e-Researcher-centric policies

e-Researcher-Centric Policies - develop the policy framework for communities, providing recommendations for baseline "policy profiles" for users, communities and identity providers, and, through such harmonisation, will reduce the "policy silos" that hinder interoperation. The policy profiles will be defined in close interaction with European and global stakeholders, specifically the e-infrastructures and research infrastructures, so that in the AAI ecosystem every participant is able to rely on well-defined predictable behaviour by the other participants in the infrastructure.

An overview of the work on researcher-centric policies is now available in the project deliverable "Recommendations for e-Researcher-Centric Policies and Assurance" (DNA3.4).

Acceptable Use Policy Development

AUP Alignment Study

Security for Collaborating Infrastructures Trust Framework says: *"Each infrastructure has the following: ... An Acceptable Use Policy (AUP) addressing at least the following areas: defined acceptable and non-acceptable use, user registration, protection and use of authentication and authorisation credentials, data protection and privacy, disclaimers, liability and sanctions" (SCI Version 2 section 6).* The AARC2 AUP alignment study aims to draft a common minimum, or 'baseline', AUP text to satisfy these requirements thereby facilitating rapid community infrastructure 'bootstrap', easing the trust of users across an infrastructure and providing a consistent and more understandable enrolment for users as users move between communities and project. More information can be found at the links below.

Baseline AUP and the implementers guide

The WISE Information Security for E-infrastructures (WISE) community SCI working group has hosted the work on the baseline AUP, with the intent of this baseline becoming a globally accepted set of points that facilitate the research workflows.

- WISE Baseline AUP specification

A draft of the implementors guide for the AUP was developed to accompany the document. It elucidates the applicaiton model of the AUP to community-first (like the Life Sciences AAI or WLCG) and user-first (such as CheckIn and eduTEAMS) membership management services.

- Implementers Guide to the WISE Baseline Acceptable Use Policy (AARC-I044)

AARC2 NA3 team working text, including active comments and version history, is stored here. (Please see the stored Version History for the recent evolution of this text.)

Baseline AUP study input

Community /Infrastructure	Policy Link	Comment
BBMRI	Acceptable Use Policy of BBMRI-ERIC Services Harmonised Access Procedure to Samples and Data European Charter for Access to Research Infrastructures	Received from Petr Holub (15/1/18)
CTSC (template policy)	Acceptable Use Policy Template	Linked from Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects as google doc.
DAFNI (UKRI)	RCUK_AcceptableUseICTSystemsServices.pdf	Downloaded from STFC homepages 1 November 2014
EGI	Acceptable Use Policy and Conditions of Use	Linked from EGI Approved Security Policies Also now at AARC Acceptable Use Policy (JSPG Evolved version)

ELIXIR	Acceptable Usage Policy and Conditions of Use	Based on the Acceptable Usage Policy of EGI, March 2015.
EUDAT	EUDAT Services Terms of Use	Linked from EUDAT homepage footer
HBP collaboratory	Terms and Conditions for Service	Version 1, released on 30 March 2016
OSG Connect	Open Science Grid User Acceptable Use Policy	Linked from OSG Security Policies
Prace	PRACE Acceptable Use Policy (Sept 2014)	Downloaded from 2014-09-08-PRACE-Acceptable-Use-Policy.pdf
SURF	Model Acceptable Use Policy for employees Model Acceptable Use Policy for students	Links provided by Alf Moens (8/2/18)
XSEDE	XSEDE Acceptable Use Policy	Linked from XSEDE documentation web pages
...		

- Google spreadsheet of AUP comparison (01/04/2018) with summary table -

Baseline AUP presentations and other materials

- Presentation of AUP alignment work in progress at the WISE security group meeting in Abingdon, UK 27/2/2018
- Presentation of AUP alignment work at AARC2 third project meeting in Athens, Greece 10-13/4/2018 and 43rd EUGridPMA meeting in Karlsruhe, Germany 23-26/5/2018 with additional material
- Presentation of AUP alignment work at EOSC-hub/AARC2/EGI/EUDAT/WLCG Joint Security Policy Workshop at CERN, Switzerland 18-20/7/2018
- Presentation of AUP alignment work given by Dave Kelsey at the WISE session at the 2018 NSF Cybersecurity Summit in Alexandria, VA, USA 21/8/2018
- Presentation of AUP alignment work at the 44th EUGridPMA meeting in Toulouse, France 26/09/2018
- Resulting AUP document (v1.2) after discussions at the EOSC-hub/AARC2/EGI/EUDAT/WLCG Joint Security Policy Workshop at Forschungszentrum Jülich, Germany, 14-16/11/2018
- Discussions at the AARC2 Fourth Meeting at Reti, Busto Arsizio, Italy, 19-22/11/2018 resulted in the drafting of AARC-I044 Implementers Guide to the WISE Baseline Acceptable Use Policy (preliminary) formatted document here.
- Discussion of adoption and sustainability of AUP and other AARC outputs at 45th EUGridPMA meeting at CERN, Switzerland 21-23/01/2019
- Resulting draft WISE AUP document (v1.3) after discussions at the EOSC-hub/AARC2/EGI/EUDAT/WLCG Joint Security Policy Workshop in Abingdon, UK 19-21/02/2019

Identity Assurance for collaborative use cases

Inventory of high-assurance identity requirements from the AARC2 use cases

This document and the associated Wiki page provide an inventory of currently identified use-cases where there is a requirement that the identity of a user accessing data or using a system or an instrument is assured with higher confidence than provided by an identification consistent with the REFEDS Assurance Framework “Cappuccino” assurance profile.

Identified use-cases come from the life sciences domain, driven by legal restrictions on the processing of human personal data. Assurance requirements include the use of multi-factor authenticators and improved “freshness” of the user’s affiliation.

Milestone Document AARC2-MNA3.5 (submitted Jan 2018) referencing wiki page with requirements identified from use-cases. Futher requirments may be added if identified during the project.

Assurance Frameworks

The e-Researcher task also contributes to the Assurance Framework activities in REFEDS (the REFEDS Assurance Framework RAF), the RAF Piloting activities, and the inter-infrastructure exchange of assurance profiles

- http://refeds.org/assurance (REFEDS Assurance Framework)
- https://wiki.refeds.org/display/GROUPS/Pilot+on+RAF+and+SFA
- Exchange of specific assurance information between Infrastructures (G021)
- Expression of REFEDS RAF assurance components for identities derived from social media accounts (G041)
- Assurance framework comparison diagram (Assurance Spaghetti)

Federated Identity Management for Research (FIM4R)

The AARC project has identified FIM4R as the primary mechanism for Community Engagement, and decided to support the reinvigoration of the group by supporting the showcasing of cross-domain demonstrators (the AARC pilots), by promoting its meetings in both Europe and globally, and by encouraging all communities to review and assess the original requirements and chart the way for the future FIM developments for research and collaboration.

We refer to the FIM4R web site and the FIM4R White Paper version 2 for further information.

Other NA3.3 work items and documents

- TNA3.3 - Researcher-centric policy - Input to NA3 meeting - 25 July 2017