UK e-Infrastructure Security and Access Management Working Group

Date: Wednesday November 27th 2013

Venue: 76 Portland Place, London. W1B 1NT

Present:

Stephen Booth (EPCC), Dave Britton (University of Glasgow), Darren Hankinson (University of Manchester), Dave Kelsey (STFC – RAL), Bridget Kenyon (UCL), Phil Kershaw(NERC / STFC), Alan Real(University of Leeds), Jeremy Olsen (Francis Crick Institute & CRUK London), Andrew Cormack (Janet (Chair)), John Chapman (Janet), Henry Hughes (Janet), David Salmon (Janet), Jeremy Sharp (Janet).

1. Introduction to the Working Group and review of Draft Terms of Reference
    a. A number of administrative activities were discussed including specific editorial comments on the draft Terms of Reference that will be incorporated in an updated version of the document. **(Actions 1, 2 & 9)**
    b. There was discussion around point 2, (coordinate access and identity management activities amongst those developing and provisioning services, with a view to ensuring that solutions are standards-based and interoperable). It was suggested that the group should aim to do something rather than just talk about it. It was suggested that "create and" could be inserted in front of coordinate activities. Following discussion there was consensus on this point. **(Action 2)**
    c. The question of funding for activities was raised. Specifically if the group was able to commission any required activity in this area. Jeremy confirmed that Janet had funding available to support activity in e-infrastructure.
    d. There was discussion around the UK scope given to the activity when many services and project were international in nature. Jeremy confirmed that the scope had to be UK focused for co-ordination and funding of activities. However, attention was drawn to point 5 under scope and objectives that sets out "provision of advice to those responsible for representing UK interests internationally".
    e. It was noted that EGI (European Grid Infrastructure) is setting up a steering committee for AAI (Authentication and Authorisation Infrastructure) as part of Horizon 2020 funded activity. **(Action 7)**
    f. It was noted that FIM4R (Federated Identity Management for Research) looked at what a range of individual projects needed. It was felt this might be a helpful basis to build from. Subsequent discussion indicated that the main blockers in this area were around getting appropriate attributes released by IdPs (Identity Providers). However, when seeking specific examples of problems that could act as use cases for the group to explore, none could be accurately identified. **(Action 5)**
    g. Given the range and mix of technologies currently in use in this area the view was expressed that perhaps the best that could be hoped for in the short/medium term is the use of bridging technologies. An alternative, longer-term, approach was to seek consensus and standardise on a set of protocols and services.
    h. At present, if the existing federation services don't provide the solution it would appear that the usual step is to establish a bespoke federation to meet the

requirement on a project by project basis. An example was given in the form of eduGAIN, which provides a solution to most interfederation requirements, but a range of projects have chosen to build their own project-specific federations independently. We need to understand why existing solutions are not meeting the requirements of the projects. **(Action 4 & 5)**

i. Jeremy stated that Janet wanted to ensure that federation services met the widest possible needs. Existing examples were eduroam and UK federation and a developing service using Moonshot technology. **(Action 5)**
j. There was a desire to try to use a common framework for federation services - all volunteered co-operation from existing projects.
k. The question was raised as to how the group should most efficiently engage and feed into European activities. The consensus was that members of this group would help to represent the projects with which they engage.
l. There was a desire for a common single sign on service that all projects and activities could use. **(Action 6 & 8)**
m. It was felt that there was confusion around the use of 'identity' attributes with some projects believing they needed individuals named and other project being comfortable with using opaque identifiers, which confirmed the same user was returning, but did not release personal information. **(Action 4 & 5)**
n. A question was raised around the use of personal certificates and how individuals could access them. It was noted they were available via TCS (TERENA Certificate Service) and that this requirement was part of the upcoming Janet Certificate Service re-procurement. **(Action 3)**
o. The basic requirement for projects appears to be for a persistent (opaque) identifier and affiliation – which is what the UK federation has been saying since 2005. If IdPs aren't doing this Janet needs to know why not, who they are and what their use case is to help address. **(Action 4, 5 & 8)**
p. There was consensus that the FIM4R paper provided a good overview of requirements, but specific detail of use cases was required in order to develop services to meet the requirement. Paper:CERN-OPEN-2012-006: https://cdsweb.cern.ch/record/1442597
q. There was discussion around what the barriers were for projects making use of federated identity. It was suggested it could be a problem of perception, a lack of implementation skills, fear or lack of confidence or that individuals were unaware of the services that were available and what they could deliver. It was noted that Janet had been asked if it could provide managed services in this area. **(Action 4, 5 & 8)**
r. It was suggested that there was a need for a scalable negotiation mechanism so that individual researchers at an institution don't need to battle with their institution's IdP to release attributes that a project required. It was noted that work on Entity Categories was attempting to help in this area.
s. The Moonshot pilot was discussed and it was agreed it was a good opportunity to work through and alongside pilot sites to help ensure their requirements were met.
t. It was noted that CERN were planning to pilot eduGAIN during 2014, but had not decided to pilot Moonshot as yet. This raised the question that they might be concentrating on a web only strategy.

