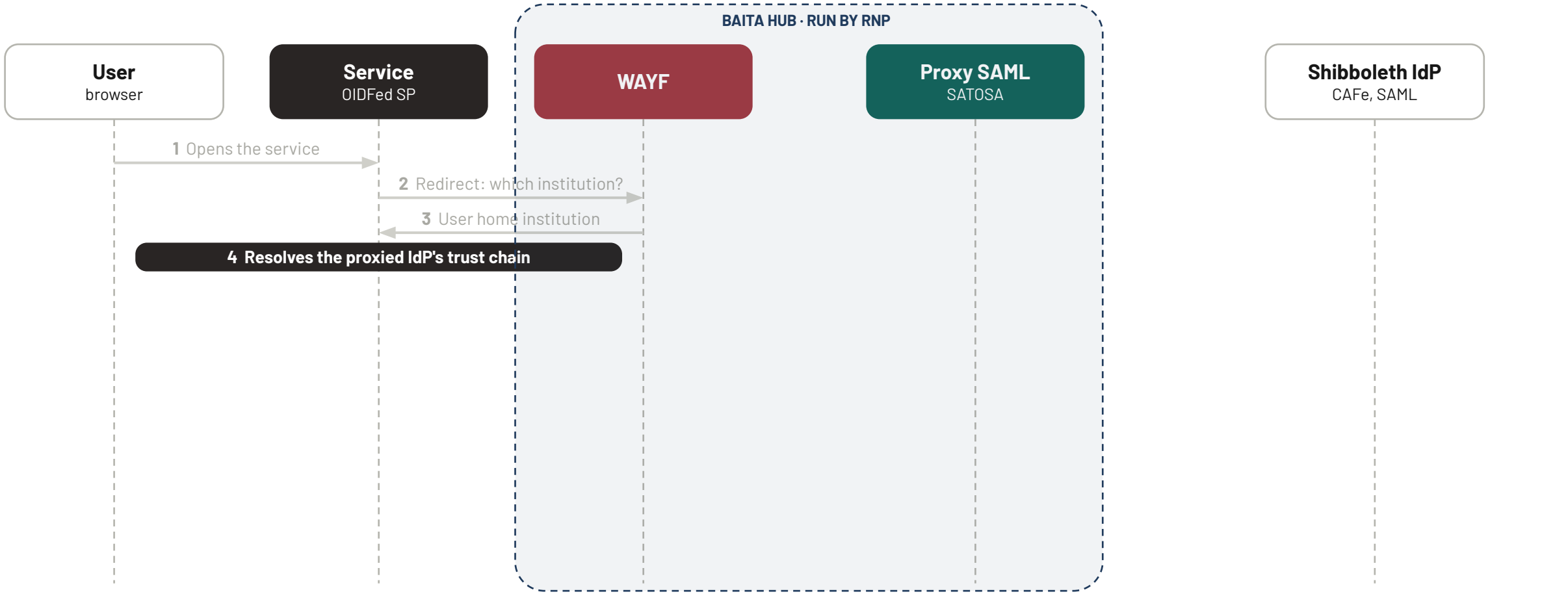
Discovery. The same WAYF lists CAFe's SAML IdPs next to the OIDC ones.

Login flow: CAFe SAML identity provider



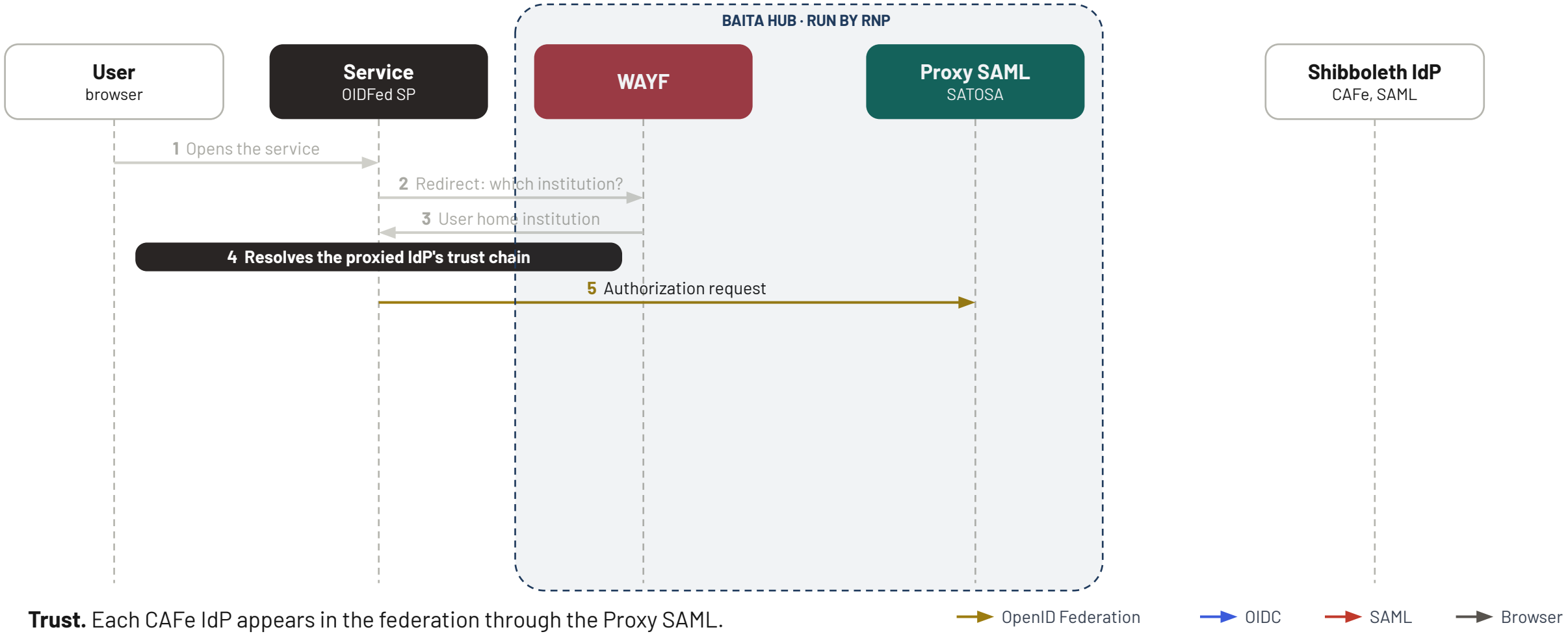
Discovery. The same WAYF lists CAFe's SAML IdPs next to the OIDC ones.

