Policy and Best Practice in AARC2's Year 1

Publication Date	2018-04-30
Authors:	David Groep
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	T0
Lead Partner:	Nikhef
Document Code:	AARC2NA3-20180430

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract

The Policy and Best Practice Activity in AARC2 aims to minimise the number of divergent AAI policies and to empower identity providers, service providers and user communities to identify interoperable policies for the open science vision.
In this document we review the progress made and show the highlights of the first year of the AARC2 project.

1. Introduction

The work carried out in NA3 was organised in four tasks. The main focus of this workpackage is to provide the necessary policy support to those infrastructures that are implementing an AAI that is compliant with the AARC BPA, and to the use cases and pilots in SA1. This workpackage offers a very effective way to ensure that best practices and AARC relevant policy frameworks are followed when the AARC BPA is deployed. The workpackage provides also consultancy to those infrastructures that require it, and takes care of global policy liaison activities.

2. Operational Security and Incident Response

Executed primarily by CERN, KIT, and Nikhef

This task extends the *Sirtfi* work and adoption in the research collaborations. In PY1 the focus was on using the deployment of Sirtfi in production federations by testing the incident response model (communications and the mitigating actions) developed in AARC1 by simulating actual incidents. In particular cross-federation and cross-community aspects were evaluated: the simulated incident involved different research infrastructures (WLCG, LIGO) and a generic e-Infrastructure service (RCauth.eu), spanned four identity federations, and two continents (to see the effect of time zone differences on communications). The report shows Sirtfi in itself is working, yet also highlighted points for improvement: raised awareness of the procedures, need for federation (not identity-provider level) security contacts, and necessary evolution of the central response capabilities.

Sirtfi adoption was supported by both training and by specific consultancy so that it becomes a basic element of complementary policy efforts (it is e.g. incorporated verbatim in the work done by GN4 on the Data Protection Code of Conduct, and in the LSAAI Policy Recommendations)

The extension of operation security elements to the community services (attribute authority operations) and to the operation of Proxies has been targeted for PY2.

3. Service Centric Policies

Executed primarily by KIT, Jülich, Nikhef, and STFC.

Initially targeting the data protection in traceability and in sharing of accounting records, it became clear in PY1 that many of the research infrastructures involved at this point in time need guidance on personal data protection and “GDPR” issues at an earlier stage in the process. While ‘resource usage accounting’ is the most visible place where personal data is collected and stored for a longer period of time, the same (but still rather limited) set of attributes is processed prior to infrastructure use. Retaining the focus on the processing of

personal data that are a result of or a prerequisite for the use of Infrastructure itself (i.e. it does - on purpose - not concern itself with personal data that may be contained within the research data), in the initial phase we provide guidance and methodology for performing the required *risk assessment* for processing of personal data by the research Infrastructures – which is an underpinning ingredient to the balancing test required when using legitimate interest as the basis for processing (which is the model used by the GEANT Data Protection Code of Conduct).
Despite the significant amount of uncertainty about the interpretation of GDPR at the moment (and different member states *still* giving conflicting and confusing guidance even about the processing in academia and research collaborations), the scoped deliverable DNA3.1 (initial phase) supports the execution of the risk assessment by communities and infrastructures and helps them explain the decisions taken to their users.

Guidance for proxy operations and cross-infrastructure harmonisation was developed to complement the work in JRA1. This includes specific recommendations on how to use assurance profiles between infrastructures (Guideline G021), the treatment of social identities (G041), and targeted guidance for the LSAAI Proxy operators - supporting the SA1 pilot - in “Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)” (G040).

The cross-infrastructure policy mapping framework, and development of the assessment methodology based on the Security for Collaboration among Infrastructures (SCI) framework (and looking at the relative comparison between the effectiveness of peer-reviewed assessment and adoption of standards-based methodologies like formal ISO 27k audits) is schedules for PY2.

Specific work on data protection for complex communities (i.e. communities with internal structure and intra-community control requirements) and aggregations of accounting data is scheduled for PY2 as well, but the effectiveness hereof will be continuously monitored to make sure the need foreseen in the AARC2 proposal actually materialises in the community pilots or in operational infrastructures.

4. e-Researcher Centric Policies

Executed primarily by STFC, BBMRI, EMBL(CSC), KIT, and Nikhef.

