Operationalising Trust in Dataspaces: Trust and Identity Framework implications

E-Research 2025

Dr Fahame Emamjome

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.

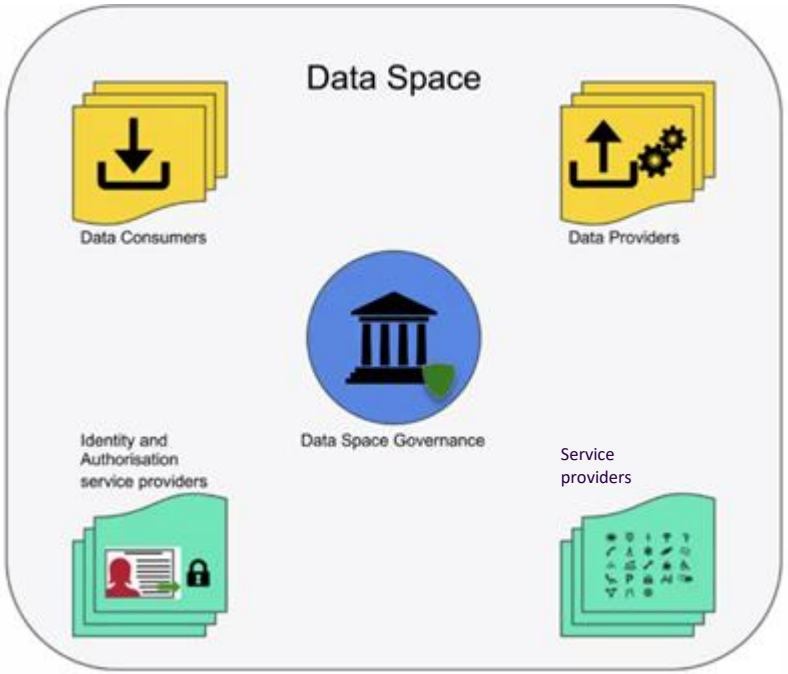
We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

What is a Dataspace?

AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity

- A dataspace is digital infrastructure that enables participants to find, access and use data based on the governance framework of that dataspace.
- It is a decentralised data ecosystem built around commonly agreed building blocks enabling an effective and trusted sharing of data among participants
- Data consumers, data providers form an ecosystem with governance structure in place to create basic data spaces
- Service providers are also part of dataspace, providing value adding services on top of data



Reference: https://www.slideshare.net/slideshow/day-1-introduction-to-i4trust-data-spaces-building-blocks-and-roles-train-the-trainers-program-247033216/247033216#5