Login flow: CAFe SAML identity provider



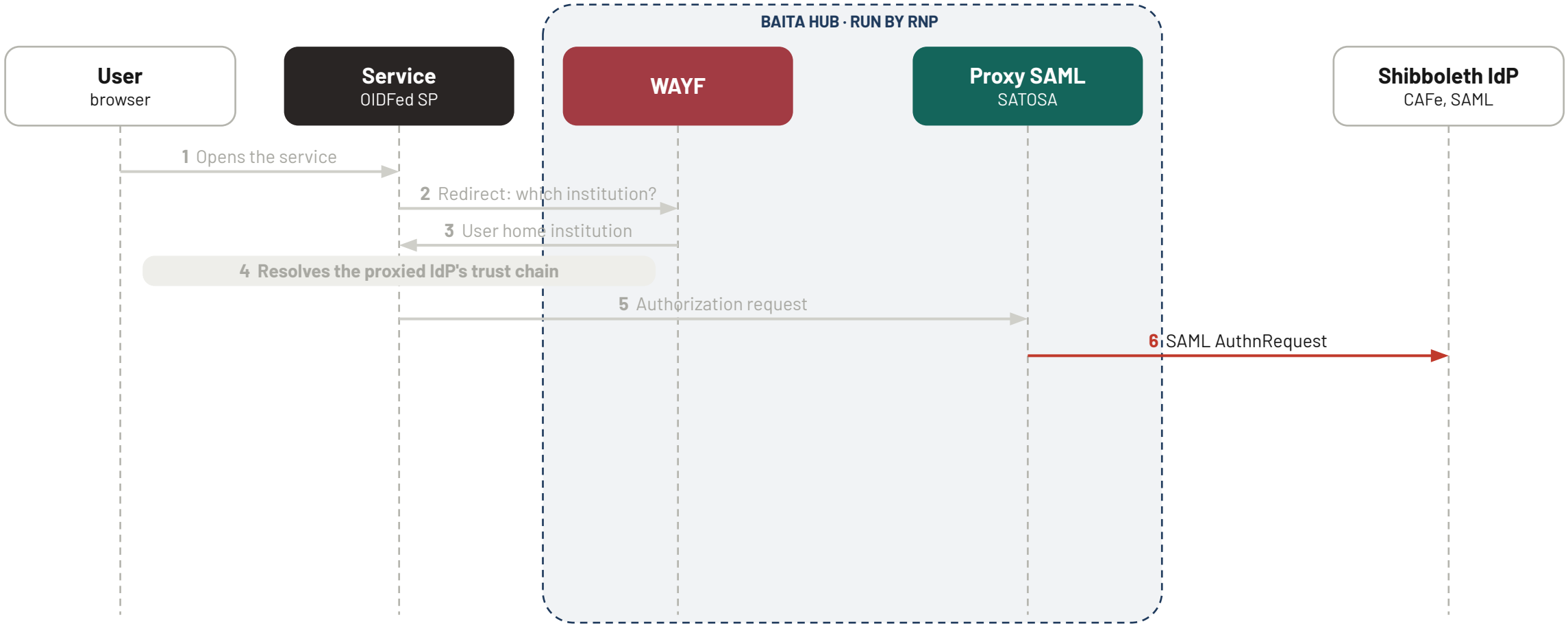
Trust. Each CAFe IdP appears in the federation through the Proxy SAML.

Login flow: CAFe SAML identity provider



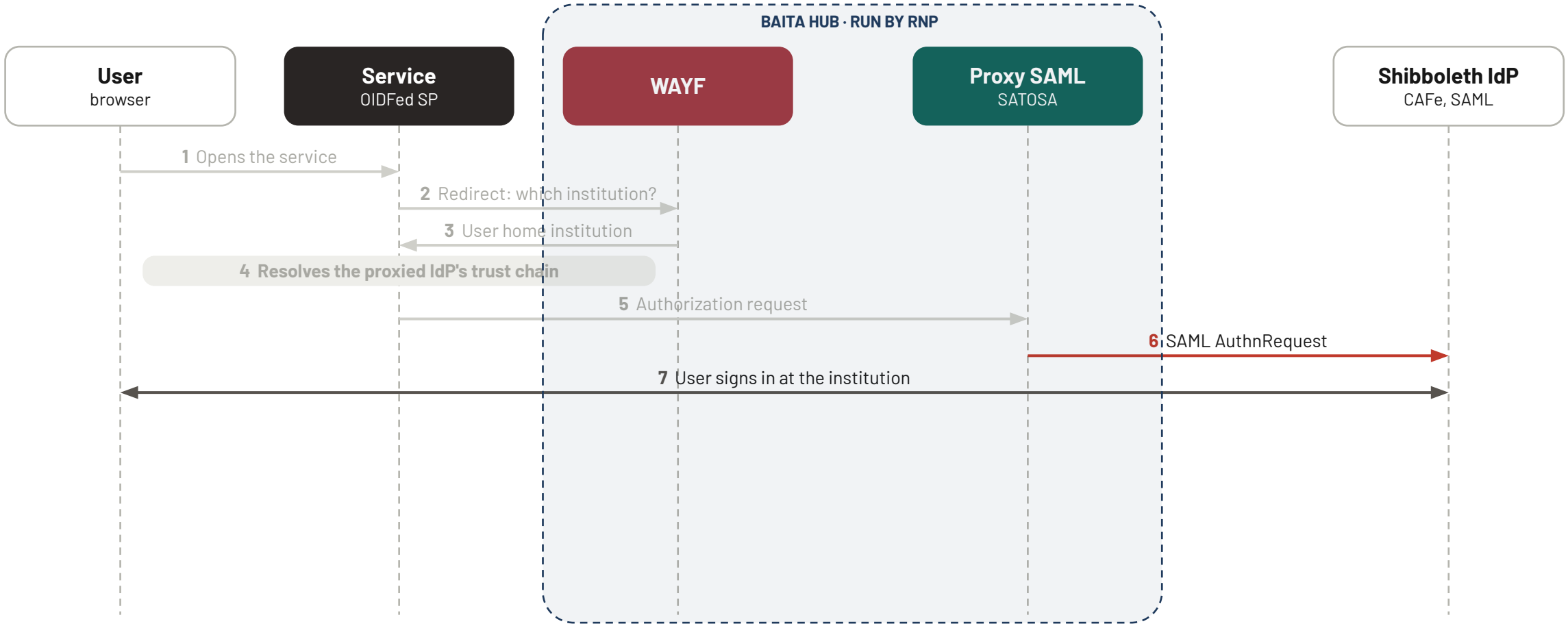
Trust. Each CAFe IdP appears in the federation through the Proxy SAML.

Login flow: CAFe SAML identity provider



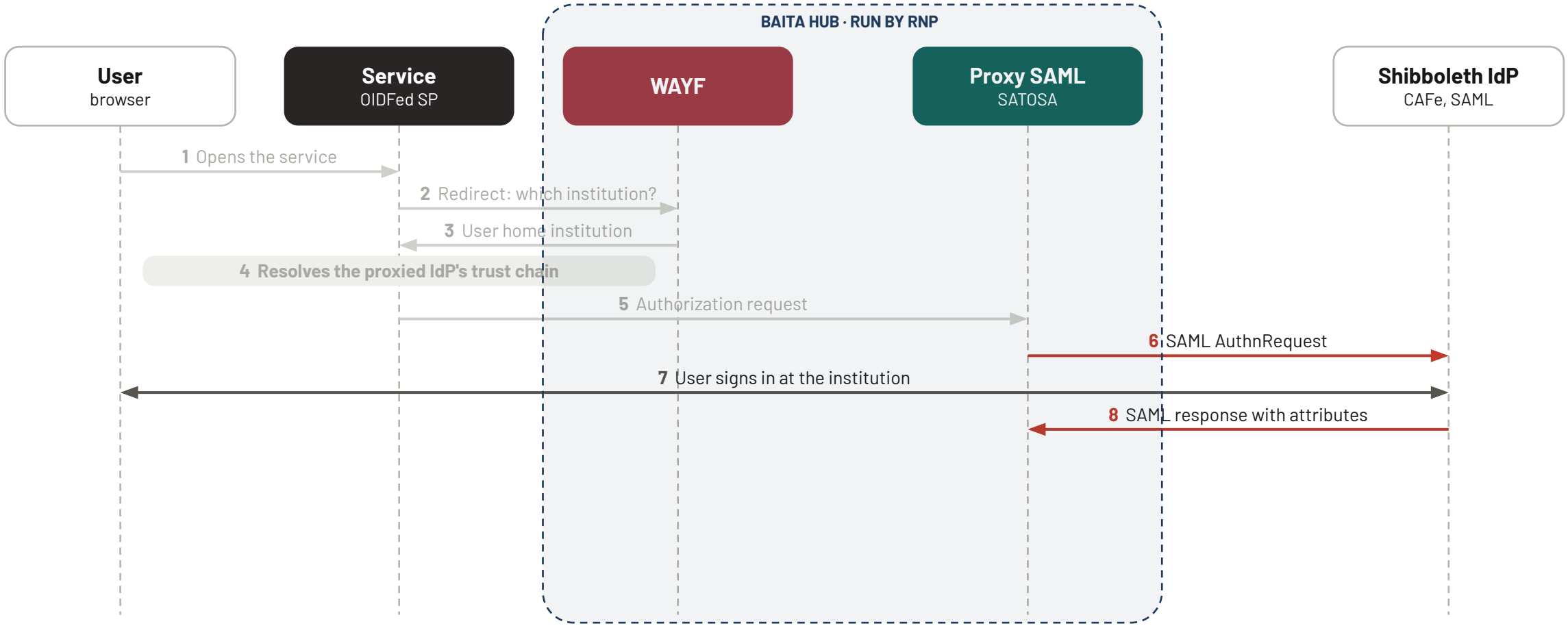
Authentication. The proxy acts as a regular CAFe SP: the Shibboleth IdP changes nothing.