The work on assurance levels was performed in the context of the REFEDS Assurance Framework (RAF) working group. Aiming to define assurance components as well as a limited set of ‘profiles’ incorporating specific combinations of identity assurance), it has to balance community and infrastructure requirements with feasibility of getting assurance components expressed by institutional identity providers through federations. Additionally, it has to work within the constraints of a standards ecosystem that separates authentication strength (single- or multi-factor tokens) from other assurance elements (identity vetting, unique identifiers, freshness of information). Although the high-level concept is well developed and significant effort has been put into coordination with the REFEDS SFA and MFA specification work, the work is still ongoing. In order to gain operational experience, a

pilot has started with both European and US institutions to evaluate deployment feasibility of the RAF assurance elements in existing home organisations.

An extensive study of existing Acceptable Use Policies (AUP) was undertaken to perform a gap and complementarity analysis. The intended outcome of the study is an aligned AUP that allows a layered approach to the construction of an AUP, where the AUP presented to the end-user (at community enrolment or later) comprises a generic AUP component, that is common to all (global) e-Infrastructures, plus a section with community-specific additions. The study is available (https://wiki.geant.org/pages/viewpage.action?pageId=86736956) and will be the basis for international consensus work on, what is intended to be, a joint AUP base texts.

The assurance model and community-specific parts of the AUP (or 'terms and conditions of use') was also evaluated against sensitive data use cases, in particular in the context of BBMRI. This in particular clarified the targeted guidance for the operators of the Life Sciences AAI in which elements of the AUP to present at which stage of the user enrolment process.

In close collaboration with the EGI-ENGAGE and EOSC-HUB projects, two community framework policies were developed that support research infrastructures in securely managing the community attribute repositories, and in aligning community membership management processes so that users can seamlessly use generic e-Infrastructures without the need for explicit sign-up (https://wiki.geant.org/display/AARC/Community+Policy+Framework+Development).

The high-assurance use cases and validation of the intra-infrastructure and REFEDS RAF assurance profiles for working in research communities dealing with sensitive (human) data is scheduled for PY2. Further work on community policy alignment and baseline AUP will also continue.

5. Policy Development Engagement and Coordination

Executed primarily by STFC, CERN, EMBL, KIT, Nikhef, and Jülich.

To promote policy baselines and interoperability across infrastructures, a *Policy Development Kit* (PDK) was built in support of both training activities as well as to act as a repository for infrastructures and communities to use as a source of current best practice templates (https://wiki.geant.org/display/AARC/Policy+Development+Kit).
Bringing together work from the other tasks within NA3, but also looking further afield at the work in WISE (wise-community.org), EGI, EUDAT, PRACE, REFEDS, and CTSC (and US NSF initiative), it comes with a process to identify and classify the community to determine policy needs, and training modules (developed jointly with NA2) and targeted consultancy where appropriate.

The PDK is in continuous evolution and will continue to be an important activity also in PY2, during which it will be trialled with specific European as well as national communities.

Collaboration with the IGTF has brought in additional support and expertise in policy assessment methodology (leveraging structured peer review and assessment matrices) and renewed development of security and operational policies around attribute authority operations and trusted credential stores – which were applied to the BPA proxy elements for token translation (TTS) and credential management for RCauth.eu-issued PKI user credentials. REFEDS continues to provide a key mechanism to both gain adoption of AARC policies and concepts, but is also an important source of input to gauge feasibility of policies directed towards the identify federations and home organizations.

The FIM4R (Federated Identity Management for Research, see fim4r.org) group was strongly reinvigorated with the support from NA3, resulting in a new White Paper bringing together FIM requirements from a much broader range of research infrastructures (from the “Arts and Humanities” to the “Virtual Atomic and Molecular Data Centre”). Although very much a collaborative effort with inputs from many individuals and projects, it is essential for AARC’s harmonization effort and the new white paper provides both a basis for targeting new activities as well as a means of measuring the results of the technical and policy alignment achieved). As such, FIM4R is an essential mechanism for AARC and NA3 to steer developments – which more than justifies the effort invested in bringing these very disparate communities together in expressing their AAI and policy requirements.

The task also supports harmonization of all AARC outputs through the Guidelines mechanism, which makes policy (and technical) recommendations easier to locate and re-use and apply.

Table of Contents