EPJ Web of Conferences **245**, 03018 (2020) https://doi.org/10.1051/epjconf/202024503018
CHEP 2019

Building an IRIS Trust Framework

David Crooks[1,*], *Ian* Neilson[1], *David P.* Kelsey[1], and *Ian* Collier[1]

[1]UKRI STFC Rutherford Appleton Laboratory, Harwell Campus, Didcot, Oxfordshire OX11 0QX, United Kingdom

Abstract. IRIS is the co-ordinating body of a UK science eInfrastructure and is a collaboration between UKRI-STFC, its resource providers and representatives from the science activities themselves. We describe an ongoing project to build a security policy trust framework suitable for use across the IRIS community using the AARC Policy Development Kit. Derived from existing practice, the AARC PDK aims to assist in efficiently bootstrapping a Research Infrastructure in the operation of an authentication and authorisation infrastructure in line with the AARC Blueprint Architecture, making resources accessible to researchers in an easy and secure fashion.
We document the experience gained to date by the IRIS community in adopting component policies of the AARC PDK to build a trust framework to form a foundation for resource sharing, access and trust for a national infrastructure collaboration.

1 Introduction

IRIS[1], eInfrastructure for Research and Innovation for STFC, is a loose collaboration of science activities and provider entities in the UK, primarily driven by the physics communities supported by UKRI-STFC[2]. It does not run an infrastructure directly - it is not a project in that sense - but instead commissions the deployment of resources available to all of its collaborators. One example of this is IRIS 4x4, which is a capital project coordinated by IRIS. Funded by UKRI-STFC at a level of £4 million per year for 4 years, this project can issue grants for equipment and grants to make tangible assets; an important caveat of this is that it has no funding for operations.

In this paper, we discuss the current work to provide IRIS with an appropriate set of security policies (the IRIS Trust Framework) by using the AARC[3] Policy Development Kit as a starting point, along with an examination of appropriate next steps.

2 The AARC Policy Development Kit

The first task for the IRIS Trust Framework team was to identify an appropriate roadmap and existing activity that could benefit this work. An important consideration is the nature of IRIS as a set of distributed communities and service providers, as is the deployment of an identity proxy to provide authentication services for the community, IRIS-IAM. This immediately

*e-mail: david.crooks@stfc.ac.uk

framed the policy work in the context of a federated infrastructure landscape and, in turn, this suggested the AARC Policy Development Kit as an appropriate starting point.

The AARC Policy Development Kit (PDK) provides help in bootstrapping infrastructure policy on two levels. Firstly, the scope of the PDK encapsulates experience of the various policy domains which should, ideally, be addressed in the formulation of a 'complete' policy framework. Secondly, the individual documents are structured as templates, providing guidance as to relevant questions which should be asked and the resulting policy statements which might be made, within each policy as it is written for the target infrastructure.

To better understand the PDK, including the current objectives of the IRIS Trust Framework activity, Figure 1 attempts to show the relationships between the documents and to place the documents of the kit within a wider context. PDK templates explicitly link to other, external documents and less well defined structures or concepts. For example, the "Top Level Infrastructure" template refers to "Local Policies" and the "Service Operations" template to "IT best practices". What requirements are placed on these external sources is not closely defined.

In reviewing the links between the documents the PDK is seen not to be self-consistent as reference is made to "Traceability and Logging" and "Community Operations Security" policies, templates for which are not included in the kit. It should also be noted that not all PDK documents are policy texts: the "Incident Response Procedure", stand-alone "Risk Assessment" and the "Privacy Statement" documents provide template guidance but are not intended to be adopted as policy per se.

3 Initial choice of policies

An initial policy sub-set for IRIS was chosen to consist of a Top Level Infrastructure Policy, an Acceptable Use Policy (AUP) together with a Privacy Notice (PN). The choice to pursue early versions of an AUP and PN in the first instance came from the deployment of, as mentioned earlier, a IRIS Identity and Access Management service (IAM) in support of the lifecycle of users of the infrastructure (i.e member registration and renewal). The presentation of a PN to users at registration is a legal requirement coming from GDPR[4]. Draft versions of these documents are, at time of writing, out for community comment within IRIS.

Although, as can be seen from Figure 1, linkage to other PDK templates from the Top Level Policy is relatively low, its reference to external frameworks SNCTFI[5], SIRTFI[6] provides important context by standardising requirements. Also, the ongoing process of formulating a Top Level Policy has provided focus for defining appropriate management structures within the project.

