Trust and Identity for National Research Infrastructure Co-designing a system-wide approach

22 October 2025

AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity

NCRIS
National Research Infrastructure for Australia
An Australian Government Initiative

Acknowledgement of country

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

In the spirit of reconciliation the Australian Access Federation (AAF) acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community.

We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

Agenda

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Activity
Introductions and Welcome
Incubator Use Cases Explored
Group Discussion
International Learnings
Group Discussion
Wrap-Up and Next Steps

Transforming Australian research infrastructure through trust and identity

Goal

- System-wide adoption of Trust and Identity
- Enabling a more researcher centric national research infrastructure for Australia.

Guiding principles

- Seamless connection
- Privacy enhancing
- Cyber secure
- Enhanced collaboration
- Increased productivity
- Underpinning an innovation and translation network
- Sovereign capability

Strengthening Australia’s research and development ecosystem for a ‘Future Made in Australia’.

National Strategic Imperatives

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Australian scientists, science institutions and infrastructure shaping Australia's future

Science at the centre of Australian industry

A diverse, skilled workforce to underpin the translation of science into new industries

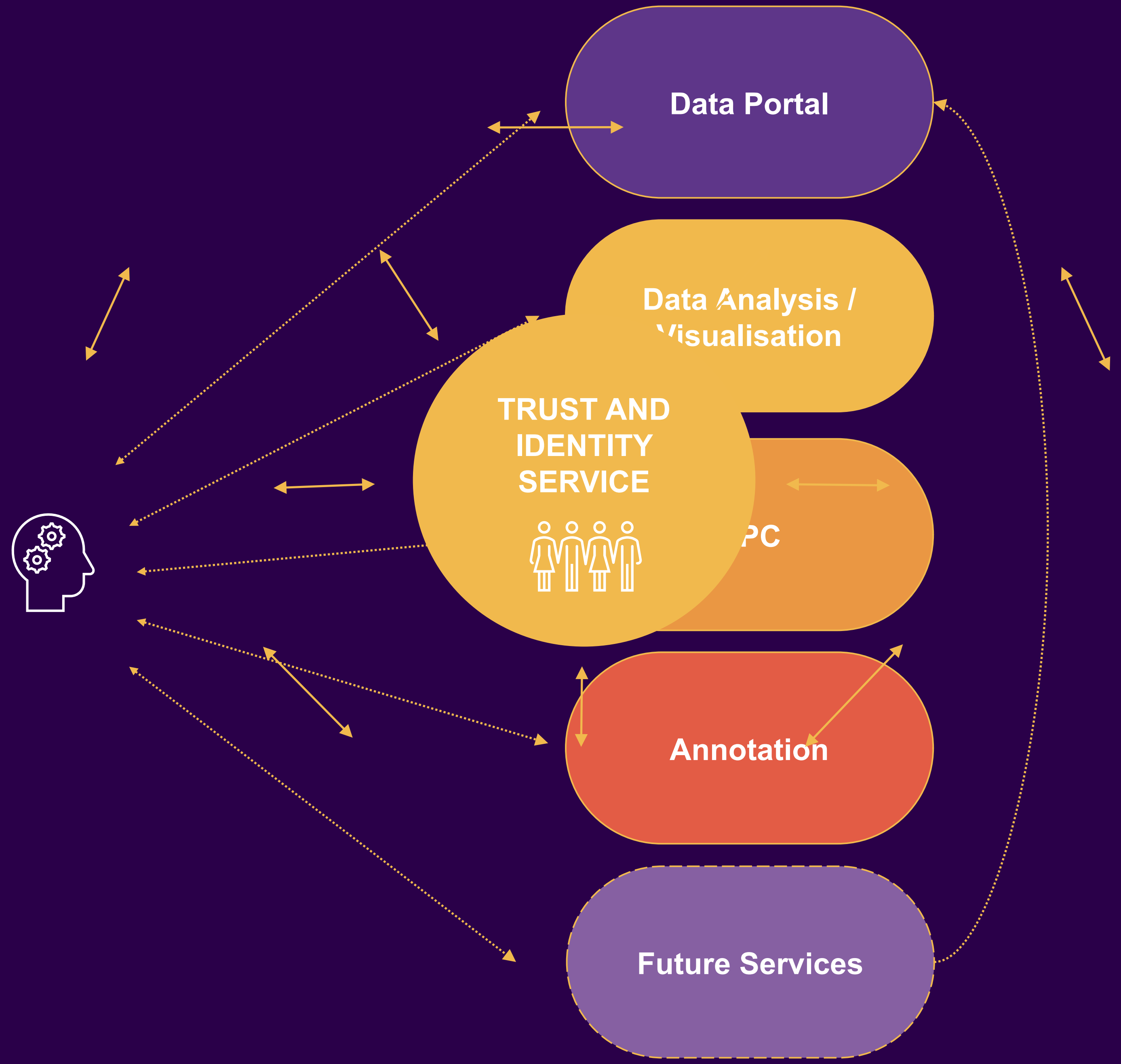
Embracing science to drive Australia's regional and global interests

