

JOINT INFORMATION SYSTEMS COMMITTEE

JISC Circular 3/06: Appendix E

e-Infrastructure Security: Identity Management and Level of Assurance

Background

- E1. The JISC e-Infrastructure Programme builds on the work arising from the JSR (JISC Support of Research Committee), the eScience Core Programme, and the OST (Office of Science and Technology) e-Infrastructure Roadmap initiative. It has also been informed by European and International developments within the Grid and e-Research communities. The Vision for the programme follows the initial five year investment in the UK e-Science infrastructure, which is being developed with other partners to expand the uptake and effective use of the e-Infrastructure from early adopters and researchers across disciplines. Its two main objectives are:
- To have enhanced and consolidated the current technologies;
 - To have established sustainable communities of use.
- E2. Security and access management have been a core part of the JISC strategy since its inception. Through development programmes and funding for services such as Athens¹, JISC has ensured that appropriate facilities have been in place to both meet the current service requirements of its community and to focus on emerging requirements in this arena.
- E3. A full history of JISC funding for access management and security can be found at: http://www.jisc.ac.uk/middleware_team.html.
- E4. The recent Core Middleware: Infrastructure programme² and Core Middleware: Technology Development programme³ have built the foundation blocks for the development of a new access management service within the UK. The UK Access Management Federation will be formally launched in September 2006⁴. This service aims to support the four strategic requirements for access management within the UK that were identified as part of the JISC AAA Programme⁵:
- I. Access Management for internal (intra-institutional) applications;
 - II. Management of access to third-party digital library-type resources;
 - III. Access Management for inter-institutional use - stable, long-term resource sharing between defined groups (e.g. shared e-learning scenarios);
 - IV. Inter-institutional use – ad hoc collaborations, potentially dynamic in nature (e.g. Virtual Organisations).
- E5. Meeting the fourth requirement will be an essential part of achieving the vision of an e-Infrastructure as described in the Science and Innovation Investment Framework 2004 - 2014⁶. Whilst the implementation of federated access management is a positive step towards provisioning an e-Infrastructure that can meet the evolving requirements of researchers, further work is required to allow institutions the opportunity to engage with new opportunities.
- E6. As such, JISC is planning an ongoing development programme for e-Infrastructure Security. Two calls will be released, the first in April and the second in September

¹ <http://www.athensams.net>

² See http://www.jisc.ac.uk/programme_cminfrastructure.html for further information.

³ See http://www.jisc.ac.uk/programme_middleware.html for further information.

⁴ Information on the UK Access Management Federation is available at <http://www.jisc.ac.uk/federation.html>.

⁵ See http://www.jisc.ac.uk/programme_aaa.html for further information.

⁶ http://www.hm-treasury.gov.uk/media/95846/spend04_sciencedoc_1_090704.pdf

2006. This circular forms the first call seeking projects to investigate Identity Management and Level of Assurance requirements for the e-Infrastructure and includes a continuation phase that will form part of the second call.

- E7. The two calls proposed will be supported by core activities to enhance the development of access management and security services at both the National Grid Service⁷ and UKERNA⁸.

Summary

- E8. The e-Infrastructure Security Programme is looking to fund four areas of activity within this call:
- Identity Management within Institutions;
 - Identity Management across Institutional Boundaries;
 - Defining levels of assurance;
 - Appropriate levels of assurance;
- E9. Funding is available up to £650,000 over two years from the date of award. This will comprise initial projects to build consensus amongst the community and consolidate existing practice. A subsequent closed call will then be available for the funded projects to bid into at the end of the first year, in order to address identified issues that have no current solution.

Outcomes and Benefits of the Programme/Project(s)

- E10. Work in this area will underpin all of the workpackages in the JISC e-Infrastructure programme by enhancing backbone services and community practices. It will specifically address requirements and interoperability at both national service level, supporting the National Grid Service and UKERNA, and within institutions to enable researchers to exploit capabilities of e-Research in a way that supports and is supported by institutional policies.
- E11. This area of activity also supports the new aims identified for Core Middleware across JISC, which provides a coherent vision of requirements across e-Research, e-Learning and Information Environment communities.