4 Feedback and response

Early feedback during the IRIS community consultation period on the Top Level Policy indicated that, whilst the PDK template provided useful structure and guidance, it is uneven in its coverage. For instance, it was felt that outlining roles and responsibilities only for Management and Security Contact roles, having defined, in addition, Users, Communities and Service Providers was insufficient. In contrast, too much emphasis was given to Physical and Network security sections. Some 're-balancing' and expansion of the template text has been achieved by the IRIS Trust Framework team and it is hoped to feed this back into the PDK.

The PDK template AUP is the Baseline Acceptable Use Policy and Conditions of Use (version 1.0) from Wise Information Security for Collaborating e-Infrastructures (WISE)[7] and, as such, has been subject to wider scrutiny than much of the rest of the PDK. Its use

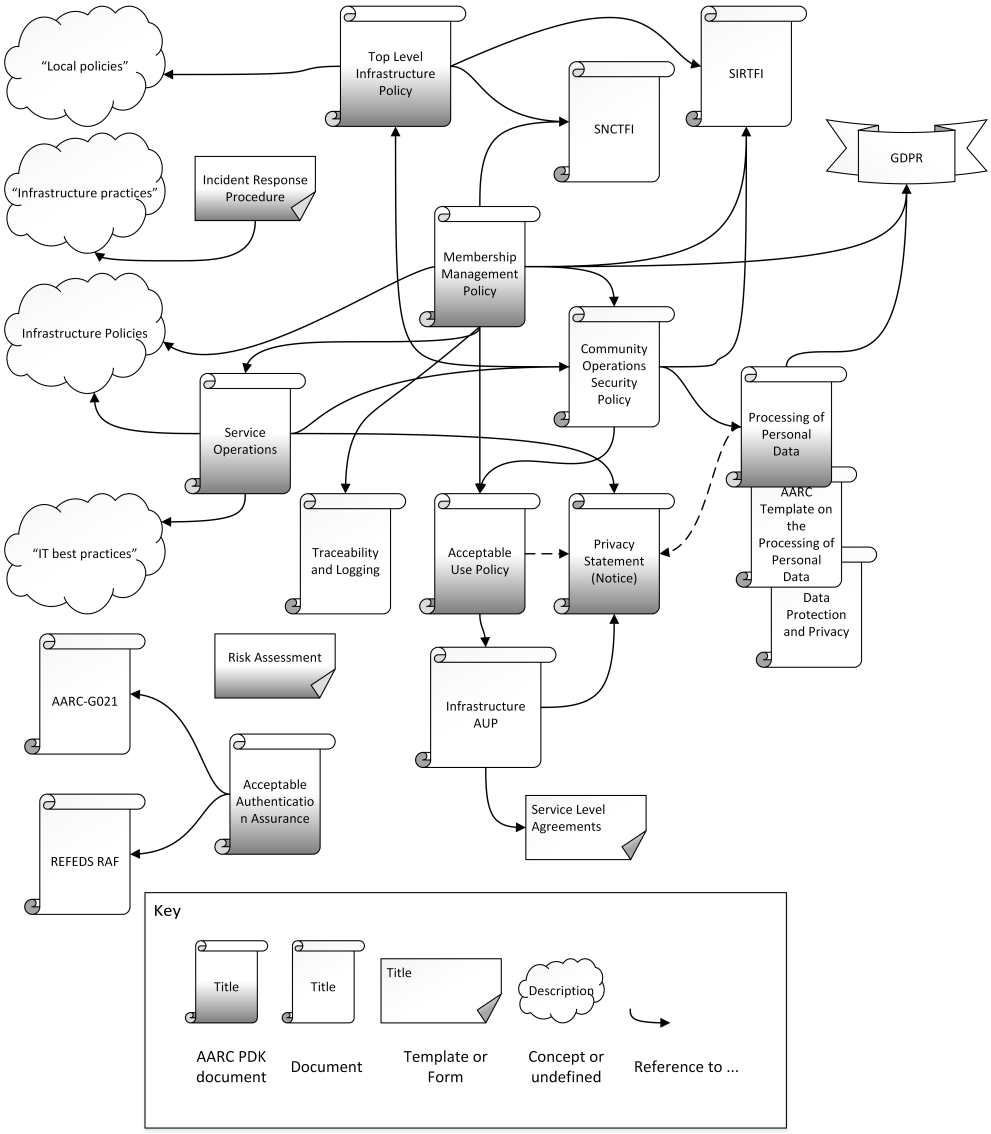

Figure 1. Relationships between the AARC Policy Development Kit and other documents