A science system prepared for future challenges

AUSTRALIAN
ACCESS FEDERATION

Traditional Research Environment

Collaborative Research Environment



NCRIS
National Research
Infrastructure for Australia
An Australian Government Initiative

Current incubators

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

NATIONAL IMAGING FACILITY

ACCESS National Research Infrastructure

MICROSCOPY AUSTRALIA

Pawsey

NCI AUSTRALIA

ARDC Australian Research Data Commons

Phenomics Australia Enabling precision medicine

Incubators

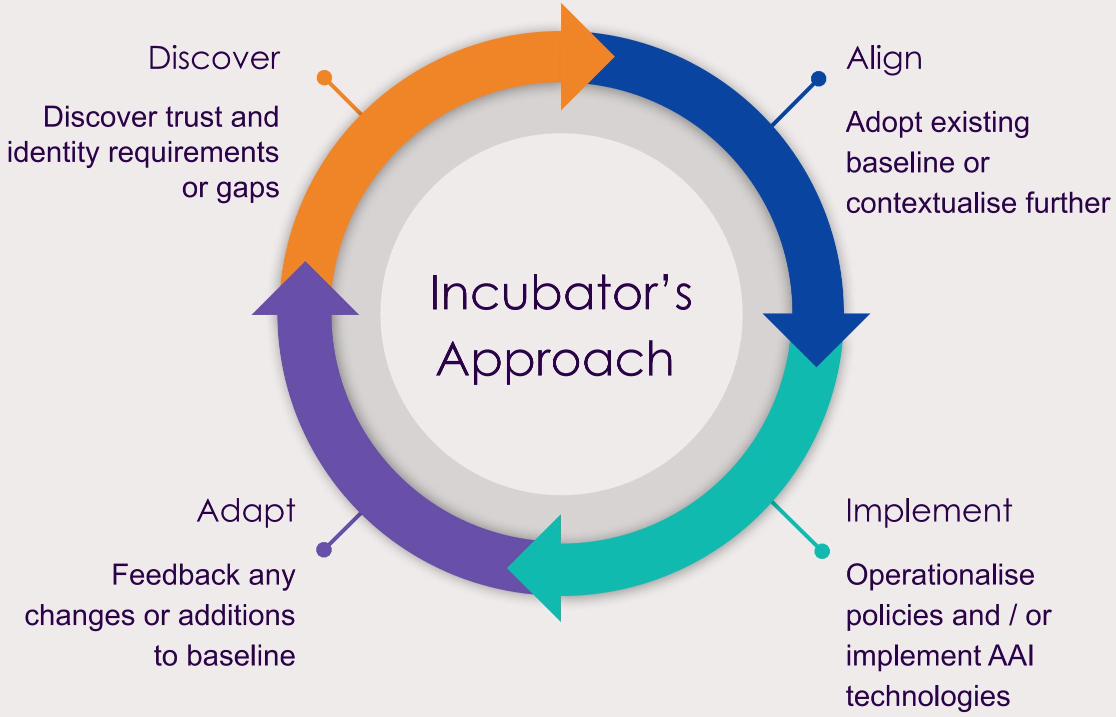
Goal: System-wide adoption of Trust & Identity (T&I) enabling a more researcher centric National Research Infrastructure (NRI) for Australia.

Challenge: Complexity of research infrastructure across Australia and internationally.

Principles:

1. Co-design and exploratory
2. Building a sustainable capability, re-usable policy and technology
3. Building long term partnership with NCRIS facilities
4. Supporting the research infrastructures through the change in processes and technologies

Approach: Utilising an internationally well-recognised Trust and Identity Framework, co-designing and testing different components of the Framework, through partnerships with research facilities towards developing trust and identity guidelines for Australian research sector.

