

MAKING THE CASE

An NCRIS Trust and Identity Capability

*Enabling a more interconnected,
efficient and secure NCRIS system*

Second edition



AUSTRALIAN
ACCESS FEDERATION
AAF.EDU.AU

MAKING THE CASE - KEY POINTS

Since 2006, successive NCRIS Roadmaps have recognised Access and Authentication as crucial national research infrastructure.

One-off seed funding was provided to the Australian Access Federation (AAF) in 2009 to take the first steps towards establishing a trust and identity federation for Australia's research and education system. Today, the AAF is globally recognised as a leader in its field.

While the AAF's core operations are supported through subscription fees, AAF receives no systemic or ongoing funding to meet the evolving access and authentication needs of the NCRIS system. Without systemic investment, the efficiency and effectiveness of the research system continues to be diminished and support for research is at risk.

High quality identity and access infrastructure is an essential component of the NCRIS Digital and Data Platforms (DDeRP) as outlined in the roadmap. Importantly it is needed to protect Australia's research infrastructure, researchers, research data and international research partnerships from cyberattacks and foreign interference.

There is a growing recognition and consensus that an urgent injection of resources towards an NCRIS Trust and Identity Accelerator and Incubator is needed.

A perishable opportunity to act now exists that would enable Australia to leverage the work of the European Union along with other international best practice systemic research infrastructure approaches to Trust and Identity. The benefits of acting now would result in:

- a key skills and expertise deficiency in the system being addressed
- research organisations and NCRIS capabilities having access to a world leading research specific access and authentication framework and support to use it
- enhanced capabilities for Australian researchers to participate in and collaborate with leading global research initiatives
- a more connected, efficient and integrated research infrastructure system
- safe and secure research infrastructure.

The AAF *Making the Case: An NCRIS Trust and Identity Capability* document outlines how the establishment and delivery of a NCRIS funded Trust and Identity program (consisting of an accelerator and incubator) is required now. An AU\$3.2M (year 1), AU\$3.3M (year 2), AU\$3.6M (year 3) investment is critical to help inform the longer-term needs of the NCRIS system. More detailed information can be found at: ncris.aaf.edu.au.



EXECUTIVE SUMMARY

Access, authentication and authorisation identity management was recognised as an important part of the National Research Infrastructure ecosystem in the first National Collaborative Research Infrastructure Strategy (NCRIS) Roadmap in 2006. The Australian Access Federation (AAF) was formally established in 2009 and received a one-off funding grant from the Commonwealth Government. Since then the AAF has established itself as a financially self-sufficient organisation that provides federated identity services which are used by every university in Australia and CSIRO and is globally recognised as a world leader in the space.

The AAF has not received any ongoing funding to support NCRIS and the research system. Without such funding the efficiency and effectiveness of the research system continues to be diminished and support for the research system is at risk. While NCRIS capabilities have been encouraged to use the AAF, historical investment in identity and access management within the NCRIS system has been disconnected and piecemeal in its nature. Individual capabilities often don't have the necessary skills, knowledge and experience to address their identity management needs. Identity and access management skills are scarce and research specific needs of the NCRIS system can't be addressed by universities. There has also been no way to nurture and retain these skills within the research and education system. At the same time, there has been a significant increase in cyber-attacks targeting Australia's Research and Education system, along with potential foreign interference. Sound identity management practices are an important part of protecting critical infrastructure and currently there is no strategy in place to help protect NCRIS.

More recently the Digital Data and eResearch Platforms (DDeRP) group (as outlined in the 2016 eResearch Infrastructure Roadmap as the AAF, AARNet, ARDC, NCI, and Pawsey Super Computing Centre) has unified to map the various components of the underpinning infrastructure that supports the research system with identity and access management being identified as a fundamental component of the system, and the AAF being the only provider of the underpinning infrastructure.

Internationally the European Union (EU) has developed the Authentication and Authorisation for Research Communities Blueprint Architecture which provides a technology neutral blueprint that standardises the implementation of Access and Authorisation Infrastructure. Combined with various reusable tools, modules and other initiatives in the USA and the rest of the world, Australia has an opportunity to leverage this work to fast track a world leading framework and approach to identity and access management for the NCRIS system and the research system more broadly.

The key components of a systemic capability for Australia would include:

- a Trust and Identity **Framework** for Research
- a series of **Trust and Identity Incubators** that work with cutting edge research infrastructure
- **re-usable software solutions, tools and modules** that could be used by research infrastructure providers
- **skills and expertise** for a cohort of identity and access management specialists that can work with and support the NCRIS system
- **Access and Authorisation Infrastructure** that builds on the AAF to support the unique needs of the research sector.

To deliver a Trust and Identity capability for NCRIS, a Trust and Identity Accelerator and Incubator program is needed. By taking advantage of the opportunities that are available to Australia today NCRIS can fast track the establishment of a system wide approach. This would greatly enhance the efficiency, effectiveness and resilience against cyber-attacks of the NCRIS system and provide much needed support. An AU\$3.2M (year 1), AU\$3.3M (year 2), AU\$3.6M (year 3) investment is critical to help to inform the longer-term needs of the NCRIS system.

BACKGROUND

The National Collaborative Research Infrastructure Strategy (NCRIS) since its inception has resulted in a national network of world-class research infrastructure projects. These projects support high-quality research that drives greater innovation in the Australian research sector and the economy more broadly.

To date, investments with NCRIS have been made through a suite of projects which are focused on particular domains or capabilities that align with national research priorities. Very early in the history of NCRIS, it was recognised that the NCRIS system needed a number of system-wide foundational capabilities, including but not limited to compute (both High Performance Computing [HPC] and Cloud), research data storage and research data management. Access, authentication and authorisation identity management was recognised as an important part of the National Research Infrastructure ecosystem in the first NCRIS Roadmap¹ in 2006. The Australian Access Federation (AAF) was formally established in 2009 and received a one-off funding grant from the Commonwealth to help with its establishment.

