AUSTRALIAN ACCESS FEDERATION

# GUARDIANS Solution Architecture Design Document

Version 1.0

Last Updated: 04 September 2025

**Audience: GUARDIANS Partner Institutions**
**Author(s): Anurag Katariya**

AUSTRALIAN ACCESS FEDERATION

## Contents

AUSTRALIAN ACCESS FEDERATION

# 1. Introduction

## Purpose

This Solution Architecture document outlines the technical design for the authentication and authorisation infrastructure (AAI) for the GUARDIANS (Genomics Unified Access for Research Data Infrastructure and National Services) program. It outlines the architecture of the federated identity and access solution built on CILogon, tailored to the genomics research ecosystem in Australia.

## Background

GUARDIANS brings together a national collaboration of genomics research institutions seeking to unify access to platforms and datasets through consistent, secure, and policy-aligned authentication and authorisation practices.

The architecture described is an output of the Design phase of the program, informed by partner input during Discovery and Definition phases. This document provides information on the implementation of the CILogon AAI platform for GUARDIANS, including configuration, integration options, and extensibility features.

The architecture is developed by AAF in collaboration with these GUARDIANS partners:

- BioCommons
- Children's Cancer Institute (CCI)
- University of Melbourne Centre for Cancer Research (UMCCR)
- Garvan Institute of Medical Research
- QIMR Berghofer Medical Research Institute (QIMRB)
- National Computational Infrastructure (NCI)

## Scope

The document focuses on how the AAF will deliver the identity and access systems needed to allow researchers to log in securely, using trusted credentials. It specifically covers:

- the proposed federated identity and access management technology (CILogon)
- partner services and their planned integration
- AAI components and protocols
- future considerations.

# 2. High-Level Architecture Overview

The GUARDIANS identity and access management solution is built on CILogon, a federated identity broker and AAI platform. CILogon integrates with external identity providers (IdPs) providing users a unified login experience across multiple genomics research services managed by different organisations.


Figure 1 shows user identity sources, CILogon core components, authentication flow, and research services. Future attribute and authorisation flows are shown with dotted lines.

The solution implements CILogon as the AAI platform, acting as a trust broker between IdPs and research services. It integrates with federated identity providers (via AAF and eduGAIN) and social identity providers (Google and Microsoft) and research applications requiring user authentication. The platform supports the future addition of external identity validation services.

The platform is hosted in AWS Sydney, managed and supported by AAF, with level three support provided by the CILogon developer team.

