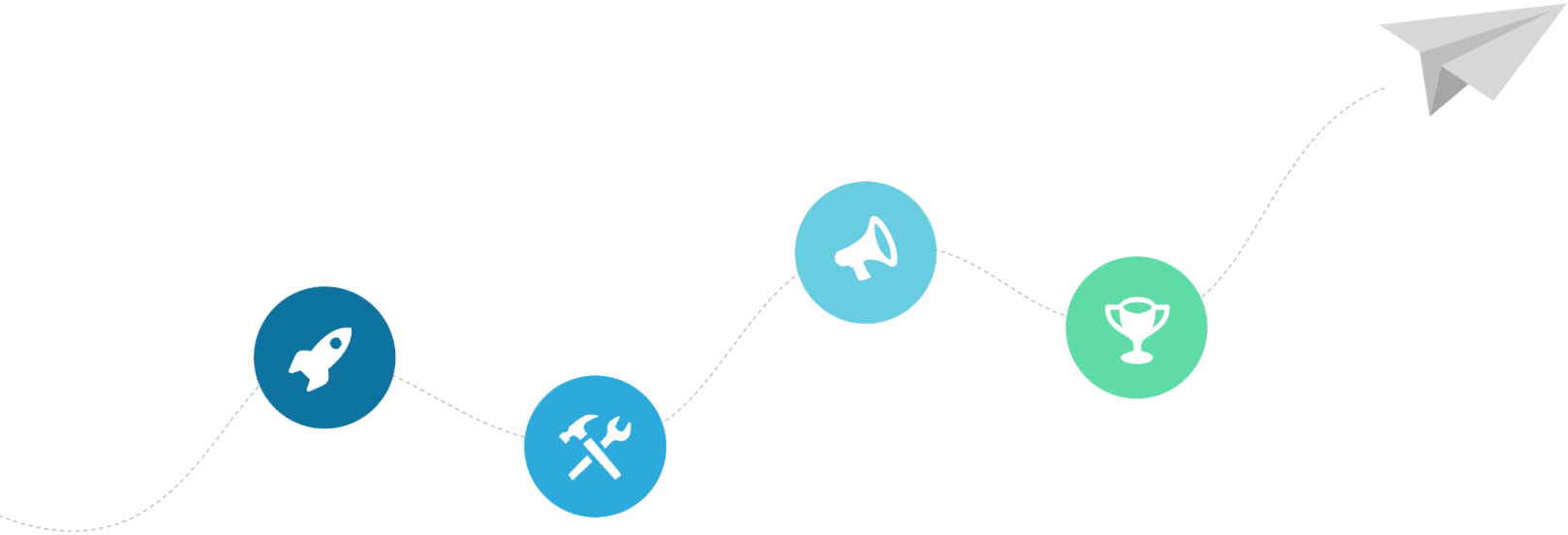
HUMAN GENOMES PLATFORM PROJECT

Federated Identity and Access Management

CANDIDATE SOLUTIONS EVALUATION REPORT

Dec 2023



Authors

in alphabetical order by surname

Carnuccio, Patrick - AAF

Cowley, Mark - ZERO CCIA

Davies, Kylie - AAF

Downton, Matthew - NCI

Dumevska, Biljana - ZERO CCIA

Green, Cherry - AAF

Hobbs, Matthew - Garvan

Holliday, Jess - BioCommons

Kummerfeld, Sarah - Garvan

Lin, Angela - ZERO CCIA

Monro, David - NCI

Patterson, Andrew - UMCCR

Pope, Bernard - BioCommons

Ravishankar, Shyamsunder - Garvan

Robinson, Andrew - NCI

Scullen, John - AAF

Shadbolt, Marion - BioCommons

Syed, Mustafa - ZERO CCI

Wood, Scott - QIMRB

Wong-Erasmus, Marie - ZERO CCIA

Acknowledgement

The HGPP formed part of Australian BioCommons' Human Genome Informatics initiative and was funded by NCRIS via the Australian Research Data Commons (https://doi.org/10.47486/PL032) and Bioplatforms Australia. Contributions were also made by partner organisations: Australian Access Federation, Garvan Institute for Medical Research, National Computational Infrastructure, QIMR Berghofer Medical Research Institute, The University of Melbourne Centre for Cancer Research, the ZERO Childhood Cancer Program and Children's Cancer Institute.