u. Discussion also focused on the Shibboleth Service Provider (SP) and some limitations about how third party APIs (Application Programming Interfaces) could be integrated. Henry noted that Janet is managing the Shibboleth Consortium so any specific requirements could be integrated into the development roadmap for the Shibboleth SP, with a suitable use case to test against.
v. There was a consensus view that the deployment of Shibboleth software (IdP and SP) needed to be improved so that it was easier to deploy and use. It was noted that a managed service might provide a better solution to some use cases. **(Action 4)**
w. The group noted that there was a perception that federated identity and access technology was seen as too complex. A possible approach here could be for Janet to provide additional training and support in support of these services. However, it was agreed that the area was inherently complex.
x. It was also noted that there appeared to be a general trend towards the use of lower assurance mechanisms. It appeared that organisations were being more pragmatic in the approach to this area.

2. Mapping the technical landscape

Attendees brainstormed what other groups/activities/technologies there are that touch on this area that the group should be aware of or engage with. These mappings included meetings and forums where access and identity management and security issues are discussed; the technologies in use; a range of identity providers; relevant standards bodies and regulators; and projects, services and initiatives with federated identity requirements. These mappings can be found in Annex A: Mappings and will be further developed by the Working Group over the course of the Group's activities. **(Action 10)**

3. Discussion
   a. There was discussion around the attribute release model in use by federations internationally. It appears some projects require the release of personally identifiable attributes where others can work with opaque, privacy preserving, attributes. It was agreed that to work effectively on solutions in this space it was essential to work from detailed use cases so that so that solutions could be effectively tested and where suitable deployed into production services.
   b. The group discussed how to approach the security of e-infrastructure. It was noted that the EGI had a security operations centre. The group concluded that the approach to security must again be focused on solving specific use cases. The security model would need to include an overarching approach to information security, and provide details of how those providing e-infrastructure services could practically test their compliance. It was felt work under the title of "security for collaboration infrastructure" would help to set out what was needed in this area.
   c. The issue of how to best co-ordinate incident response activities with reference to federation operators was raised. It was noted that there were standard processes in place for incident response teams to co-ordinate activities. However, it was felt that there would be value in exploring if additional co-ordination would be helpful between those operating e-infrastructure services. It was agreed that federations should actively participate in security incident response.