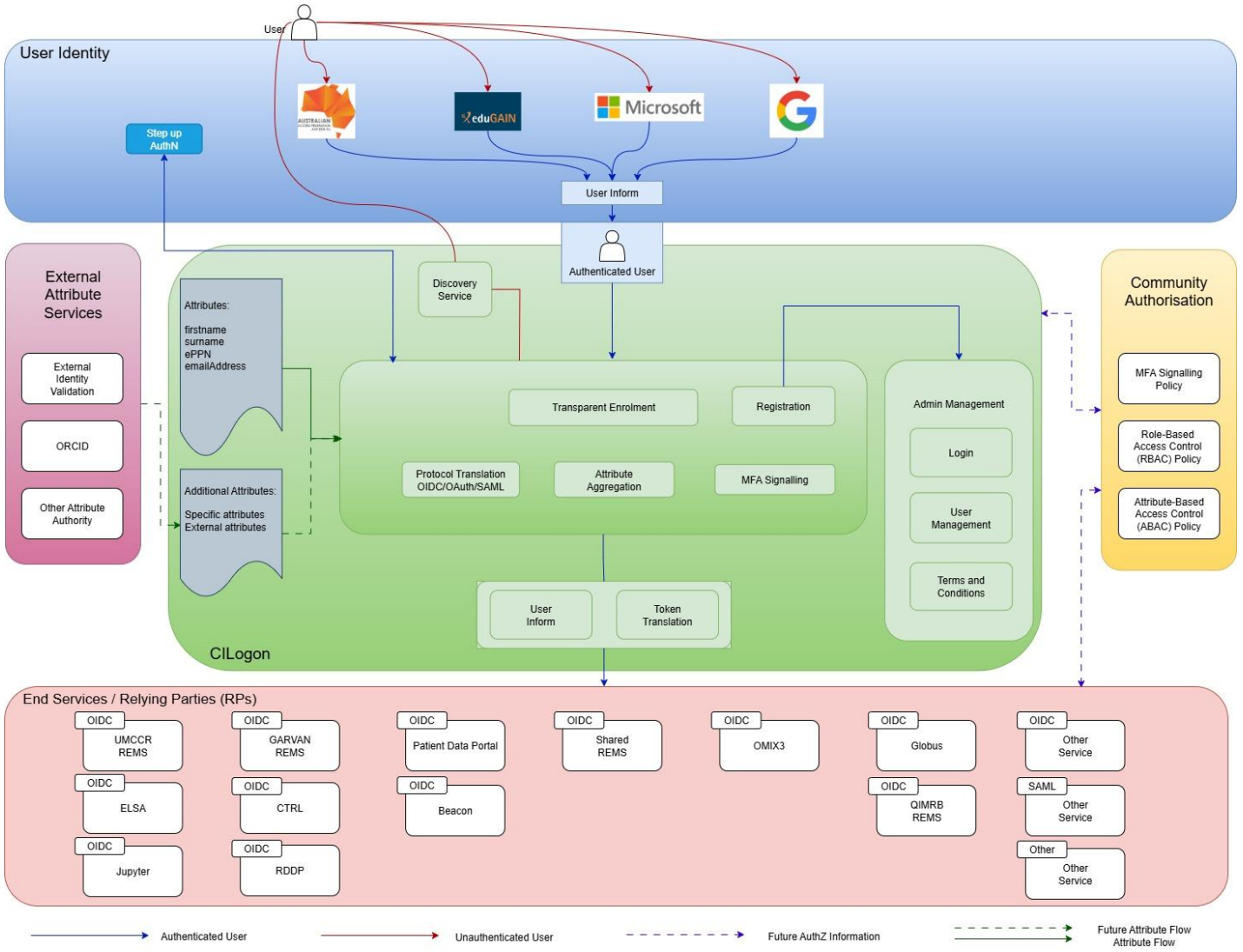


*Figure 1: End-to-End System Architecture Overview*

# 3. Components of the Architecture

This section outlines the key technical components that make up the AAI for GUARDIANS.

## 3.1 Identity Provider Federation

Supported IdPs:

- eduGAIN Federation (for global research identities)
- Social Identity Providers: Google, Microsoft

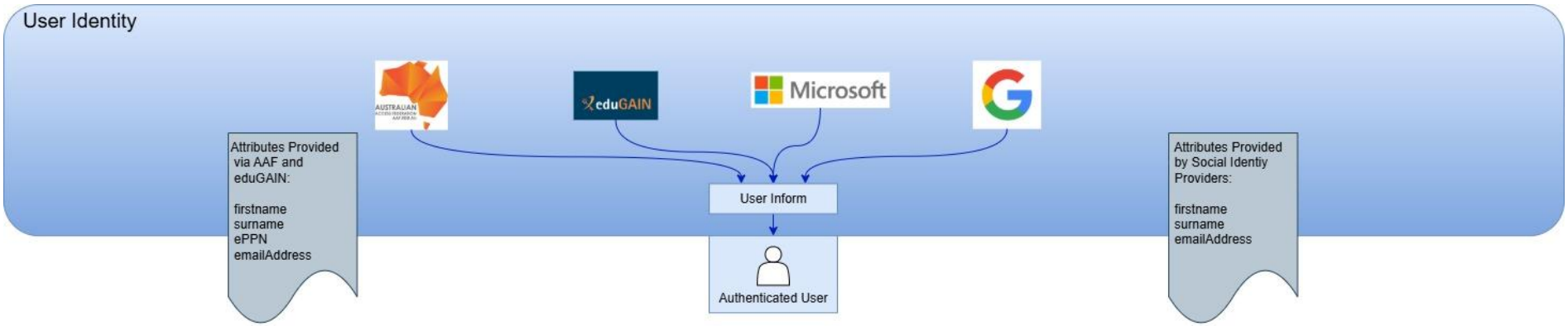


*Figure 2: Identity Providers*

Figure 2 shows attribute release, for IdPs via CILogon discovery service.