Table of Contents

Glossary

AAF (Australian Access Federation)	A national identity federation that simplifies inter-organisational authentication and authorisation for research and education organisations.
Attributes	Identity attributes are the set data about a user. Attributes may include the type of user (staff, student) or personal metadata such as name, email address, phone, etc. Can be known as “claims” in international standards documentation, such as GA4GH.
Credentials	Combination of inputs that a user enters into an interface to be authorised into a system or service. A username and password, biometric data such as a fingerprint, and a one-time verification code are examples of credentials.
GA4GH	Global Alliance for Genomics & Health.
HGPP	Human Genomes Platform Project.
IAM	Identity and Access Management.
JWT (JSON Web Token)	Cryptographic token that enables web standard-based methods for asserting and verifying claims.
NCI	National Computational Infrastructure. A nationally-funded, high-performance data, storage, and research computing centre based in Canberra.
OAuth2 (Open Authorisation)	An open standard for allowing users to login to a service with credentials from an alternate resource.
OIDC (OpenID Connect)	Third generation standard of the OpenID Authentication Protocol (adheres to OAuth2).
openLDAP	Open-source implementation of Lightweight Directory Access Protocol.
Personal Information	Personal information includes a broad range of information, or an opinion, that could identify an individual as defined in the Privacy Act 1988. The Office of the Australian Information Commissioner provides examples at: https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information.
SAML (Security Assertion Markup Language)	Open-standard for exchanging authentication and authorisation data between an identity provider and a service provider.

1. Introduction

The Human Genomes Platform Project (hereafter 'HGPP' or 'the project') is a collaborative research project aiming to enhance secure and responsible sharing of human genomic data for research purposes. National and international connectivity is important to maximise the utility of these sensitive and valuable assets. The project partners represent many of the largest human genome sequencing and analysis organisations in Australia.

Federated Identity and Access Management (IAM) is a collection of standards, policies, and technologies that enable a platform to determine whether to permit access to a user. Federated IAM employs technologies, such as cryptography, and coordinated policies that outline common expectations between ecosystem participants. In a federated environment like the Australian and global genomics communities, IAM is the glue that enables loosely coupled systems to establish strong trust relationships for the purposes of data sharing.

IAM is a core component of the Human Genomes Platform Project (HGPP), designed to explore and implement systems that can be used to confirm that someone being granted access is in fact who they say they are and that their professional identity and role is considered. Federated IAM solutions were piloted across multiple repositories during the project.

Specifically, the federated IAM sub-project aimed to explore and pilot systems that organisations can deploy to leverage:

- Federated authentication infrastructure to streamline access to genomic data and analysis tools; and

- Attributes about the user and their home organisation identity to increase the level of confidence, to the point where service providers can make reliable authorisation decisions.

Beginning with a knowledge discovery phase[1], the federated IAM sub-project team established the formal requirements of the system through community consultation, identified several candidate solutions, and assessed those solutions against selection criteria. CILogon emerged as the leading candidate and was selected for the subsequent pilot implementation phase. In this report, we summarise our approach to testing the deployment of CILogon and its integration with the Beacon network explored in the virtual cohorts sub-project.

[1] Human Genomes Platform Project: Federated Identity and Access Management (IAM) Discovery Phase Report https://doi.org/10.5281/zenodo.6644009

2. Candidate solution analysis

Several potential solutions were identified during the discovery phase[2] and assessed in the context of the Australian human genome research community. Exploration of candidate solutions formed the basis of work packages in the project. The following products and solutions were identified for further exploration:

- GA4GH Passports/Visas[3]
- AARC Blueprint Architecture[4]
- Elixir AAI[5], European Open Science Cloud (EOSC) Life[6], and eduTeams[7]
- Commercial IAM solutions, such as Okta[8] and Auth0[9]
- CILogon[10]
- DIY build using open source components

GA4GH Passports/Visas

Project team members joined several GA4GH working groups and helped develop version 1.2 of the Passports/Visas specification[11]. This process provided an in-depth understanding of the strengths and limitations of this specification.

GA4GH Passports add a rich set of standardised cryptographically attributable claims to a user's federated identity, extending the basic capabilities of federated IAM. In particular, claims can be more complex standardised statements (e.g., "person X is able to access dataset Y under condition Z") and these claims are cryptographically signed by the source organisation that makes the claim (they retain the original authority of the source organisation).

In the spirit of walking before running, the project team deferred the implementation of GA4GH passports until more fundamental IAM capabilities were operational. Existing GA4GH passport ecosystems extend established IAM services (see NIH RAS[12] and Elixir). Until Australia has established an IAM infrastructure to support human genome research, we do not recommend pursuing these more advanced use cases.

