UK e-Infrastructure Security and Access Management Working Group

Date: Friday 3rd October 2014

Venue: Brettenham House, 5 Lancaster Place, London, WC2E 7EN

Present:

Stephen Booth (EPCC), Andrew Cormack (Janet (Chair)), John Chapman (Janet), Henry Hughes (Janet), Paul Kennedy (University of Nottingham), David Salmon (Janet), David Kelsey (STFC), Jeremy Olsen (Francis Crick Institute), Jens Jensen (STFC), Steven Newhouse (EBI), Darren Hankinson (University of Manchester), Josh Howlett (Janet)

Apologies:

Phil Kershaw (NERC / STFC RAL), Jeremy Sharp (Janet), Melanie Wright (Essex), Dave Britton (Glasgow).

1. Actions from previous meeting

1.1. Janet to provide assistance to SB with registering EPCC to join the UK federation.
DONE

1.2. Janet to arrange a meeting between SB and Rhys Smith to discuss Moonshot and SAFE
DONE

1.3. AC to draft skeleton document addressing group management.
DONE

1.4. Janet to determine if other federations can do traceability in the same way as UK fed Section 6.
According to a REFEDS survey (https://refeds.terena.org/index.php/FederationIncidentHandling) it looks like the following do: Australia, Canada, the Czechs, Switzerland, Germany, Denmark, Spain, Finland, France, Croatia, Italy, Latvia, Netherlands, Norway, New Zealand, Slovenia, US and Ireland.

DK mentioned that a working group building on CERT collaboration has been set up, called SirTfi (A Security Incident Response Trust Framework for Federated Identity), with participants from e-Infrastructures and global NREN members.

1.5. ALL to feedback detailed comments on AuthN paper to AC by 21/7/2014
Feedback received and paper published at https://community.ja.net/groups/uk-e-infrastructure-security-access-management-wg/document/federated-authentication-e

1.6. AC to document Top 20 Controls discussion.
The Top 20 Controls document has been drafted. It will be further updated following this meeting and circulated via email to the group prior to publication before the next meeting.

1.7. JJ to provide short case studies on the Community Group.
ON GOING

1.8. JC to Poll for dates for next meeting (aiming for end Jan 2015)
DONE - Date of next meeting: Friday 23rd January, Jisc Brettenham House, London

2. Update on other activities

2.1. Farr Project - Funding approved (http://www.jisc.ac.uk/news/jisc-enables-the-safe-and-secure-sharing-of-medical-research-data-02-oct-2014). This is a 2-year project. Will be an encrypted overlay to an organisation's secure area. Whatever controls are in place for central infrastructure and the edge will have to be mirrored. Lots of work to do on policies. Will run native IPv6 for scalability so all participant organisations will have to run IPv6 in their secure areas. There will have to be a gateway (with appropriate controls) and a decision to be made will be whether all have gateways at the edge or have one at the core. We will have to bridge between PSN and NHS domains. Infrastructure should be in by Q2 2015, but the policy space will take longer. Experience will show whether a generalisable overlay service could be developed e.g. for industry collaboration. There will be a connection agreement to bind an organisation into the context of the overlay. The overlay will have to transit over a campus network and then hand off to the secure area.

2.2. Elixir - funding is available from EC for developing Elixir infrastructure. Looking at federated identity as a particular focus over the next year. Group access, shared ownership, shared use of resources etc. Knowing who is a member of Elixir is actually quite challenging to answer. Elixir (and CLARIN) looking at REMS (see https://confluence.csc.fi/display/REMS/Home & http://www.terena.org/activities/tf-emc2/meetings/26/rems.pdf). The workflow around authorisation is something REMS does nicely.

2.3. The Research Data Alliance has established a FIM interest group (FIMig) to broaden the current discussions within the FIM4R group using RDA contacts to the global community (not just Europe). Plan is for another FIM4R meeting in Helsinki sometime.

2.4. The AARC project bid for Horizon2020 is led by TERENA and was presented at the recent RDA meeting by Licia Florio: https://rd-alliance.org/sites/default/files/2014_09_RDA-FIM4R-LF.pdf. €3m for 2 years to get a production AAI for eInfrastructures. EUDAT is a consumer of that AAI. Lots of funding is for training and dissemination to include non-partners.

3. Group Management/Authorisation Paper

3.1. Some attributes are provided by IdPs, some by group management.

3.2. REFEDS have agreed on an R&S category and will now go to a 30 day final consultation

3.3. Communities control the policies.

3.4. Policy as to what an attribute means e.g. a user can access certain content with a GridPP attribute.

3.5. Need a system to prevent clashes of group names e.g. how to stop two different projects both declaring an "administrators" group - can either have each service configure AAA system to take attributes from a community server or have a DNS-like global publishing system.

3.6. Do we need standardised attributes: e.g. Normal user; Community Administrator; Federation Administrator?

3.7. Service Provider needs to know what permissions a user has not how they received those permissions.

3.8. The Janet Community site has ways of inviting or subscribing members – a good model to use, but is it scalable?

3.9. If you want 10,000 people, but not 'him' then how do you block the 10,001 person? Can have a tree of people that can authorise new members, but much harder to stop someone. Central list? Attribute that institutional IdP can provide? Distributed community management role? This is the challenge for e Infrastructures as it isn't the home IdP that knows if a user can have access or not.

