

JISC Project Plan
ES-LoA
(E-infrastructure Security: Levels of Assurance)

Ning Zhang
Aleksandra Nenadić
School of Computer Science
University of Manchester

Stephen Pickles, Mike Jones, Ross MacIntyre and Terry Morrow
Manchester Computing
University of Manchester

May 2007

| | |
|--|-------------------------------|
| Cover Sheet for Proposals (All sections must be completed) | JISC Capital Programme |
|--|-------------------------------|

| | | |
|---|-----------------------|-----------|
| Name of Capital Programme: (e-Learning; e-Infrastructure; Repositories; and Preservation) e-Infrastructure | | |
| Name of Lead Institution: The University of Manchester | | |
| Name of Proposed Project: ES-LoA (E-infrastructure Security: Levels of Assurance) | | |
| Name of Project Partners: The University of Manchester: School of Computer Science, Manchester Computing, and Northwest Regional e-Science Centre. | | |
| Full Contact Details for Primary Contact: Name: Dr Ning Zhang Position: Senior Lecturer in Computer Networks and Network Security Email: nzhang@cs.man.ac.uk Address: School of Computer Science, University of Manchester, Kilburn Building, Oxford Road, Manchester, UK, M13 9PL Tel No: (0161) 275 6117 Fax No: (0161) 275 6204 | | |
| Length of Project: 12 months | | |
| Project Start and End Dates: Nov 1, 2006 – Oct 30, 2007 | | |
| Total Funding Requested from JISC: £160,000 | | |
| Funding Broken Down over Project Years (a project year runs from August – July): Year 1 (Oct 2006 – July 2007): £132,217 Year 2 (August 2007 – Sept 2007): £27,783 | | |
| Total Institutional Contributions: £38,200 | | |
| Outline Project Description To examine the existing definitions of authentication levels of assurance both at the UK and international levels, and to build consensus and make proposals regarding standard definitions for use in UK education and research community; To examine the current applications of levels of assurance, and to establish consensus and make recommendations with regard to how different levels of assurance are assigned to resources with varying levels of sensitivity. | | |
| I have read the Circular and associated Terms and Conditions of Grant at Appendix B (Tick Box) | Yes √ (yes) | No |



Overview of the Project:

ES-LoA (E-infrastructure Security: Levels of Assurance)

1. Background

Supporting secure and dynamic resource (including data, knowledge, and services) sharing and collaborations across institutional boundaries, i.e. the concept of a Virtual Organisation (VO), is an essential part of achieving the vision of an e-Infrastructure¹. Robust electronic authentication (e-authentication) capable of reliably identifying remote users (human beings or software components) with a certain level of assurance in authentication strength is an important pre-requisite to facilitate effective user authorisation and fine-grained access control to distributed services and resources in the VO environment. As a result of the JISC's strategic investment in security and federated access management (principally Shibboleth), we look forward to an environment in which authentication and authorisation processes are separated. In this environment, users within a VO are referred back to their home or affiliated institutions for authentication, but can gain access to resources/services provided by other institutions through the use of authorisation attributes asserted by their respective home institutions.

Resources provided in this e-world usually have varying levels of sensitivity. For example, e-catalogue services typically have a lower sensitivity level than subscribed e-resources such as e-journals and e-learning materials, whereas e-journals are less sensitive than exam papers that should only be accessible to staff members who are responsible for setting and moderating the exams. Similarly, raw patient data sets uploaded into a central repository for anonymisation processing are much more sensitive than the processed data sets that have already had private and sensitive information removed. Clearly, there should be a minimum agreed level of trust between a user and his/her home institution and between the home institution and a service provider for the granting of, and access to, resources with varying levels of sensitivity. A determining factor in this trust level derivation is the strength, or Level of Assurance (LoA), of the underlying authentication systems used. In other words, to provide a fine-grained access control to resources, there is a need to link access privileges to the authentication LoA derived based upon the method/token used to identify the user and the underlying access management systems used by the home institution.

