AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity

Top Five

Trust and Identity Themes for Australia's higher education and research sector

DISCUSSION PAPER
APRIL 2026

Australian Access Federation

The Australian Access Federation (AAF), operates the trust and identity Federation for the higher education and research sector, and is recognised by the Australian Government's National Collaborative Research Infrastructure Strategy as the Trust and Identity Capability for the national research infrastructure ecosystem.

The AAF delivers a trusted digital access layer that enables students, educators, and researchers to seamlessly and securely access national and international digital resources. Including enabling researchers, industry, government and international partners, to securely access and share high value digital research infrastructure, data, platforms and high-performance computing at national and global scale.

Alongside this work, the AAF leads the Australian ORCID Consortium — bringing together universities and government agencies from across the country to support researchers in adopting ORCID, a universal persistent identifier, at both national and regional levels.

Our subscribers

We are a member based organisation with more than 108 subscribing organisations. These include all public Australian universities, CSIRO, the Australian Research Council (ARC), the National Health and Medical Research Council (NHMRC), the Council of Australasian University Directors of Information Technology (CAUDIT), and the Department of the Prime Minister and Cabinet.

Acknowledgement of Country

In the spirit of reconciliation, AAF would like to Acknowledge the Traditional Custodians of the lands on which we live and work. We support their connection to land, sea and sky Country and pay our deepest respects to Aboriginal and/or Torres Strait Islander Elders, past and present.

Contents

Top Five Trust and Identity Themes for Australia's higher education and research sector

In September 2025, the Australian Access Federation (AAF) held the inaugural Advancing Trust and Identity for Higher Education and Research Roundtable during the CAUDIT Spring Members Meeting and AHECS Cybersecurity Summit.

This Roundtable marked the first in a national series convening leaders from across the community to share insights and consider emerging challenges and opportunities, with the aim of informing future sector roadmaps and strategic directions.

This discussion paper captures the key themes from that first Roundtable in collaboration with leaders in the higher education and research sectors in information research, technology, and cybersecurity. Its purpose is to identify key characteristics of future-ready trust and identity (T&I) for the sector.

The paper presents the Top Five Themes identified during that first Roundtable.

Top Five Themes

Theme 1 - Beyond campus identity

Theme 2 - Lifelong identity

Theme 3 - Future ready trust models

Theme 4 - T&I in an AI world

Theme 5 - Cybersecurity

For discussion

When reading this paper, we ask you to consider the following questions:

- How do the themes reflect the need for future-ready trust within your organisation and between collaboration partners over the next 3-5 years?
- What business value could be gained if all your staff, students, contractors and other stakeholders had a persistent, highly assured identity before, during and after their relationship to your organisation?
- Which use cases (research collaboration, student lifecycle, sensitive data access, cross-sector translation, automation/AI etc.) are most limited by today's identity model?
- Where do you see the largest trust gaps (assurance, governance, accountability, interoperability)?
- What dependencies or risks should be considered (legal, privacy, international participation, sustainability, security)?
- What is missing?

THEME 1

Beyond campus identity: a model for a wider ecosystem

Today's federated identity ecosystems in higher education are shaped around a relatively clear perimeter: higher education institutions and research organisations issuing identities to their staff and students, and service providers that trust those institutional identities for access to applications supporting research and education. Over time, this boundary has grown less distinct as modern collaboration routinely includes clinicians, hospital researchers, government analysts, industry partners, contractors, visiting scholars, international collaborators, citizen scientists, and other contributors who sit outside the .edu domain.

When stakeholders cannot participate using their organisational identity, collaboration reverts to ad-hoc workarounds like local accounts, manual approvals, inconsistent onboarding, and bespoke integrations. This increases costs for service operators, creates an inconsistent user experience, and can increase risk (particularly where ad-hoc access is granted).

A future-ready model needs an inclusive and interoperable T&I ecosystem and trust infrastructure that facilitates governance and technical standards to work across sectors. It must support cross-sector use cases (for example, a private sector researcher accessing a university-hosted compute platform, or a government analyst accessing bushfire modelling data) without forcing every participant into a single operational model.

We want to know:

- What minimum trust expectations (claims, governance, liability etc) would you need to accept identities from adjacent sectors (and what would you be willing to assert about your own identities to them)?
- Are there specific cross-sector use cases where "good enough" interoperability is sufficient? What use cases require stricter policy and assurance?
- What sustainability models could enable broader participation without creating excessive overhead for occasional collaborators?

THEME 2

Lifelong identity

Institution-issued identities are inherently tied to employment or enrolment. Researchers, professional staff, clinicians, students, and contractors change roles and organisations regularly, sometimes multiple times over the life of a single research project. To support these scenarios, we need to shift to a lifelong user identity that can be applied in different contexts.