The AAF today is:

- part of a global network of over 61 federations around the world
- globally recognised as a world leader in enabling researchers to securely access Australia's national research infrastructure and global research infrastructure collaborations
- considerably influential within the international community
- on the steering committee for the international Research and Education Federations (REFEDS)² group
- Chair of the international eduGAIN³ Steering Committee
- delivering programs on behalf of the European Union (EU) within the Asia Pacific region as well as helping to establish a number of federations in the Asia Pacific region
- a world leader in verification services through its VeriFID Global⁴ program which the UK has recently licensed as a whole of country solution.

Following the first NCRIS Roadmap, identity and access management (IDAM) has continued to be an important part of the National Research Infrastructure in successive NCRIS roadmaps, including in the most recent 2016 NCRIS Roadmap. Despite this, the AAF does not receive any ongoing direct funding from the Commonwealth to support the needs of the NCRIS system. The AAF has become financially self-sufficient and independent for its core operations, but without funding to support NCRIS and the research system, the efficiency of the research system continues to be diminished and support for the research system is at risk.

For more information on the AAF, go to aaf.edu.au/media/2020/pubs/AAF_NCRIS_flyer_2019_FIN.pdf

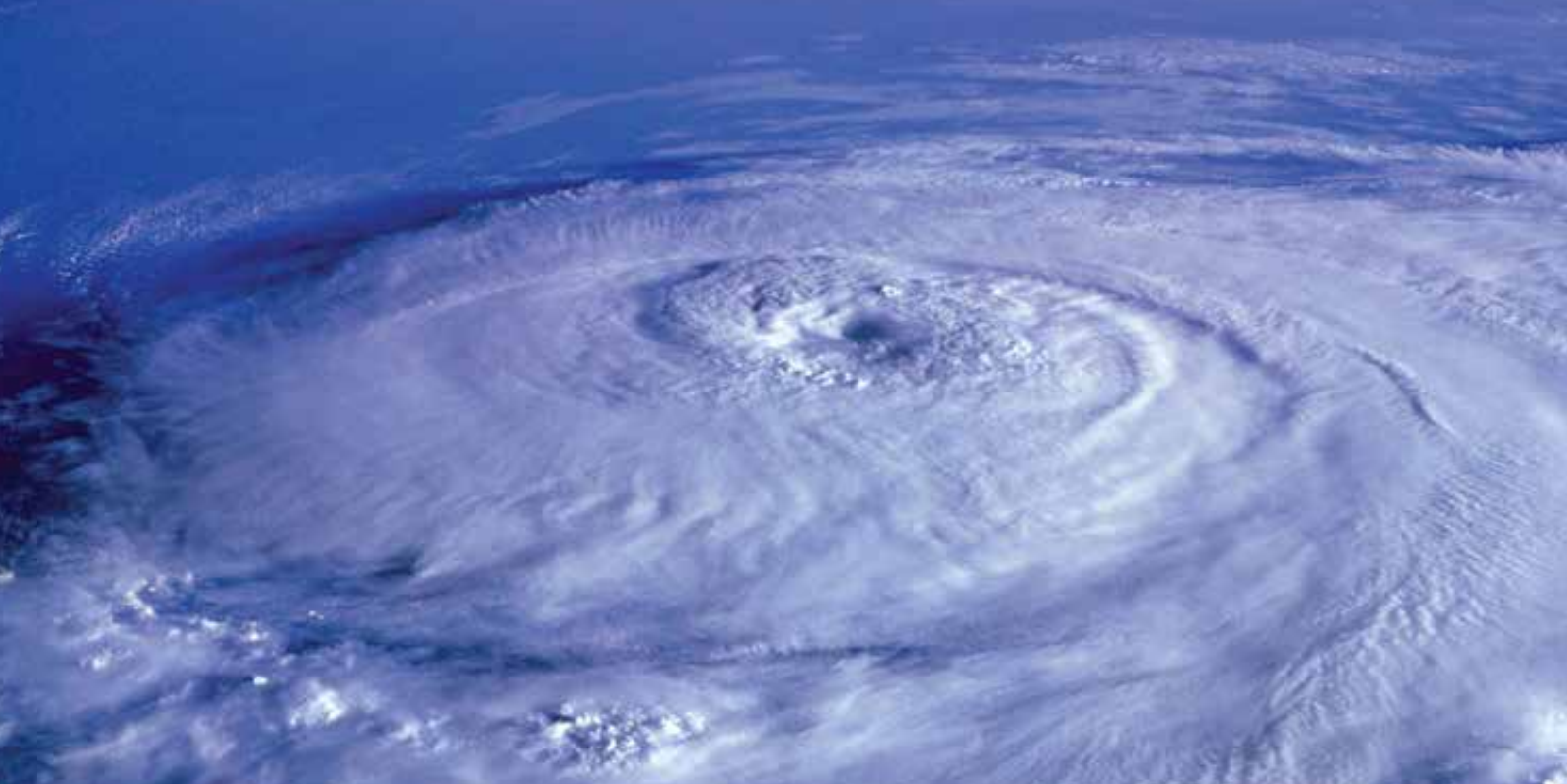


¹ <https://docs.education.gov.au/node/34113>

² <https://refeds.org/>

³ The eduGAIN interfederation service connects identity federations around the world, simplifying access to content, services and resources for global research – <https://edugain.org>

⁴ <https://verifid.global>



THE CURRENT ENVIRONMENT

AUSTRALIA

Identity and access management within the NCRIS system has historically been implemented as part of the services offered through:

- legacy initiatives such as the Australian National Data Service, National eResearch Collaboration Tool and Resources project and Research Data Services project
- National Computational Infrastructure (NCI)
- Pawsey Supercomputing Centre
- more recently, BioPlatforms Australia (BPA).

These efforts were often disconnected initiatives, with the AAF being engaged by projects on a piecemeal basis to address one-off identity and access management use cases. Across the NCRIS system, identity and access management has been an afterthought as research infrastructure has been created. Individual capabilities often don't have the necessary skills, knowledge and experience to design and implement identity and access management solutions, and understandably they focus their efforts within their domain of expertise. Whilst capabilities have been encouraged to use the AAF, without access to the necessary expertise, the barriers to adopting federated identity management that is interoperable across the NCRIS system have simply been too high.

As NCRIS capabilities update/evolve their infrastructure, they are using information and communication technologies, including Access and Authorisation Infrastructure (AAI) to transform the scientific process. This process of digitalisation has been recognised in the Organisation for Economic Cooperation and Development (OECD) Global Science Forum Paper on Open and Inclusive Collaboration⁵ as being one of the key elements of open and inclusive collaboration in science.

