UK e-Infrastructure Security and Access Management Working Group

Date: Friday 23rd January 2015

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

Present:

Stephen Booth (EPCC), Andrew Cormack (Jisc (Chair)), John Chapman (Jisc), Henry Hughes (Jisc), Paul Kennedy (University of Nottingham), David Salmon (Jisc), Frances Burton (Jisc), David Kelsey (STFC), Jens Jensen (STFC), Darren Hankinson (University of Manchester), Dave Britton (Glasgow), Alan Real (Leeds).

Apologies:

Phil Kershaw (NERC / STFC RAL), Jeremy Sharp (Jisc), Jeremy Olsen (Francis Crick Institute), Josh Howlett (Jisc), Paul Lewis (Cranfield).

1. Actions from previous meeting

    1.1. AC to circulate draft e-Infrastructure perimeter picture and update documents
    DONE

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

2. Update on papers:

    2.1. Authentication[1]

        2.1.1. This paper will be reformatted into the same series style as the Security paper (see below).

    2.2. Authorisation/Group management

        2.2.1. This has been updated following the October meeting. An additional paragraph is needed to explain the link between the group manager / PI function and the VO instantiation.

        2.2.2. In GRID-land the user owns the attribute (the certificate) and they push it.

        2.2.3. Group manager and site (service provider) have their own policies, so technology has to support this.

        2.2.4. Start of Section 5 Conclusions and Next steps – GRID probably does have the features, clusters of software components around VOMs.

[1] https://community.ja.net/groups/uk-e-infrastructure-security-access-management-wg/document/federated-authentication-e

2.2.5. EUDAT is a good example of how groups should be working together - need to ensure no clash of names etc.

2.2.6. Section 5 really continues the discussion - needs some real next step recommendations.

2.2.7. The safe share project should come up with more universal recommendations e.g. a user authenticates with their federated login demonstrating they are a current user in good standing and then combines this with a 2FA token from the service. 2FA as authorisation?

2.2.8. We have more than 2 well established national/international authentication services. Are we working towards national authorisation solutions? Big international projects have their own solutions, what do small guys do? How would we fund people to run these types of services? It won't be secure if you don't have a well-resourced team to run it.

2.2.9. We tend to delegate identity not authorisation.

2.3. Security

2.3.1. The 'Technical Security for e-infrastructures' document been rebranded by Jisc marketing. Looks good. Still determining a common image for all front covers in the series.

3. E-infrastructure security and access management for non-specialists – discussion for input into a new paper

3.1. Are there any 'What is an e-infrastructure' documents?

3.2. Need to decide who this is aimed at – is it just information, or are they marketing messages (with examples and case studies etc.)? This is aimed at a non-techie audience.

3.3. Are there any issues that funders have had in misunderstanding e-infrastructures? Funders think hardware is the biggest cost for GRIDs etc. but the biggest cost is people. Hardware is getting cheaper and cheaper, but manpower isn't.

3.4. There is often confusion between HPC and HTC, with a tendency to think HPC covers everything. Need to explain there are three key resources: compute/data/network and the different levels of optimisation: some jobs will never be suitable for cloud, for example.

3.5. There's also a difference between lots of kit and an infrastructure (kit plus coordination plus management etc.).

3.6. Challenges of complex, networked architectures.

3.7. From a user perspective, the important factor is this is remote computing rather than local.

3.8. Although we have the separate documents, this one also needs to cover authentication and authorisation – the concepts and why they are different; what resources are available; and where to start if you are doing eScience.

3.9. Need to explain the difference between single sign-on and single credential.

3.10.Need to explain traceability versus privacy/confidentiality.

3.11.Security needs mentioning, perhaps referencing CIA. Explain why we're doing security and the trade-off between security and ease of use.

3.12. More challenges: group management; Open Access, curation, data preservation

3.13.ACTION - AC to draft e-infrastructure security and access management for non-specialists document.

4. Policies and Processes – review of paper with a view to repurposing content

4.1. Useful to draft a document explaining how policies may overlap.

4.2. Data policies depend on location.

4.3. Funders may have different policy requirements.

4.4. Putting constraints in will increase costs.

5. Future plans for Working Group

5.1. What are the next steps? Are we just documenting requirements?

5.2. Pulling out access management as a function is the key to greater interoperability so this is a useful way of pushing interoperability without dictating technology.

5.3. An immediate driver is pushing the message to Research Councils that this is the way to do security and access management. Could be a stepping stone to requesting funding for a pilot.

5.4. New sites could be given these documents as instructions to join e-Infrastructures. – this is okay for new sites, but very hard to retrofit.

5.5. Where you need a standards-based approach or where you need 2 components to work together it would be useful to get funders to make recommendations or even mandate as a prerequisite for funding.

5.6. Should we be looking at requesting funding for central services e.g. CILogin for UK (for less technically advanced sites to use)?

5.7. Should we run a gateway to hide the complexity and multiple solutions?

5.8. Discussion about interoperability between Moonshot, Shibboleth, Certificates. Can we give guidance for new sites, for example on how to link IDs?

5.9. Ease of future interoperability is the end goal.

5.10.One possible recommendation is further work to find out what the recommendation should be!

5.11. Need to push RCUK to respond to what has been written so far and request funding to put these steps into practice. Are there a couple of partners that want or need to push this forwards?

5.12. DB and Steven Newhouse have a discussion soon about moving data and VMs between different infrastructures. Could this be funded to put into practice this group's outputs?

5.13. These documents can provide a framework for pilot projects to work off to prove or disprove the findings of this group.

5.14. The consensus was that we should continue to hold face-to-face meetings, rather than just drop down to a mailing list and to look to coordinate our work with AARC.

6. AoB

6.1. Horizon2020 AARC paper has been approved.

6.1.1. ACTION Find out what overlap there is with H2020 AARC and our work.

7. Actions

7.1. AC to draft e-infrastructure security and access management for non-specialists document.

7.2. AC to draft Policy document

7.3. JC to poll for date of next meeting – looking for May 2015 unless it can be scheduled before the next RCUK meeting – DS to advise.

7.4. Find out what overlap there is with H2020 AARC and our work - see attached AARC document.