---

[2] Human Genomes Platform Project: Federated Identity and Access Management (IAM) Discovery Phase Report
[3] https://www.ga4gh.org/product/ga4gh-passports/
[4] https://aarc-project.eu/architecture/
[5] https://elixir-europe.org/platforms/compute/aai
[6] https://www.eosc-life.eu/
[7] https://eduteams.org/
[8] https://www.okta.com/
[9] https://auth0.com/
[10] https://www.cilogon.org/
[11] https://github.com/ga4gh-duri/ga4gh-duri.github.io/blob/master/researcher_ids/ga4gh_passport_v1.md
[12] https://datascience.nih.gov/researcher-auth-service-initiative

In summary, whilst this work is particularly relevant to the international human genomics community, implementing this as part of a candidate solution has been deferred until more fundamental IAM requirements have been delivered.

AARC Blueprint Architecture and Policy Development Kit

The AARC Blueprint Architecture and Policy Development Kit[13] support the IAM technical architecture and policy requirements for distributed research communities. For Australia to align its genomic research with international efforts, it makes sense to base IAM designs on a common architecture. This improves the likelihood of international compatibility. We limited evaluation of IAM technologies to those that were well aligned with the AARC Blueprint Architecture.

Policy-related work was limited to analysis of the components and agreement that the Policy Development Kit components would be needed in a production deployment. The priority of this early phase was to demonstrate the viability of technical solutions. Policy development will be an essential prerequisite to a future production deployment.

In summary, this architecture has guided the solution but, in itself, is not something that could be implemented specifically as a candidate solution.

Elixir AAI, EOSC Life, and eduTEAMS

Elixir AAI is the solution that most closely resembles the user identity solution we would need in the project. During the course of the project, the Elixir AAI was moved into a broader Life Science Login[14] solution offering similar capability to a wider scope of European research activities.

The underlying Life Science Login is based on the eduTEAMS[15] core AAI platform that follows the AARC Blueprint Architecture. Ideally we would have piloted this platform in the project, however it is currently only available to research communities based in Europe.

In summary, whilst the platform appears to cover most of our requirements, it was not possible to examine this solution as a candidate due to licensing/availability restrictions.

[13] https://aarc-project.eu/
[14] https://lifescience-ri.eu/home.html
[15] https://eduteams.org

Commercial IAM Solutions

There are many commercial IAM solutions, such as Okta and Auth0, to address enterprise identity and access challenges. These products solve many identity management and integration challenges *within* an organisation but they cannot directly support multiple sources of identity and multiple external service providers, as is common in research federations. Other tools are needed to extend these enterprise-focused identity management tools to deliver the community management functionality needed in research communities. Enterprise solutions will play a part in the federation (to connect some organisations to research federations), but are not sufficient in their own right.

In summary, other tools are needed to extend the capabilities of enterprise identity management tools in the context of collaborative research communities. As such, there was no exploration of these tools directly as a potential candidate.

DIY Build Using Open Source Components

Both eduTEAMS and CILogon employ a variety of open source software components built for education and research collaborations. These as-a-service solutions incorporate open source components, such as COmanage, SATOSA, Perun, pyFF and OpenLDAP. We briefly considered building our own bespoke IAM solution in the project, however constraints on time and expertise meant it was better to leverage the many years of experience that existing providers could offer.

In summary, a lack of developer resources and time within the project ruled out considering implementing a DIY solution. Equally, this would be replication of work already included in other candidate solutions.

CILogon

CILogon is an integrated as-a-service identity and access management platform for research collaborations, combining federated identity and access management with collaborative organisation management. Like eduTEAMS, it follows the AARC Blueprint Architecture and both products share many open source components. The ability to create self-managed communities made it a strong candidate for our pilot.

Attractive features of CILogon include:

- CILogon has a proven track record in delivering federated authentication and authorisation services to collaborative research science communities.

- There are no other as-a-service options available to us that deliver the required functionality.
- The CILogon team demonstrated a willingness to accommodate new development requirements for capabilities, such as GA4GH passports, and have extended the product to support specific features required by the project.
- CILogon uses open standards (SAML/OIDC/GA4GH/X.509 and LDAP) and open source components addressing federated identity and access management problems specific to education and research.

In summary, this solution is an ideal candidate to test as a pilot solution for the project's identity and access management requirements.

Testing methods

Early piloting used a CILogon instance deployed for the Australian BioCommons, initially in the US region. Many project partners were already Australian Access Federation (AAF) subscribers and could use their home organisation identity to authenticate, once the initial platform was deployed and configured. This enabled exploration and testing work to begin within a few weeks, and meant the project team did not need to understand each component in detail or to deploy and operate authentication infrastructure. The CILogon infrastructure was later deployed to the Australian region during the project and services migrated to use that instance. This overcame data sovereignty concerns raised by some stakeholders.