3.10.For ARCHER people apply. But they normally have to be told they need to apply...

3.11.Australians have a policy for moving a unique id from one IdP to another. The process is to ask to transfer. Could have a "park it" service. This could be a community 'thing' e.g. the community knows that Jens has moved from one org to another, but is still in the same community.

3.12.Options? Use an existing lifelong identifier e.g. Scottish Government myaccount or an Estonian smart card, or multiple email addresses to link multiple accounts - catch is if you have different LOA. Otherwise you may have to rely on manual helpdesk approach of phoning up institution to check someone still works there or phone PI to check they are still allowed to access a resource/service.

3.13.EBI is involved in a project to use social id to log in to SPs.

3.14.A lot of groups don't do accounting, some VOs do it. Grids do accounting.

3.15.Accounting/accountability can cover everything from usage logs, to data security/incident handling, to billing. The following table identifies some open issues within the Group Management paper for discussion:

	Issue	Example implementation	Questions
Enrolment	Invitation	SWITCH[1]	
	Joining request	ARCHER	This is the reverse of invitation – “may I join your group?” Does anyone implement it digitally?
Authentication	3rd party AuthN, including social	Diamond/Umbrella[2]	Does the Platform need to provide an IdP gateway so SPs don’t need to support every AuthN protocol too? Which AuthN protocols provide most benefit?
	Home for the Homeless	DARIAH[3]	
Group management	Distributed Group Mgmt		Is a hierarchy (“I grant you my group management rights”) sufficient or are things like web of trust, member recommendations, reputation, etc. of interest?
	Accounting/ Traceability/ etc.		May be separate requirements in here
Link to IdP	IdP to Group Mgmt interface		Can we combine, e.g. Shib/Moonshot, or X509/Shib where one is used for AuthN and the other for AuthZ? Is this already being done?
	Account linking		May be needed as a fallback if IdPs can’t be persuaded to release untargeted identifiers
	SAML/X509 interworking	MyProxy, SARoNGS etc.	Do we need to support linking further down the chain too? E.g. could a SAML-based group management system issue X509 proxy certs, a la SWITCH SLCS?
Link to SP	Group Mgmt to SP protocol	Too many options ☹	Which AuthZ protocol(s) should we suggest supporting?
	Group Mgmt to SP semantics	e.g. Janet Community (member, contributor, editor)	Can we provide meaningful (cross-SP) information, or just opaque group names, which Group/SP need to negotiate?

[1] https://www.switch.ch/aai/downloads/AAIgmt_documentation.pdf Page 9

[2] https://community.ja.net/system/files/288/MoonshotDiamond.pdf

[3] http://dasish.eu/dasishevents/aaiworkshop/Report_on_the_DASISH_SSH_AAI_strategy_meeting_V3.pdf

4. Comments on Security Paper

    4.1. If someone builds a network of communicating VMs, what OpSec do we want to put in place (logging, patches, etc.)? What if the VMs change their ownership?

    4.2. VM freezing as a new incident response option.

    4.3. Host service policy should say where you are on the prevention/cure axis; granularity of response may depend on use case too.

    4.4. "Turn it off" might be the right solution.

    4.5. Say that there are CERTS/CPNI/ etc.

    4.6. How about recommending to a national VM support service? Library of VMs that people could select/configure. Plus advice to universities etc. on facilities needed to host them.

    4.7. Sample Threats to e-Infrastructures, add:

        4.7.1. - pure theft

        4.7.2. - disgruntled researcher who wants to discredit PI

        4.7.3. - split competitor into thief and sabotage

        4.7.4. - Hacktivist may discredit or DDoS against

        4.7.5. - Incompetent programmer/admin (job runs amok, unpatched)

        4.7.6. - social engineering of infrastructure admins, or end users (DNS takeover)

    4.8. Make these into stories - how do you protect, and what would you do?

    4.9. Could Janet provide a national sandbox health test service? So you upload a VM and run a series of tests on it. Could have some benefits, but not a single solution.

5. Consideration of Future Work Items

    5.1. Possibly something like an operational guide - Common Information Assurance (not special purpose)

    5.2. Capture / reference / disseminate the security for collaborating infrastructures work (DK)

    5.3. Workflow probably well enough done already

    5.4. Instructions for how to integrate new e Infrastructures with AAA services? E.g. how to hook up to UK federation; how to hook up to Moonshot etc.?

    5.5. Case Studies - how X does Authentication, Authorisation AND Accounting; Guidance for designers -think about federated authentication earlier.

6. Review and agreement on actions

    6.1. Action: AC to circulate draft eInfrastructure perimeter picture and update documents

6.2. Action: JJ to provide short case studies on the Community Group.
(carried over from June Meeting)

7. AoB

7.1. Date of next meeting: Friday 23rd January, Jisc Brettenham House, London - http://www.jisc.ac.uk/contact#tab-5-1