As an example, capabilities like Microscopy Australia are increasingly acquiring instruments which include technology that has access and authorisation infrastructure built-in or needs to be integrated with other access and authorisation infrastructure solutions. NCRIS capabilities also offer additional services, allowing researchers to process and visualise their data. These service offerings rely on access and authorisation infrastructure, not only to function but to ensure the right people access the right data.

Sensitive data has also emerged as a strategically important and growing area of need within the NCRIS system. Existing systems, such as SURE⁶, were developed as a standalone island of identity management without using the AAF. To successfully develop interoperable access and authorisation infrastructure solutions for sensitive data within the NCRIS system will require a set of skills, knowledge and expertise that does not exist in any one NCRIS capability or project.

⁵ https://www.oecd-ilibrary.org/industry-and-services/open-and-inclusive-collaboration-in-science_2dbff737-en

⁶ <https://www.saxinstitute.org.au/our-work/sure/>

At the same time, the prevalence of cyber-attacks has grown dramatically, with the Bureau of Meteorology and the Australian National University being two recent high-profile examples. Australia’s national research infrastructure faces similar challenges, with a significant amount of Australia’s research output being derived from data which sits on national research infrastructure. The commercial value of this data will continue to make this infrastructure a very attractive target.

More recently the Digital Data and eResearch Platforms (DDeRP) group

(as outlined in the 2016 eResearch Infrastructure Roadmap as the AAF, AARNet, ARDC, NCI, and Pawsey Super Computing Centre) has unified to map the various components of the eResearch Platforms that support the research system (Figure 1). This strategic mapping provides the roadmap for the overall environment and underpinning infrastructure along with clearly delineating the components each organisation has a core competency in delivering. Identity and access management is clearly identified as a fundamental component of the system, with the AAF being the only provider of the underpinning infrastructure.

DDeRP AREAS OF ACTIVITY OVERVIEW

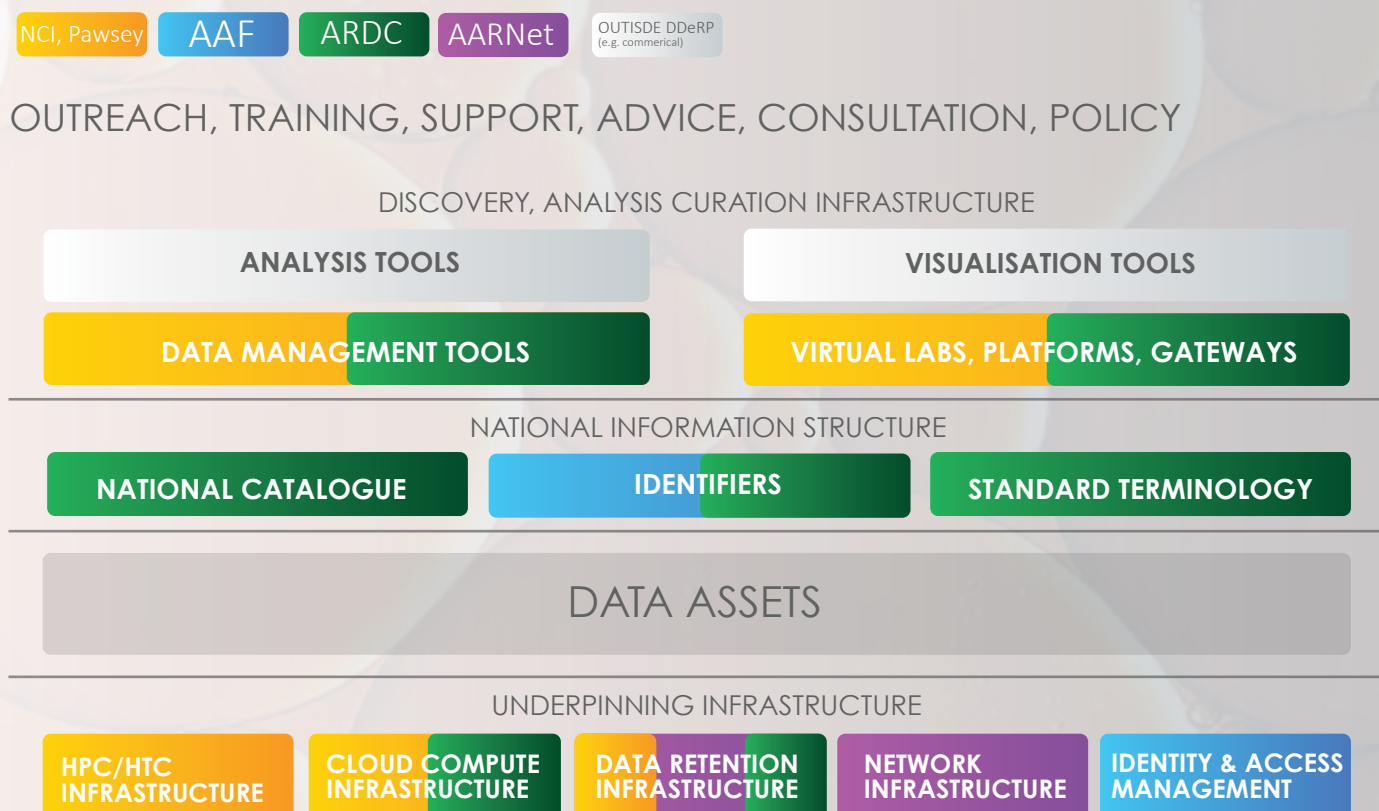


Figure 1 – Digital Data and eResearch Platform (DDeRP) components that underpin Australia’s eResearch

THE CURRENT ENVIRONMENT

INTERNATIONAL

The approach taken by the EU to advance their Access and Authentication Infrastructure currently represents the best approach being taken in the world, and offers an excellent framework that can be easily translated to an Australian context. A number of initiatives in the identity space in the USA and elsewhere offer innovative approaches for particular domains or disciplines without the same system-wide focus typically taken in Australia. The combination of the European framework approach with best practice domain or discipline approaches elsewhere in the world offers an interesting opportunity for NCRIS and the Australian research system.