The project team carried out test scenarios to explore how well CILogon was able to meet each of the identified requirements. Several accounts were onboarded to CILogon using enrolment flows we created. The test users were configured with one of the roles likely to be needed in a production instance (researcher, community manager, administrator).

These accounts were used to confirm whether the requirements could be met. In some cases we modified the CILogon configuration to better reflect the documented requirement and iterated several times through the test case to meet the requirement as closely as possible.

Summarised test results are discussed in the following section.

3. Test results against requirements

The following tables summarise the "Scoped and Reviewed Fed IAM Mandatory and Should Have Requirements", derived from the traceability matrix in Appendix 1.

Table 1. A breakdown showing the testing pass rate of "Mandatory" and "Should Have" requirements for CILogon.

Category	Number	Passed	Percent Passed
Mandatory	30	27	90%
Should Have	4	4	100%

Table 2. Details of the three failed “Mandatory” requirements and plans to address them.

Requirement Number & Short Description	Plans to Address
HGPPREQ-056 Primary sources of users' identities should be the users' external identity providers that are the most authoritative source for their role and affiliations in their home organisation.	The community needs to determine if some identity providers are more authoritative than others (ie: institutional vs social login). Once policy is defined we expect to be able to create different processes to address identities coming from less trusted identity providers.
HGPPREQ-103 The administrators of the services connected to the system should abide by Australian privacy laws (with regards the users' personal information, not the human genome data which is considered separately) and display relevant privacy policy information (for example on their website.)	This requirement failed because the policy work has not yet been undertaken. An Australian privacy policy will be crafted in future projects. This will comprise a general policy and a community level policy.
HGPPREQ-106 The system must implement authentication to the standard specified by the Infrastructure's policies for minimum requirements (Technical implementation of HGPPREQ-100).	This requirement needs further investigation to clarify and agree requirements between service providers’. We are confident the IAM solutions can support the service provider needs once requirements have been specified.

CILogon Service Deployment Model

Most of the pilot work was conducted using CILogon’s US-based infrastructure. This was not an issue for proof-of-concept work, but any future production service would need to run in Australian data centres to address the data sovereignty objections we expected future collaborators to raise.

Early in 2023 the CILogon deployed the service to the Australian AWS region while simultaneously using the opportunity to update some infrastructure components to more modern solutions. We have subsequently migrated the connected applications to use the Australian infrastructure ensuring that personal information does not leave Australia.

Penetration testing

The sensitive nature of human genomic data means that any authentication solution must adequately protect access to connected applications and resources. The AAF engaged an independent third party to conduct penetration testing against the Australian CILogon deployment supporting the HGPP work. The scope of the test included authentication processes, privilege escalation, orchestration APIs, and common user APIs. Testing revealed CILogon is resilient against typical security attacks and there were no critical or high severity findings. The CILogon team acted quickly to remediate the potential vulnerabilities, with the higher risk items having already been addressed.

4. Technical exploration and edge cases

The project team ran various technical demonstrators to understand the limitations of how CILogon supported various edge cases.

CILogon exists as a service run by the University of Illinois from US data centres. During the course of this project, a deployment of CILogon was also made in Australian data centres. Both CILogon services have been used in our technical explorations.

Users from each HGPP member institute were given administrator level privileges in one tenant of the HGPP CILogon service. This allowed them to experiment with creating virtual communities and connecting services to test software in their own institutes. Members also used personal email accounts (e.g., Gmail) where they simulated workflows as two different users.

Group membership via OIDC

Group membership (i.e., as a feature of community building) is a key driver of the choice of CILogon over some other solutions. Downstream services must be capable of consuming group membership claims to use this data for authorising access within connected services. For example, it should be possible for a standard web server to allow or deny access to a website based on whether the user has logged in and their login is part of a nominated “group” in CILogon.

CILogon provides a facility for mapping attributes stored in its internal LDAP directory, to OIDC claims that can be consumed by downstream services. Group membership is exposed as the "isMemberOf" LDAP attribute within CILogon, and thus can be mapped into an OIDC claim. An example configuration including this mapping is shown in Figure 1.