Trust and Identity Framework

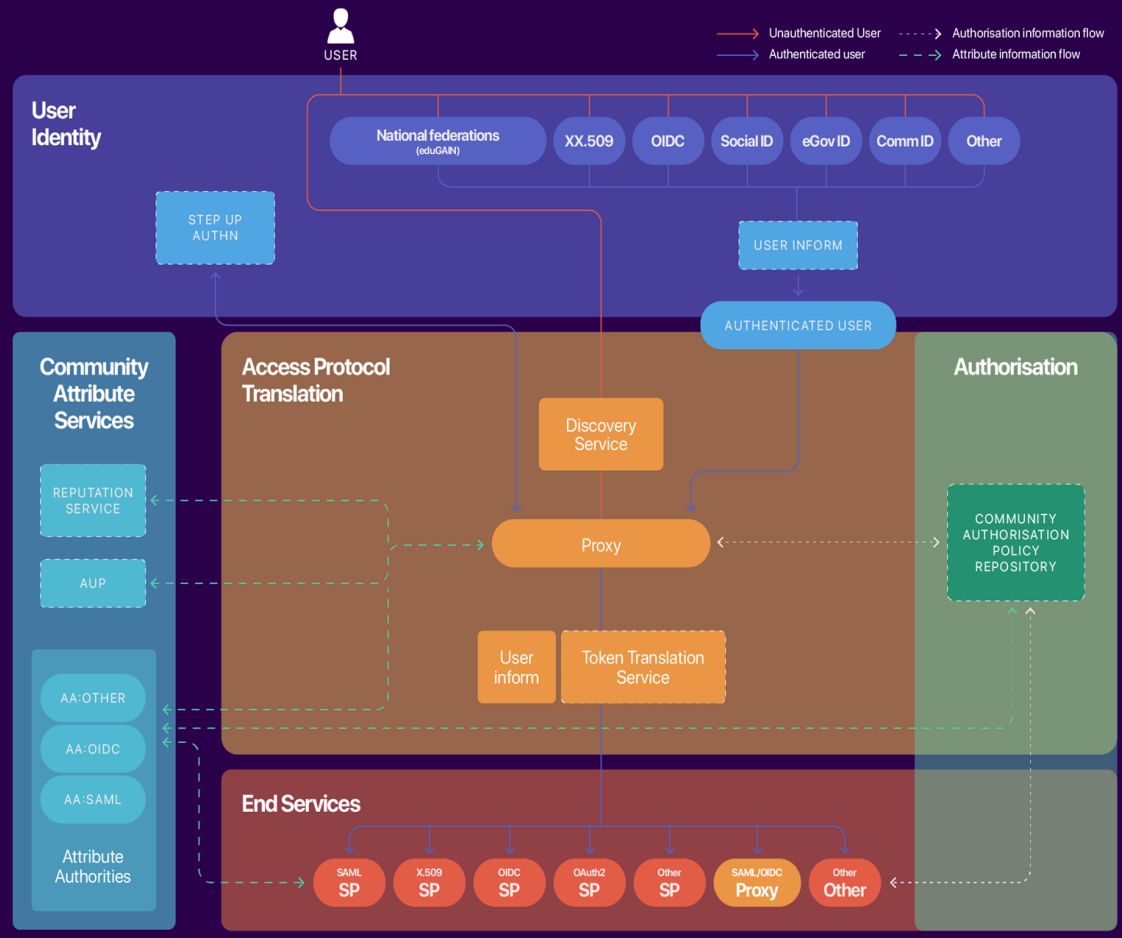
AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity

Policy Development Kit

- Governance Model
- Membership Management Policies
- Data Protection Policies
- Operational Security Policies

Technology Components



Motivations and objectives

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Could we use the T&I Framework in implementation of Dataspaces in Australia?

To answer these questions, we needed to

1. Understand the alignment between the T&I Framework and Dataspaces frameworks
2. Identify the gaps in Dataspaces frameworks in relation to enabling trust in Australia - specifically for research collaborations
3. Explore how the T&I Framework can support implementation of Dataspaces.

Existing Dataspaces Frameworks

AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity

Framework	Governance	Legal	Business / Organisational	Technical / Infrastructure
International Data Spaces Association (IDSA)	Partial	Strong	Strong	Strong
Sitra Rulebook	Strong	Strong	Strong	Partial
Dataspaces Support Centre (DSSC)	Strong	Partial	Strong	Strong
iSHARE Trust Framework	Partial	Strong	Strong	Strong
Gaia-X Trust Framework	Strong	Partial	Strong	Strong

Focus	Symbol
Strong cover	Strong
Partial cover	Partial
Not addressed	Not addressed

BDV BIG DATA VALUE ASSOCIATION

FIWARE

gaia-x

iSHARE

DATA SPACES SUPPORT CENTRE

SITRA

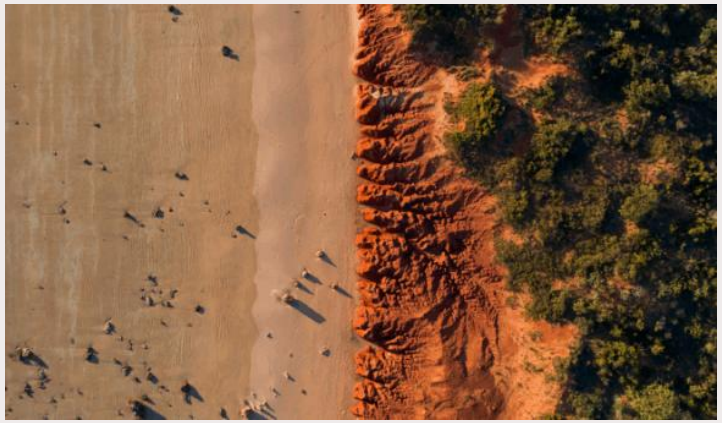
INTERNATIONAL DATA SPACES ASSOCIATION

Dataspace Use Cases in Australia

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Data sharing for Shared Environmental Analytics Facility (SEAF)

To enable data sharing across industry and government and research sector.