is also intended to be more constrained than other PDK templates in that it defines a core (baseline) set of clauses which should not be modified. The WISE Baseline AUP is intended to place a common set of behavioural expectations and obligations on users as they register to use an infrastructure and, with wide, cross-infrastructure and community acceptance of these core constraints, assist both user experience and their inter-infrastructure mobility, and, ultimately, the security of all participants. No significant blocks have been identified to date with IRIS adopting the WISE Baseline AUP.

After initially drafting a IRIS Privacy Notice based on the PDK template, the IRIS Trust Framework team felt that the structure of the resulting document lacked clarity in not presenting sufficient context to the reader - it lacks user 'friendliness'. Being based on an early

version of the GEANT Code of Conduct version 2 (see REFEDS[8] wiki) recommendations, the PDK template does, however, provide a complete set of requirements arising from GDPR. As such, a reformatting of the text resulting from a use of the template, with some additional explanation of context, seemed all that was necessary. Identifying that the Worldwide LHC Computing Grid (WLCG)[9] project had been through a similar exercise, IRIS adopted the WLCG Privacy Notice as a suitable alternative, with modifications to present the IRIS context.

5 Operational Security

Alongside the work to define overall policy, a parallel task for the IRIS Trust Framework team was to suggest an operational framework to provide IRIS with an incident response (IR) capability. The basis of this work was the set of existing procedures and structures used for the IR capability of the GridPP project within IRIS, provided at the UK level by a security team made up primarily of operational staff within GridPP and the GridPP Security Officer, and on an international level ultimately the EGI CSIRT[10].

With an existing distributed UK team in place, the decision was made to expand this team with representatives from IRIS providers. To facilitate this, agreements were put in place to allow information sharing between the expanded IRIS security team and the EGI CSIRT, focusing specifically on the adoption by the IRIS team of a common operational code of practice[11]. At time of writing the first meeting of this expanded team is due to take place by the end of March 2020 - as such, an exploration of the growth of this team would form the subject of a future publication.

6 Next steps

In the discussion below, we look beyond the initial set of policies developed by the IRIS Trust Framework team and consider appropriate next steps for the team. Consideration of policy domains covered by the PDK, as illustrated in Figure 1, shows candidate policies which might be introduced into the IRIS policy framework beyond the initial set described above.

6.1 Community and Service Provider policy

One policy domain - the Community[1] - stands out as being closely coupled with many others and, as such, should be important in completing any policy framework. Additional weight is given to this as a choice by further developments of the IRIS IAM to extend Community and Community-group management functionality. These developments require the delegation of Community management functions by the IAM administrator. Security considerations require that policy defines clear expectations of the behaviour of individuals assuming these delegated responsibilities within the IAM be defined.

The PDK [Community] Membership Management template makes reference to several other policy documents and external sources, of which only the IRIS AUP would exist if adopted as is. The PDK template is also quite extensive and detailed in its requirements of Community managers and, referencing an undefined Community Operations Security Policy, increases the complexity faced not only by the IRIS Trust Framework team, but also as presented to the end-user - the Community management. Whilst this may be practical for large,

[1] *A group of individuals (members), organised with a common purpose, and jointly granted access to the IRIS infrastructure. A IRIS Community may act as the interface between individual members and the IRIS Infrastructure.* - Draft IRIS Infrastructure Security Policy

well structured and resourced Communities, adoption and conformance would be a daunting task for less formal, ad-hoc communities or those that are by nature more disperse. Such considerations indicate that the PDK is correct in identifying the centrality of Community policy to an infrastructure framework but does not address this domain in a manner which would be appropriate for IRIS to adopt directly. Consequently the IRIS Trust Framework team would work towards a higher level, 'lighter' Community policy.