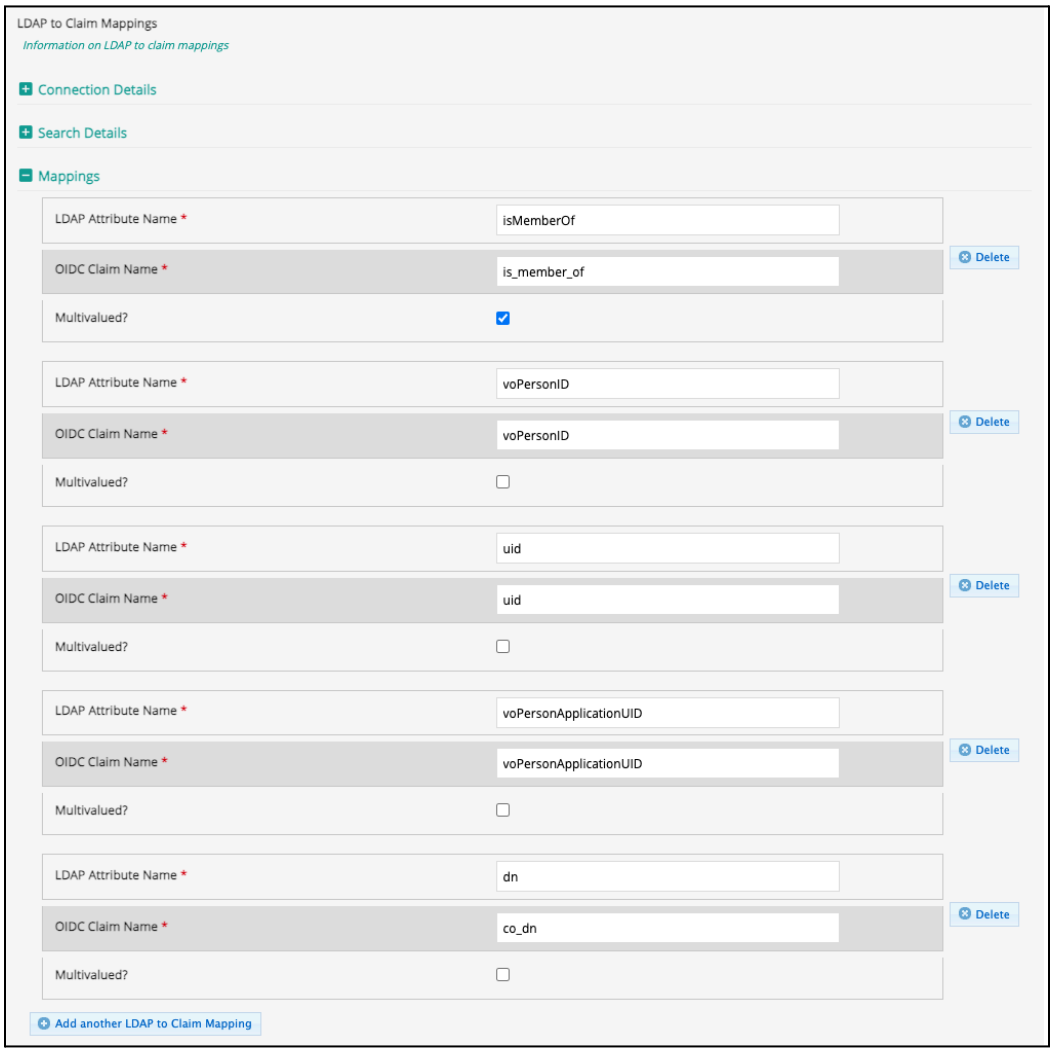


Figure 1. CILogon control panel showing group membership.

To confirm that this mapping could be consumed successfully by a downstream service for authorising access, an instance of the Apache http server was configured with the mod_auth_openidc module on a virtual server at NCI. CILogon group membership was mapped into OIDC claims, as per Figure 1. It was demonstrated that authorisation of access to example resources hosted on this server could be successfully controlled in this manner, using standard Apache configuration directives, and did not require any software development effort.

Custom JWT to support the Beacon Network

Another HGPP sub-project, Virtual Cohorts, had a requirement to add authorisation and authentication into their network of "Beacon" nodes[16]. The Virtual Cohorts Discovery Phase Report[17] details the current state of processes and tools for virtual cohort querying, national community needs, candidate solutions to enable cross-institutional virtual cohort querying, and recommendations on preferred technology and proposed implementation.

The underlying IAM problem here is one of distributing permissions across a wider network of servers, rather than just interactions between a single client and server.

The scenario they needed to test was to have a user interface (the "Beacon Network UI") allow login via federated login, but to then use the results of this authentication downstream in unconnected servers ("Beacon Nodes") who will respond with differing levels of details depending on the "researcher status" of the logged in user. Specifically, a casual user may only see a count of the number of cases with some particular requested phenotype (e.g., diabetes), but a trusted researcher may see row-level details of each case with diabetes.

JSON Web Tokens (JWT) bearer tokens[18] with limited life spans were chosen to pass the user status downstream because this fits best with the short, bursty pattern of usage of the Beacon service. In simpler terms, the user will login once at the main server, but a special key is generated that the user can pass downstream to other servers for a limited amount of time. This special key will unlock data, but only as much data as is permitted for the given user.