Key Features:

- MFA signalling support from IdPs where available
- eduPersonPrincipalName (ePPN), email, name.


Limitations of Social Identity Providers:

- **no MFA signalling**: Social IdPs (e.g. Google) do not support standardised MFA signalling. There is no way to determine if MFA was used during authentication from outside of the social IdP's own ecosystem.
- **no ePPN Provided**: Social IdPs do not support and therefore cannot release ePPN, the primary identifier used for GURADIANS services. CILogon will mint synthetic ePPN values for users authenticating via social IdPs.

AUSTRALIAN ACCESS FEDERATION

## 3.2 Discovery Service Configuration

CILogon's Discovery Service is configurable to present all available IdPs or a subset of IdPs for a specific service.

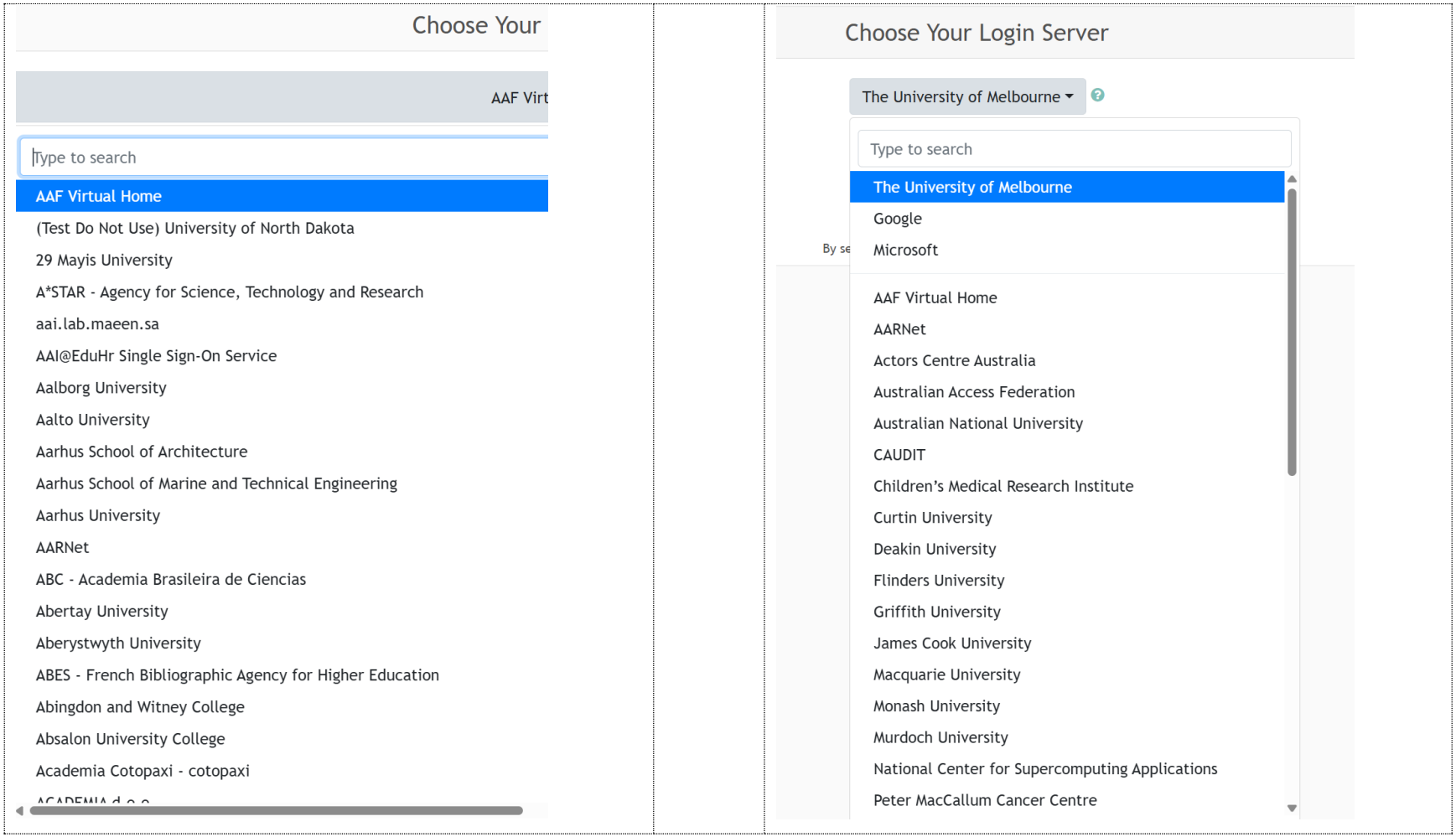


*Figure3: Discovery Service Customisation*

Figure 3 shows the default (all IdPs) discovery service (left) vs a customised set for a specific service (right).


## 3.3 CILogon Service Layer

The following CILogon features used as part of the GUARDIANS AAI solution are included in the service layer:

- user management
- protocol translation (OIDC ↔ SAML)
- transparent enrolment
- attribute aggregation
- token translation
- MFA signalling and error handling.

