



Project Information			
Project Acronym	ES-LoA		
Project Title	E-infrastructure Security: Levels of Assurance		
Start Date	Nov 1, 2006	End Date	Oct 30, 2007
Lead Institution	The University of Manchester		
Project Director	Dr Ning Zhang		
Project Manager & contact details	Dr Ning Zhang ning.zhang@manchester.ac.uk 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		
Partner Institutions	None		
Project Web URL	http://www.es-loa.org		
Programme Name (and number)	(e-Learning; e-Infrastructure; Repositories; and Preservation) e-Infrastructure		
Programme Manager	James Farnhill		

Document Name			
Document Title	<i>Final Report</i>		
Reporting Period	N/A		
Author(s) & project role	Mike Jones (Research Officer), Ross MacIntyre (Co-Investigator), Terry Morrow (Consultant), Aleksandra Nenadić (Research Associate), Stephen Pickles (Co-Investigator), Ning Zhang (Project Manager)		
Date	Nov 2007	Filename	finalreport.pdf
URL	http://www.es-loa.org/images/deliverables/finalreport.pdf		
Access	<input type="checkbox"/> Project and JISC internal	<input checked="" type="checkbox"/> General dissemination	

Document History		
Version	Date	Comments
V1	1 Nov 2007	
V2	5 th Nov 2007	

Table of Contents

Acknowledgements	3
Executive Summary	4
1. Background	5
2. Aims and Objectives	6
3. Methodology	7
4. Implementation	7
4.1. Task 1: Existing LoA Definitions	7
4.2. Tasks 2, 3 and 4: Agreement on LoA Definitions, Investigation of Current LoA Applications and Building Consensus.....	8
5. Outputs and Results	9
5.1. Review of Existing LoA Definitions	9
5.2. Identified LoA Stakeholders.....	10
5.3. Community Consultation.....	10
5.4. Publications and Dissemination Activities	16
5.5. Engagement with the Communities of Interest.....	17
6. Outcomes	18
7. Conclusions	19
8. Gap Analysis and Recommendations to JISC	21
9. References	23
Appendix A: Workpackage 1 Deliverable	24
Appendix B: Workpackage 2 Deliverable	24
Appendix C: Workpackages 3 & 4 Deliverables	24

Acknowledgements

We gratefully acknowledge the funding support by JISC in its Capital Programme: the e-Infrastructure Security Programme and would like to thank James Farnhill for his assistance throughout.

We would also like to express our sincere thanks to our stakeholders who took part in our survey, and provided the project with valuable input with regard to potential applications of LoA (Levels of Assurance).

We are grateful to the JISC Identity Project, the OGF (Open Grid Forum) and the organisers of the UKSG and IAS07 conferences.

Executive Summary

- The introduction of a distributed authentication and authorisation environment (eg using Shibboleth), creates a new requirement for mechanisms that support feedback on the confidence level of the authentication process. Some resources may be considered more valuable or sensitive than others thus require greater levels of assurance (LoA) that the person or process attempting to gain access is really who or what they purport to be. Standard mechanisms need to be defined and agreed to enable this information to be exchanged securely and with confidence in a wide variety of environments.
- The e-Infrastructure Security: Levels of Assurance project (ES-LoA) has investigated current definitions of LoA emerging in the UK at government level, and internationally. It has also surveyed potential users of LoA technology, both identity providers (such as universities, colleges) who have to register people to permit access to services, and service providers (including commercial and JISC-funded services).
- The work included desktop research on current LoA activities, consultation with key stakeholders in the wider community, and two surveys. The Brief Survey was designed for commercial publishers and other service suppliers to test awareness of a federated approach to access control and basic LoA concepts. The Full Survey was a more in-depth investigation aimed at identity providers (IdPs), service providers (SPs) and the grid community. The ES-LoA project also collaborated with the JISC's Identity Project who kindly included LoA questions in their widely circulated survey.
- The project found that the US Government (OMB – Office of Management and Budget; NIST – National Institute of Standards and Technology) has produced the most detailed and widely accepted approach to LoA, based on a four level model, and a critical mass of institutions adopting this approach has been established. It has created an inter-federation interoperability partnership with the US InCommon HE federation. InCommon is also piloting an inter-federation project with the US National Institutes of Health (NIH) using LoA access controls.
- The suppliers' Brief Survey found a surprisingly high level of awareness of both federated access management systems and LoA concepts. Respondents suggested a number of scenarios where LoA mechanisms could be usefully employed including financial transactions, sensitive content, account maintenance, pre-publication access and society membership privileges.
- The Full Survey found that 70% of the service providers think that more valuable/sensitive resources should be protected by a stronger form of user identification/authentication. Almost all the respondents (92%) are willing to respect national or international standards on e-authentication, with the great majority (80%) wanting medium to high levels of federation governance.
- In terms of user registration, identity vetting and record keeping, 67% of IdPs do not satisfy even minimum record keeping requirements for the NIST level 2. In terms of criteria for password selection, periods of validity and the number of unsuccessful attempts allowed, none of the respondents could satisfy even the minimal requirements for NIST level 1.
- The questions included in the Identity Project's survey revealed that there was a perceived need for "graded authentication" (i.e. LoA), although there was a lack of confidence in their ability to implement it.
- The report makes 7 recommendations, including drafting a set of definitions for the UK academic community compatible with emerging international standards based on the OMB/NIST model.
- The final recommendation is the creation of a demonstrator covering a small number of differing use cases as the most effective way to widen understanding and show how the concepts might work in practice. This would highlight issues related to the real-life deployment of fine-grained access control.