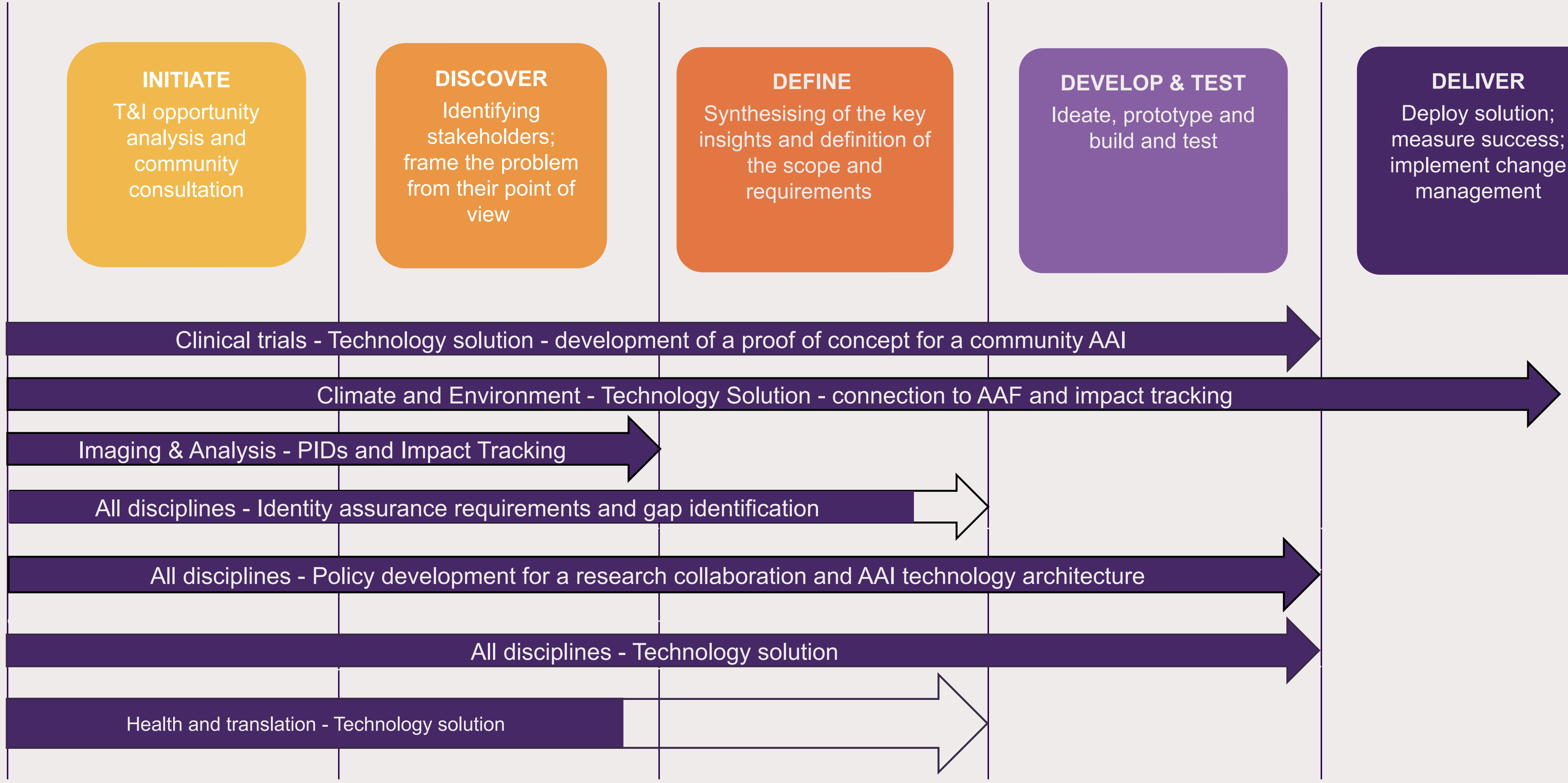


AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Overview of Incubator progress

AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity



Use Case 1: Providing Secure access to users from non-AAF institutions and government

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Description

To allow researchers from institutions that are not currently AAF members to securely access research services through their institutional credentials without the need to create local accounts.

- Phenomics:
- Pawsey
- NCI
- TERN

Challenges

- Technical: AAF currently working on possible technological solution that minimises security risks
- Governance: how that will change the existing federation service model?
- For Government users: requires integration with government federation or identity systems.
- Process change: both non-member institutions and their researchers need to go through and update processes of registry at least once.

Use Case 2: Providing secure and seamless access to resources distributed across institutions

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Description

Researchers (from a specific research discipline or research community, e.g., clinical trial, HASS and indigenous) to be able to manage and access the services required for their research (services may be hosted by multiple institutes) using their institutional credential through a central access management system.