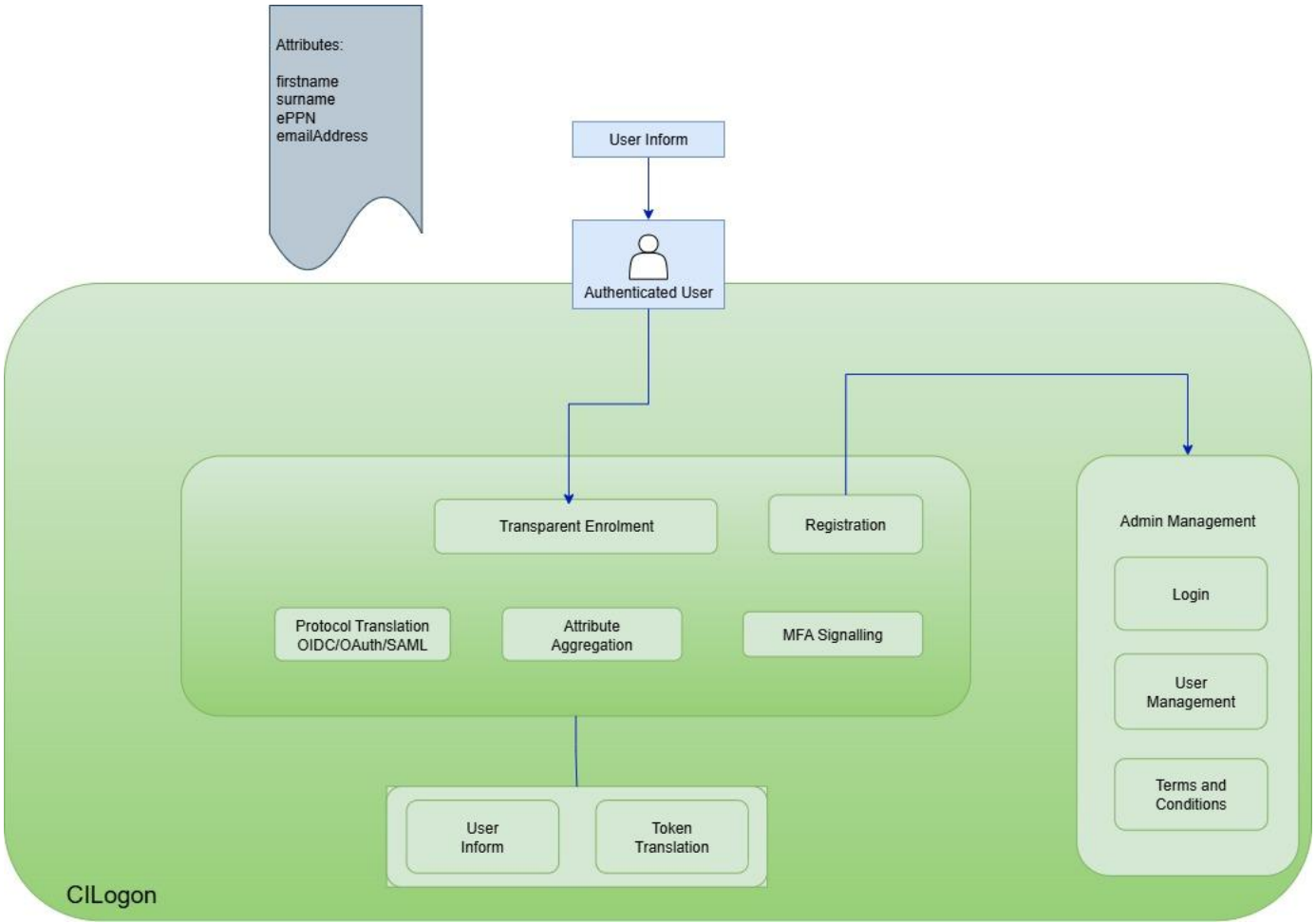


*Figure 4: CILogon Internal Components*

Figure 4 shows the CILogon service components within the GUARDIANS architecture, showing how authenticated users progress through transparent enrolment. It also shows the user attributes passed during the authentication process.