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-Infrastructure [eInf]. 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 (using Shibboleth [Shib]), 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 on-line environment usually have varying levels of sensitivity. For example, electronic catalogue services typically have a lower sensitivity level than subscribed electronic 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 with the authentication process influence the LoA established. These include the process of identity proofing, the type of authentication credential 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 with 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 identity provider (IdP) has sufficient operating procedures, processes and policy frameworks to establish the required level of trust.

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 Cabinet Office e-Government Unit) [eGov] was the first to introduce the concept of an 'authentication level' in its 'E-government Authentication Framework' guideline published in 2000 [UK-AuthFram]. The guideline defined four authentication levels of assurance depending on the sensitivity and importance of electronic transactions. In September 2002, version 3 of this guideline called 'Registration and Authentication e-Government Strategy Framework Policy and Guidelines' [UK-RegAuth] was published. It further specifies that authentication levels of assurance are not only affected by the importance of transactions but are also dependent on the severity of the consequences that might arise from misuse of a client's identity. Following up the efforts by the UK government, in December 2003, the US Office of Management and Budget (OMB) issued Memorandum M-04-04, 'E-Authentication Guidance for Federal Agencies' [OMB-M0404], to help government agencies to carry out risk assessments and to classify their transactions into four categories (corresponding to the four defined LoAs) based on the perceived harm or impact to their resources due to authentication errors. The accompanying specification SP 800-63 by the US National Institute of Standards and Technology (NIST), called the 'Electronic Authentication Guideline', was first published in January 2004 and then a revised version in April 2006 [NIST-SP800-60], defines specific technical requirements for implementing systems achieving each of the four

levels of assurance. The NIST specification takes into account the effects of *registration and identity vetting procedures*, *authentication token types*, *authentication protocols* and *assertion mechanisms* on the authentication assurance levels. To date, the OMB/NIST LoA specification remains the most comprehensive set of guidelines for identity providers to implement systems achieving a defined LoA and for service providers to utilise the LoA for a fine-grained access control. A number of worldwide communities have either adopted this approach or are in the process of making their approaches compatible or interoperable with the OMB/NIST LoA specification. These communities include the governments of US, UK, Australia, Canada, and EU, Higher Education (HE) federations of the US, Switzerland, Denmark, Finland, Sweden, Norway, France and Australia and New Zealand, the US National Institutes of Health [NIH], the US federal Electronic Authentication Federation [EAF] and the industry-led Electronic Authentication Partnership [EAP]. Furthermore, the global industrial body Liberty Alliance [LA] is working on establishing SAML-based open business standards for digital identity management, etc.

To the best of our knowledge, the first effort to put the LoA-linked access control concept into software implementation was made by the FAME-PERMISS project [FAME-PERMISS] funded by the JISC. The project developed middleware extensions for the Shibboleth infrastructure to facilitate multi-faceted authentication and LoA-linked fine-grained access control. The FAME system integrates a wide range of authentication services, supporting the use of IP addresses, username/password pairs, certificate-based soft tokens and smart cards, and derives levels of authentication assurance in conformance with the NIST standard. Upon a successful authentication with an IdP, FAME derives an LoA value based upon the authentication method and the token used by the user in the authentication instance, which is then transported by the IdP in an SAML [SAML] assertion via the Shibboleth message protocol to a service provider, where it is fed along with the user's other attributes into the PERMISS engine for an authorisation decision. In this way, an authorisation decision is now made based on the following factors (*Subject, Target, Action, LoA*), rather than the traditional (*Subject, Target, Action*).

However, despite these efforts and activities, the definition and application of authentication LoA in the context of Grids and VO environments has not been well examined. Are the existing definitions of LoA suited to the UK education and research community? Are they suited to the Grid and VO environments? How might LoA be employed to safeguard the UK NGS, JISC, ESRC and UKERNA services and 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 of the onerous registration requirements or special condition stipulations due to perceived inadequacies in the strength of authentication? What are the effects of authentication delegation and the use of GSI proxy credentials [GSI] on LoA? Are there any limitations in terms of user accessibility, scalability and interoperability? The ES-LoA project tried to address some of these issues.