- This is the AAI use case from an AARC perspective
- NIF
- LDACA
- Phenomics Australia

Challenges

- Defining the concept of research communities stays vague in practice, specifically when it comes to the governance aspect
- Many communities do not have the technical resources to support the technical implementations
- Research services are managed by institutions - even when they are funded by NCRIS facilities - the proposed approach requires change/adaptation in the governance models across sector.
- Technical: integration with variety and growing number of services with different technologies and maturity.
- Technical : Customising the solution to different communities' ways of working and language

Use Case 3: Sensitive data and requirements for higher levels of assurance

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Description

Research communities are constantly balancing the drive for open access with the mandate to protect sensitive data and uphold data sovereignty. This balance could be easier achieved by providing service providers with users’ profile assurance level during the authentication process.

- NCI
- GAURDIANS

Challenges:

- Current dependency to assurance processes at universities and institutions and limited incentives for universities to uplift processes
- Institutions need to provide assurance attributes
- Sensitive data projects (e.g. health, Indigenous data sovereignty) require layered assurance that current federated login flows do not fully support

Use Case 4: Collaboration and data sharing between research communities, industry and government

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Description

Providing access to industry data for researchers and enabling integration with research services, managing users access and providing access to research outcomes for industry and government users.

- SEAF
- This is the use case for Dataspaces

Challenges:

- Using different systems for user management, one specific for researchers and academic users and one for industry and government users.
- Providing transparency and traceability of shared data
- Supporting data sharing agreements

Use Case 5: Providing support and technical guidelines for communities to implement their own AAI

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Description

AAF can provide both policy and technical guidelines to support the community to implement their own AAIs that complies with internation standards.

- Health Data Australia
- Biosecurity Commons

Challenges

- Usually, research communities don't think about Access and Identity management in early stages of building the infrastructures.
- Researchers are not trust and identity experts.
- Integration of the implemented AAI with the other communities if the requirements for interoperability are not considered.

Use Case 6: Traceability of Usage and Impact Tracking Across Multiple Research Services

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Description

To be able to have a traceability of the researchers' journey and use of multiple research service and datasets until they complete the journey and publish their outcomes.

- ACCESS-NRI
- Phenomics Australia
- Microscopy Australia

Challenges

- Technical: integration with AAF or ORCID across research facilities or through separate authentication
- Governance: Institutions to provide users' ORCID ID as part of their user attributes to AAF. (this can be achieved if AAF can make the case using NCRIS requirement)

Use Case 7: HPC Federated Access

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Description

Researchers to be able to use their institutional credential in a secure and seamless way to connect to HPC resources.

- Pawsey
- NCI
- Tier 2 HPCs

Challenges:

- Current technical solutions (OIDC device flow) is not as easy as other methods of access like using SSH key pairs.

Use Case 8: Cross collaboration/institutions access and identity management

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Description

Research infrastructures (collaborations) to provide access to researchers from other communities to their services ,i.e., the collaboration knows if a researchers is a member of another research community. (scenarios where AAIs themselves must be federated, i.e. each AAI in a federation trusts the users and attributes released by the others)

- This is the case for EOSC in Europe
- In Australia GUARDIANS is an example of that?

Challenges

- More complicate architecture models
- Change in existing processes across institutions and research sector

Group activity

- Individually, think about any other examples supporting similar use cases? If yes write the use case number from the list and a brief description.
- If you can think of Trust and identity use cases that are not included in the list below, please add them separately.
- Discuss your list with your group.

AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity

List of use cases

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Use case No.	Use Case
Use Case 1	Providing Secure access to users from non-AAF institutions and government
Use Case 2	Providing secure and seamless access to resources distributed across institutions
Use Case 3	Sensitive data and requirements for higher levels of assurance
Use Case 4	Collaboration and data sharing between research communities, industry and government
Use Case 5	Providing support and technical guidelines for communities to implement their own AAI
Use Case 6	Traceability of Usage and Impact Tracking Across Multiple Research Services
Use Case 7	Federated access to HPCs
Use Case 8	Cross collaboration/institutions access and identity management

How has the international community addressed these use cases?

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

	Use case	Examples across international community
Use case 1	Providing Secure access to users from non-AAF institutions and government	In Europe, GEANT are using a service that can integrate national eIDs via eIDAS, EU Login, Community AAIs and other trusted authentication sources. For users utilising their national eIDs, the system adheres to the eIDAS regulation.
Use case 2	Providing secure and seamless access to research software for research communities	Developing Community AAI which is compliant with AARC BPA and policies. Surf and SRAM examples. AARC community, updates requirements and guidelines for implementation and also provides list of AARC compliant AAIs
Use Case 3	Sensitive data and requirements for higher levels of assurance	REFEDs assurance levels AARC provides guidelines on how assurance attributes are asserted.