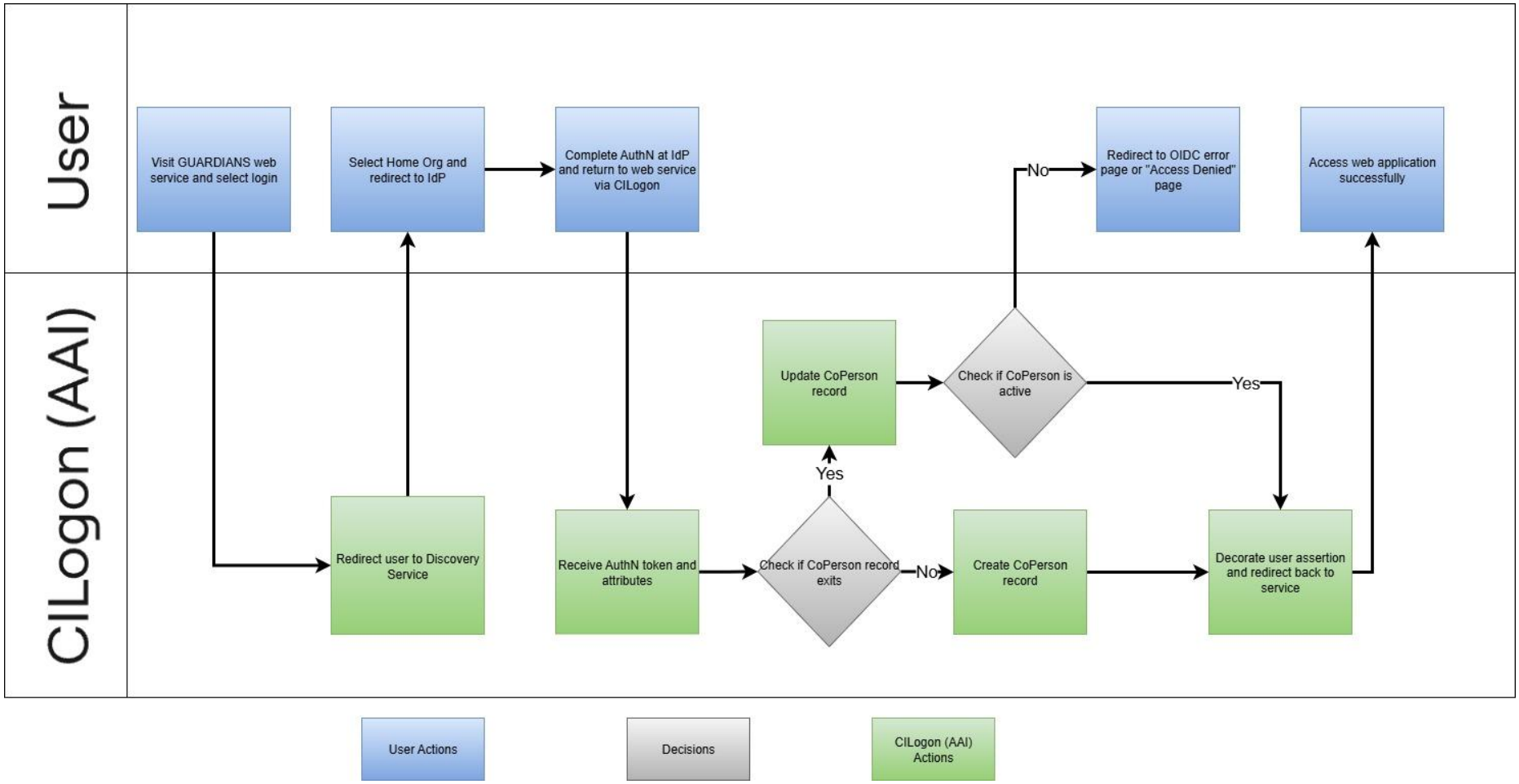


*Figure 5: Transparent Enrolment Flow*

Figure 5 illustrates the Transparent Enrolment user flow that automatically creates a user's CoPerson record in the AAI system when a user authenticates.

## 3.4 Use of ePPN

ePPN is a person identifier in URI format that is used as the primary unique user identifier across the GUARDIANS ecosystem. It will be represented in the form "user@scope" where 'user' is a user identifier for the person and the "scope" portion will be the administrative domain of the identity provider where the identifier was created and assigned. Each value of 'scope' defines a namespace within which the assigned ‘user’ identifier will be unique. It is:

- globally unique and scoped per organisation (e.g. userIdentifier@organisation.edu.au)
- issued by the relevant federation (AAF/eduGAIN) IdPs
- suitable for linking user sessions and accounts across multiple services.

The choice of ePPN is based on its inclusion in the REFEDS Research and Scholarship Entity Category attribute policy.[1] REFEDS R&S is a widely adopted attribute bundle in research federations.

As a persistent user identifier, GUARDIANS services can use ePPN to track access, audit, and enforce consistent identity handling.