LoA reflects the degree of confidence in an authentication process used to establish the identity of an entity (an individual or a software component) to whom the credential was issued, and the degree of confidence that the entity using the credential is indeed the entity that the credential was issued to. All the processes and procedures associated to the authentication process influence the LoA established. These include the process of identity proofing, the type of authentication *credential* (or *authenticator* or *token*) being used by the entity, and the authentication protocol/method used by the underlying authentication service. More importantly, LoA is also influenced by how credentials are managed as well as the procedures associated to identity and access management. These include the token technology that is used to store the credential, the manner in which a claimed identity is bound to an authentication credential, the life cycle management of the credential, whether the Credential Service Provider (CSP) has sufficient operating procedures, processes and policy frameworks to establish the required level of trust. Furthermore, the extent to which an authentication event is coupled to an authorisation event should also be taken into account when LoA is established.

The need for considering authentication LoA in making authorisation decisions has been recognised by various stakeholders. This is reflected by national and international efforts in defining the levels of assurance and specifying requirements for these levels. The UK Office of the e-Envoy (now the CabinetOffice e-Government Unit)² was the first to introduce the concept of 'authentication level' in its

¹ http://www.hm-treasury.gov.uk/media/95846/spend04_sciencedoc_1_0907.pdf

² <http://www.cabinetoffice.gov.uk/e-government/>

'E-government authentication framework' guideline published in 2000³. The guideline defined 4 authentication levels of assurance depending on the sensitivity and importance of electronic transactions. In September 2002, version 3 of this guideline: 'Registration and Authentication e-Government Strategy Framework Policy and Guidelines'⁴ was published. It further clarified that authentication levels of assurance are not only affected by the importance of transactions but also dependent on the severity of the consequences that might arise from misuse of a client's real-world identity. Following up these works, in December 2003, the US Office of Management and Budget (OMB) issued Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*⁵, to help government agencies and departments to determine which LoA a particular credential is attached to. It also provided a thorough discussion of the specific technical requirements for each authentication level. NIST advanced this work by developing a technical guidance. Its 'Electronic Authentication Guideline' published in Jan 2004⁶ defines specific technical requirements for each of the four levels of assurance. The definition takes into account the effects of *authentication token types*, *authentication protocols* and *assertion mechanisms* for remote communication on the authentication strengths. Other related activities include the Australian eGovernment Evolution 2006 initiative⁷ and the Electronic Authentication Partnership led by US industry⁸.

According to our best knowledge, the first ever effort, both nationally and internationally, to put this LoA linked authorisation concept into practice is made by the FAME-PERMISS project (<http://www.fame-permiss.org/index.html>) funded by the UK JISC funding body. The project develops middleware extensions to facilitate uniform and multi-factor authentication and authentication strength linked fine-grained access control. The middleware integrates a wide range of authentication services supporting the use of IP addresses, usernames/passwords, certificate-based soft tokens, and smart/Java cards, and derives levels of authentication assurance based upon the draft standard as defined by NIST.

In detail, the FAME-PERMISS middleware extensions consist of two major software components, FAME and PERMISS, linked through the Shibboleth infrastructure and protocols. FAME can be run as a standalone service, or as an extension to the Shibboleth Identity Provider (IdP). It calculates a LoA based upon the authentication method/token used in an authentication instance, and feeds this LoA along with the user's other attributes to Shibboleth targets via the SHIBBOLETH SAML message. PERMISS, the authorisation decision engine deployed at a Shibboleth target, has now been extended to include LoA in its authorisation decision making process. In this way, an authorisation decision is now made based on the following tuple, (*Subject, Target, Action, LoA*), rather than the traditional (*Subject, Target, Action*) attributes.