For the Beacon Network UI, the user logs in via a custom backend that initiates an OIDC flow to retrieve user attributes and community (group) information from CILogon. Whilst it would have been possible to perform a pure authentication from the React user interface alone, CILogon prevents the release of any user attributes to these "public" clients[19], instead using a backend which allows "confidential" clients.

Whilst CILogon can and does issue bearer tokens, the audience/use of these bearer tokens should be limited to services that are directly integrated with CILogon. Instead of passing CILogon tokens downstream, the Beacon Network backend uses the information it receives from CILogon to create a new bearer token (JWT) that is signed by the Beacon Network UI (Figure 2).

[16] https://docs.genomebeacons.org/
[17] https://zenodo.org/record/7439886#.ZF3hnOxBw04
[18] https://oauth.net/2/bearer-tokens
[19] https://oauth.net/2/client-types

In short, we want the user to login via CILogon and for the Beacon UI to mint a bearer token for the user specific only for the virtual cohorts use case. This new token can then be used across the Beacon Network as proof of “researcher status”. The rules defining the group or attribute values that determine the “researcher status” can then be centralised in one spot in the Beacon Network UI backend.

The proof of concept for this federated network of Beacon nodes has been implemented in Python[20]. Figure 2 shows the authentication flow and how the bearer tokens are employed for authorisation.

[20] https://github.com/AustralianBioCommons/beacon-network/blob/master/aggregator/jwt_helper.py