Scope of the Programme

- E12. A key part of an access management federation is the trust between members that their respective identity management arrangements are equivalent or at least meet a minimum agreed level. The provision of access to resources by one member to another can then be based on that assurance. However, certain resources will only be shared given higher levels of assurance as to the identity of those wishing to access that resource. Agreeing these higher levels of assurance is also needed for members of a federation to feel able to share their more sensitive resources. For federated access management to work coherently within the research community, it will need to be able to support different strengths of authentication. This recognises the fact that resources used by researchers need to be appropriately protected according to their usage, expense and capacity. Hence there is a need to establish consensus across the community on:
- the equivalence of various identity management arrangements, including technologies, practices and processes
 - how different levels of assurance are established and how different levels of assurance are assigned to various types of resource.

⁷ National Grid Service: <http://www.ngs.ac.uk>.

⁸ UKERNA: <http://www.ukerna.ac.uk>.

- E13. A key part of the vision for a national e-Infrastructure is the concept of Virtual Organisations, which enables groups of researchers to collaborate seamlessly across institutional boundaries.
- E14. Federated access management supports Virtual Organisations by separating the authentication and authorisation processes. Users within a Virtual Organisation are authenticated by their home or affiliated institution, but can gain access to resources at other institutions working within their research group through the use of authorisation attributes which identify users as part of the research collaboration.
- E15. This may require significant changes to the way in which institutions currently operate. It will be necessary for institutions to be able to store appropriate levels of information about users in a standard format with guaranteed accuracy, to be able to act as a Service Provider to enable external access to research tools and environments and to be able to appropriately delegate authority for the management of these services to research groups.
- E16. This call sets out to establish agreement on and, where necessary, enhance the underlying Identity Management and Level of Assurance mechanisms and corresponding practices and processes that are needed to meet the requirements described above at both an institutional and national level.
- E17. Identity Management is defined as the processes and systems used by an institution or organisation to store information about users and their rights in terms of resource access and privileges.
- E18. Level of Assurance is defined as the strength of authentication required for a Service Provider to be assured that a resource is only being accessed by authorised users. A username and password set would typically be seen as medium-strength authentication; whereas a digital certificate is typically regarded as having a higher level of assurance.

Scope of the Projects

- E19. This call seeks to help establish consolidation and consensus amongst the community on existing practice in, the areas of identity management and level of assurance. It is envisioned that this will be enabled through a process of studying current technology, information structures, practices and processes, assessing usability (which can significantly impact level of security), identifying good practices, identifying and closely studying common problems and issues, seeking consensus on ways to resolve them and finally, in the second phase, developing new solutions as appropriate.
- E20. Projects in the first phase are sought in four areas:
- **Identity Management within Institutions:** work in this area will examine current practice in a representative range of institutions in terms of identity management within directory structures, use of attributes and institutional ability to use this information to support the requirements of resource access in general and of Virtual Organisations in particular. It should also examine existing tools for managing user information and the role of such tools within an institutional context⁹. Detailed observational (e.g. ethnographic) studies of current identity management and user practices may be used to identify the type and nature of the problems and issues that need to be addressed. Working with experts, practitioners and stakeholders in the community, projects will recommend good

⁹ Potential tools of interest are PERMIS: <http://www.permis.org> and VOMS: <http://edg-wp2.web.cern.ch/edg-wp2/security/voms/>.

practices, seek to identify solutions to common problems, and where necessary identify areas for further work.

- Identity Management across Institutional Boundaries: work in this area will carry out technical evaluation of the tools and detailed observational studies of the corresponding practices and processes for managing identities across institutional boundaries, and of end-users in terms of Personal Identity Management. Working with experts, practitioners and stakeholders in the community, projects will recommend good practices, seek to identify solutions to common problems, and where necessary identify areas for further work, examining emerging technologies in the field such as Liberty Alliance¹⁰, Microsoft InfoCard¹¹, A-Select¹², Higgins¹³, and SAML¹⁴ and WS-Security¹⁵ developments, suggesting how these might be effectively deployed.
- Defining Level of Assurance: before institutions and services can apply level of assurance to resources within the UK, an agreement is required on the definition and number of these levels. This work area will look at existing definitions, both at the UK and international levels. It will then build community consensus and make proposals regarding standard definitions for use within the UK education and research community, taking into account wider international development.
- Appropriate Level of Assurance: strength of authentication for resources within the UK is currently defined by environment (grid resource, library resource, e-learning resource), rather than by the worth of the resource. This has led to resources, which could be made widely available, being protected by credentials that are difficult to acquire, and to valuable resources being protected by weak authentication methods. This area of work will examine the current application of levels of assurance to various types of resource and, through building community consensus, make recommendations for appropriate policies and practices for UK services and institutions.

