**8th UK e-Infrastructure Security and Access Management Working Group**

**Date:** Monday 25th April 2016

**Venue:** De Vere Venues Holborn Bars 138-142 Holborn, London, EC1N 2NQ

**Present**:

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

 **Apologies:**

Henry Hughes (Jisc), Andy Richards (Oxford e-Research Centre), Dave Britton (Glasgow)

1. Actions from previous meeting[[1]](#footnote-1)
	1. ACTION - Papers should be presented at PDG and RCUK meetings – Jisc (carried over from May meeting) - physical papers not sent, but Jisc attendees have been asked to mention these papers at these meetings. PDG has moved from more of a governance structure to responsive workshops. SN will take hard copies to PDG workshop on 26/4.
	2. ACTION - AC to update and circulate Policy paper via email – DONE
	3. ACTION - ALL to approve or otherwise via email. Silence will be taken as approval. – DONE
	4. ACTION - AC to update and circulate Overview paper via email – DONE
	5. ACTION - ALL to approve or otherwise via email. Silence will be taken as approval. – DONE
	6. ACTION – JC to see if Stefan Paetow (Jisc) is attending the next AARC meeting in November. – DONE. He did attend.
	7. ACTION – JC to send JJ details of GÉANT Moonshot activity. – No public link yet available. A Moonshot service specification is awaiting publication, but is currently marked as confidential so unable to share. Within the next phase of GN4 which starts next month there will be a transition to a production service with GÉANT operating a central Trust Router and NRENs expected to connect their own Trust Router. Currently looking at the end of this year at the earliest for the launch and is likely to be branded as an eduGAIN service. Likely to follow the UK in having a core set of users initially and then growing.
	8. ACTION - DS to talk to Tim Chown (Jisc) about linking up with end to end performance. – DS has had many discussions, but this is a future issue that isn’t a current high priority.
	9. ACTION AC to talk to Dan Perry (Jisc) about the type of cloud contract models he is thinking of and whether this group can have input. – Agenda item.
	10. ACTION - DS to ask Tim Chown (Jisc) if he can attend UK-T0.- MD to send meeting details to TC.
2. eIWG reports – Andrew Cormack
	1. AC requested suggestions to disseminate this group’s documents. The print run was for 250 copies of the brochures and 500 of the leaflet.
	2. MD mentioned that the EGI conference in October is a possibility

ACTION - All to let AC know of opportunities to distribute copies of the documents

1. Cloud contract models - Dan Perry. See <https://community.jisc.ac.uk/groups/uk-e-infrastructure-security-access-management-wg/document/jisc-cloud-activity-dan-perry>
	1. Amazon and Microsoft. Jisc worked with 3 universities to understand their requirements for Amazon Web Services (AWS) including technical requirements, billing issues and the lack of predictability. A portal was developed that allows institutions to better adopt the technology. The pilot sites discussed their technical and legal needs with Amazon, as did Jisc who also wanted to move some service to the cloud.
	2. SN has some issues with the current portal so DP asked if he would send feedback to cloud@jisc.ac.uk. The portal is an early version so will be developed further.
	3. AWS aggregation model is in place so it is treated as one customer.
	4. Data egress waiver - The maximum discount is 15% of total monthly spending on AWS services. If using for storage of lots of data then this is beneficial, but doesn't cover things like hosting MOOCs. Need to be careful of how you use it as although egress charges have gone away for some use cases, depending on how you do your compute and storage, there will still be some. This is a good result for the use cases looked at so far. If there are research cases that this currently doesn't benefit then let DP know.
	5. SN requested more breakdown of tracking and costs as the portal doesn't give this as you are consuming it.
	6. Jisc is starting to look at AWS Direct Connect (<https://aws.amazon.com/directconnect/>) and ExpressRoute for Azure (<https://azure.microsoft.com/en-gb/services/expressroute/>). Looking at technical and commercial models.
	7. With Microsoft Jisc started with O365 - undertook due diligence on behalf of the sector, looking at compliance and any necessary amendments. This led to Common Online Service Terms.
	8. For Azure, Jisc has linked up with GÉANT for an Infrastructure as a Service procurement to get a mechanism for buying Azure services. Some concerns over the implementation of the framework, but it depends on how Microsoft responds. Lots of UK addendums, but devil will be in the detail.
	9. SN would ideally like a single portal to manage billing, charging and expenditure across different cloud vendors.
	10. Jisc has signed a contract to run ExpressRoute over the Janet network. Piloting is in progress.
	11. 80% of Russell Group members have Microsoft Premier Support, but only 20% of the rest of the sector. Kings is leading work for renewal of this support to extract the right sort of things from Microsoft. There are potentially 50 institutions who want this agreement.
	12. Major challenge of supporting moving to Azure. Plug our teams into Microsoft? One day training course? Quick access to expertise.
	13. If there is a commitment to an Azure instance in our shared data centre then Microsoft would do so.
	14. Is there a roadmap? The plan is for a Cloud services strategy to be available by September 2016.
	15. EBI is being rejected from academic licenses as it is not counted as an HEI for licenses. DP thinks this is sorted for Cloud, but will check with Microsoft.
	16. Question: Do we have a formal operational security model with cloud providers? Not formally, but Amazon and Microsoft responded very well to recent events by offering to help. A workshop is happening soon with respective security groups.