d. The group agreed that a common trajectory existed with a shift towards greater use of federated credentials. However, it was felt essential that a roadmap was produced to try to map all the multiplicity of solutions being employed both nationally and internationally.
e. The group agreed that the general approach should be practical so that both service providers and identity providers could take incremental steps to improving services to their customers.
f. The group noted that there were issues to address at both a policy and technical level.
g. The group agreed that current solutions did not meet all requirements. E.g. Shibboleth doesn't do non-web, user delegation or groups, so a bridge between technologies would be useful. The group noted it would be helpful if a roadmap could indicate how long bridging might be required for.
h. The group noted that as institutions trust Janet to carry traffic, this could be extended to holding identities. This took the discussion back towards flexible managed identity services that would allow users to connect to the fullest possible range of service providers. This in turn took discussion towards the existing architecture of the federation in the UK. It was noted that other federations had adopted a "hub and spoke" model in contrast to the "full mesh" approach employed by the UK federation. The group concluded that there might be value in re-examining the architectural approach deployed in the UK.
i. The group also noted that CPNI were working closely with a number of Universities and where there was overlap, work should be co-ordinated where possible.
j. It was noted that with Industry use of e-infrastructure – and connectivity to Janet in some cases – encryption during transit appeared to be a standard approach – processing and storage of data presented issues and operational security was felt to be a key area of discussion to allow wider access to e-infrastructure resources.
k. The group noted that the RUGIT meeting in April 2013 had presentation on CPNI Top 20 Controls survey carried out by the RUGIT IT Security Group : http://www.rugit.ac.uk/meetings/presentationsnotes/april2013/RUGIT-CPNI-Results.pdf
l. There was discussion of the "Embassy Cloud" concept – a place for Industry to come and engage with Research.
m. There was further discussion around a potential identity provider hosting service that Janet could establish. There was consensus that a hosted IdP service should be investigated along with possible services for virtual organisations and Janet acting as a home for the homeless.

4. Actions
    1. Janet to set up email list [done - uk-e-infrastructure-security@jiscmail.ac.uk]
    2. Revise draft TOR and circulate with the aim of reaching agreement by email or at next meeting.
    3. Janet to talk to Dave Kelsey about personal certificates via IGTF and Janet Certificate Service.
    4. Produce an initial outline draft specification for what identity provider hosting, a virtual organisation service and a home for the homeless might look like.

5. Janet to talk to “SKA (Square Kilometre Array)” as a large scale project to see if their activity and requirements could help define example use cases.
6. Write up proposed deliverables, timescales and circulate for comments.
7. Joint REFEDS/EGI/UK e-infrastructure discussion - David to follow up.
8. Janet to establish small team to offer practical advice to projects in early 2014. E.g. what should DiRAC be doing?
9. Janet to poll for dates of next meeting.
10. Janet to use the discussion around mapping of the technical landscape as the basis for a document that the group could keep under regular review.

Annex A: Mappings

To better understand the access and identity management and security technical landscape, the UK e-infrastructure Security and Access Management Working Group produced a mapping of the various groups, activities and technologies that the Group is aware of.

These mappings will be updated and developed by the Working Group over the course of the Working Group.

Discussion places

Federated Identity Management for Research - FIM4R - https://refeds.org/meetings/oct13/

EIROforum - http://www.eiroforum.org/

REFEDS - https://refeds.org/

VAMP – Virtual organisation Architectural Middleware Planning - www.terena.org/activities/vamp/

Open Grid Forum - http://www.ogf.org

Research Data Alliance - RDA - https://rd-alliance.org/

EDUCAUSE - http://www.educause.edu/

Internet2 – www.internet2.edu

UCISA - http://www.ucisa.ac.uk/

RUGIT - http://www.rugit.ac.uk/

Technologies

SAML - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

OpenID Connect - http://openid.net/connect/

OAuth 2.0 - http://oauth.net/2/

Moonshot – www.ja.net/moonshot

Shibboleth – www.shibboleth.net

Identity Providers

Facebook

Amazon

Google

Mozilla

Members of Research and Education federations

Members of eduGAIN

Standards bodies / Regulators

OASIS

IETF

OpenID Foundation

Mozilla

IGTF

ISO24760-1

eduroam

Kantara

PSN

Stork

UK Government / Cabinet Office / CESG

Research Councils

NIST

PCI-DSS

CPNI

Projects / services /initiatives with federated Id requirements

EGI - http://www.egi.eu/

WLCG - http://wlcg.web.cern.ch/

DiRAC - http://www.dirac.ac.uk/

PRACE - http://www.prace-ri.eu/

EUDAT - http://www.eudat.eu/

DARIAH - http://www.dariah.eu/

ESA - http://www.esa.int/

CLARIN - http://www.clarin.eu/

GridPP - http://www.gridpp.ac.uk/

Helix Nebula - http://www.helix-nebula.eu

VPH - http://www.vph-noe.eu/

Earth System Grid Federation - https://www.esgf.org

Farr Institute - http://www.farrinstitute.org

Met Office - http://www.metoffice.gov.uk/

ORCID – http://www.orcid.org