2. Aims and Objectives

The ES-LoA project was aimed at finding out the answers to some of 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 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. Through building community consensus in using the appropriate LoAs as defined by the worth and sensitivity of the resources, make recommendations for the appropriate policies and practices for UK services and institutions.
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.

There has been no change to these initial project objectives.

3. Methodology

The project program of work involved four tasks:

- Task 1 - examining existing LoA definitions,
- Task 2 - establishing agreement on LoA definitions,
- Task 3 - investigating current LoA applications, and
- Task 4 - building consensus on LoA applications.

The methodology used for Task 1 is mainly based upon desktop research. We have conducted literature research to investigate existing definitions of LoA, and reviewed on-going efforts made by various international communities (e.g. [OASIS-SAML-TC], [OGF], and [Internet2]) on defining LoA specifications and authentication profiles. In addition, we have also reported our research findings to the international communities and have actively engaged with them for the purpose of consultation, dissemination and soliciting feedback, e.g. via the OGF (Open Grid Forum) LoA-RG research group [LoA-RG] at the last three Open Grid Forums (OGFs) and the IAS07 international conference [IAS07]). The results and outcomes of this task are presented in the Workpackage 1 deliverable 'Using LoA to Achieve Risk-based Access Control: A Study Report' [WP1-D].

Tasks 2, 3 and 4 investigated current applications of LoA in protecting various types of resources, and, through building community consensus, made recommendations with regard to the standard definitions and applications of LoA for both institutions and UK national level services. The methods of stakeholder identification, survey and community consultation were used to perform these tasks, as well as following the developments in the area via different mailing lists, community discussions, and forums. Results of Task 2 are described in Workpackage 2 deliverable 'A Defined Set of LoA Recommendations for the Use within the UK Education and Research Communities' [WP2-D].

It was decided that Tasks 3 and 4 (i.e. investigating current LoA applications and building consensus on LoA applications) should be coalesced into a single task. This was because it quickly became clear that there were very few, if any, existing LoA applications in the HE and FE arenas (although work had been done at the government level in several countries). So the focus shifted to establishing the potential for LoA applications by means of surveys. The results of the two surveys we conducted are given in a two-part report: 'Part 1 - Suppliers' Survey on Levels of Assurance: Report on Brief Survey Findings' and 'Part 2 - Service Providers, Identity Providers and Grid Community Survey on Levels of Assurance: Report on Full Survey Findings', which jointly constitute the workpackages 3 and 4 deliverables [WP3-D].

4. Implementation

4.1. Task 1: Existing LoA Definitions

A thorough reference search was conducted, starting with the first LoA-related efforts by the UK e-Government initiative, and the follow-up LoA specifications by the US OMB and NIST. Various communities were searched or engaged with for signs of LoA activities, including the US government and federal agencies (Electronic Authentication Initiative [EAI] and Federation [EAF]), US national health sector [NIH], governments of Australia, Canada and EU, industrial and private sector (Electronic Authentication Partnership [EAP] and Liberty Alliance [LA]), HE worldwide communities of the US [inCommon], Australia and New Zealand [AAF], Switzerland [Switch], Finland [HAKA], Norway [Feide], Sweden [Swami], Denmark [DK-AAI] and France [CRU], grid community's International Grid Trust Federation (IGTF), open source network consortiums and standardisation organisations (OGF, Internet2, MACE, OASIS SAML Technical Committee, ISO/IEC [ISO/IEC]), etc. We have also followed activities and actively participated in LoA discussions via various mailing lists (MACE's mace-dir and Internet2 shibboleth-users mailing lists, Educause's IdM discussion list, OGF LoA-RG mailing list, etc). In addition, using personal contacts of the project team members, we have informally investigated the current state of LoA developments at selected organisations (e.g. Internet 2, the MAPS Project (Middleware Action Plan and Strategy) at the University of Queensland in Australia, the HAKA HE federation in Finland, the State Library in Denmark, the SWITCH HE federation in Switzerland, the FEIDE HE federation in Norway, and JSTOR in the USA).

4.2. Tasks 2, 3 and 4: Agreement on LoA Definitions, Investigation of Current LoA Applications and Building Consensus

Tasks 2, 3 and 4 were implemented as a 5-step process: stakeholder analysis, framework building, community survey, survey result analysis and further community consultation.

4.2.1. Stakeholder analysis

We framed our approach by identifying stakeholders and made sure that key communities are represented. These include education and research communities at national as well as international levels (e.g. the UK JISC and e-Science communities and the OGF community), international HE federations and commercial service providers. Table 1 gives a detailed list of the stakeholders identified.

The JISC Identity Project were contacted and asked to incorporate certain LoA-related questions in to their extensive survey on Identity Management.

4.2.2. Framework building

The stakeholders were classified into three groups: service providers (SPs), identity providers (IdPs), and the grid community, based upon the aspects of LoA they would be potentially more interested in or concerned with.

Because of doubts about the level of awareness of distributed authentication and authorisation and LoA concepts among commercial and other service providers, the LoA Briefing Paper [LoA-Brief] and Brief Questionnaire [Quest-Brief] were written and distributed to these communities. More information on this exercise is given in section 5.3.1.

Preliminary results from the Brief Questionnaire indicated that the contacted SPs were aware of the underlying principles and some were familiar with the technicalities, so a single consistent approach was feasible and those that indicated willingness to help further (the majority) were contacted again to complete the Full Questionnaire.

The Full Questionnaire was designed to have four sections:

- *Section 1* contained general questions about respondents' institutions and was meant to be completed by all respondents.
- *Section 2* was designed for SPs. It covered various types of service provision, including commercial and not-for-profit network services, as well as services operated within institutions.
- *Section 3* was designed for IdPs, i.e. organisations providing registration and authentication services for users requiring access to protected resources.
- *Section 4* was designed for respondents running or providing services on grids.

4.2.3. Community survey

The full survey questionnaire was distributed using the following three methods:

- Via e-mail attachments to the communities of interest, including the JISC community (through several JISC mailing lists and the UCISA directors mailing list), international federations (listed in Table 1, and commercial SPs (listed in Table 3)
- Via e-Science Newsletters, and
- Via paper distributions at OGF20, NGS User Forum and May 2007 JISC Access Management Programme Meeting.

An on-line version of the Full Questionnaire was also made available on the project's Web site.

The survey was first launched on 1st May 2007, and conducted in three stages with three deadlines set to maximise the number of responses. The first survey deadline was set to 8th June 2007 to allow us to collect the first batch of responses, make initial observations and give recommendations for the follow-on work on LoA ('Initial Survey Findings and Recommendations for Further Work', available at <http://www.es-loa.org/deliverables>), which was due in July 2007. A reminder was then sent out with the second deadline set to 6th July 2007. Another reminder was then sent out with the third deadline set to the end of July 2007.

4.2.4. Full survey result analysis

Survey responses were mostly received via our on-line survey facility, though some arrived via e-mail, and one via post. Responses that arrived via e-mail and post were manually transcribed into a spreadsheet, while those filled-in via the on-line facility were processed through a script to automate the response-to-spreadsheet transcription process. The use of the spreadsheet allowed for automated analysis of survey responses and creation of corresponding charts and histograms, which were included in the survey reports [WP3-D]. Cross-analysis of responses among different questions was also conducted where it was deemed potentially interesting. Several questions were marked down either as particularly interesting or in the need of some follow-up clarification. Authors of such responses were further contacted to confirm the accuracy of their answers.

4.2.5. Further community consultation

Following the analysis of the survey results, two study reports were written describing survey findings and observations. These reports were published on the project website for further community consultation. In addition, we used the following methods to solicit further comments and feedback on our survey findings.

- After collecting the first round of survey responses in July 2007, we followed this up by e-mailing the survey respondents asking for their further comments by 21st September 2007.
- We organised a panel session on the use of LoA for aiding the e-infrastructure security in conjunction with the third International Symposium on Information Assurance and Security (IAS07), held on 29-31 August 2007 in Manchester, for consultation with a wider community and for soliciting feedback on the survey findings.
- We continued to engage with the grid community, reporting our findings and soliciting comments and feedback from them via the OGF's LoA-RG (Levels of Assurance Research Group) facility. The chair and document editors of this research group are three members of the ES-LoA project team.
- In collaboration with the Identity Project [ID], we incorporated a small number of LoA-related questions into their 'Identity Management Survey' and used their results to cross-check with our findings and to see what we can derive from their results in relation to LoA issues.

5. Outputs and Results

The ES-LoA project has produced the following outputs.

5.1. Review of Existing LoA Definitions

As part of WP1, we conducted an up-to-date review and investigation of current definitions of LoA at national and international levels [WP1-D]. To date, the US Government's efforts in defining LoA are by far the most complete and comprehensive. The specification comprises two companion documents: the Office of Management and Budget's (OMB) Memorandum 'E-Authentication Guidance for Federal Agencies' [OMB-M0404] and the National Institute of Standards and Technology's (NIST) SP 800-63 'Electronic Authentication Guideline' [NIST-SP800-63].

This specification defines a 4-level (Levels 1 to 4) LoA model in terms of likelihood of authentication errors and misuse of credentials, where Level 1 is defined as the lowest and Level 4 as the highest. The OMB Memorandum specifies a set of guidelines to assist organisations to carry out risk assessments due to unauthorised access to their resources as a result of authentication errors, and to help them to classify resources into four classes based on the severity or impacts of the identified risks. Impact profiles are provided to allow the mapping of identified risk levels to appropriate assurance levels, so that a request to access resources in a particular class should only be granted provided that the user requesting the access has been identified and authenticated to the minimum LoA level as required by that resource class. The higher the sensitivity level of the resources, the higher the potential impact or harm it would cause should the underlying authentication process fail, and the higher level of the authentication assurance is required. The related NIST guidelines further specify detailed technical requirements on how to achieve these four levels of authentication assurance, in terms of user registration, identity vetting, credential issuance and management, authentication protocols, the strength of authentication credentials and tokens, and authentication assertions in cases where users are identified by a third party IdP.