Biosecurity Dataspace

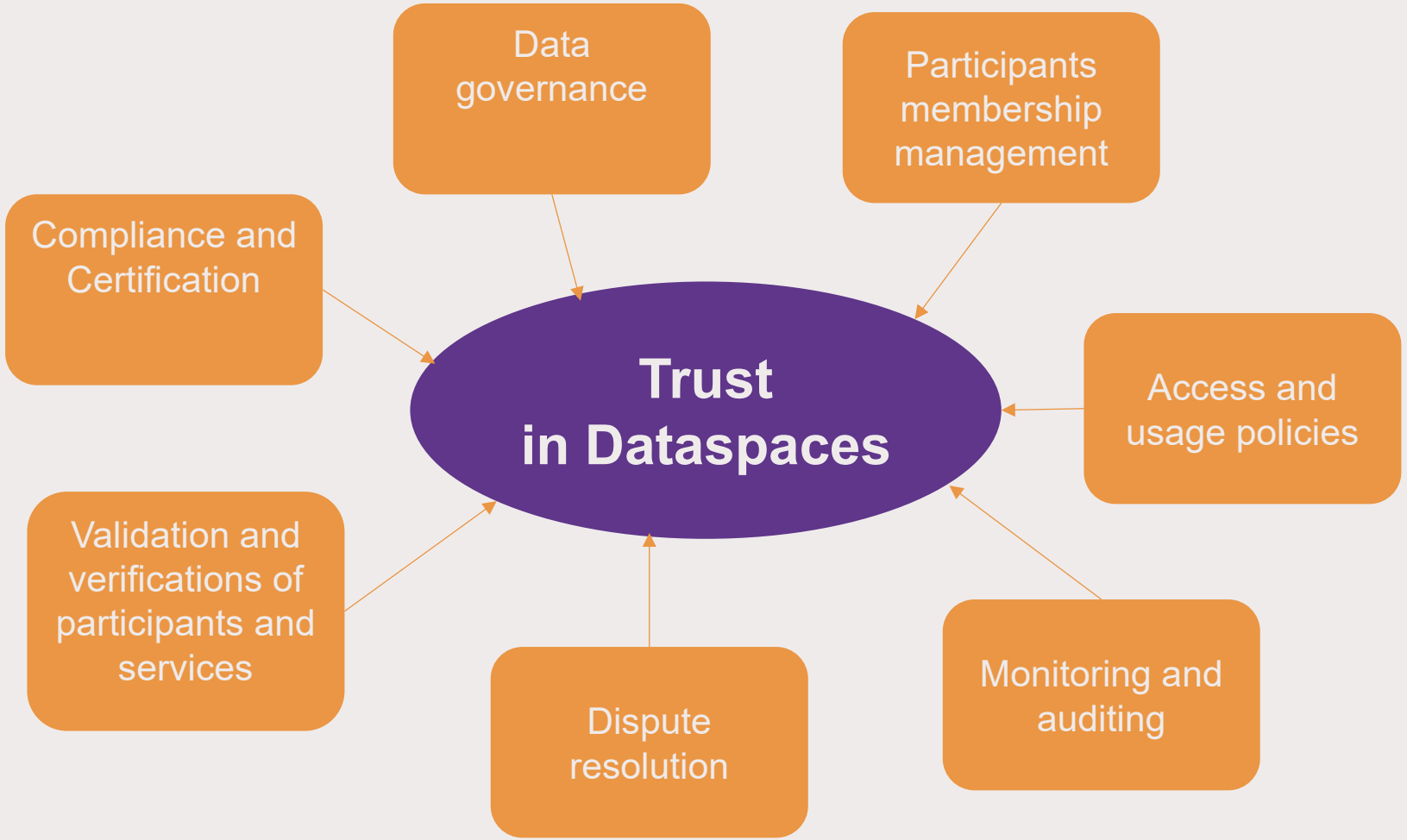
To enable data sharing and aggregation of plant health surveillance data, considering varying policies and registrations