## 3.5 MFA Signalling

Multi-Factor Authentication (MFA)[2] signalling enables services to receive information about the level of authentication assurance a user has completed during authentication at their home institution. Services can use the presence of the MFA signal to determine access. Application developers must separately implement support for MFA signalling and determine how the application will respond to signals.

In future, the MFA signal may also include the type of MFA undertaken (OTP, token, phishing resistant, etc) and when it occurred.

CILogon can pass assurance values or MFA context indicators as part of the identity token.

Possible Approaches:

- enforce MFA at IdP level (via REFEDS MFA profile)
- signal MFA via acr_values or custom claims in the token.

[1] REFEDS Research and Scholarship Entity Category https://refeds.org/category/research-and-scholarship

[2] https://refeds.org/profile/mfa, see also https://incommon.org/news/the-national-institutes-of-health-multi-factor-authentication-requirement/

Example Claims in ID Token:


```
{
  "acr": "https://refeds.org/profile/mfa",
  "auth_time": 1692700000,
  "amr": ["pwd", "otp"]
}
```


Future Work:

- implement AAI specific MFA enforcement rules
- use assurance indicators to trigger different access policies in downstream services.

AUSTRALIAN ACCESS FEDERATION

### 3.6 Community Authorisation Layer

While current implementation focuses on authentication, the architecture is extensible to support:

- MFA signalling policies
- role-based access control (RBAC)
- attribute-based access control (ABAC)

Figure 6 shows how authorisation policies interact before access is granted to an application.