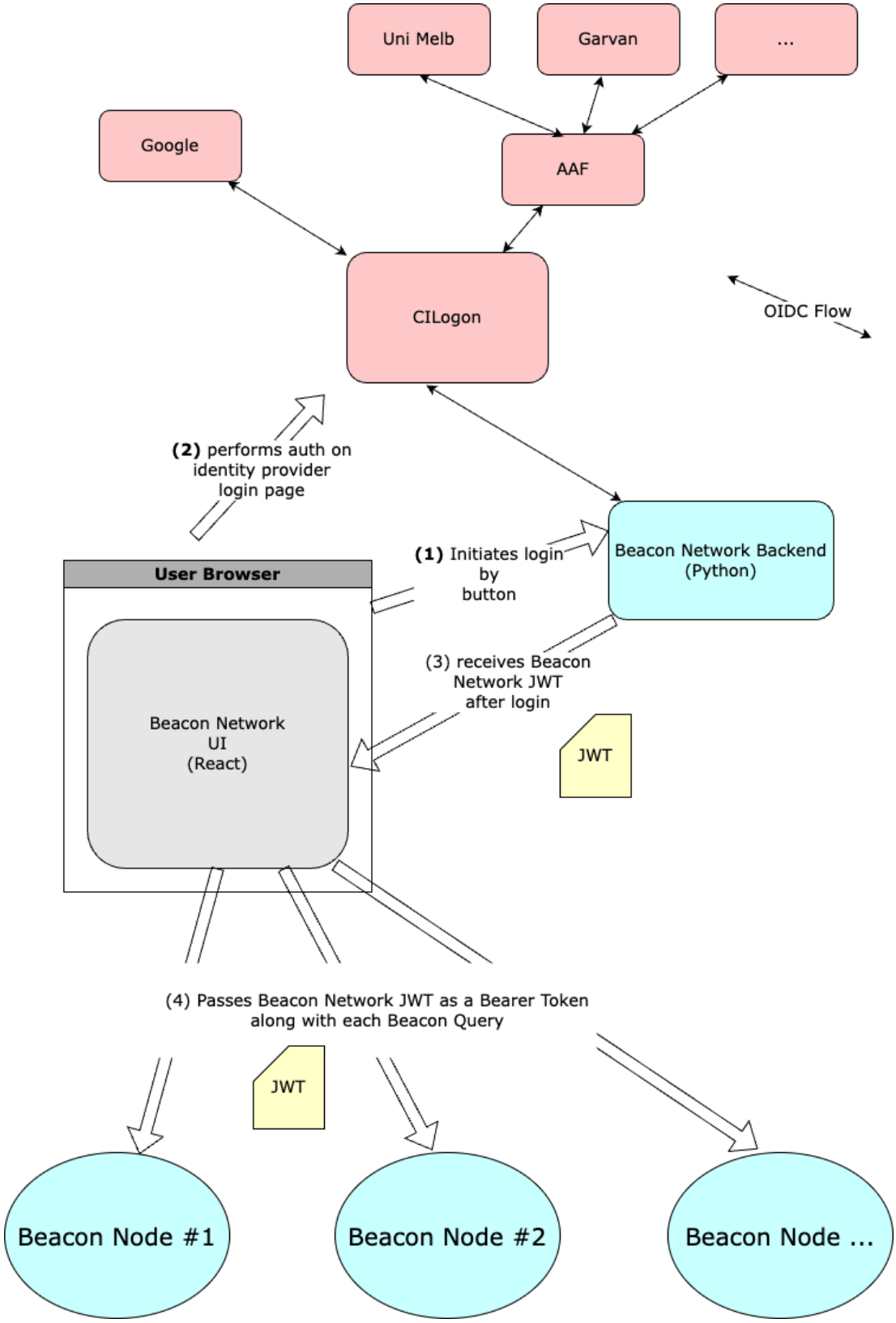


Figure 2. Data flows of JWT bearer tokens throughout the beacon network.

5. Conclusions

The aims of the HGPP Federated IAM sub-project were to explore digital research infrastructure for enabling federated user authentication for streamlined access to genomic data repositories and analysis platforms. Ideally, such systems should allow attributes about users and their primary organisations to be used to increase confidence and reliability in authorisation decisions.

During the project's discovery phase we established the formal requirements of the system through community consultation, identified several candidate solutions, and assessed those solutions against the selection criteria. Through this process, CILogon was identified as the leading candidate and was selected for a pilot implementation. In this report, we have summarised our approach to testing the deployment of CILogon and its integration with the Beacon network explored in the virtual cohorts sub-project.

We integrated several applications (e.g., Beacon) and used CILogon to enable users to join the community using their existing home organisation identity and single sign-on into several applications operated by different organisations. The effort to integrate new services into the human genomics community varies with the application architecture. Modern applications that support OIDC are generally straightforward. Some applications are significantly more challenging to integrate and require custom development to create plugins or new functionality to leverage federated identity sources.

The CILogon development team accommodated new development work to support testing GA4GH passports and visas. This is a more advanced use case but we were pleased with the responsiveness of the development team and the capability to extend the solution to support new authorisation tools.

Policy development remains the biggest gap and must be explored in future work. The federated network of service providers must have common expectations about the user community with respect to aspects like scope of membership, the level of trust in the identities presented, security practices, and privacy policies. Understanding these needs and developing a common baseline will be a major component of any future work. Once this baseline is agreed by community members we will be in a position to document processes and configure CILogon to support the process.

Appendix 1

The requirements shown in the table below were presented as Tables 7-14 in the preceding discovery phase report[21]. They are reproduced here in a consolidated form for convenience, with minor clarifications of language and the removal of extraneous comments.

ID	CATEGORY	REQUIREMENT	FAIL
HGPPREQ-004	Mandatory	The system consumes verified identities from users' home organisations and these are central to the authentication process to ensure verified identity.	
HGPPREQ-005	Mandatory	The system consumes verified institutional affiliations from users' home organisations.	
HGPPREQ-006	Mandatory	The system represents and manages working group memberships and can assert these memberships to relying services. **See HGPPREQ-052 for relying service types.**	
HGPPREQ-034	Mandatory	Data Access team members can be assured that researchers accessing data understand the need to maintain data anonymity and encryption, so as to reduce the need for them to provide one-on-one education and to ensure patient privacy is protected. The system should have the capability to retain training/ethical quals attribute information and this is available for potential consumption by downstream services. **See HGPPREQ-052 for types of services.**	
HGPPREQ-041	Mandatory	The system should support a qualified human genome researcher ID, indicating the researcher is part of the genome research community.	
HGPPREQ-044	Mandatory	The system must support authentication to CLI tools - for example a bioinformatics tool accessing data would need to be supported in this way.	
HGPPREQ-045	Mandatory	The system must support web flows (OAuth, OIDC, SAML)	
HGPPREQ-046	Mandatory	People with a role as an administrator within the system (exact role name to be confirmed) can create and administer arbitrary subsets of users to limit access to tools, data and storage etc to managed workgroups and also delegate this function to other users as required.	