Through Horizon 2020,⁷ the EU has established a long-running Trust and Identity Program. The AARC2 (Authentication and Authorisation for Research Communities) work package (as part of the program) aims to design a framework to develop interoperable AAI, enabling researchers to access the whole research and infrastructure portfolio with a single login identity.

Through the AARC2 program the EU has already funded a discovery phase which has resulted in the AARC Blueprint Architecture⁸ (AARC BPA) which provides a technology neutral blueprint that standardises the implementation of an AAI for research collaborations, accompanied by a set of policy documents and guidelines for its deployment. This AARC BPA describes a suite of customisable software modules that provide the necessary building blocks to effectively enable federated access management for local and international collaborations. EduGAIN was chosen as an underlying technology foundation to manage users' identities.

Building on the AARC BPA, the EU is now funding a program of work which is developing a cohort of AAI experts that are working with research infrastructure providers to help them successfully adopt the AARC BPA. EU-based initiatives, such as ELIXIR and EMBL (which Australian researchers engage with), are adopting the AARC BPA.

The Trust and Identity Incubator work package (as part of the EU Trust and Identity Program) provides specific funding to develop, foster and mature innovative ideas and approaches for research infrastructure. This is an important element as research infrastructure often sits at the cutting edge of technology, requiring new access and authentication infrastructure that the market and community is not able to provide.

Australia is already well aligned with the EU efforts. Much of the technology and approaches used by the AAF when it was established in 2009 were built on EU initiatives. Through a close partnership with key organisations in the EU, the AAF has maintained a level of alignment with the EU through its various programs of work when appropriate. Through its international leadership in the federation space, it also has strong connections with key players in the EU.

One key differentiator is that while the EU has been investing in specific programs for AAI, there has been no ongoing program of funding in Australia to enable a research system-wide approach to support the unique needs of the research infrastructure providers within NCRIS or across Australia.

INTERNATIONAL RESEARCHERS CAN NOW MAP THE UNIVERSE WITH MURCHISON

The Murchison Widefield Array (MWA) is one of Australia's leading radio telescopes enabling astronomers from around the world to explore the universe. Global collaboration is integral to the success of the MWA and researcher outputs. To ensure seamless and secure collaboration the MWA has connected to eduGAIN, a connection which is made possible by the AAF.

The MWA Director, Professor Melanie Johnston-Hollitt, said, "the eduGAIN connection is a vital service for an international collaboration like the MWA making it simple for our team of global researchers to access data from the telescope". Connecting the MWA to eduGAIN not only enhances and accelerates innovation in astrophysics, it enables borderless research.

⁷. The European Union (EU) Framework Program for Research and Innovation

⁸. <https://aarc-project.eu/architecture/>

CURRENT RESEARCH SYSTEM ENVIRONMENT

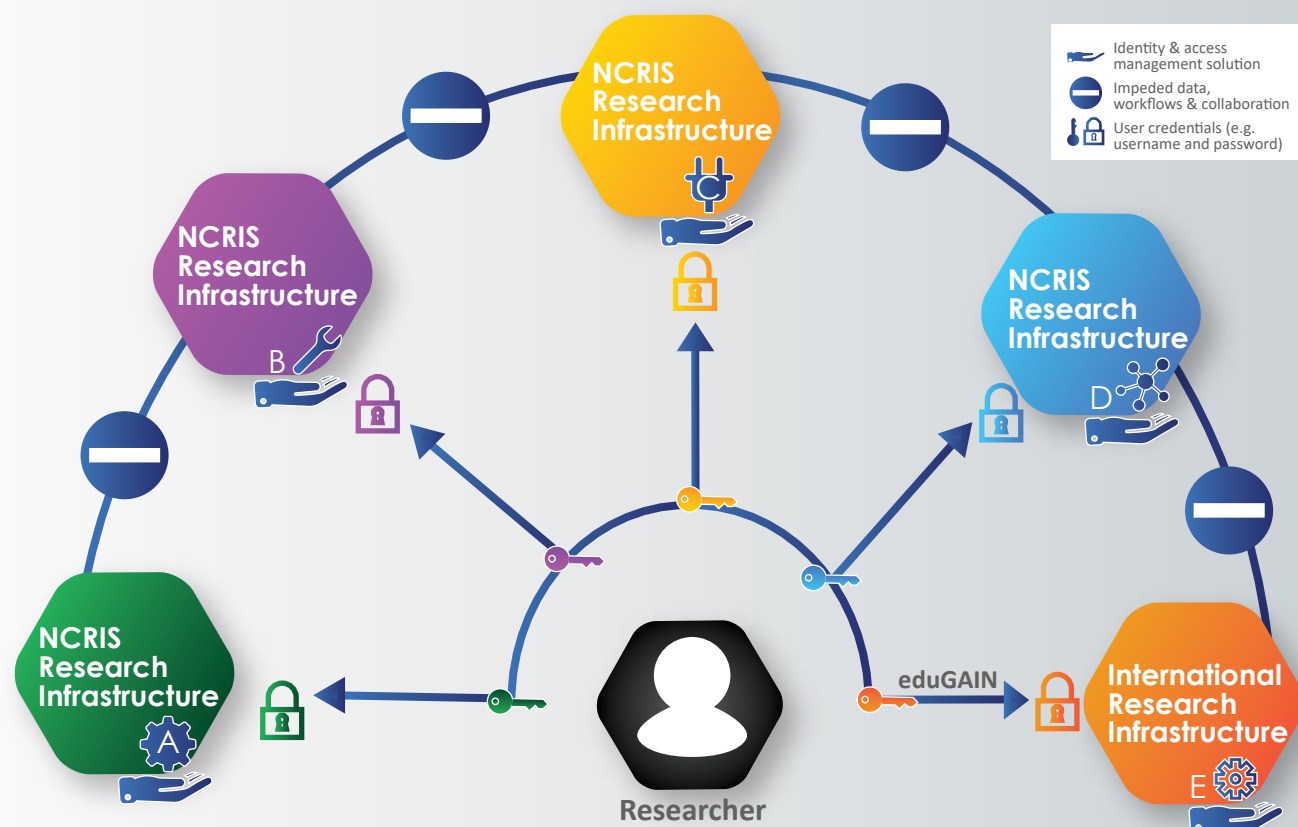


Figure 2 – The current environment where there is no common framework and each capability has different IDAM technologies and solutions, with researchers holding multiple identities and some systems with insecure backdoors.

