AUSTRALIAN ACCESS FEDERATION

NCRIS National Research Infrastructure for Australia An Australian Government Initiative

AAF is enabled by NCRIS

[PDK05]

Acceptable Authentication Assurance Policy

Key questions to inform policy development:

- Which identity providers are acceptable for your infrastructure? SAML Identity Federation IdPs? Social providers such as Google, Facebook, etc.?
- How much certainty does your community require of the identity? Review each of the elements (personal accounts, uniqueness, freshness, vetting quality, and authentication strength). How will you validate this for each source of (federated) identity?
- How can you ensure that each user is covered by a security incident response capability at their home organisation?
- Do your services, or a subset, require multi-factor authentication?

The Australian Access Federation (AAF) recommends applying the Research and Education Federations Group (REFEDS) Assurance Profiles (RAF) Cappuccino or Espresso, in accordance with the requirements of the Collaboration. Note that RAF applies only to natural persons. Where a Collaboration wishes to allow the use of Hosts, Robots, or similar, an appropriate assurance profile will need to be identified and applied. This decision will need to be explicitly made by the Collaboration governance body and recorded. Refer also to AARC Guideline 21.

**Delete this box after completing the policy.*

1 Introduction and Purpose

1.1 Objectives

To protect its assets, Service Providers must authenticate, identify, and trace Users granted access to Collaboration Services. The authentication and identification must be sufficient to meet the requirements of the Security Policy and any specific ancillary policies, bearing in mind the nature of data stored within the Collaboration's infrastructure and the available authentication options.

1.2 Scope

This Policy applies to all Collaboration Service Providers and the Services offered to Users of the Collaboration.

1.3 Definitions

Authentication: The process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorised users or in a data authentication server.

REFEDS: Research and Education Federations Group

Additional terms are defined in the Top-Level Collaboration Policy.[1]

[1] [Link to PDK01]

Other Sources / Attribution / Acknowledgements: EGI Policy on Acceptable Authentication Assurance, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

2 Definition of Approved Authentication Assurance Services

The Collaboration applies REFEDS Assurance Framework v2.0[2] Identity Assurance Profiles (IAPs) relevant to the risk profile of the Services and/or data accessed and requires multifactor authorisation (MFA) for all Users:

- For high-risk use cases, RAF Espresso (IAP High) (`https://refeds.org/assurance/IAP/high`) and MFA applies (`https://refeds.org/profile/mfa`).
- For low-risk use cases, RAF Cappuccino (IAP Medium) (`https://refeds.org/assurance/IAP/medium`) and MFA applies (`https://refeds.org/profile/mfa`).

[The following is an adaptation of Appendix C of RAF 2.0, as an example of authentication assurance values a Community Manager would need to apply to a User's profile at registration and manage as part of the membership lifecycle]

In accordance with the following Reasons (#), a Community Manager guarantees its members (Users) (as defined in [eduPerson])

1. *Have unique non-reassignable identifier values,*
2. *Are ID-proofed face-to-face using a government-issued photo-ID and the attributes on the photo-ID are checked against an authoritative source, and*
3. *Are authorised to access Collaboration Services*

And for which the Community Manager or designated manager of such attributes:

4. *Promptly reflects departure or role change into eduPerson affiliation value(s)*
5. *Uses an identity management system which qualifies to the baseline expectations for Identity Providers, and*
6. *Implements an identity-proofing process which conforms to RAF 2.0 process-based criteria will assert the following claims for its Users as multiple values of the eduPerson Assurance attribute:*

Claim	***Reason (#)***
`https://refeds.org/assurance/version/2`	*6 (RAF 2.0, s4)*
`https://refeds.org/assurance`	*5 (RAF 2.0, s3)*
`https://refeds.org/assurance/ID/unique`	*1 (RAF 2.0, s5.1.1)*
`https://refeds.org/assurance/IAP/local-enterprise`	*3 (RAF 2.0, s5.2.2)*
`https://refeds.org/assurance/IAP/high`	*2 (RAF 2.0, s5.2.1)*
`https://refeds.org/assurance/IAP/medium`	*2 (RAF 2.0, s5.2.1)*
`https://refeds.org/assurance/IAP/low`	*2 (RAF 2.0, s5.2.1)*

[2] *REFEDS Assurance Framework v2.0*, https://refeds.org/wp-content/uploads/2023/12/RAF-2.0-Final-version.pdf

Other Sources / Attribution / Acknowledgements: EGI Policy on Acceptable Authentication Assurance, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

`https://refeds.org/assurance/ATP/ePA-1d`	*4 (RAF 2.0, s5.3)*
`https://refeds.org/assurance/ATP/ePA-1m`	*4 (RAF 2.0, s5.3)*
`https://refeds.org/assurance/profile/cappuccino`	*RAF 2.0, s6*
`https://refeds.org/assurance/profile/espresso`	*RAF 2.0, s6*

3 Operational Matters

<Authentication assurance will be propagated with the User's authentication token for Relying Parties to include in authorisation decisions.>

[OR]

<Only Users conforming to one of the approved authentication assurance profiles shall be granted access to Collaboration Services.>

4 Ancillary Policies

In specific cases, where a risk evaluation and assessment has been completed, the Collaboration may accept the application of different authentication assurance policies. These policies must meet or exceed the relevant RAF profile in line with the risk profile of the Services and/or data being accessed.

The Collaboration must maintain a registry of such policies, their area of applicability, and the term for which the ancillary policy may apply.

5 Associated Documents

5.1 Collaboration Policies

- Privacy Policy [PDK02]
- Policy on the Processing of Personal Information [PDK03]
- Acceptable Use Policy [PDK04]
- Membership Management Policy [PDK06]
- Service Operations Security Agreement [PDK07]
- Incident Response Procedure [PDK08]

AUSTRALIAN ACCESS FEDERATION

NCRIS National Research Infrastructure for Australia An Australian Government Initiative

AAF is enabled by NCRIS

Version Control

Document Control			
Document Approved:		**Date Effective:**	
Last Review Date:		**Next Review Date:**	
Version Control			
Version	**Author**	**Summary of Changes**	**Date**
1.5	AAF	Review and alignment of language, population of REFEDS examples. Refinement of context statements. Corrected attributions. Updated disclaimer.	March 2025

Other Sources / Attribution / Acknowledgements: EGI Policy on Acceptable Authentication Assurance, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).