However, despite these efforts and activities, the definition and application of authentication LoA in the context of Grids and VO environments has not been examined. Are the existing definitions of LoA suited to UK education and research community? Are they suited to the Grid and VO environment? How to apply LoA to safeguard the UK NGS, JISC, ESRC and UKERNA services/resources? In addition to authentication token types and protocols, how could other factors that have the potential to influence authentication LoA be taken into account in a systematic manner? Are some onerous registration requirements or special condition stipulations due to perceived inadequacies in the strength of authentication? What are the effects of authentication depths and the use of proxy credentials on LoA? Are there any limitations in terms of user accessibility, scalability and interoperability?

³ e-Government AUTHENTICATION FRAMEWORK, Version 1.0, December 2000; available at: [http://archive.cabinetoffice.gov.uk/e-envoy/resources-pdfs/\\$file/authentic.pdf](http://archive.cabinetoffice.gov.uk/e-envoy/resources-pdfs/$file/authentic.pdf).

⁴ Registration and Authentication e-Government Strategy Framework Policy and Guidelines, Version 3.0, September 2002; available at: [http://archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication/\\$file/Registration-AuthenticationV3.pdf](http://archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication/$file/Registration-AuthenticationV3.pdf).

⁵ OMB Memorandum M-04-04, E-Authentication Guidance for Federal agencies, December 16, 2003; available at: <http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf>.

⁶ W. E. Burr et al., DRAFT Recommendation for Electronic Authentication, NIST Special Publication 800-63, April 2006.

⁷ <http://www.iqpc.com.au/cgi-bin/templates/>.

⁸ <http://www.eapartnership.org/>.

2. Aims and Objectives

This proposed project, E-infrastructure Security: Levels of Assurance (ES-LoA), is aimed at finding out the answers to the above questions, and building consensus amongst the UK education and research community on the definition and application of LoA. In detail, the principle objectives of the ES-LoA project are summarised as follows:

1. To investigate existing definitions of LoA at both the UK and international levels.
2. To build community consensus and make proposals with regard to standard definitions of LoA for use within the UK education and research community, taking into account international developments and efforts.
3. To examine the current applications of LoA to various types of resources, including Grid/e-Science resources, library resources and e-learning resources.
4. To make recommendations for appropriate policies and practices for UK services and institutions, through building community consensus, in using the appropriate LoA as defined by the worth and sensitivity of the resources.
5. To identify any gaps in existing authentication and authorization policies, procedures and infrastructure structure and processes in the use of LoA in long term in the UK education and research community.
6. To report the work in writing to JISC.

3. Overall Approach

The project work is divided into five tasks jointly performed by the School of Computer Science, and Manchester Computing, at the University of Manchester. Tasks 1 and 2 are to investigate existing definitions of LoA and to build community consensus and make proposals with regard to standard definitions of LoA for use within the UK education and research community. These two tasks will be largely undertaken by Dr Aleksandra Nenadic under the supervision of Dr Ning Zhang, who are the principal investigator and principal developer of the FAME-PERMISS project, respectively. Tasks 3 and 4 focus on examining the current applications of LoA to various types of resources and making recommendations for appropriate policies and practices for UK services and institutions, through building community consensus, in using the appropriate LoA as defined by the worth and sensitivity of the resources. Dr Michael Jones and Mr Terry Morrow will jointly be responsible for these tasks and under the supervision of Stephen Pickles and Ross MacIntyre. Finally, task 5 will be undertaken by all the researchers. The team brings representatives for both service providers and service consumers (or end users) from the whole range of inter-institutional data and resource sharing scenarios ranging from social science and bibliographic data, medical data to Grid services.

We thoroughly understand that this proposed project is not just about research. Interacting with various stakeholders, including the UK NGS, UKERNA and JISC community, understanding their business processes, concerns and requirements, and building community consensus on the definition and application of LoA in protecting VO resources are crucial to the success of the project. For this reason, we have been in contact with JISC and UKERNA to establish good communication channels for consultation and consensus building. Also, the SHEBANGS project, for which Dr Pickles and Dr Zhang are the investigators, provides this proposed project with leads into the NGS community, and in addition, Stephen Pickles is currently the Technical Director of the Grid Operations Support Centre, which co-ordinates the operation of the NGS. We will be using these platforms to communicate with the community.