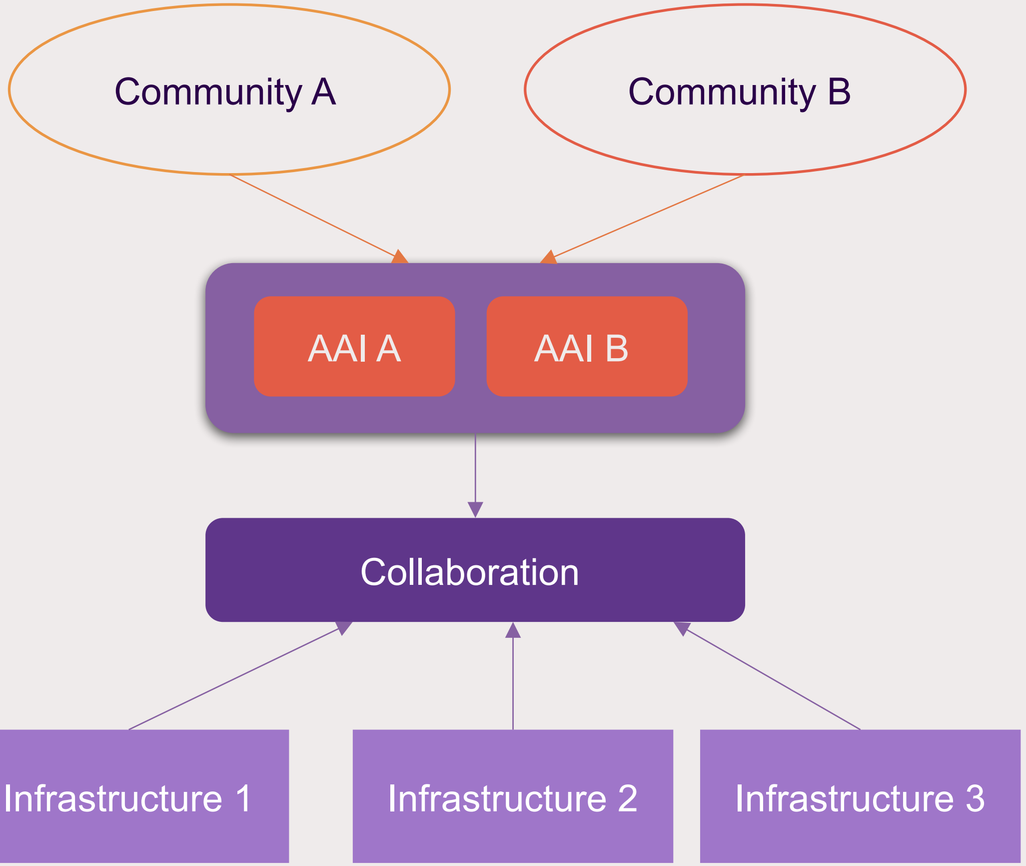
How international community addressed these use cases?

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

	Use case	Examples across international community
Use Case 4	Data sharing between research communities, industry and government	In the R&E sector, EOSC is an example of data sharing network and infrastructures based on AARC BPA.
Use case 5	Providing support and technical guidelines for communities to implement their own AAI	AARC community provides supports for small research communities by providing guidelines and minimum requirements for policies and AAI implementation. Also, communities can share an AAI instance.
Use case 6	Traceability of Usage and impact tracking across multiple research services	EGI federated accounting service, EOSC PID-based usage tracking, GA4GH Passport logging for controlled data usage.
Use case 7	HPC Federated Access	EGI check-in for federated access to web services, SSH key provisioning using token translation service. OIDC device flow using CIlogon
Use case 8	Cross collaboration/institutions access and identity management	An example is EOSC which leverages federation of AAIs given every AAI implementation is AARC compliant

Discussion Points

- Does "community first“ approach suits Australian research sector?
- Does each community need an AAI? Why?
- Who will be in charge of developing compliant AAIs?
- Who will be responsible for managing and owning collaboration policies when research infrastructure are providing services together?



AUSTRALIAN ACCESS FEDERATION

Any questions?

Visit: aaf.edu.au
Email: support@aaf.edu.au

NCRIS
National Research Infrastructure for Australia
An Australian Government Initiative

AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity