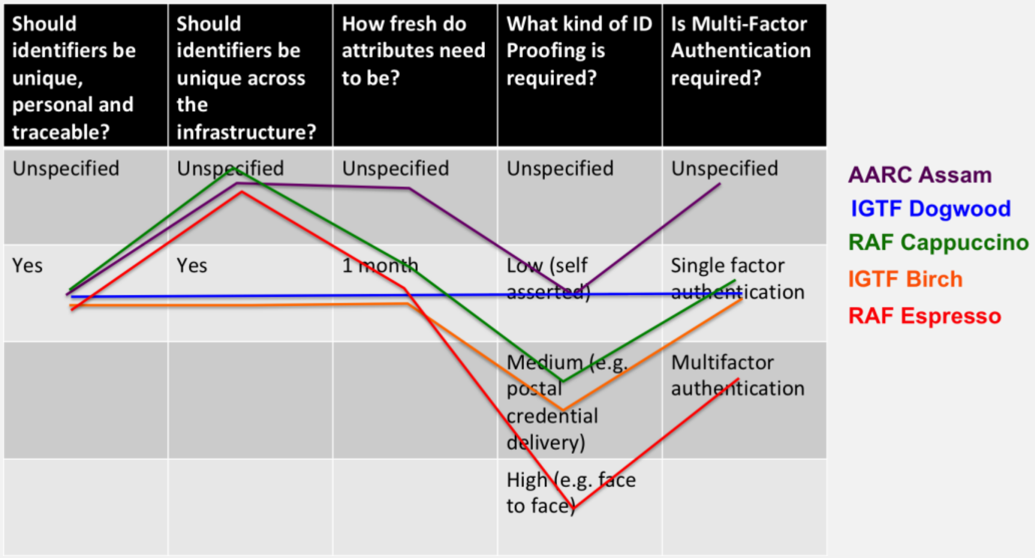
Questions to ask yourself when defining this policy:

- 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 following chart can be used to help determine an appropriate assurance profile for you. Refer also to AARC Guideline 21:



Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	

**delete this box after completing the policy.*

Acceptable Authentication Assurance Policy

This policy is effective from <insert date>.

Introduction

In order to protect its assets, the Infrastructure needs to authenticate, identify, and trace *Users* granted access to its *Services*. The authentication and identification must be sufficient to meet the requirements of the Security Policy and any ancillary Specific

Other Sources / Attribution / Acknowledgements: SCIv2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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).

Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.

Policies, bearing in mind the nature of data stored within the Infrastructure and the available authentication options.

Definition of approved authentication assurance sources

<Enter the details of the Assurance profiles relevant for your infrastructure, as defined in AARC-G021. When using the REFEDS RAF profiles Cappuccino and Espresso, also define whether single or multi-factor authentication is required.>

Operational matters

<Authentication Assurance will be propagated with the user's authentication token for relying services to include in Authorisation decisions.>|<Only users conforming to one of the approved authentication assurance profiles shall be granted access to the Infrastructure.>

More-specific policies

For specific cases, a risk evaluation and assessment having been completed, different authentication assurance policies may apply. The Infrastructure shall maintain a registry of such specific policies and their area of applicability.

Other Sources / Attribution / Acknowledgements: SCIv2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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).

Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.