We will also be having regular meetings with, and set up a Web facility to gather comments and feedback from, stakeholders. We have planned an ES-LoA workshop to bring stakeholders and interested parties together to reach consensus on LoA definitions and applications.

The important issues to be taken into account and the critical success factors for the project are:

1. To have good communication channels with stakeholders including the UK NGS, UKERNA and JISC community.
2. To understand the stakeholders' business processes and procedures, and to address their requirements and interoperability concerns, in the use of LoA.
3. To interact with other e-Infrastructure projects investigating identity and access management.
4. To take into account national and international developments in terms of LoA definitions and applications.
5. To employ RAs with sufficient and pertinent skills.

The ES-LoA project will investigate, and help to build community consensus among JISC, the UK NGS, UKERNA and other stakeholders, how different levels of assurance are established and how different levels of assurance are assigned to various types of resources. It is envisioned that the project will study current technologies and developments with regard to authentication strengths and LoA definitions. It will also investigate practices and processes in using LoA to achieve fine-grained access control for both within institutions and across institution boundaries. There will be no development work in this project in relation to LoA application and deployment.

4. Project Outputs

The project will produce the following tangible deliverables:

- D1: A full review and investigation of current definitions of LoA at both national and international levels. (Month 6)
- D2: Recommendations for follow-on work on LoA. (Month 9)
- D3: A full review of current applications of LoA. (Month 10)
- D4: A defined set of LoA recommendations for use within the UK education and research communities. (Month 12)
- D5: Recommendations and exemplars with regard to the applications of LoA. (Month 12)
- D6: Final report consisted of two parts – Defining Level of Assurance and Applying Level of Assurance. (Month 12)

We will build and share the knowledge of different e-authentication technologies, their security strengths and management implications. We will also investigate, and share the knowledge of, the suitability of current LoA definitions as applied in Grid and inter-institutional VO environments.

5. Project Outcomes

The work of the ES-LoA project will make an important contribution to the vision of the JISC e-Infrastructure programme. It will address the need for more fine-grained access control within institutions as well as across institutional boundaries. Specifically, it will make it a step closer for members of a federation to be able to share their more sensitive resources based upon different strengths of authentication. Therefore, we envisage that our project outcome will help the UK NGS and UKERNA to strengthen their backbone services and community practices. It will also enable the UK HE/FE community, the e-Science community, and health/medical community to be more confident in sharing their sensitive resources so as to exploit more fully the capabilities of e-Research, e-Learning, e-Health, and virtual collaborations, etc. In addition, as the FAME-PERMISS project is the first ever such effort in the world to develop middleware to support authentication levels of assurance linked authorisation decision making, we foresee that its follow-up project, the ES-LoA project, will only strengthen our international standing in developing e-Infrastructure security.

6. Stakeholder Analysis

| Stakeholders | Interest / stake | Importance |
|---|------------------|----------------|
| JISC Community | | |
| UKERNA | High | High |
| UK NGS | High | High |
| JISC middleware projects | Medium | Medium to High |
| MIMAS & EDINA | Medium | Medium to High |
| Other JISC service providers, including UKDA and EduServ | Medium | Medium to High |
| E-Science/Grid | | |
| GridSite | High | Medium |
| Public Health Research and CLEF-services (for NHS) | High | High |
| Verisign, White Rose, TERENA, Portal users and developers (via ShibGrid and GridShib), VOs (GridPP/NeS/LC), CTS (credential translation service), SAML, UK E-Government | Medium to High | Medium to High |

| | | |
|--|--------|----------------|
| Other service providers | | |
| Elsevier, ONS, etc (via STM, UKSG) Major publishers, such as Elsevier, Thomson, IoPP Subscription agents, such as Swets and EBSCO Intermediaries, including organisations such as Ingenta Database suppliers, such as Ovid Technology vendors, such as Xrefer and Ex Libris | Medium | Medium to High |
| International federations for information: US InCommon, Australia MAMS, Finland HAKA, Denmark DK-AAI, France CRU, Norway FEIDE, Switzerland SWITCH | Medium | Medium to High |
| IGTF, OGF CLOPS – WG, UK e-Science CA, US InCommon, Internet2 | High | High |
| | | |