Login flow: CAFe SAML identity provider



Authentication. The proxy acts as a regular CAFe SP: the Shibboleth IdP changes nothing.

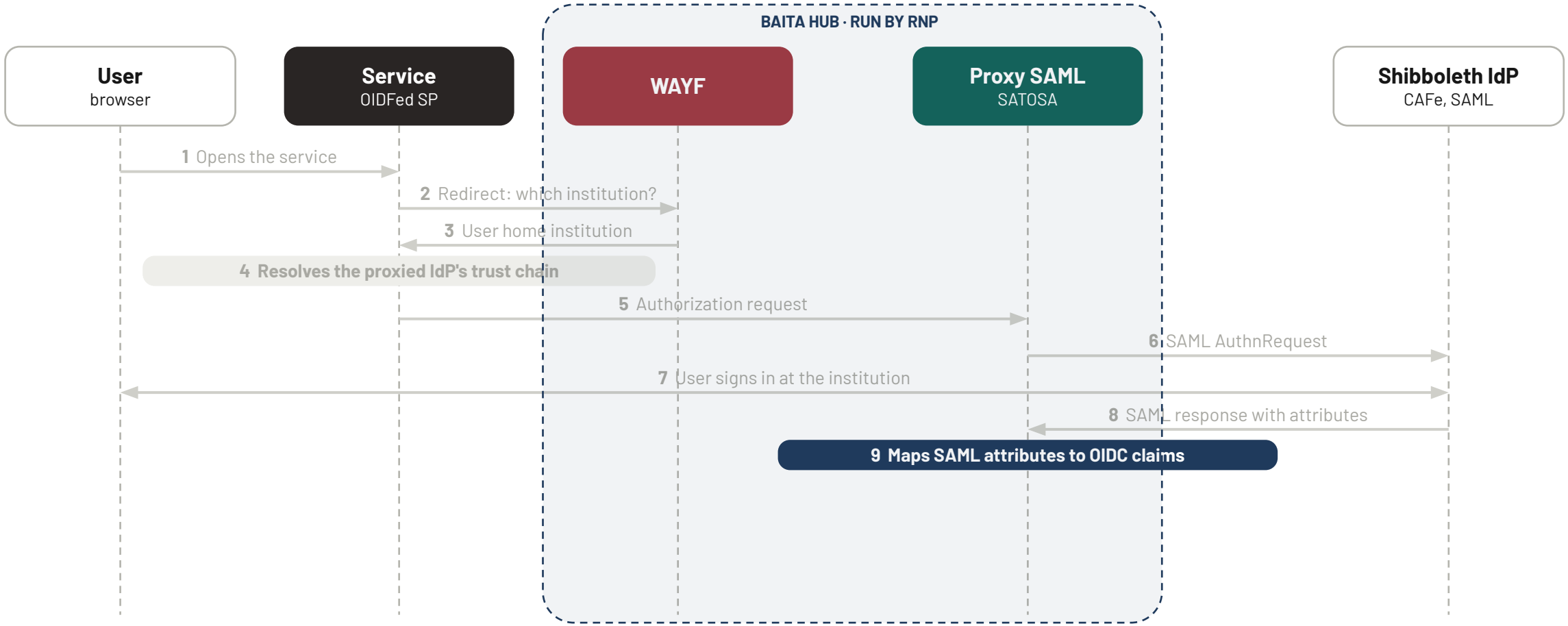
Login flow: CAFe SAML identity provider



Authentication. The proxy acts as a regular CAFe SP: the Shibboleth IdP changes nothing.

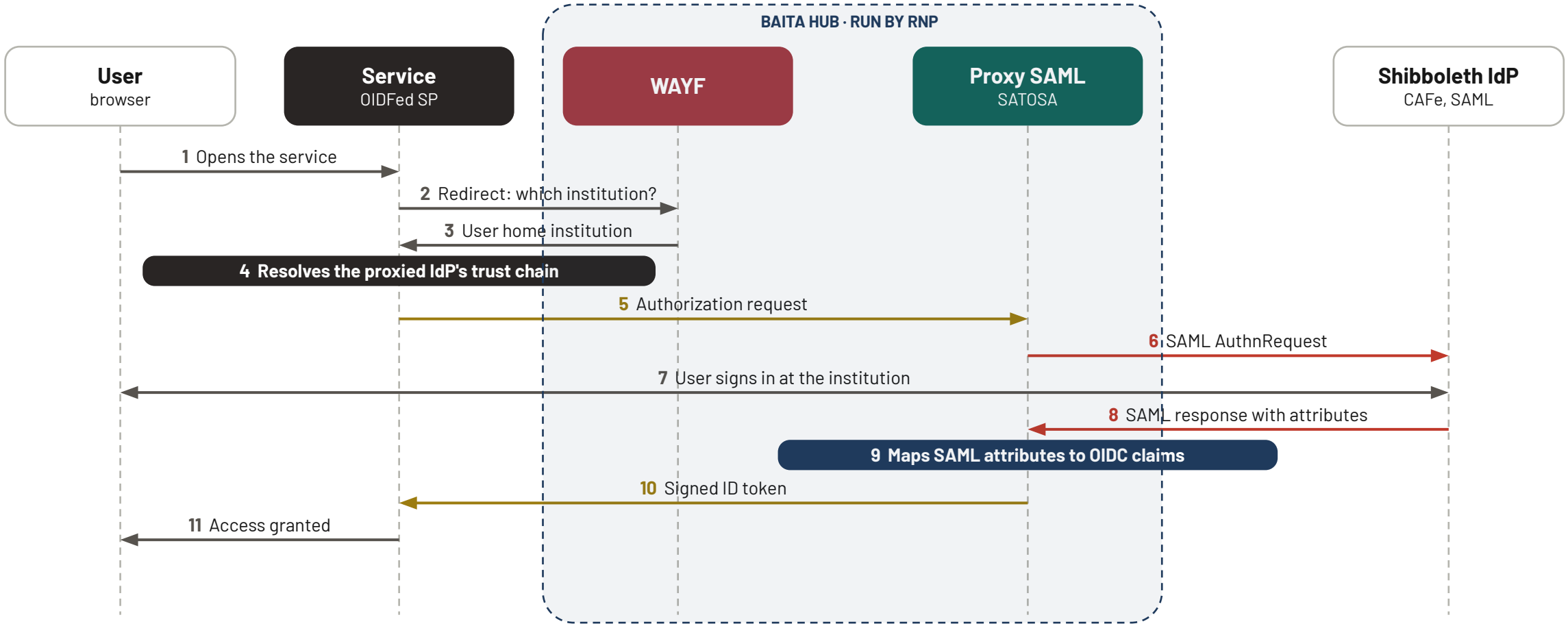
OpenID Federation · OIDC · SAML · Browser

Login flow: CAFe SAML identity provider



What the bus adds. The proxy maps eduPerson and brEduPerson attributes to OIDC claims.