For example, the sector-wide MortarCAPS initiative aims to reduce complexity and duplication in university systems and enable students to move learning records (academic qualifications, skills, portfolio data etc) cleanly and consistently between institutions, systems, and jurisdictions.

Such a model depends on a persistent, trustworthy identity outside of the university to associate the users' achievements and capabilities with a lifelong, persistent identity that belongs to the individual and can be reused across contexts, which would simplify many collaboration scenarios.

At the same time, where someone works (and in what capacity) remain important attributes for authorising access to data and resources. Separating the more stable, person-centric identity from context-specific attributes such as organisational affiliation, role, project membership, eligibility, or qualifications is a potential future model. Services can then request only what they need and avoid unnecessary data sharing.

We want to know:

- Where would a persistent, person-owned identifier add the most value for your organisation (continuity of access, alumni access, cross-institution projects, cross-sector translation, international collaboration etc)?

THEME 3

Future-ready trust models

Trust between a user's digital identity and the services they are accessing is key for efficient collaboration and value exchange. Institutions issue local identity today because there was no reliable external identity they could trust. Local processes to increase trust were prioritised over reusability of the identity in other contexts. Rather than a local system as the single source of truth, future solutions will combine trust signals from multiple organisations. This richer view will evaluate trust requirements relevant to the specific use case.

Viable options for trusted external identity are emerging, and will need integration with **multiple identity sources**. Any single national scheme (for example, the Australian Government Digital Identity System (AGDIS) is unlikely to cover the breadth and diversity of research and education stakeholders. Future models must support interoperability with multiple highly assured identity sources and pathways for international participants to integrate with equivalent trust marks.

While basic identity attributes (e.g. name, date of birth, contact information) are sometimes sufficient, other transactions need more specific information to further increase trust. Trust marks can build on basic identity data to express characteristics such as attainment of an industry certification, membership of a group, or a role within a community. Emerging trust models will start with a stable external identity but also evaluate trust marks from multiple data providers to evaluate what an individual is permitted to do within an information system.

We want to know:

- What safeguards would you require to trust external identity sources?

THEME 4

T&I in an AI world (non-human identity and delegation)

Until recently it was safe to assume that people authenticated to systems as an interactive process. Now we have automated workflows, service accounts, instruments and sensors, and new agentic AI systems that act with varying degrees of autonomy. Attempting to shoehorn these agents into the human identity model undermines security (shared credentials, weak accountability) and leads to unsatisfactory governance outcomes (unclear responsibility for actions).

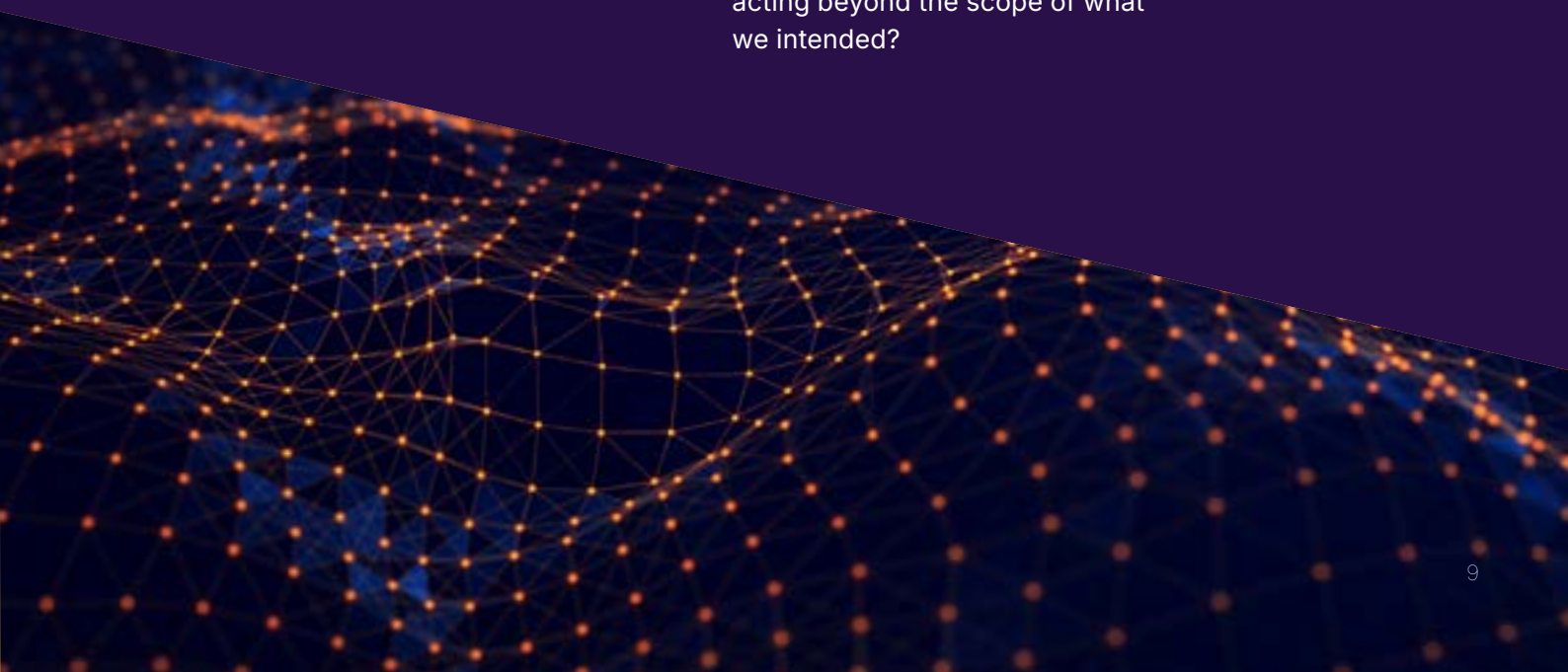
Agentic AI has escalated the need for delegation models to enable a human or organisational account holder to authorise an agent (human or non-human) to perform specific actions, without overreaching on our intentions, and without giving that agent full access or impersonating the delegator by handing over their credentials. Effective auditing and governance requires systems that can trace the provenance of delegation back to a responsible party (individual, team or corporation) especially when AI can enlist other intermediate services without specific direction.