7. Risk Analysis

| Risk | Probability (1-5) | Severity (1-5) | Score (P x S) | Action to Prevent/Manage Risk |
|--|-------------------|----------------|---------------|--|
| Staffing | 3 | 5 | 15 | Request to delay the project starting date for 3 months as Aleksandra only becomes free of existing commitments in January 2007. We have rescheduled the tasks so that Aleksandra started working on this project from 1 st November. |
| Organisational | 1 | 5 | 5 | All project partners are from the same institution, organisational stability is high, and the investigators are committed. However, careful co-ordination and planning will be important to ensure the success of the project. The project team has therefore agreed that we will have monthly meetings to co-ordinate activities, and discuss the project work and progress made. |
| Technical – Fail to keep up with the most recent developments. | 2 | 5 | 10 | We will do desk research to keep ourselves at the forefront of the technological developments in the area related to the project. |
| External suppliers | 3 | 5 | 15 | The project does not specifically rely on the provision of any special software. However, timely collection of stakeholders' practices and processes and their views on accessing usability and interoperability in relation to real-life deployment of LoA are very |

| | | | | |
|--|---|---|----|--|
| | | | | important. We will maintain good communication channels with JISC and stakeholders. |
| Legal | 1 | 1 | 1 | We do not foresee any risk related to legal aspects, but if we do, we will consult the legal experts in our university and, if necessary, JISC. |
| Failing to communicate with stakeholders and address their concerns and requirements | 3 | 5 | 15 | We will work closely with stakeholders. We are in the process of liaison with JISC and UKERNA to establish a platform for communication and consultation. |
| Failing to team work | 2 | 5 | 10 | All project participants have collaborated previously and have healthy working relationships. However, vigilance is required, and team work will be monitored by the investigators. The monthly project meetings will be instrumental in doing this. |

8. Standards

| Name of standard or specification | Version | Notes |
|---|------------------------------|---|
| Electronic Authentication Guideline – NIST Special Publication 800-63 | Version 1.0.2 | This is by far the only (draft) international standard produced in relation to electronic authentication (the document originally released in June 2004, and updated on April 2006). |
| E-Authentication Guidance for Federal agencies - OMB Memorandum M-04-04 | | This guideline was published by the US Office of Management and Budget (OMB) (2003). |
| Registration and Authentication - e-Government Strategy Framework Policy and Guidelines | Version 3.0 | This was a follow-up of the earlier guideline published by the UK government (2002). |
| e-Government Authentication Framework | Version 1.0 | The concept of <i>authentication strengths</i> was first introduced by the UK government in this 'E-government authentication framework' guideline (2000). |
| Shibboleth | Version 1.2, and Version 1.3 | To achieve the vision of LoA linked fine-grained access control long-term in the UK education and research community, it is important for us to keep up with the developments in the Shibboleth project, and its future releases. |
| | | |

9. Technical Development

N/A

10. Intellectual Property Rights

1. We will give JISC a royalty free indefinite licence to copy and disseminate the deliverables to the UK HE and FE community.

2. Due to the involvement with OGF, it is expected that some contents of the project deliverables may be used in the OGF deliverables, and vice versa. The natural timescales of ES-LoA and OGF would

mean that material would first be published by the project and some of the content or text would later be re-used in an OGF document. We here confirm that any materials delivered that incorporate OGF materials are made available to JISC under the conditions mentioned in point 1 above, and NOT under the terms normally imposed by OGF. If we are unable to obtain such a permission from OGF then we will not incorporate OGF materials in the project deliverables.

Project Resources

11. Project Partners

The project partners are all from the University of Manchester: School of Computer Science, Manchester Computing, and Northwest Regional e-Science Centre.