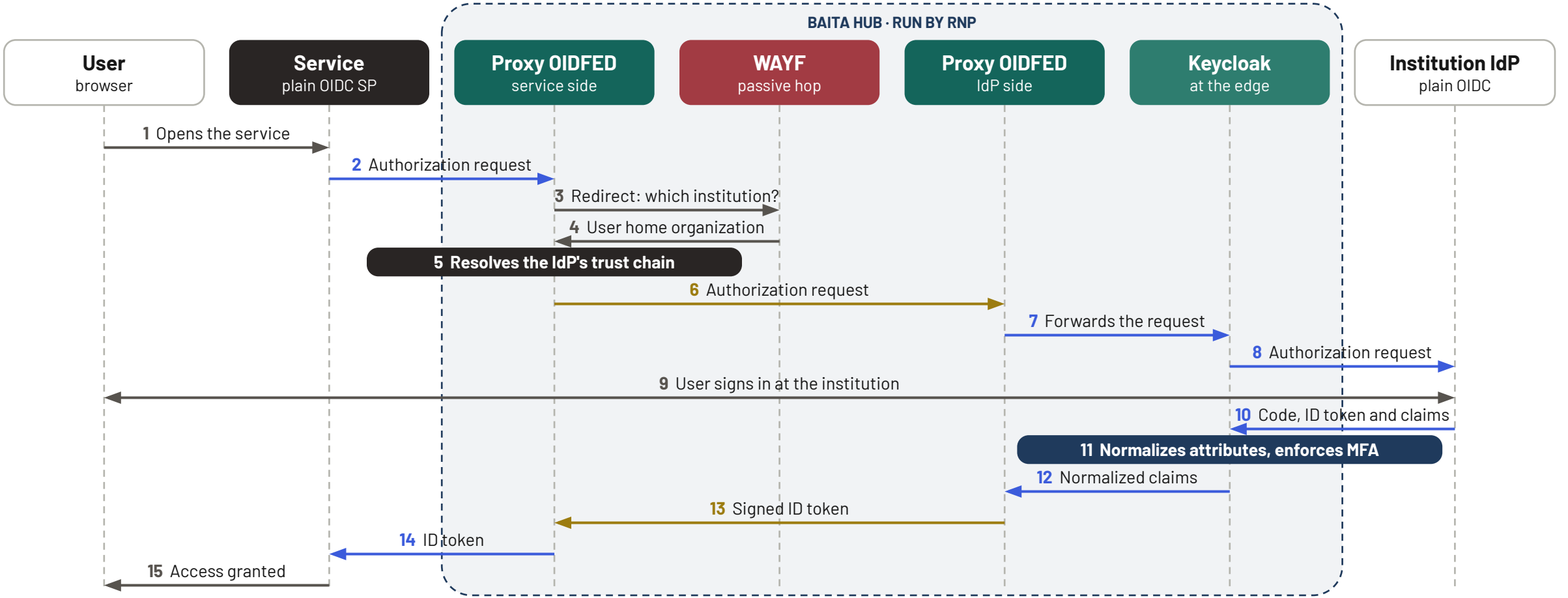
Login flow: CAFe SAML identity provider



Response. The service gets the same signed ID token as in the OIDC flow.

APPENDIX

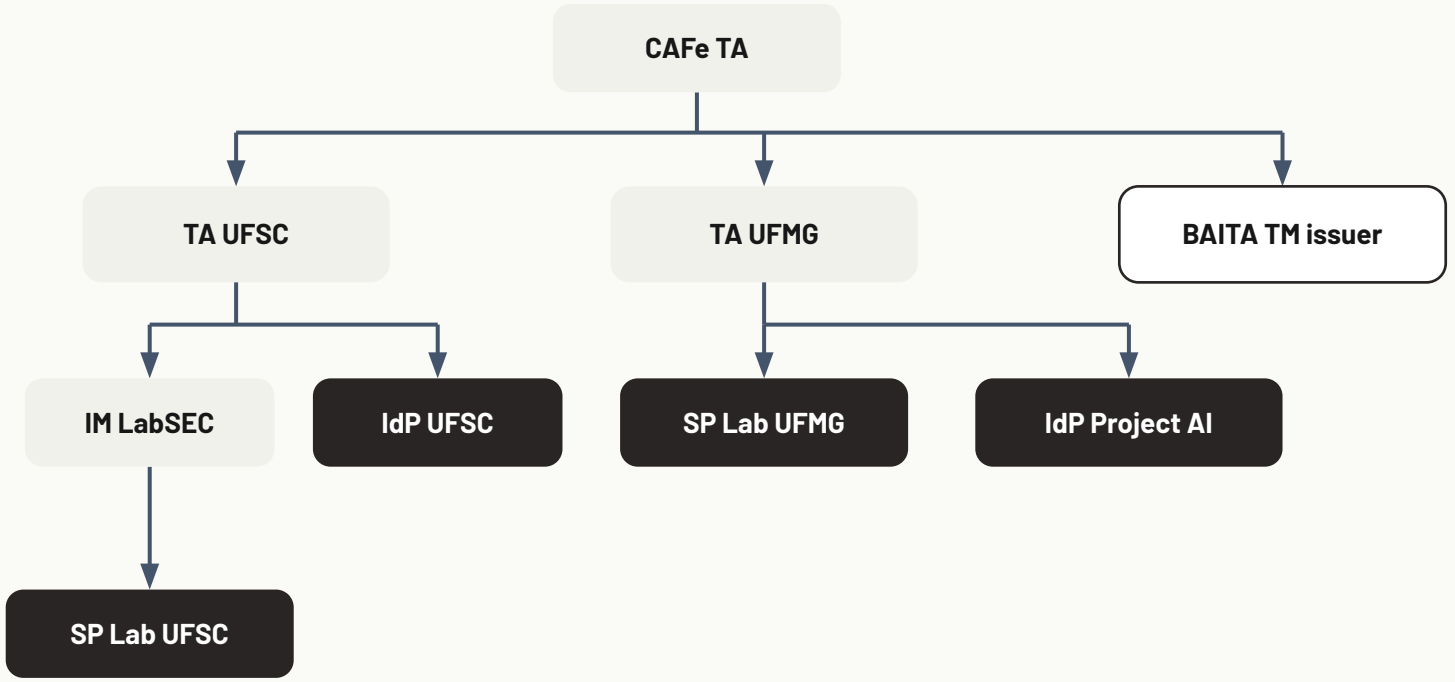
Login flow: OIDC service and IdP



OIDC at both ends. In between, the bus runs OpenID Federation.