The OMB/NIST 4-level LoA model has been accepted by e-government, e-commerce and research initiatives in several countries. The approach has already been implemented by the US government's E-Authentication Initiative (EAI) and E-Authentication Federation (a partnership between the US federal agencies and private sector organisations), which has also struck an inter-federation interoperability partnership with the US InCommon HE federation. The US National Institutes of Health (NIH) together with US InCommon HE federation are making an inter-federation pilot [NIH-Pilot] that will allow users from the HE sector to access NIH resources based on their authentication LoA. Governments of the UK, US, Australia and Canada, the industrial and private sectors' Liberty Alliance and E-Authentication Partnership (EAP), the HE federations of the US, Australia and New Zealand, Switzerland, Finland, Norway, Sweden and Denmark have also decided to go along the same route and either adopt the NIST approach fully or make their systems compatible with it. For example, the US InCommon HE federation has defined two of their own authentication profiles, called Bronze and Silver, which directly map onto NIST Levels 1 and 2. Therefore, a critical mass of institutions that are taking on this approach has already been established.

5.2. Identified LoA Stakeholders

Our stakeholder analysis has come up with the following list of institutions and organisations from the communities concerned, namely, the JISC community, the e-Science/grid community, commercial service providers, international federations, and certification authorities, which may have interest in the adoption of LoAs.

Table 1: Stakeholders

Stakeholders	Interest / stake in LoA	Importance
JISC Community		
UKERNA and UK NGS	High	High
JISC middleware projects, MIMAS & EDINA, Other JISC service providers, e.g. UKDA and EduServ	Medium	Medium to High
E-Science/Grid		
GridSite	High	Medium
Public Health Research, PsyGrid and CLEF-services (for NHS)	High	High
White Rose, TERENA, Portal users and developers (via ShibGrid and GridShib), VO's (GridPP/NeS/LC), CTS, OASIS, UK E-Government	Medium to High	Medium to High
Other service providers		
Major publishers, e.g. Elsevier, Thomson, IoPP; Subscription agents, e.g. Swets and EBSCO; Intermediaries, e.g. Ingenta; Database suppliers, e.g. Ovid; Technology vendors, e.g. Xrefer and Ex Libris; and others, e.g. ONS.	Medium	Medium to High
International federations for information:		
US InCommon, Internet2, Australia MAMS, Finland HAKA, Denmark DK-AAI, France CRU, Norway FEIDE, Switzerland SWITCH	Medium	Medium to High
Certificate Authorities:		
Verisign, IGTF, OGF CLOPS – WG, UK e-Science CA	High	High

5.3. Community Consultation

5.3.1. The Brief Survey – rationale and results

At the start of the project, during the Stakeholder Analysis and Risk Assessment, it was unclear to what extent commercial organisations such as academic publishers, subscription agents, database suppliers and similar organisations were even aware of distributed authentication/authorisation models such as Shibboleth, or the concept of different levels of confidence (assurance) in the authentication process.

In order to find out more about this community, two items were prepared:

- a two-sided briefing document titled 'LoA Briefing Document' explaining concepts such as authentication, authorisation and assurance and the background to the project [WP3-D].

- a brief, two-sided survey form containing eight simple questions, including two inviting free-text answers [WP3-D].

A total of 30 organisations were contacted directly, either in person at events such as the UK Serials Group conference, the Library and Information Show at the NEC, and the Umbrella Conference at the University of Hatfield, or by email. There was also a return from a grid research team in Greece that presumably was the result of general publicity through emails to lists, or the project website.

24 publishers/intermediaries were contacted. In addition four European federations, in Norway, Finland, Denmark and Switzerland, were invited to complete either the brief or full survey.

A total of 19 responses to the brief survey were received. Four of the contacted organisations completed the more detailed full survey instead of the brief one. Seven organisations completed both brief and full surveys. The project team are grateful for their time and effort spent on these surveys.

The results can be found in the report 'Suppliers' Survey on Level of Assurance: Report on Brief Survey Findings' [WP3-D] and were somewhat of a surprise to the project team. All but two of the respondents said they were implementing or planning to implement a federated access management scheme such as Shibboleth. The two who were not were arguably outside the mainstream UK HE/FE communities (one was a national library and the other a Greek research institute).

Even more surprising was the response to a question about understanding of LoA concepts with at least 89% of respondents answering positively, though there was a more mixed picture in response to the question about how well informed the respondents' organisations were on the subject. Equally surprising was the figure of 56% claiming their organisation had considered or investigated possible applications of LoA. These figures should perhaps be treated with some caution; the high numbers could be a mixture of an effective briefing document plus a self-selecting body of respondents.