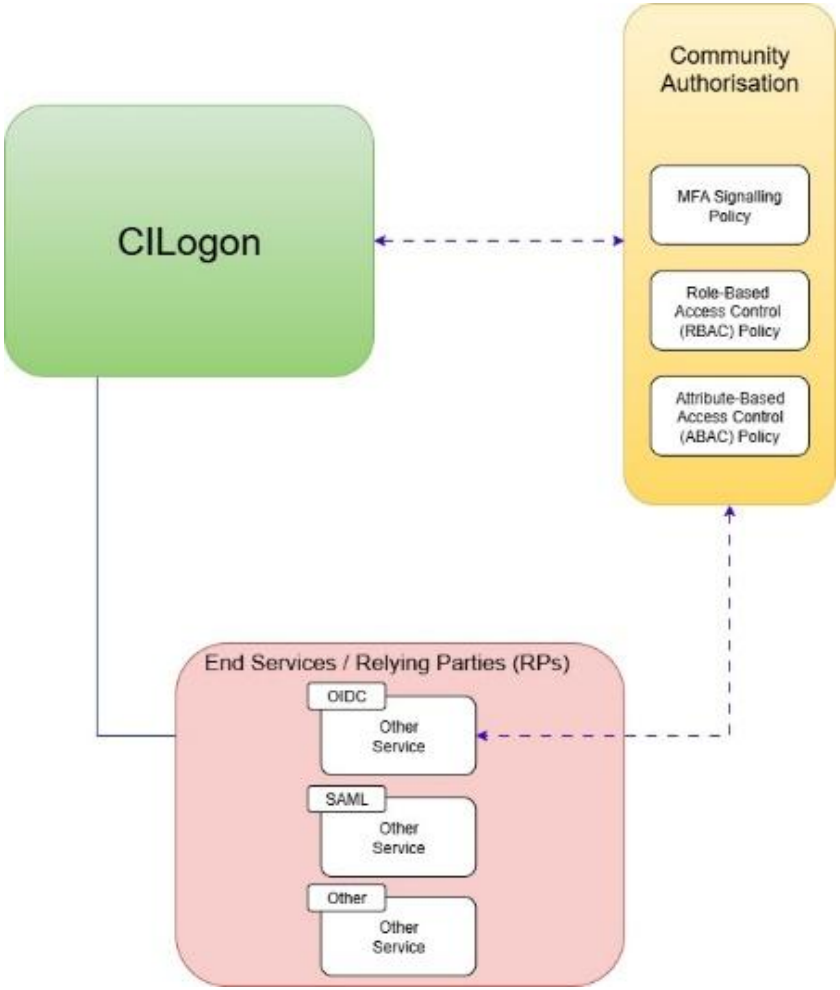


*Figure 6: Future Authorisation Layer Integration*

# 4. User Journey

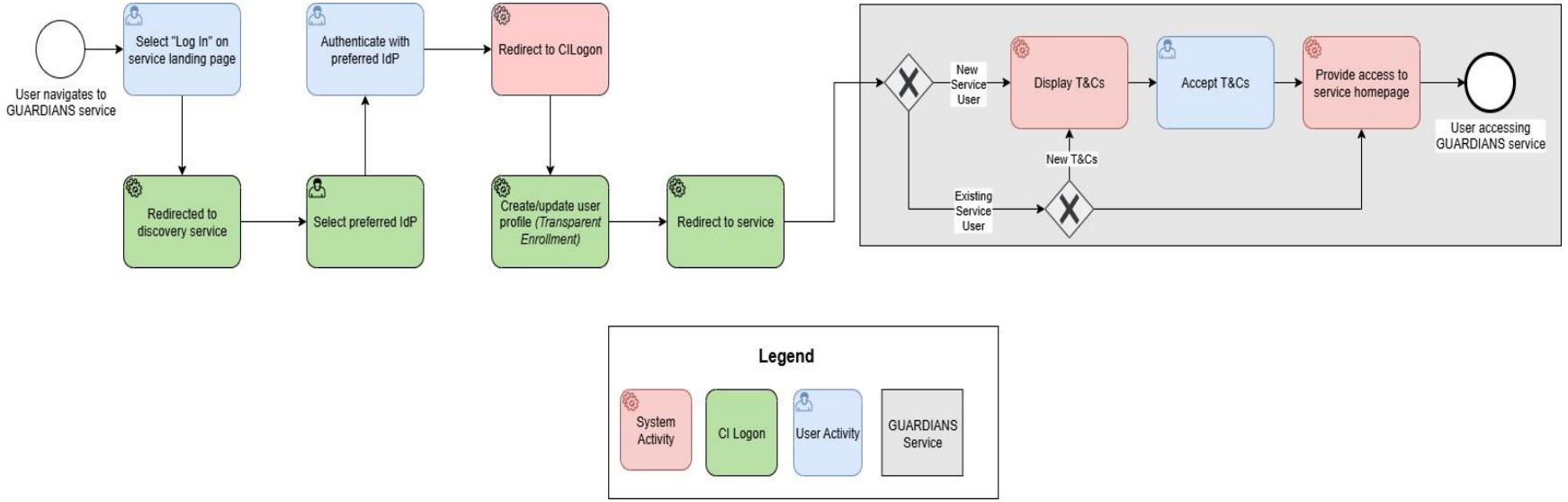


*Figure 7: User Journey*

Figure 7 illustrates the end-user experience during authentication, helping service providers and developers understand key integration points.


# 5. Integrated Research Applications

This section tracks test and production URLs of integrated services. Many URLs are still to be determined.

| Service | Partner | Protocol | Test URL | Prod URL |
|---|---|---|---|---|
| REMS | UMCCR | OIDC | TBC | TBC |
| Elsa | UMCCR | OIDC | TBC | TBC |
| REDCap | Garvan | OIDC | TBC | TBC |
| CTRL | Garvan | OIDC | TBC | TBC |
| REMS | Garvan | OIDC | TBC | TBC |
| RDDP | Garvan | OIDC | TBC | TBC |
| Beacon | CCI | OIDC | TBC | TBC |
| Patient Data Portal | CCI | OIDC | https://insightsdev.zerochildhoodcancer.cloud | TBC |
| Gen3 (OMIX3) | UoM | OIDC | TBC | TBC |
| Globus | QIMRB | OIDC | TBC | TBC |
| REMS | QIMRB | OIDC | TBC | TBC |
| Shared REMS | CCI/BioCommons | OIDC | https://rems.test.biocommons.org.au | TBC |

# 6. Hosting and Support Model

Hosting Location: AWS Sydney

Managed by: AAF

Support Provided By:

- AAF (onboarding, identity integration, metadata, metrics, platform customisation)
- CILogon Dev Team (platform customisation, L3 support).

Environment Details

| Component | Test URL | Production URL |
|---|---|---|
| CILogon | https://registry-test.biocommons.org.au/ | https://registry.biocommons.org.au/ |


# 7. Security & Compliance Considerations

The following security settings have been applied to the GUARDIANS AAI environment:

- All communications secured via HTTPS (TLS 1.2+)
- No credentials stored; identity assertions passed securely
- MFA signalling when supported by IdP
- Attribute release governed by GUARDIANS policies