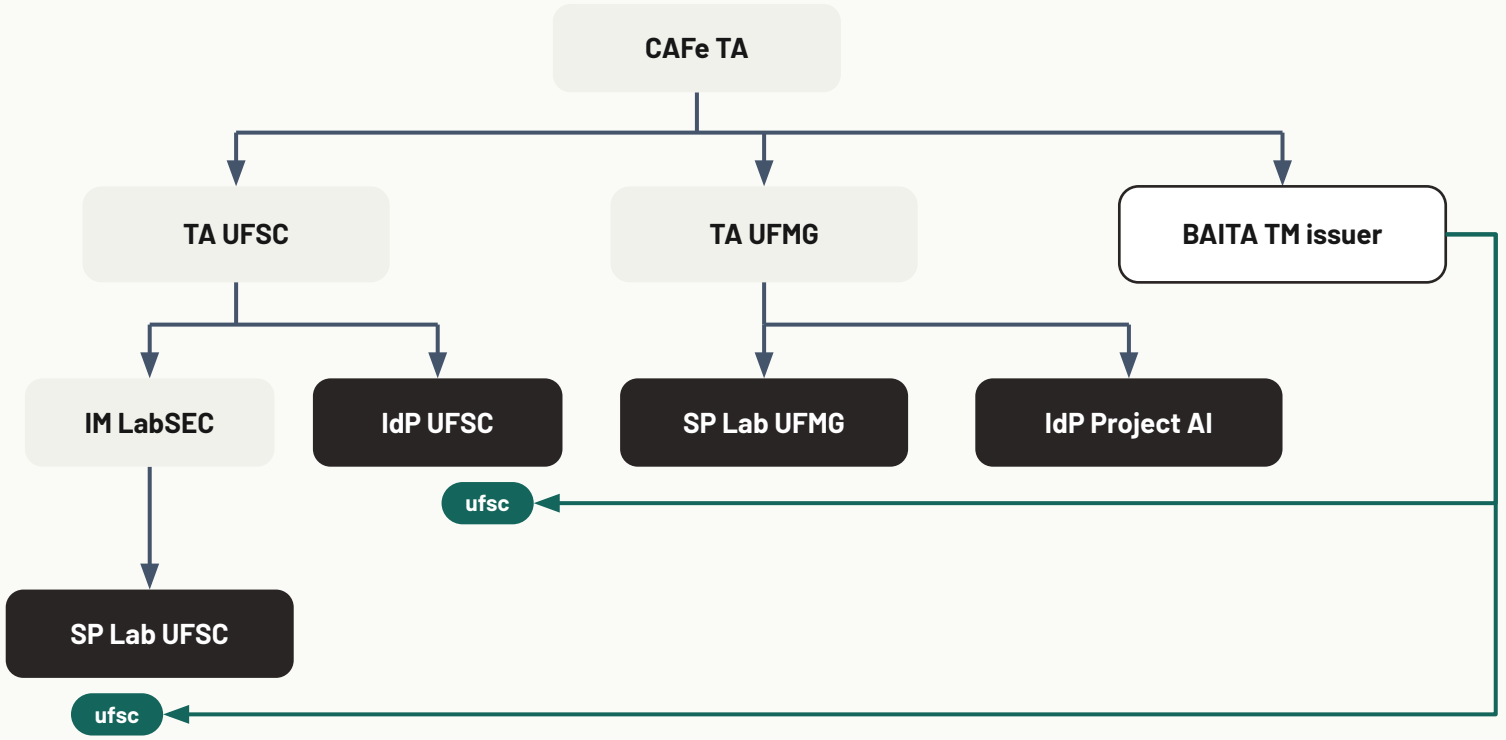
Subfederations: trust scopes as trust marks

Proposal



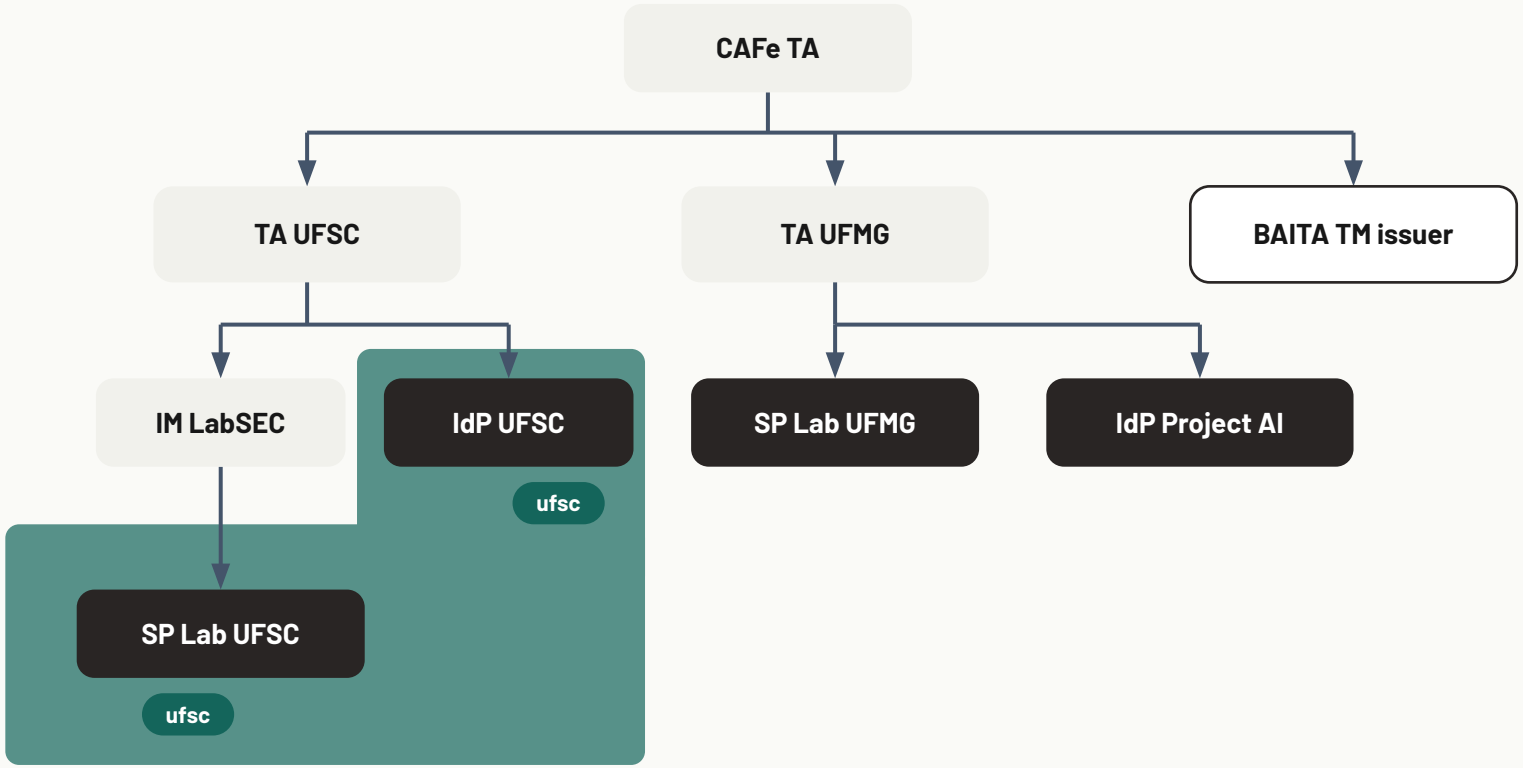
Subfederations: trust scopes as trust marks

Proposal



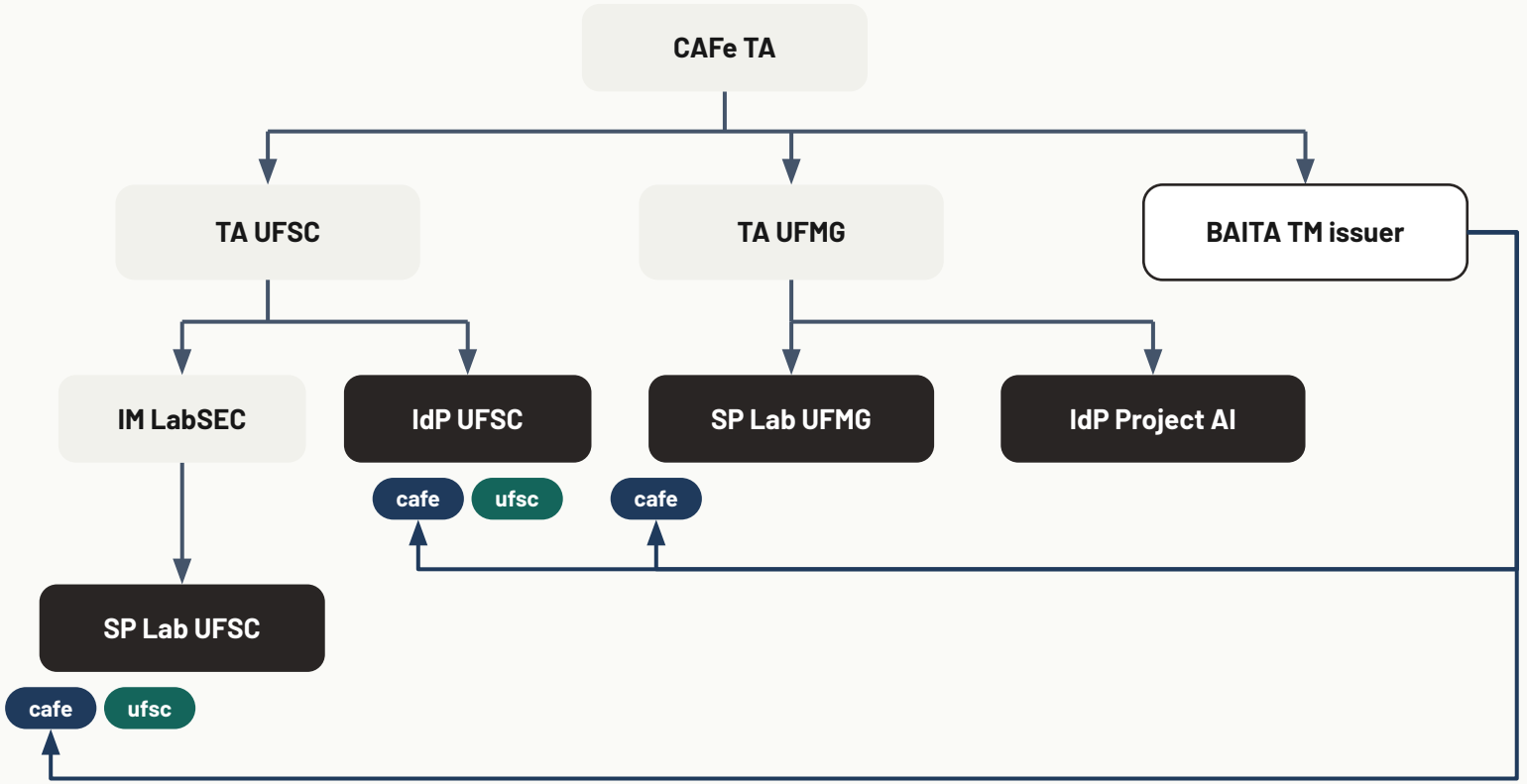
Subfederations: trust scopes as trust marks