IMPACTS OF THE CURRENT APPROACH

Choosing and implementing the most appropriate access and identity infrastructure requires a specialist set of knowledge and skills, which are in short supply. The complexity of research infrastructure goes beyond managing organisational identity management systems, which has traditionally been the purview of university information technology departments. It requires a complex combination of research specific processes, policies and technologies in order to work effectively. The scale and size of the staffing profile of many of the NCRIS capabilities means that it is simply not practical for each NCRIS capability to hire staff with the necessary skills. Likewise, individual universities are increasingly unable to provide the necessary research specific identity management skills nor are they able to act as an incubator for staff with the right skills.

RESEARCH IS INCREASINGLY MULTIDISCIPLINARY

Today's researchers employ a range of analysis techniques and methods that span different parts of the research infrastructure. For example, a researcher might undertake an initial analysis of their data as it streams off an instrument within the capability that supports the instrument. Before they apply a different set of analysis tools that reside in another capability, and end with a final analysis at their home institution, within the research cloud or national computational infrastructure.

With NCRIS projects implementing their own identity and access management solutions, the researcher has to navigate various disjointed identity and access management systems across different elements of the research infrastructure. The impact of this includes:

- reducing the opportunity for researchers to use innovative research methods that span multiple research infrastructures which reduces their ability to conduct world class research
- increasing the time that researchers spend gaining access to various elements of research infrastructure, affecting the efficiency of the research system
- making it more difficult to 'glue' individual pieces of national research infrastructure together into a seamless set of tools, further reducing the efficiency of the research system
- Australian research infrastructure being less interoperable with international research infrastructure, making it more difficult for Australian researchers to collaborate with their peers around the world
- research infrastructure that is less safe and secure, leading to an increased risk of cyber-attack and foreign interference.

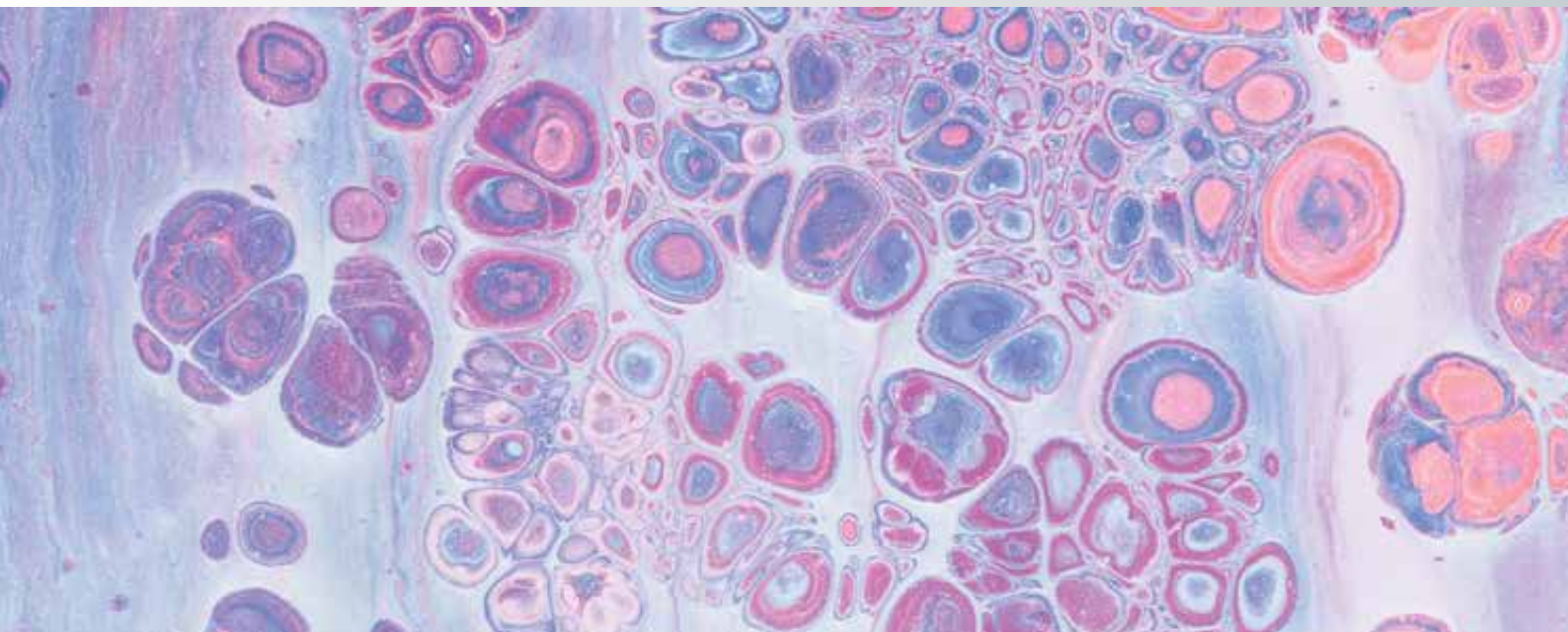
ENABLING A MORE INTERCONNECTED AND SECURE NCRIS SYSTEM

A system-wide holistic approach to identity and access management will ultimately lead to all NCRIS capabilities using a common Trust and Identity Framework for Research. This would result in standardised and interoperable access and authentication infrastructure connecting researchers nationally and internationally.

SKILLS AND EXPERTISE

The benefits would include:

- scarce identity and access management knowledge, skills and experience would be successfully sustained and nurtured, creating a pipeline of research specific trust and identity experts within the workforce
- NCRIS capabilities and research infrastructure providers would not need to recruit or retain trust and identity experts, allowing them to focus on delivering world-class research infrastructure
- the skills and expertise needed to address complex trust and identity issues associated with sensitive personal data would be retained within the NCRIS system, resulting in the alignment of strategies and solutions.



SUPPORT RESEARCH ORGANISATIONS AND CAPABILITIES

The benefits would include:

- the barriers to implement identity and access management solutions by NCRIS capabilities and research infrastructure providers would be greatly reduced
- NCRIS capabilities would be able to focus on delivering world-class research infrastructure and not need to divert precious resources to implementing access and authentication infrastructure
- NCRIS capabilities and research infrastructure providers could more easily participate in global research
- small research groups and organisations, along with commercial research groups who currently experience difficulties accessing national research infrastructure could more easily be part of the Trust and Identity Framework and leverage the research specific access and authentication infrastructure
- NCRIS capabilities and research infrastructure providers would have access to high quality support, assistance and expertise in the event that they experience cyber-attack, causing a data breach or compromised system.

ACCELERATING RESEARCH INTO OUR TOWNS, CITIES AND COMMUNITIES

The Regional Innovation Data Lab (RIDL), at Griffith University helps to build thriving communities by providing policy makers from local, state and federal governments, practitioners from industry partners such as Ausgrid and researchers with data to solve real world social planning problems. Facilitated by AAF's seamless login, RIDL accesses baseline data from NCRIS capability, AURIN (Australian Urban Research Infrastructure Network) to accelerate this research. AURIN's data enables researchers to make informed decisions about future infrastructure for urban environments using evidence-based analysis. "A primary consideration for AURIN is FAIR data access in a safe and secure manner for its research community. This requires high-quality trusted security solutions to be in place", said Professor Stuart Barr, AURIN Director. By leveraging the AAF to provide researchers across Australia with authenticated access to these data resources and tools, users can find the 'right answer' to Australia's social planning problems.

LEVERAGE GLOBAL CONNECTIVITY

The benefits would include:

- NCRIS capabilities and national research providers would be able to leverage the AAF's international connections, enabling researchers to more readily collaborate and participate with their global peers and research collaborations
- identity and access management solutions would no longer be bespoke or isolated, allowing interoperability with international research infrastructure
- the barriers for researchers to participate in global research efforts using Australian research infrastructure would be reduced.

CONNECTED RESEARCH INFRASTRUCTURE

The benefits would include:

- researchers would be able to access different parts of the NCRIS systems with ease, using the same institutional or organisational credentials
- various components of the national research system could be more easily 'glued' together to form an integrated research workflow, improving the efficiency of the system
- a more systematic view of who uses national research infrastructure could be achieved, enabling higher quality usage and statistical data to be automatically generated for research infrastructure providers and government
- alignment of national research infrastructure with the Commonwealth Government's Trusted Digital Identity Framework,⁹ enabling researchers to more readily access public data and policy makers to access research data to accelerate research and better inform policy development.

SAFE AND SECURE RESEARCH INFRASTRUCTURE

The benefits would include:

- there would be a greater degree of certainty that the right people are accessing research data and systems, lowering the risk of data breaches and foreign interference
- there would be a system-wide lift in the knowledge and practices around identity and access management, including awareness of good identity and access management practices across the research system
- the robustness of the identity and access management that underpins the national research infrastructure would be dramatically enhanced through the broad use of a common Trust and Identity Framework and access and authentication infrastructure
- cyber-attackers would be faced with an increased number of well defended targets that must be breached, as well as a dramatic increase in the complexity to successfully compromise the identity and access management component of any element of the national research infrastructure
- a proactive and effective cyber-security strategy would be in place to ensure the access and authentication infrastructure components of the system can successfully withstand any cyber-attack today and into the future
- strategies and practices could be implemented to ensure that breaches are detected on an ongoing basis.