The School of Computer Science team is largely responsible for Tasks 1, 2, and 5 of the proposed project. The main contact is:

Name: Dr Ning Zhang;

Email: nzhang@cs.man.ac.uk;

Address: School of Computer Science, University of Manchester, Kilburn Building, Oxford Road, Manchester, UK, M13 9PL;

Tel: (0161) 275 6117;

Fax: (0161) 275 6204.

The Manchester Computing team is largely responsible for Tasks 3, 4, and 5 of the proposed project. The main contact is:

Name: Dr Stephen Pickles and Ross MacIntyre

Email: stephen.pickles@manchester.ac.uk; ross.macintyre@manchester.ac.uk;

Address: Manchester Computing, University of Manchester, Kilburn Building, Oxford Road, Manchester, M13 9PL

Tel: (0161) 275 5974

Fax: (0161) 275 6800

The Northwest Regional e-Science Centre hosts a number of e-Science projects that will act as stakeholders. The main contact is:

Name: Constantinos Astreos;

Email: castreos@cs.man.ac.uk;

Address: School of Computer Science, University of Manchester, Kilburn Building, Oxford Road, Manchester, UK, M13 9PL;

Tel: (0161) 306 9280;

Fax: (0161) 275 6204.

As the project partners are all from the University of Manchester, so there is no consortium agreement to be signed.

12. Project Management

The project team will hold monthly meetings. Project decisions will be made collectively by Dr Ning Zhang, Dr Stephen Pickles and Ross MacIntyre in consultation with other investigators and researchers.

Dr Ning Zhang is responsible for the overall management of the ES-LoA project. Dr Zhang will spend 7 hours/week on the project management.

Contact Details: the School of Computer Science at the University of Manchester.

Email: nzhang@cs.man.ac.uk. Tel: (+44) (0)161 275 6117. Fax: (+44) (0)161 275 6204.

Dr Aleksandra Nenadic is responsible for project tasks 1, 2, and 5.

Contact Details: the School of Computer Science at the University of Manchester.

Email: nenadic@cs.man.ac.uk. Tel: (+44) (0)161 275 6270. Fax: (+44) (0)161 275 6204.

Dr Stephen Pickles and Ross MacIntyre will jointly manage the tasks 3 and 4 of the project. They will also be responsible for liaison with other JISC funded projects. Stephen and Ross will each spend 5 hours/week on the project management.

Contact Details: Email: stephen.pickles@manchester.ac.uk; Ross.Macintyre@manchester.ac.uk;
Address: Manchester Computing, University of Manchester, Kilburn Building, Oxford Road, Manchester, M13 9PL; Tel: (0161) 275 5974; Fax: (0161) 275 6800.

Dr Mike Jones and Terry Morrow are jointly responsible for project tasks 3, 4 and 5.

Contact Details: Email: Mike.Jones@manchester.ac.uk; tm_morrow@yahoo.co.uk;
Address: Manchester Computing, University of Manchester, Kilburn Building, Oxford Road, Manchester, M13 9PL; Tel: (0161) 275 5974; Fax: (0161) 275 6800.

We do not foresee that the project will have any training needs.

Programme Support

Regular workshops and meetings with JISC, UKERNA and other project consortia are a good idea. We will welcome advice from the programme on current best practice on obtaining releases from external stakeholders and workshop participants so that intellectual property arising out of these interactions can be incorporated or annexed to project deliverables.

14. Budget

Please see the separate sheet.

Detailed Project Planning

15. Workpackages

Please see the separate sheet.