[21] Human Genomes Platform Project: Federated Identity and Access Management (IAM) Discovery Phase Report https://zenodo.org/records/6644009

HGPPREQ-052	Mandatory	The system presents user attributes to a number of different types of relying services. Examples include instruments (producing data for research purposes), data archives (managing data for secondary use), computing and cloud services (enabling researchers to compute on data) and various collaborative tools that support researchers' interaction (such as wikis, content management systems, mailing lists or e-learning environments).	
HGPPREQ-053	Mandatory	The system supports proxy capability to translate between supported protocols including or at a minimum SAML, OIDC.	
HGPPREQ-056	Mandatory	Primary sources of users' identities should be the users' external identity providers that are the most authoritative source for their role and affiliations in their home organisation.	❌
HGPPREQ-057	Mandatory	The system allows the linking of multiple identities. eg. a Gmail account can be linked with a university identity for the same person.	
HGPPREQ-058	Mandatory	The identity management system should provide a user interface where delegated community managers can manage their users, organise them in groups to enable access to data and objects.	
HGPPREQ-059	Mandatory	The identity management system should enable community managers to define registration flows to individual groups including user life cycle in the groups.	
HGPPREQ-062	Mandatory	The system enables logins at the users institutes / home organisation to be used across the network of services - without necessarily requiring login over and over again.	
HGPPREQ-064	Mandatory	The system allows a user to link and unlink multiple external identities. To link additional identity a user should have to prove that they are able to authenticate with a new one as well as the one which is already linked. (This also could help when a user is moving from one home organisation to another.)	
HGPPREQ-065	Mandatory	The system has a mechanism to help prevent duplicate registration/signup of the same user with the same login credentials.	
HGPPREQ-067	Mandatory	The system enables integration of applications using SAML 2 and OIDC protocols at a minimum	
HGPPREQ-068	Mandatory	The system provides identity provider discovery service(s) for an end user to select their authentication provider.	

HGPPREQ-071	Mandatory	The system allows for access control, where a relying service requests the Proxy to deny access for users who don't qualify to the access policy (e.g. group membership) configured for the relying service. This requirement does not not prevent a service making additional authorisation decisions (and the latter is probably the standard way of doing it).	
HGPPREQ-074	Mandatory	The identity management system incorporates other attributes relevant for relying services.	
HGPPREQ-075	Mandatory	The identity management system provides credential translation, enabling an end user to receive an X.509 certificate or other short lived token if required for accessing a particular relying service.	
HGPPREQ-085	Mandatory	The system provides a process to ensure that all users are aware of, and accept the requirement to abide by, the Acceptable Use Policy (AUP). One mechanism is: The policy must be presented at the time of registration and the new user must read and accept before completing registration. **(HGPPREQ-085 and HGPPREQ-086 are technical implementations of HGPPREQ-084 policy).**	
HGPPREQ-086	Mandatory	The system must present to users any changes to the AUP and/or additional restrictions or requirements on acceptable use that arise out of new collaborative partnerships (if any). User must reaffirm commitment including changes. **(HGPPREQ-085 and HGPPREQ-086 are technical implementations of HGPPREQ-084 policy).**	
HGPPREQ-088	Mandatory	A service may have an additional or supplementary set of acceptable usage policies/T&Cs and the system supports the presentation of those policies and the users' acceptance of them. **(Technical implementation of HGPPREQ-087)**.	
HGPPREQ-091	Mandatory	The system enables the recording of membership management actions traceable to a user ID. **(We are imagining something like an audit trail with facility to input notes, this is Technical Implementation of HGPPREQ-089 and HGPPREQ-090).**	
HGPPREQ-103	Mandatory	The administrators of the services connected to the system should abide by Australian privacy laws (with regards the system users' data - not the human genome data which is considered separately) and display relevant privacy policy information (for example on their website.)	❌
HGPPREQ-104	Mandatory	The system must display a privacy collection notice to users, stating the personal information collected from users and how that data will be used. **(Technical implementation of HGPPREQ-095)**	

HGPPREQ-105	Mandatory	The system must implement identity assurance to the level specified by the Infrastructure's policies for minimum requirements. (**Technical implementation of HGPPREQ-099).**	
HGPPREQ-106	Mandatory	The system must implement authentication to the standard specified by the Infrastructure's policies for minimum requirements (**Technical implementation of HGPPREQ-100).**	❌
HGPPREQ-054	Should have	The system can interrupt the user flow and interact with the user. Typical use cases to include: - to redirect new users to registration; - to check if the user is authorised to use the service which they are trying to access; - if the user doesn't fulfil all conditions, the system can offer a solution in the form of immediate action. (For example redirection to a page where they can make an initial enquiry about access.)	
HGPPREQ-055	Should have	The service has the power to deny access if the user has not satisfied minimum identity and authentication assurance requirements.	
HGPPREQ-060	Should have	The identity management system within the platform should allow users without a manager role to view their **own** user profile, linked identities and other credentials.	
HGPPREQ-069	Should have	The system collects usage reporting data.	
HGPPREQ-102	Nice to have	The system must display the common aims and purposes, i.e. the research or scholarship goals of collections of users and have a mechanism to display changes **(Technical implementation of HGPPREQ-092 and HGPPREQ-093)**.	