BENEFITS



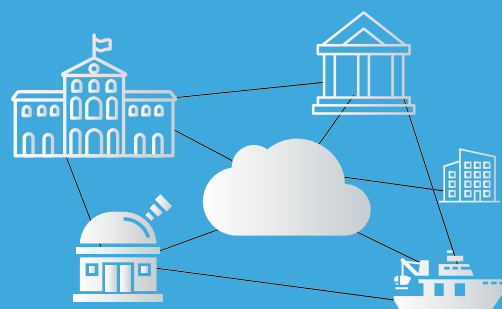
SUPPORT RESEARCH
ORGANISATIONS AND
CAPABILITIES



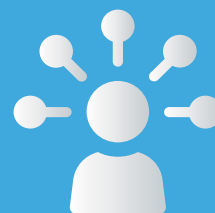
LEVERAGE GLOBAL
CONNECTIVITY



CONNECTING RESEARCH
INFRASTRUCTURE



SKILLS &
EXPERTISE



⁹ <https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework>

FUTURE RESEARCH SYSTEM ENVIRONMENT

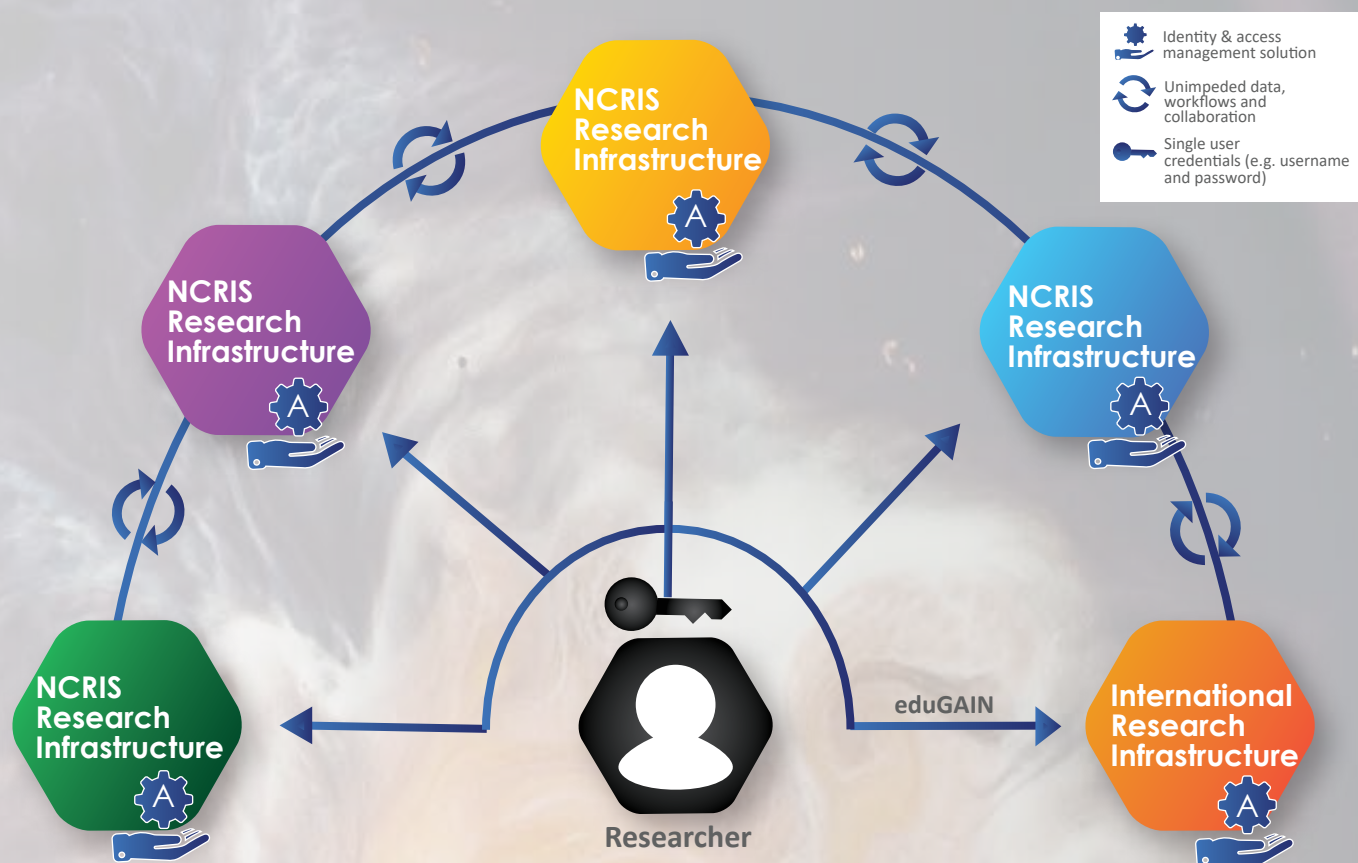


Figure 3 – The future where each capability adopts a common Trust and Identity Framework and uses interoperable access and authentication infrastructure, with researchers holding a single identity and all systems being more secure.

HOW A CAPABILITY WOULD HELP RESEARCHERS TACKLE COVID-19

Researchers at the University of Queensland working on a COVID-19 vaccine are already collaborating closely with Commonwealth Serum Laboratories (CSL), CSIRO as well as many other researchers around the world, including researchers at the Dutch company Viroclinics Xplore. All of these collaborations require the sharing of data, as well as reciprocal access to cutting edge research instruments and analysis tools. Allowing access to national research infrastructure by researchers from the EU for example, often comes with a high degree of administrative burden for research teams as they try and manage identities, credentials and access rights across disparate access and authorisation infrastructure. It can also make it difficult to connect cutting edge research infrastructure from two different research groups or countries to accelerate the research effort. Currently access to research infrastructure is often granted on an ad hoc basis, with no strategy or processes in place to ensure that access is subsequently revoked once the collaboration has been completed. This leaves Australia's national research infrastructure vulnerable to the wrong people subsequently having the wrong access to critical infrastructure and data.

An investment in an NCRIS capability would result in a systemic approach to access and authorisation infrastructure across the national research infrastructure that is well supported, making the process of granting access to other researchers such as those at Viroclinics Xplore easy, safe and secure. This would enable researchers to focus their efforts on cutting edge research problems. Whilst the search for a COVID-19 vaccine is a good example of the challenges researchers face and how a Trust and Identity Framework would help, the same benefits could be realised across almost all research domains and problems.

WHAT DOES AN NCRIS TRUST AND IDENTITY CAPABILITY LOOK LIKE?

The AAF is recognised as one of the leading federations in the world, and the work that has been done to build the AAF represents a strong platform which can be used to meet the needs of the NCRIS system today. AAF staff are well connected and have linkages to the international federation community that do not exist in any other organisation in Australia.

Building on the experience of the AAF and learnings from initiatives like the Horizon 2020 Trust and Identity program, Australia is well positioned to fast-track a system-wide initiative to build the necessary framework, building blocks and expertise to achieve a system-wide approach to identity and access management for research. With the EU forging ahead with the AARC BPA and the international connectiveness of Australian research, Australia has a fleeting opportunity to take its research infrastructure to the next level for the benefit of Australian researchers.

The time to act is now.