The first of the two free text questions asked respondents for examples of services where they would like to be able to require higher levels of assurance before granting access. Respondents suggested five different areas:

- *Financial*: several respondents wanted higher levels of assurance for money transactions
- *Sensitive content*: examples given included health information and exam papers.
- *Account maintenance and administration*: examples included changing or resetting passwords.
- *Author/editor/reviewer access to pre-publication material*: mentioned by three publishers.
- *Membership privileges*: society membership, premium services.

The second free text question asked for reasons why organisations might have considered LoA but decided it was not applicable to their services. Several said that, while they don't think it appropriate at the moment, they envisaged possible applications in the future. One said they already employ different levels of security, but didn't reveal how they did this. One major publisher expressed concern about making their site more difficult to use than competitors.

5.3.2. The Full Survey – results and observations

In the following, we summarise the major findings and observations from the full Survey, and then go through the findings specific to service providers, identity providers and grid community. Full details can be found in the WP3 deliverable, 'Service Providers, Identity Providers and Grid Community Survey on Levels of Assurance: Report on Full Survey Findings' [WP3-D].

A total of 30 organisations responded to the Full Questionnaire [Quest-Full], mainly from the UK and worldwide HE federations. We had a good spread of different types of organisations - identity providers, service providers, publishers, Certification and Registration Authorities, grid service providers, etc, a surprisingly large number of which (77%) classified themselves as innovators or early adopters.

Summary of service providers' responses:

- *Adoption of Federated Access Management (FAM)*: A vast majority of service providers (88%) is either adopting or planning to adopt FAM, roughly half of which have partly or fully operational deployments. Two responded negatively, one of which is outside the UK and the other is concerned with medical and health information.
- *Service provider's LoA requirements*: The questionnaire was designed to investigate the current applications of LoA to various types of resources and to understand LoA requirements from

service providers' perspective. We needed to find out if service providers performed risk assessments, and if they did, what are the perceived impact levels of the identified risk categories. This would enable us to map the potential impact levels to the required assurance levels (as recommended by the OMB guideline) for user authentication and identification.

- Half of the respondents claimed to have carried out some form of risk assessments on the consequences of unauthorised access to their resources, and a further 12% are planning to do so.
- Respondents were asked to look at the following impact categories: *damage to reputation, harm to systems, assets or public interests, financial loss or potential legal liability, unauthorised release of sensitive information, potential for legal action, and personal safety or security*, and rate the level of perceived impact in each category as 'Low', 'Medium', 'High' or 'N/A' if they do not perceive any harm from a particular impact category. From the responses we are able to create an impact profile and then compare it to the impact profiles associated with each assurance level given by the OMB guideline. From this analysis, we are able to make the following observations: (1) damage to reputation; harm to systems, assets or public interests; financial loss or potential legal liability; and unauthorised release of sensitive information are the top four risk categories perceived by the respondents to have medium to high levels of impacts (these may require an LoA level of 3 or 4); (2) almost all service providers (93%) require some level of confidence in an asserted user's identity (equivalent to Level 2), while about half (46%) claim to have resources that would require a high level of confidence and 27% have resources requiring a very high level of confidence. There also appears to be a correlation between service providers requiring the highest LoA and those perceiving risk impacts to their resources as stronger, which is in line with the OMB-proposed approach to risk-based access control. In addition, for a small proportion of responding service providers (11%), who were not employing or were not sure about employing Federated Access Management, their overall perceived impact of risk was high to medium in the four most important impact categories. This leads us to the conclusion that there is a proportion of service providers that have some high-value assets that they are not willing to share or make available through a federation. However, the majority of those service providers are from outside the UK.
- 70% of the service providers agree that more valuable or sensitive resources should be matched with a stronger form of user identification and authentication. On a scale of 1 to 4, nearly all the service providers said that they needed some confidence in a user's identity (Level 2), and 27% of them required the highest level (Level 4). These 27% also seem to correlate with the service providers perceiving risk impacts to their services as strong, i.e. those wanting the highest LoA are the ones most concerned about damage to reputation or system security. No correlation appears to exist between attitude to joining a federation and those wanting a high LoA.
- In cases where authentication is performed by a third party identity provider, almost all service providers wanted to know the mechanism by which a remote user was identified and authenticated. Confidence in 'quality' of users' attributes (i.e. attribute LoA) appears to be as important as confidence in 'quality' of authentication (i.e. credential LoA).
- Almost all service providers surveyed (92%) would be willing to respect some national or international standards or guidelines on e-authentication, and a great majority (80%) would want medium to high levels of federation governance to be in place to ensure that users are identified with a certain degree of confidence before they are allowed to access their resources. Only a small number (4%) were against any form of governance regarding LoA. 77% of service providers believe that putting some formal LoA guidelines into practice within a federation would make them more willing to share their more valuable or sensitive resources, while only 7% think that imposing LoA guidelines would make no difference.
- 68% of service providers agreed that some of their resources were more sensitive than others, but a small majority (61%) of them nevertheless uses the same authentication procedure for all resources (perhaps because they do not have any alternative due to a lack of LoA applications).