https://ardc.edu.au/program/australian-dataspaces/

Trust in Dataspaces

AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity



Terminology alignment

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

AAF T&I Framework terminologies	Dataspaces equivalent terms	Alignment Note
Collaboration	**Dataspace**	Both define the shared environment enabling trusted data exchange
Community	**Use Case Participant**	Describes the actors governed by a common purpose to use the infrastructure
Infrastructure	**Digital Computing Infrastructure**	The physical or cloud platforms underpinning collaboration or dataspaces
Service	**Value-Creation Service / Operators**	Entities providing the functions. Any service aimed to create value out of the data shared in the data space
User	**Data User/affiliate**	An individual, company, corporation, partnership or other entity that, authorised to access and use data and services

T&I and Dataspace's Focus areas

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

Focus Area	IDSA / Dataspaces Approach	AAF / AARC / T&I Approach
Interoperability	Achieved through **Connectors** and standardised contracts.	Achieved through **AAIs** (Authentication and Authorisation Infrastructures) and the Policy Kit.
Technology use	Promotes **re-use of existing open standards** (IDS connectors, OAuth2, etc.).	Builds on **federated identity and assurance standards** (REFEDS, OIDC, SAML).
Trust model	Legal & technical trust anchored in certified participants and trusted connectors, verified via the existing Trust Frameworks.	Operational trust anchored in federated assurance, attributes, and policies.
Governance scope	Data-exchange governance between organisations, participant roles, and certification processes.	Governs cross-infrastructure identity, assurance, and access across domains and services.

Alignment between T&I Framework and Sitra Rulebook (checklist)

- **Governance**: Roles, policies and participation rules.
- **Ethical**: fairness and transparency, consumer rights etc.
- **Legal**: contractual principles, reusable policies and agreements
- **Business and Ops**: business purpose and value.
- **Technical**: ensuring the infrastructure meets security standards and governance requirements.

Category	Sitra Component	T&I / AARC Alignment
Governance	Role definitions, participation rules	T&I Policy Kit
Ethical	Ethical maturity model	T&I Policy Kit
Legal	Contractual premises	T&I Policy Kit
Business & Ops	Canvas & checklist	Policy Kit + Risk + AARC
Technical	Infrastructure checklist	T&I Policy Kit + AARC guidelines

What are the implementation Gaps (trust and identity) in existing Dataspaces Frameworks ?

Framework	Limitations
IDSA Rulebook	Focused on contractual & connector-level trust — lacks federated identity assurance, attribute management, and interoperability across identity providers.• Limited guidance on end-to-end user provisioning and access lifecycle.
iShare	Trust model assumes business/legal registration but not research federations or community-based identity.• Minimal treatment of delegation and token translation between identity systems.
Gaia-X	Strong on sovereignty & certification, less mature on operational AAI interoperability across domains.• Focus on B2B entities, less on individual researcher access or multi-IdP scenarios.
Sitra Rulebook	Comprehensive on business & legal rules, but abstract on technical trust anchors (AAI, assurance, logging).• Does not specify how to verify participant or component trustworthiness technically.

How can T&I framework Support Trust Implementation in Data Spaces?

Policy support:

- Bridges multiple frameworks such as; GDPR, REFED CoCo, and assurance obligations through structured attribute management and privacy guidance
- T&I policy defines assurance and assurance attributes.
- Provides protocols and procedures for compliance with Sitra rulebook expectations around risk and incident response.

Technical implementation:

- AAI is defined as the main technical component for managing user attributes and connecting different services and communities
- Directly implements core policies through attribute exchange, assurance levels, and scalable authorisation mentation support.
- Enables cross-domain trust between heterogeneous IdPs.
- Enables delegated access and federated authorization (OAuth2/OIDC).
- Assurance profiles (REFEDS + AARC) can operationalise Sitra's "trust verification" layer through audit-ready AAI practices.

AUSTRALIAN ACCESS FEDERATION | Experts in Trust & Identity

AUSTRALIAN ACCESS FEDERATION

Any questions?

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

NCRIS National Research Infrastructure for Australia
An Australian Government Initiative