6.2 Service Operations

With the top-level Infrastructure policy providing an overall framework for subsidiary policies, and the proposed Community policy and draft AUP providing structure for Communities and end-users, a missing element in a future IRIS trust framework is expectations and requirements on those offering infrastructure services - Service Providers (SPs). For a trust framework to be beneficial to all parties, by enhancing the security of the infrastructure, trust must be bidirectional. For example, SPs should be able to trust that Users, and the Communities they belong to, that they allow to access resources (e.g. storage or compute) will only use those resources for agreed purposes. Equally, Users and Communities must place trust in the actions of those SPs whose services they use, for instance by properly handling their data or protecting identity credentials they release to the SP to enable them to act on their behalf. The former case is covered by AUP and Community policies discussed above. Expectations of SPs, in the form of a IRIS Service Operations security policy, would be an appropriate balancing document to a Community Management policy.

6.3 Processing of Personal Data

The Processing of Personal Data is, to some extent, handled by the creation of the IRIS Privacy Notice combined with reliance on locally applicable service policies (i.e the policy of the organisation offering the service), but the IRIS Trust Framework team recognises that this should, eventually, be backed up by a IRIS-specific policy. However, a likely candidate to satisfy this requirement - the GÉANT Data Protection Code of Conduct version 2 (see REFEDS wiki) - is currently undergoing formal review by the Dutch Data Protection Authority (the designated, local EU jurisdiction) and the IRIS Trust Framework team believe that action in this domain should wait until the situation in this respect is clearer. Hopefully this will be by the end of 2020 when details of the effects of BREXIT should also be apparent.

6.4 Acceptable Authentication Assurance

Acceptable Authentication Assurance - answering the question: what level of confidence does an SP have to place in a digital identity presented by, or on behalf of, a user that it actually originated with the expected real-world user - is also an important topic. However, the identity assurance 'landscape' is complex, with several different assurance frameworks and little guidance as to how each relates to the other. REFEDS has designed an Assurance Framework to "satisfy the needs of R&E federations for a common, lightweight set of assurance specifications" (RAF; see REFEDS wiki). The RAF leverages other assurance standards in the area of identity proofing and provides a relatively accessible approach to assurance. However, little guidance is available for SPs and Communities on how to make the decision on the risk analysis behind the question posed above. In addition to this, as a broad range of Communities and SPs is expected to be supported by IRIS, each with its own requirements with regard to protecting data and resources coming from the field they support, it seems likely that an Acceptable Authentication Assurance policy for IRIS as a whole must take this into account.

Work is ongoing on this topic as part of the EU H2020 GEANT GN4-3 project and the IRIS Trust Framework team feels that further consideration should be delayed until the results of this work can be assessed. Until this time, authentication of individuals to the IRIS IAM, which corresponds roughly to RAF "medium" assurance, is considered adequate for the general case. Specific, higher requirements, probably originating from external regulatory (e.g. biomedical) or license bodies, seen in other contexts, have not yet been identified for IRIS.

7 Conclusions

The first year of activity on generating a set of security policies for the IRIS community has shown that the AARC Policy Development Kit is a useful basis to bootstrap such a policy set. Feedback from the community has suggested some amendments particularly to the Top Level Security Policy which the team will provide as input to future WISE deliberations on changes to the PDK. While drafts of the AUP, PN and Top Level policy are being reviewed by the IRIS community, work has proceeded in identifying the most important policies to add to the set.

Alongside the policy work, an operational security framework is also being developed, with the first step of implementing an expanded distributed security team to take place in the first quarter of 2020.

References

[1] https://www.iris.ac.uk

[2] https://stfc.ukri.org/

[3] https://aarc-community.org/

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[5] D. Kelsey, D. Groep, L. Florio, C. Kanellopoulos, M. Linden, I. Neilson, S. Paetow, W. Pempe, V. Ribaillier, M. Sallé, H. Short, U. Stevanovic, G. Venekamp (2017) "Can R&E federations trust Research Infrastructures? - The "Snctfi" Trust Framework". International Symposium on Grids and Clouds 2017: Global Challenges: From Open Data to Open Science (ISGC 2017): Taipei, Taiwan, March 5-10, 2017

[6] H. Short and R. Wartel (2016) "Building Security and Trust in Inter-Federation". International Symposium on Grids and Clouds (ISGC) 2016 (ISGC 2016), Academia Sinica, Taipei, Taiwan, 13-18 March 2016

[7] https://wise-community.org/

[8] https://refeds.org/

[9] https://wlcg.web.cern.ch/computer-security/

[10] https://csirt.egi.eu

[11] https://www.trusted-introducer.org/TI-CCoP.pdf