ACTION – SN to send portal feedback to cloud@jisc.ac.uk

ACTION DP - to check EBI academic status within Microsoft

ACTION – All to send DP examples of use cases for AWS data egress that don't benefit from the current model.

1. Cloud and e-infrastructure in research - Matthew Dovey. See <https://community.jisc.ac.uk/groups/uk-e-infrastructure-security-access-management-wg/document/european-open-science-cloud>
	1. European Open Science Cloud - Similar concepts to the Grid, just different names. Lots of research infrastructures built around disciplines; multiple research communities wanting to use technology; HPC centres of excellence; regional and national groups; policy groups; EU initiatives – lots of similar and related activity.
	2. European Research Area - <http://ec.europa.eu/research/era/index_en.htm>
	3. Open Science (data and research methods as distinct from Open Access), but different ‘Philosophies’ of Open Science with different communities thinking of open science in different ways.
	4. The "Commons" an attempt to manage all this for the ‘common good’ - not just technology, but security, policies, financial sustainability.
	5. Journey from Science 2.0 to Open Science Cloud – INFRADEV-04 2 year pilot with €10m funding.
	6. EOSC Policy Recommendations:

P1: Take immediate, affirmative action in close concert with Member States
P2: Close discussions about the ‘perceived need’
P3: Build on existing capacity and expertise where possible
P4: Frame the EOSC as supporting Internet based protocols & applications

* 1. European Data Infrastructure – Exascale supercomputers using EU technology by 2022 – planned to be in top 3 in the world.
	2. Start with science, then “Government as a Service”, then SMEs.
1. Network service agents discussion – Jens Jensen
	1. Network Services Initiative - “High performance networks offer advanced network services to end users with differing requirements. The user/application/middleware may request network services from one or more network service providers through a network service interface. The network service setup then requires configuration, monitoring and orchestration of network resources under particular agreements and policies. Provisioning mechanisms support allocating, configuring, and maintaining network internal resources.” - see <https://redmine.ogf.org/projects/nsi-wg>
	2. Not happening for some years realistically. Conceptually - yes, in practice - no.
	3. SDN being used by network researchers, but that's all.
	4. What are the applications one would want to configure? Logical address partitioning? For security or reserved bandwidth? Where does AAI come in? Is there enough interest to do some trialling?
	5. When start moving data from A to B it takes a long time before this is happening smoothly. Is science DMZ a better approach? Grid PP is an example of science DMZ as can fairly easily move data from one site to another but more difficult to add a new site or VO - needs to be more dynamic?
	6. STFC is looking ahead to moving large amounts of climate data in 2030. Is there anything AAAI related we need to be thinking about now? More about moving large lumps from A to B (so may need some reserved bandwidth) rather than allowing individuals to move bits themselves.
	7. Mainly hypothetical at the moment. Needs an immediate need to focus a solution on rather than a general solution
	8. Human effort for housekeeping is tougher than the base layer networking.
	9. Network Service Agent Description Document - <https://redmine.ogf.org/dmsf_files/13338?download>=
	10. NSI Authentication and Authorization document - <https://redmine.ogf.org/dmsf_files/13424?download>=
2. SAFE update – Stephen Booth
	1. Putting together a funding call to EPSRC to fund a pathfinder project. Gone in and gone silent. Identified work packages to work on.
	2. Jisc will provide national AAI trust fabric through existing services. Business Case - don't envisage significant new funding being required for pathfinder.
	3. Some requirements regarding sustainability of SAFE is critical, but will be relatively modest.
	4. Assent is the main platform and exploring use cases to tie distributed organisations into that.
	5. Stefan Paetow (Jisc) can provide some help with Moonshot implementation, but this isn't sufficient and scalable. Hopefully as sites start gearing up there will be less requirement for more detailed hand-holding. The Pathfinder will show if this is optimistic or not.
	6. SB: Archer 2 should kick off at the end of this year. Should EPSRC recommend Moonshot support? JH: Should have pretty good penetration in HE through next year (so yes).
	7. Support for Assent is in place from PDG, but needs driving and ownership. Can't let this slip through the gaps. The e-infrastructure security and access management working group can comment and review, but not appropriate to lead.