Summary of identity providers' responses:

- **Adoption of FAM:** All the identity providers surveyed have implemented, are currently implementing or are planning to, implement FAM.

- *LoA procedures and implementations from identity providers' perspective*: Survey questions were designed to investigate current user identification and authentication procedures used by the IdP community, so as to allow us to identify any gaps in existing policies, infrastructures and implementations for the long-term use of LoAs. The following summarises our findings:
 - Username and password pairs, sent over a TLS/SSL channel, seem to be the most widely used authentication method among the identity providers. However, several other authentication mechanisms, e.g. Kerberos tickets, soft and hard PKI credentials, proxy credentials, are also supported by a good number of IdPs; 57% of the IdPs claimed that they already support the use of multiple authentication mechanisms. When asked who actually made the decision as which authentication method to use at run time, the survey revealed that 22% of the cases were made by SPs, 33% by users, and 45% by IdPs.
 - For organisations that support different authentication mechanisms and authenticate users from both within and outside their administrative domain, 86% said that they do not impose different authentication methods to identify home and foreign users. In cases where the respondents support the use of more than one authentication methods, the following details the resource types for which (or other circumstances under which) different authentication method was used:
 - A UK e-Science establishment is using a combination of username/passwords and proxy credentials; the latter are used for NGS and GSI applications.
 - An international science laboratory uses a combination of username/passwords and PKI credentials stored in both browsers and smartcards; smartcard credentials locked with PIN are used for highly secured experiments.
 - A foreign national e-Science centre is currently using username/passwords, but is experimenting with PKI/smartcards which are currently not in production use and are also waiting for Shibboleth v2.0 that will support SAML v2.0.
 - A foreign national identity federation is currently using username/passwords and PKI certificates from browsers and smart tokens; so far PKI credentials are just used as an additional way of authenticating but are not yet required by any application since they still do not have applications that require the higher LoA a user gets using PKI.
 - A UK University Computing Services unit is using username/password pairs and proxy credentials; they also use forwardable Kerberos tickets for some back-end services (e.g. IMAP).
 - A grid member is using PKI credentials stored in browsers for accessing Web pages (such as Wikis); PKI and proxy credentials stored on file systems are used to access grid resources (such as Resource Brokers, Computing Elements, Storage Elements); PKI credentials stored in hard tokens may be used via browsers to access Web resources or to generate a proxy to access grid resources.
 - A US based national laboratory controls access to CA operations by hard tokens.
 - A large proportion of institutions (92%) authenticate users that are both on and off-site, and 42% of them said that the same authentication method is required for both user groups, while the rest said that the same authentication method is sufficient. That is, a majority of the IdPs surveyed do not see the need to differentiate between on and off-site users when choosing authentication methods.
 - In terms of user registration, identity vetting and record keeping, we investigated current practices employed by IdPs in order to see to what extent they already satisfy the requirements specified by NIST. The survey results show that 67% of the responding IdPs currently do not even satisfy the minimum record keeping requirements for the NIST Level 2. As far as in-person user registration and identity vetting is concerned, almost all IdPs record user's full name, but only 30% ask for date of birth and 30% record home address, and many do not verify the supplied data. For remote registration, 83% based their verification on previously issued matriculation cards or payroll numbers. In either case, not even NIST Level 2 requirements are being met. However, it should be taken into account that the NIST specification was designed for federal agencies, which have different user registration and identity vetting procedures. The federal agencies can access federal databases for cross-checking users' driving licences or passports, which is currently not available to the HE

community. As far as record keeping is concerned, 75% of identity providers preserve user registration records. However, among these, only 8% keep them for more than 7 years and 6 months, which is the minimal requirement for Level 2 according to the NIST specification. Authentication protocols supported by identity providers involve sending unencrypted passwords over a network in 8% cases (not even achieving Level 1), password challenge-response protocols in 25% cases (nearly reaching Level 1), encrypted passwords sent over a TLS/SSL session in 92% cases (aiming at Level 2), Kerberos tickets in 25% cases (Level 2) and certificate-based authentication in 25% cases (Levels 3 and 4).