# 8. Access Options for Non-AAF Researchers

The GUARDIANS platform is optimised for users whose home institutions are members of the AAF and eduGAIN. GUARDIANS requires researchers from outside the AAF and eduGAIN federations to access services as well. These researchers and collaborators belong to hospitals, smaller research institutes, government agencies, commercial organisations and independent researchers.

The **Access Options for Non-AAF Researchers** paper discusses the choices available to collaborations to support participation by researchers from non AAF or eduGAIN institutions.

# 9. Future Considerations

This document outlines the design based on the requirements that emerged through the discovery process. As the solution evolves, further requirements and detail will become available. Future iterations of this document will add further detail such as:

- adding REMS authorisation workflows
- defining and enforcing ABAC policies per service
- enabling service specific IdP discovery filtering
- configuring attribute release for advanced claims (e.g., eduPersonEntitlement and groupMembership/isMemberOf)
- documenting service registration and approval workflow

# 10. Appendices

## Appendix A: Glossary

- **AAI** – Authentication and Authorisation Infrastructure
- **IdP** – Identity Provider
- **RP** – Relying Party (Service)
- **OIDC** – OpenID Connect
- **SAML** – Security Assertion Markup Language
- **ePPN** – eduPersonPrincipalName
- **RBAC** – Role-Based Access Control
- **ABAC** – Attribute-Based Access Control
- **MFA** – Multi-Factor Authentication
- **REFEDS** – The Research and Education FEDerations group

## Appendix B: References

- AARC Blueprint Architecture: https://aarc-project.eu/architecture/
- CILogon: https://www.cilogon.org/
- eduGAIN: https://edugain.org/
- AAF: https://aaf.edu.au
- REFEDS: https://refeds.org/