Explainability and traceability becomes more important as autonomy increases. Services must have means to determine:

- What safeguards would you require to trust external identity sources?
- What is the relationship of this agent to a human researcher, and should I grant access to this dataset?
- What data sharing agreements need to be evaluated to inform the authorisation decision?
- What was the scope and duration of the delegated authority?
- These questions relate to trust and governance as much as they do AI. AI's rapid advancement has brought questions like these into sharper focus and both standards groups and practitioners are looking for answers.

We want to know:

- Where do you already rely on non-human identities (service accounts, automation, pipelines, instruments). What's working well and what are the challenges?
- What minimum audit and traceability requirements do you expect for autonomous agents interacting with sensitive services and datasets?
- How do we prevent AI from acting beyond the scope of what we intended?



THEME 5

Cybersecurity

Cybersecurity threats to the higher education and research sector continue to grow in scale and sophistication. Identity is a foundational control for maintaining security since many incidents begin with compromised credentials. Harvested credentials are often used as a launchpad for later attacks like phishing campaigns, privilege escalation, data exfiltration, fraud, and ransomware. Improving identity controls, therefore, improves the effectiveness of security investments.

While multi-factor authentication (MFA) is widely used by institutions to help protect information assets, more work is needed to relay this information to third-party systems to convey stronger trust. Standardised signalling of authentication strength (including whether phishing-resistant methods were used) and identity assurance helps services make risk-based access decisions, particularly where they host sensitive research data

For service providers to rely on an external identity, it must be highly assured. Assurance has two dimensions:

1. **Identity assurance** — confidence that the person is who they claim to be, established through robust identity proofing and record keeping.
2. **Authentication assurance** — confidence that the person authenticating is in control of the credential by using a second authentication factor.

Trust signals about both these dimensions must be conveyed to relying parties in standard formats.

Exploitation and abuse of onboarding and user lifecycle processes is on the rise. “Ghost” student enrolments are used to obtain legitimate credentials and gain a foothold inside an institution. From there, attackers may explore other systems, target staff, or pivot into partners via trusted connections. This reinforces the need for robust identity proofing, continuous behaviour monitoring, dependable processes for changes to enrolment or employment status, and timely deprovisioning.

We want to know:

- Where do you need better assurance signals to support risk-based access decisions (sensitive data platforms, privileged administration, high-value research, financial transactions)?
- What controls or processes have proven effective against fraudulent onboarding and “ghost” enrolments, and where are the gaps?
- What would you need from an ecosystem-wide approach (shared patterns, common standards, shared telemetry) to make identity a stronger security foundation?

Bringing the themes together

These themes are highly interdependent.

- Broader participation beyond .edu is difficult without interoperable trust frameworks.
- Persistent identity is only valuable when it can be augmented with relevant data from a network of reliable sources.
- Delegation and non-human identities introduce new audit and governance requirements.
- Sophisticated security threats demand higher assurance, better auditability and clear accountability.
- Solutions must address the spectrum of governance, policy, standards, operations, and technology.

AUSTRALIAN ACCESS FEDERATION

Experts in Trust & Identity

Australian Government
Department of Education

NCRIS
National Research Infrastructure for Australia
An Australian Government Initiative

Enabled by NCRIS

Australian Access Federation receives funding from the Australian Government through the National Collaborative Research Infrastructure Strategy (NCRIS).

Written by a human, some editing by CoPilot, verified by the AAF.

Publication correct as of April 2026