KEY COMPONENTS

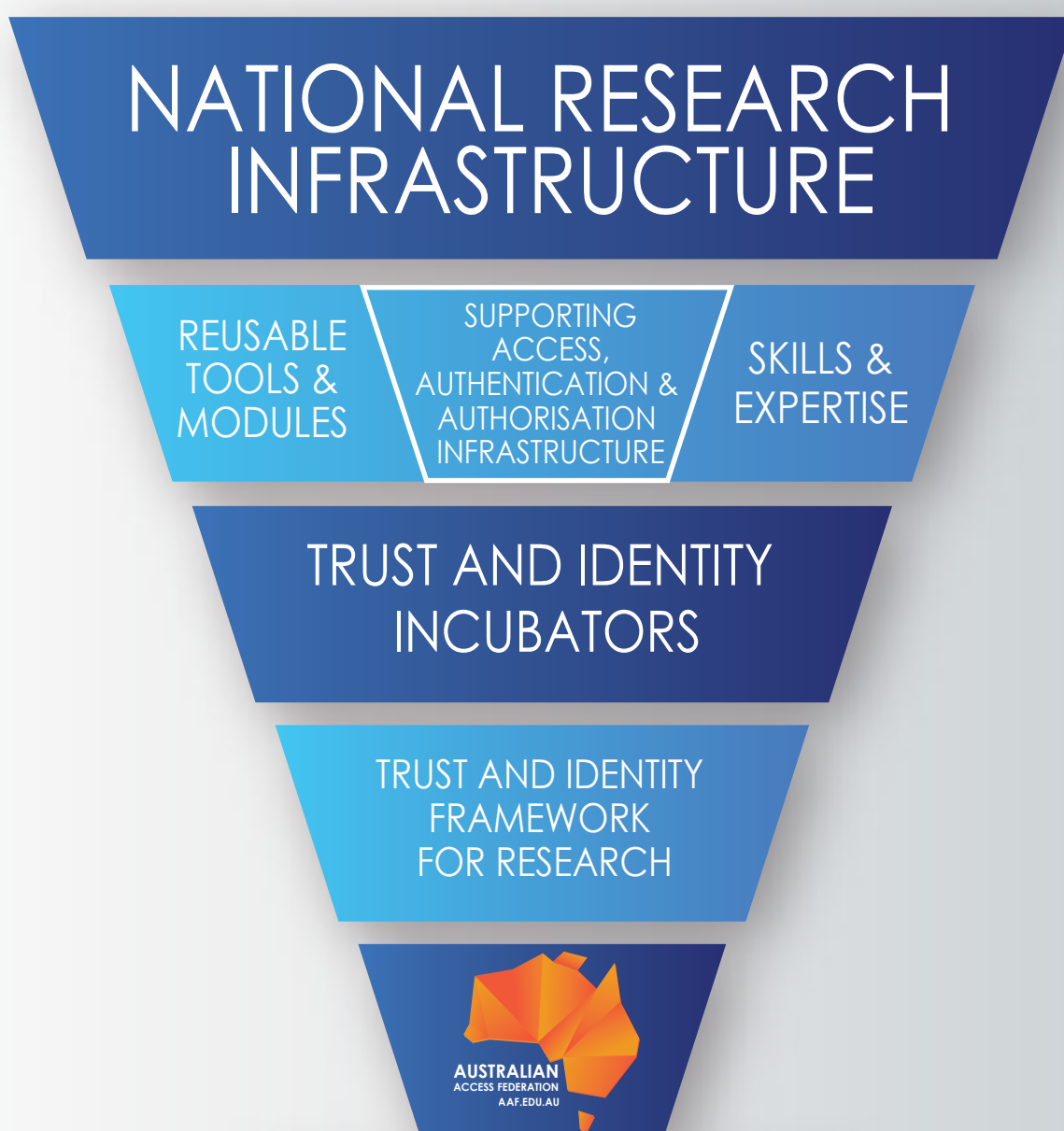


Figure 4 – Key components of a Trust and Identity Capability

KEY COMPONENTS

1
FRAMEWORK

A Trust and Identity Framework for Research which would guide identity, access management and authorisation for all research infrastructure providers.

2
**TRUST & IDENTITY
INCUBATORS**

A series of Trust and Identity Incubators to develop, foster and mature new ideas and approaches in trust and identity that work with cutting-edge research infrastructure.

3
**REUSEABLE
TOOLS &
MODULES**

A suite of reusable software solutions, tools and modules that could be used by research infrastructure providers.

4
**SKILLS &
EXPERTISE**

A cohort of identity and access management specialists that can work with research infrastructure providers to:

- assemble access and authentication infrastructure solutions, tools and modules in a manner that meet their unique needs
- assist research infrastructure providers with their implementation
- provide ongoing technical support for the solutions, tools and modules
- evolve and refresh the access and authentication infrastructure solutions, tools and modules to ensure the underlying technologies are up-to-date and are meeting the needs of the community.

**SUPPORTING
ACCESS,
AUTHENTICATION &
AUTHORISATION
INFRASTRUCTURE**

Additional access, authentication and authorisation infrastructure that builds on the AAF to support the unique needs of the research sector.

DELIVERING A SYSTEM-WIDE TRUST AND IDENTITY CAPABILITY FOR NCRIS

STAGE 1 – AN NCRIS TRUST AND IDENTITY ACCELERATOR AND INCUBATOR

An urgent three-year injection of resources towards an NCRIS Trust and Identity Accelerator and Incubator program would change the nature of what is possible from the Australian Access Federation and significantly benefit the NCRIS system and research sector more broadly.

ACCELERATOR

The intent would be to:

- take the European Union's AARC BPA framework, along with best practice examples from the USA and the world and adapt them where necessary to the Australian context
- build the necessary skills that span trust, identity and its application in a research context, through the creation of a cohort of identity and access specialists with an eResearch background, along with other specialists and support staff within the AAF that can directly assist NCRIS capabilities
- build on the work in the European Union and the rest of the world, bringing together a set of reuseable software solutions, tools, and modules along with the necessary research specific Access and Authentication Infrastructure.

INCUBATOR

The intent would be to:

- provide access to incubator resources to NCRIS capabilities. This will enable capabilities to adopt the framework and implement the necessary research specific tools, modules, software solutions and Access and Authentication Infrastructure. It will also deliver improved cyber-security and specific access, authentication and authorisation outcomes to address their needs.

The Accelerator and Incubator are framed around three years, with the view to establishing a review point to coincide with the scoping of new long term stable services for the NCRIS system and to extend over a National Research Infrastructure roadmap and response process, likely to occur in the next two years. It is proposed that it be governed by a steering committee structured as a sub committee of the AAF Board, with representation from NCRIS and external experts.

The cost to establish an NCRIS Trust and Identity Accelerator and Incubator is estimated to be AU\$3.2M (year 1), AU\$3.3M (year 2), AU\$3.6M (year 3).

STAGE 2 – OPERATING AN NCRIS TRUST AND IDENTITY CAPABILITY

The final resourcing envelope of Stage 2 will in part be informed by Stage 1. A key difference however, will be that the focus of Stage 2 will shift from helping individual NCRIS capabilities to implement new trust and identity solutions within the framework to supporting and extending these solutions across the entire NCRIS System. This would include, but is not limited to extending the functionality of current solutions, implementing new identity and access technologies and solutions as they emerge and assisting capabilities when they undertake major infrastructure refreshes.

Another key focus would be the ongoing maintenance of the trust and identity solutions implemented and the access and authentication infrastructure. This would include an ongoing proactive cyber-security program to ensure the integrity of the Access and Authentication Infrastructure is maintained and continues to ensure that the right people access the right infrastructure, analysis tools and data.

The cost to sustain an ongoing NCRIS Trust and Identity Capability is estimated to be 3% of the total NCRIS budget per annum.