Proposal



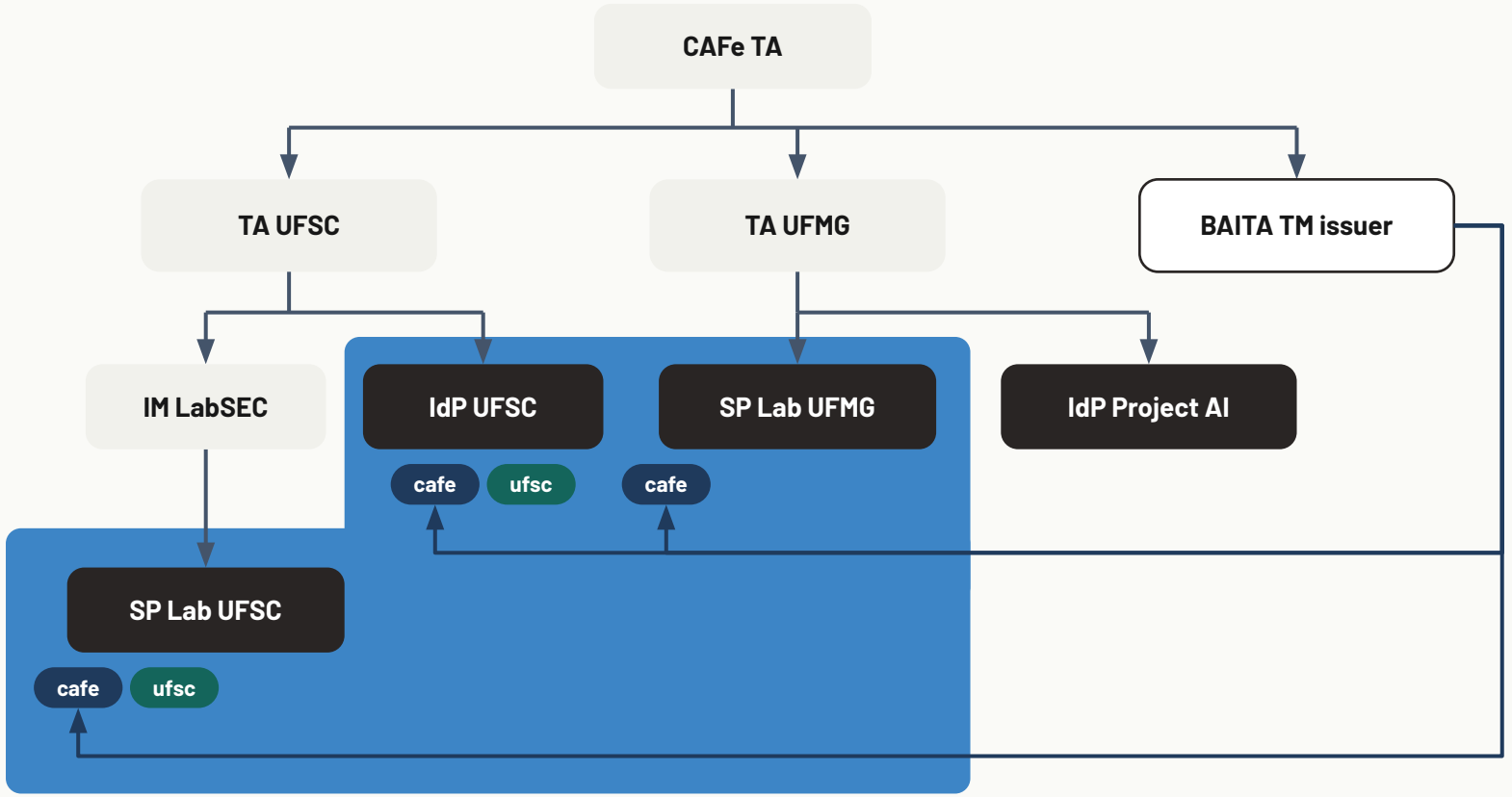
Subfederations: trust scopes as trust marks

Proposal



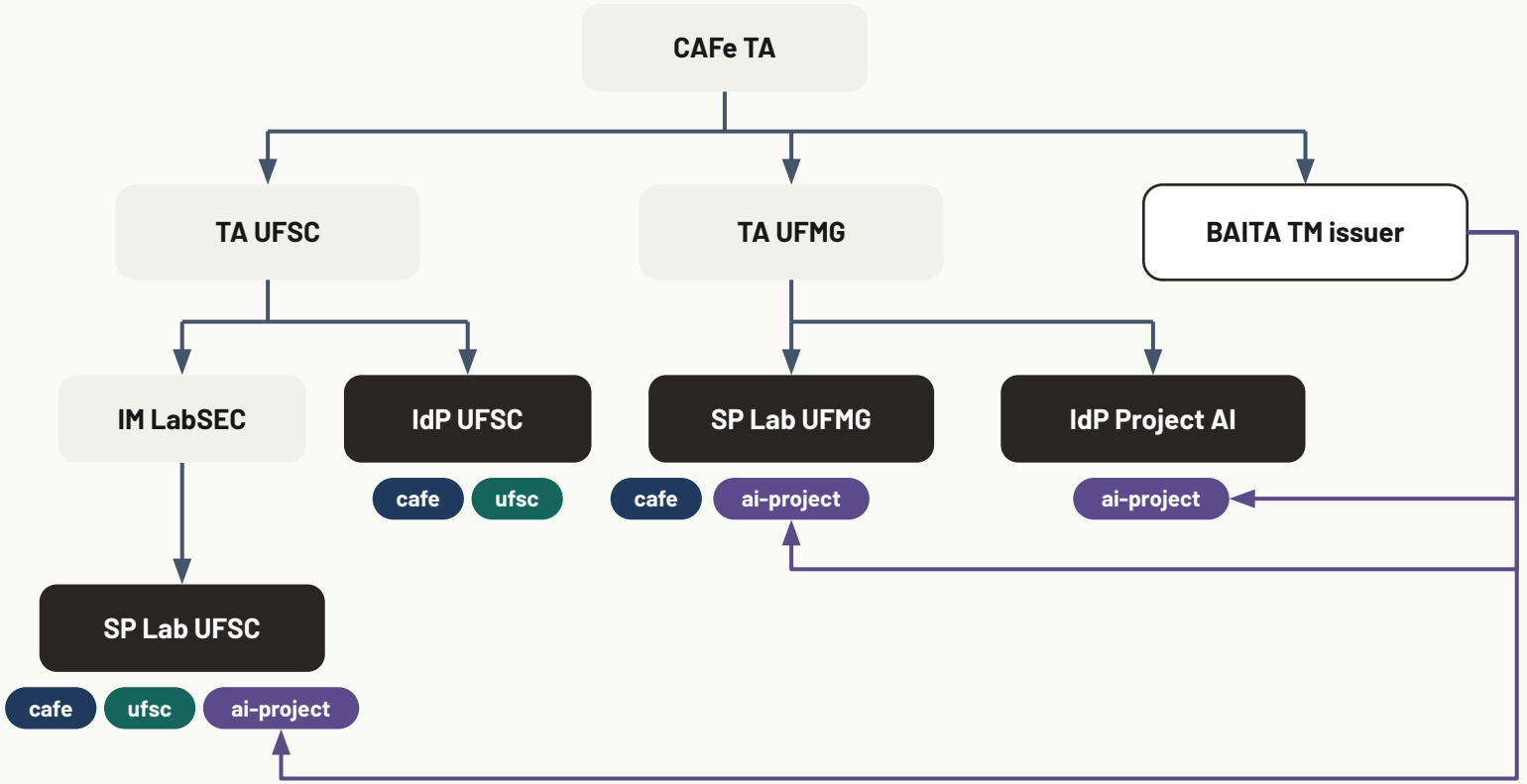
Subfederations: trust scopes as trust marks