E21. Where a clear need is identified, based on the findings of the projects carried out in the first phase, further development work to overcome the limitations of existing tools and/or practices, or to develop new tools and/or practices, may be carried out through a subsequent closed call at the end of the first year. In addition, trials of these solutions, together with additional observational studies, may be undertaken. In all cases, the proposed solutions must address identified common issues.

E22. Funding is available up to £650,000 over two years from the date of award. It is anticipated that 4 main projects, one in each area, will be funded as part of this call. The initial funding for these will be up to £400,000. Teams may bid for more than one project. All projects will be expected to take into account each others' work, and, where necessary, collaborate on common areas, such as open or prototype standards. The remaining funds will be available as a closed call for the funded projects to bid into at the end of the first year, in order to address identified issues that have no current solution. Extension projects may run for a further 6 months beyond the initial two year period.

E23. It is anticipated that most of the initial work will take the form of reviews, case studies, consensus agreements and recommendation reports.

¹⁰ Liberty Alliance: <http://www.projectliberty.org>.

¹¹ Microsoft Infocard: <http://msdn.microsoft.com/winfx/reference/infocard/default.aspx>.

¹² A-Select: <http://a-select.surfnet.nl>.

¹³ Higgins: <http://www.eclipse.org/higgins>.

¹⁴ SAML: <http://www.oasis-open.org/committees/security>.

¹⁵ WS-Security: <http://www.oasis-open.org/committees/wss/>.

Project Outputs/Deliverables

- E24. Projects in the first phase will, as appropriate, include the following outputs:
- A full review of current institutional practice with regard to identity management;
 - Recommendations as to institutional readiness for Virtual Organisation developments in relation to identity management;
 - Recommendations regarding current provision of tools for identity management within institutions;
 - A review of current and emerging tools for personal identity management and cross-affiliation identity management;
 - Recommendations for future JISC developments in relation to personal identity management;
 - A defined set of Level of Assurance recommendations for use within the UK education and research communities;
 - Recommendations and exemplars with regard to the application of appropriate Levels of Assurance for resources protected by the National Grid Service, the UK Federated Access Management Federation and Athens;
 - Solutions to support the application of recommendations made within projects.
- E25. All projects will contribute, where appropriate, to the e-Framework for Education and Research¹⁶ as follows:
- 'Reference models' derived from consensus-based practices and processes and supporting systems will be contributed to the e-Framework's Reference Model section.
 - Where not already recorded in the e-Framework, additional services identified in the course of the projects, and any emergent interoperability specifications, will similarly be contributed to the e-Framework's Services section.
- E26. All projects will be expected to support JISC dissemination activities, to ensure that their outputs are made available to the community.
- E27. It is expected that the projects in the second phase will include the following outputs:
- Documentation on:
 - the problem addressed
 - the roles and processes involved in the solution
 - use cases outlining interactions with the systems involved
 - the applications and services used, and mechanisms for integration of these applications and services
 - appropriate interoperability standards
 - Software that is:
 - available to the community as open source (unless agreed otherwise)
 - documented for developers
 - documented for users
 - Documentation of trials that provide:
 - case studies
 - a report on their findings in terms of the degree to which the issues addressed have been resolved
 - updates to the original proposed solution where necessary
 - Contribute to the e-Framework for Education and Research

¹⁶ The e-Framework for education and research: <http://www.e-framework.org>

Submission of Proposals

- E28. Information on the bidding process and submission of proposals is set out in the main text of the circular (paragraphs 40-49.) Bids in response to this call for projects on Identity Management and Levels of Assurance should be sent to efrastructure-bids@jisc.ac.uk, with the name of the lead institution in the subject line. If more than one bid is submitted by an institution, these must be submitted in separate messages.

Further Information

- E29. All general enquiries regarding this appendix should be sent to James Farnhill (tel: 07766 442259, email: j.farnhill@jisc.ac.uk).
- E30. Any enquiries regarding the proposal submission process should be sent to Joseph Hutcheon (tel: 0117 931 7251; email: j.hutcheon@jisc.ac.uk).

JISC Executive
April 2006