16. Evaluation Plan

| Timing | Factor to Evaluate | Questions to Address | Method(s) | Measure of Success |
|---------------------|------------------------|--|---|--|
| Through out project | Dissemination | How successful has dissemination been in raising awareness of ES-LoA? | Feedback form at dissemination events Web log analysis | Number of refereed papers published (aiming for two). Attendance at dissemination activities and feedback. Web logs |
| Through out project | Community consultation | How successfully have we engaged with our stakeholders and how wide a representation have we got? | Feedback form after meetings. Review of which stakeholders consulted. | Percentage of stakeholders who feed back that they are likely to adopt proposals. Degree to which stakeholders consulted matches with those identified. |
| End of project | Project deliverables | Have the project deliverables made a firm and sustainable start to establishing LoAs that can be used? | Feedback forms from community consultation meetings. Peer review of project. | Deliverables are assessed by the community and peers to have made a firm and sustainable start to establishing LoAs that can be used. |

17. Quality Plan

| Output Timing | Quality criteria | QA method(s) | Evidence of compliance | Quality responsibilities | Quality tools (if applicable) |
|----------------------|--|--|---|---------------------------------|--------------------------------------|
| Month 6 | Adherence to specifications and guidelines | Desktop research and review specifications and guidelines | Report produced. | Project team | NA |
| Throughout | Fitness for purpose | Using questionnaires for the collection of stakeholders' requirements. | Stakeholders confirm satisfaction with deliverables | Project team | NA |
| throughout | Spelling and grammar | Review by peers | Grammar and spelling in reports is accurate | Peers to be determined | Word spell check and grammar check |
| | | | | | |

18. Dissemination Plan

| Timing | Dissemination Activity | Audience | Purpose | Key Message |
|-------------------------------------|--|---------------------------------|--|---|
| As organised by JISC | Attend JISC related workshops | JISC community | To publicise project outputs and to get views/comments/feedback from the community – i.e. for community consultation | LoA definitions and applications in securing resources with varying levels of sensitivity |
| As organised by e-Science consortia | Attend UK e-Science workshops and Grid workshops Produce flyers and posters | UK Grid/e-Science community | For community consultation | The same as above |
| Month 11 of the project | ES-LoA workshop | JISC, UK NGS, UKERNA, e-Science | For consultation | The same as above |
| Aim for 1 conf./year | Attend international conferences of Grid Computing and Web Services | International community | For dissemination and consultation in a wider community | Research findings and lessons learnt in using LoA lined authorisation. |
| Throughout | Publish materials on project/JISC web site | List stakeholder groups above | To make the community aware of what the project is doing and to feed back its comments | LoA definitions and applications in securing resources with varying levels of sensitivity |
| Throughout | Networking | All stakeholders | To get a network of those who will use LoAs and get them to engage with the project | LoAs can be used easily and effectively. |

19. Exit and Sustainability Plans

| Project Outputs | Action for Take-up & Embedding | Action for Exit |
|---------------------------------------|---|--|
| Deliverables and Final project report | Will be submitted to JISC and disseminated to JISC, UKERNA, and national e-Science community as well as international Grid community (include other relevant stakeholder groups here). | Will be put on project web site, which will be active for two years and JISC web site. Key stakeholders will be contacted to ensure they take the work forward, such as OGF |
| Knowledge | We will be helpful if asked to share our knowledge even after the project is completed. We will include the results in our computer science teaching to disseminate to CS students (PG and UG) at Manchester. | Already liaising with OGF re input into deliverables so will liaise further with relevant standards bodies and stakeholders to ensure knowledge is used beyond end of project. |
| | | |

| Project Outputs | Why Sustainable | Scenarios for Taking Forward | Issues to Address |
|----------------------|--|--|--|
| Project deliverables | The issues addressed in the project are essential for the support of flexible, fine-grained and secure resource sharing in VO environments, which underpins the JISC's vision of e-infrastructure to support secure e-service provision, e-learning, and e-research. This vision echoes with the UK government's vision of e-government, e-health, and e-commerce. Therefore, we expect that the project outputs can be sustained beyond the project period. | The UK NGS, UKERNA and JISC community will take the recommendations produced by the project and apply them to secure national backbone services, as well as HE/FE inter- and intra institutional resource sharing. | Interoperability and identify any gaps in existing authentication and authorization policies, procedures and infrastructure structure and processes in the use of LoA in long term in the UK education and research community. |
| | | | |

Appendixes

Appendix A. Project Budget

Appendix B. Workpackages