Proposal



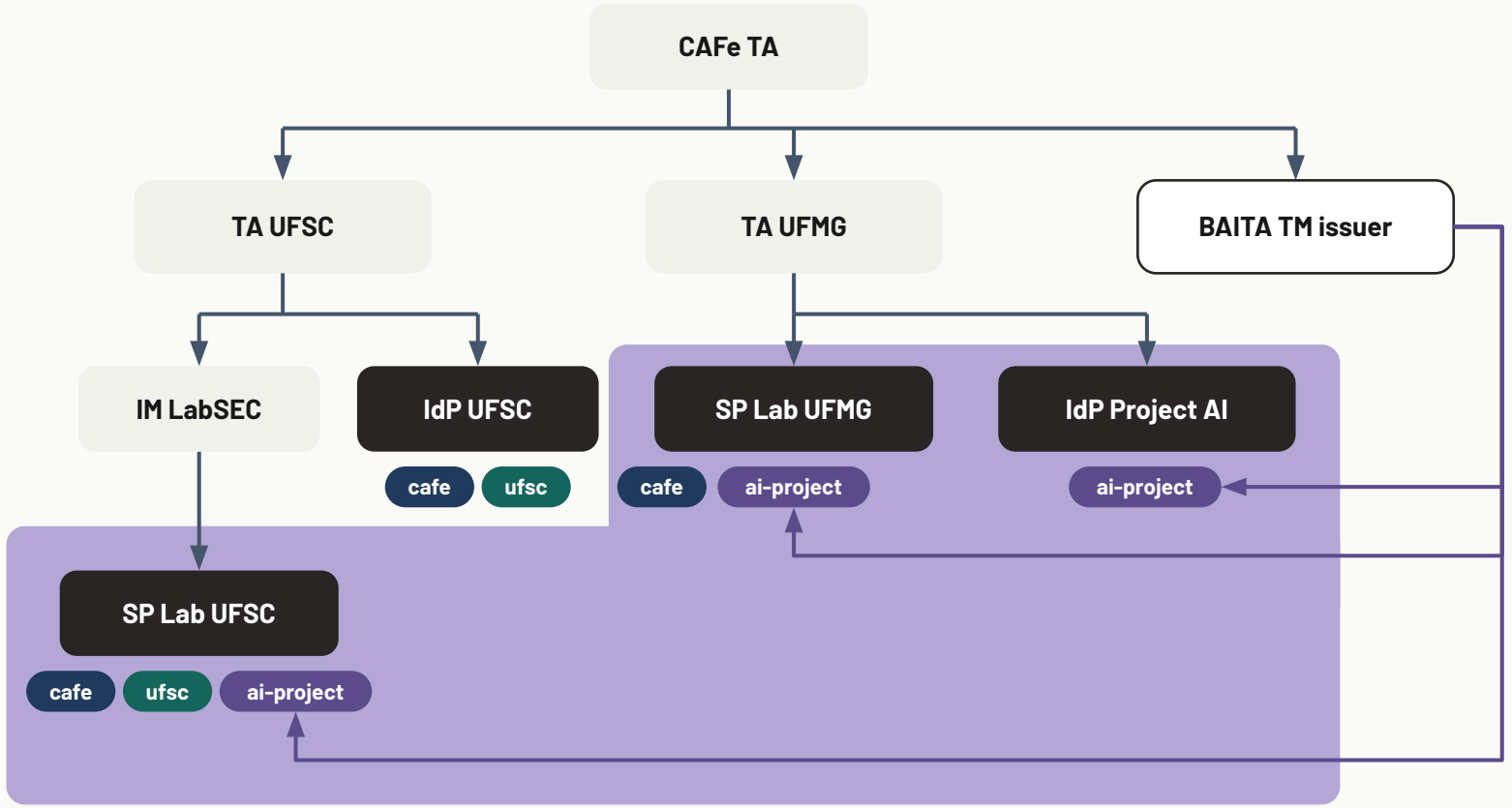
Subfederations: trust scopes as trust marks

Proposal



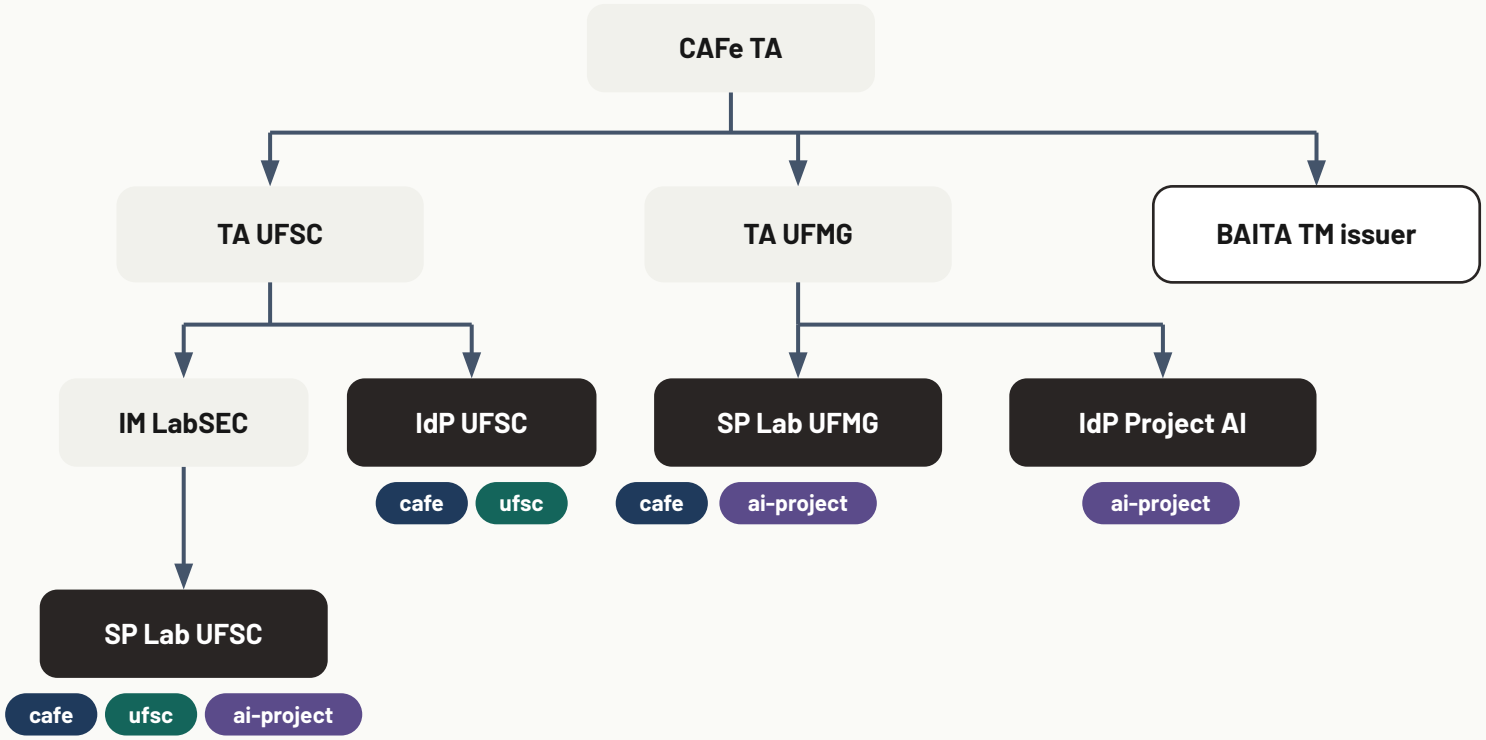
Subfederations: trust scopes as trust marks