Action for SN to chat to Jeremy Yates at PDG workshop about moving forward the SAFE project

1. Safe share / Moonshot / Assent update- John Chapman
	1. Higher Assurance Network project - since the last meeting we have performed an initial test with St Andrews, but have since experienced some delays due to competing priorities (DDoS).We have also moved from Pre-shared keys to a PKI using a Hardware Security Module. Looking to move things on this week and hoping to be able to ship configured routers to remaining pilot sites next week.
	2. Still lots of support from stakeholders for safe share, but need them to identify real use cases from researchers / data owners who need the extra security.
	3. AAAI - Centos7 packages complete and on internal server. Just waiting for Painless Security to incorporate into their build this week or next and then can tell people about it.
	4. Stefan to look at 2 factor authentication with Moonshot in the next few weeks.
	5. Planning an AAAI workshop with eMedlab/Crick/Sanger/EBI in June / July.
	6. Mac support work to be starting for Assent shortly (subject to funding).
2. AARC update – Dave Kelsey /Jens Jensen – see <https://community.jisc.ac.uk/groups/uk-e-infrastructure-security-access-management-wg/document/aarc-update-dave-kelsey>
	1. AARC 2 year project starting May last year. Proposal for AARC2 just submitted.
	2. 2 parts - outreach and training; technical and policy work
	3. Defined basic LoA for low risk research.
	4. Working on incident response engagement via Sirtfi (<https://refeds.org/sirtfi>)
	5. Scalable policy discussion beyond bilaterals.
	6. Community proxies - trust frameworks behind them.
	7. Accounting and data privacy complications.
	8. Milestone 3.1 baseline authentication assurance profile.
	9. Lots done, but lots still to do. 3.1 covers simple use cases - need to do differentiated assurance.
	10. Many solutions require the use of a 'bridge'.
	11. AARC2 proposal - support user driven innovation of T&I; deploy AARC results; more training and outreach.
	12. Deliverable MJRA.1 describes existing AAI and available technologies for federated access including Moonshot and safe share.
	13. Deliverable MJRA1.2 is a design document for deploying solutions for 'guest identities' - Using identities outside of their original context e.g. Google or LinkedIn ids within research - what are the risks?
	14. It is hard for different infrastructures to re-use identities from other infrastructures.
3. Workflows – Jens Jensen
	1. How do you distribute workflows across different infrastructures? Triggered by events. Separation for licensing reasons. Connecting physically separate institutions.
	2. Workflow engines are hard to reuse.
	3. Within climate research they want to know who is accessing their data.
	4. Single identity needed across all components of workflow - needs persistence across data provenance, accounting, accountability. Needs to support collaborative environment.
4. Review and agreement on actions
	1. ACTION - MD to send details of UK-T0 to Tim Chown
	2. ACTION - All to let AC know of opportunities to distribute copies of the documents
	3. ACTION – SN to send portal feedback to cloud@jisc.ac.uk
	4. ACTION – All to send DP examples of use cases for AWS data egress that don't benefit from the current model
	5. ACTION - DP to check EBI academic status within Microsoft
	6. ACTION - SN to chat to Jeremy Yates at PDG workshop about moving forward the SAFE project
	7. ACTION - all to let AC know for a theme for the next working group meeting(s)
5. AoB
	1. Themes / topics for next meeting:
		1. National AAAI (review, impact, thought) - invite Jeremy Yates
		2. The third A – Accounting. What are you accounting for? DiRAC accounting is a site to central location activity and isn't of interest to (most) end users. Accounting for HPC use is different from accounting for VM use. Accounting for auditing or billing? Why, what data sources, policies, use cases? (not everything is counted).
		3. Jisc's strategy for Trust and Identity - a future agenda item rather than a theme.

Date of Next Meeting: TBD - Late June/ early July

1. https://community.jisc.ac.uk/groups/uk-e-infrastructure-security-access-management-wg/document/minutes-wg-meeting-180915 [↑](#footnote-ref-1)