Proposal



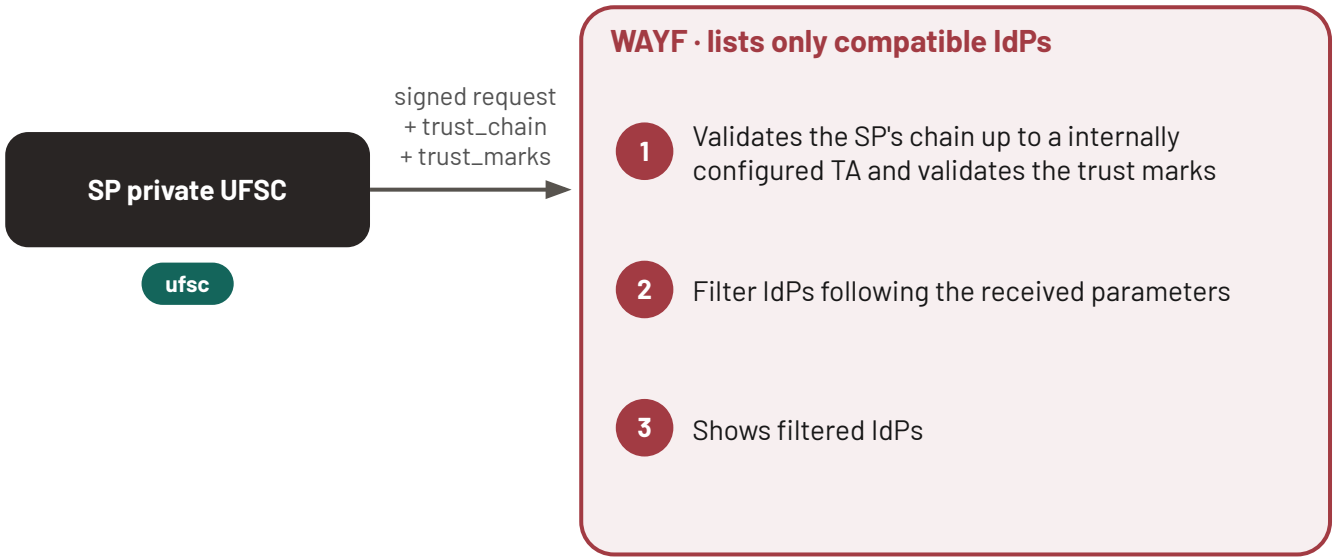
Subfederations: trust scopes as trust marks

Proposal



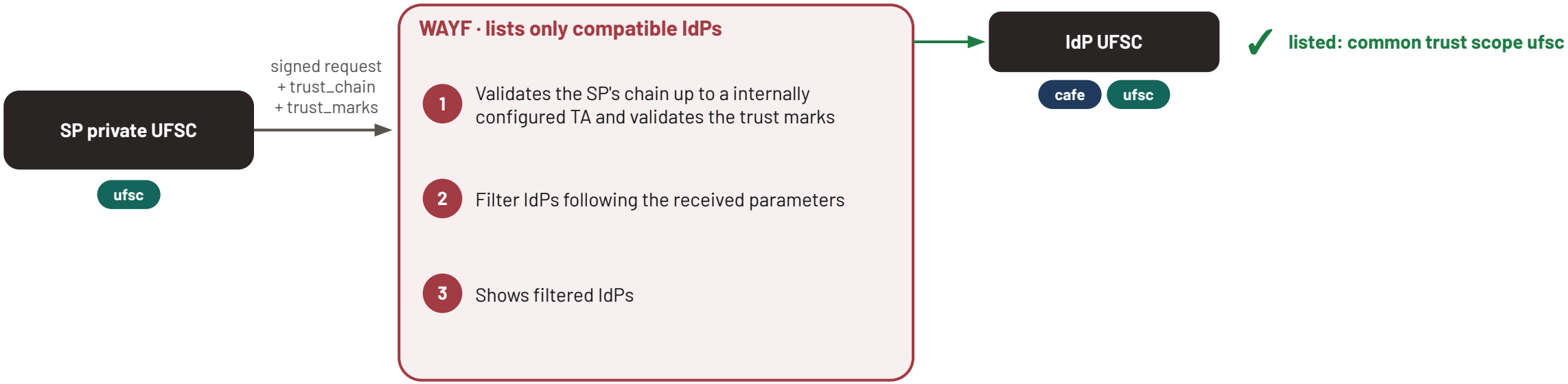
Subfederations at the WAYF

Proposal



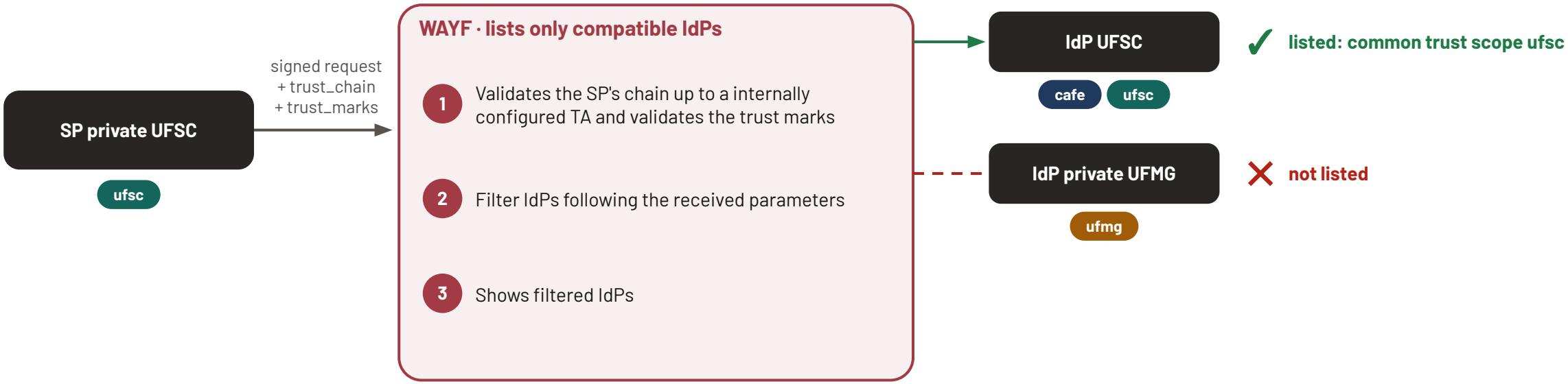
Subfederations at the WAYF

Proposal



Subfederations at the WAYF

Proposal



Subfederations at the WAYF

Proposal