- As username and password based authentication is by far the most prevalent among the IdP community surveyed, we further investigated if they have imposed any criteria for password selection, password validity periods, and the number of unsuccessful attempts allowed before an account being locked out. These parameters affect the password entropy (i.e. the 'strength' of a password). Knowing the answer to these parameters would allow us to deduce if the IdPs concerned could achieve NIST Levels 1 or 2 (note that NIST LoA Levels 3 and 4 do not allow the use of password based authentication methods). As it turned out, only four respondents provided some of the required information, and only two out of the four provided enough information for us to conclude that neither of the two satisfies even the minimal requirements for Level 1. One of the two IdPs could achieve Level 1 by further imposing a 7-character password length from a 94-character alphabet (requiring at least one special character) and checking for dictionary collisions. Increasing the password length to 8 characters would help them achieve Level 2. With regard to the other IdP, if it were to achieve Level 1, it would have to make changes to several of their password management practices: to reduce the number of password guessing attempts and to impose dictionary collision checks. In order to achieve Level 2, they would in addition have to reduce the password validity period and increase the time period during which unsuccessful password trials are measured. This leads to the conclusion that, even among password-based authentication systems, a multitude of different practises are in place and, thus, policies and guidelines are required on the selection and management of passwords and on the enforcement of these policies.
- *Attitude towards formal LoA governance:* 83% of the IdPs surveyed would be willing to follow some technical guidance on LoA if there were any, and 92% of the IdPs would be willing to adopt the risk-based approach to access control that incorporates LoA.
- *The use of attribute assertions:* Nearly two thirds of identity providers supply identity assertions. Federations appear to be the biggest consumers of identity assertions - 86% of the IdPs surveyed issue identity assertions to institutions in the same federation or within the same country. External academic and commercial services seem to be the major consumers of the assertions. However, IdPs are currently not issuing identity assertions to governmental services, and there may be an overlap in LoA-related efforts between the HE communities and the government sector, since various governments seem to be taking the same risk-based approach.

Summary of the e-Science/grid community's responses:

Survey questions were designed to investigate the types and sensitivity levels of applications and services currently managed in grids, along with the associated authentication requirements. The following summarises our findings.

- *Service types exposed via grid mechanisms:* resource brokers (22%), computer applications (15%), collaborative environment (14%), visualisation (7%), application hosting (7%), computer terminal access (7%) data sets (7%), databases (7%), other (7%), and credential translation (0%).
- *Sensitivity levels of the data available through grids:* 30% of respondents rated their resources as extremely sensitive (could potentially require Level 4), 20% as highly sensitive (could potentially require Level 3), 30% as somewhat sensitive (could potentially require Level 2), 20% as hardly sensitive (could potentially require Level 1), and none of the respondents claimed that their data is not sensitive at all. In other words, all respondents place some level of sensitivity on their data, and there is a fairly even distribution across the range of sensitivity levels.
- *Risk levels experienced by grid service providers:* To evaluate risk levels, we put forward some questions to see if there are higher risk services in grids. A large proportion (80%) of grid service providers allow user-generated code to be run on their systems, which can potentially increase the risk to service provider and may affect the LoA value required. In addition, 80% of grid service

providers also provide access to powerful compute resources. Again, these providers are in a greater risk from authentication errors as consequences of misuse of their resources can be more costly.

- *Grid authentication requirements*: All respondents said that they required users to be identified with some level of certainty. In order to achieve this level of certainty, 90% of respondents said they were able to use a PKI with one or more certificate authorities vouching for users' identities; 80% said they were able to do this by direct key exchange; 10% said they were able to do this by other means which, in this case, was via a community portal. Furthermore, the survey shows that 80% believe they are able to achieve a sufficient level of authentication on grids. Those 20% that think current grid authentication is not enough feel that this is because of the grid community's reluctance to standardise and agree on mechanisms or the lack of traceability between the work done on a worker node with the identity (e.g. certificate's subject DN) recorded at the start of the job. In addition, one grid provider within the area of research involving medical records noted that there were unique and complicated requirements for identification of users in the medical area and these are currently being established. Requirements for user identification are more complex and challenging in the context of medical applications, and access control has to be more sophisticated and rigorous. They believe that current grid middleware cannot satisfy their needs and more work is needed to establish the requirements themselves as well as the grid middleware that can provide them.
- *Enforcement of Certificate Practices/Certificate Policy Statements (CP/CPS)*: Three quarters of grid service providers require a CA to publish a CP/CPS, and 84% of them require the CA to actually adhere to its own CP/CPS. However, even among those who require the CA's adherence to its own CP/CPS, under half of them do not actually have mechanisms in place to ascertain this. The rest rely on a third party accreditor (typically IGTF, which has a similar role to the role of metadata in Federated Access Management).
- *Requirements imposed on certificate chains*: Certificate chain lengths are not perceived as an important factor when determining the strength of authentication to the majority of grid resource providers; however, a fair proportion of respondents were unsure as to the affect of differing certificate chain lengths in the process of a PKI authentication.
- *Requirements imposed on namespaces*: The purpose of the questions was to highlight the split between the PKIX community's idea of authorisation based upon X.509 certificates and the grid community's. The majority of grid service providers (66%) require a well defined namespace. Grids have evolved in such a way as to have a multiplicity of top level CAs. In such an environment each CA has the ability to assert an identity in terms of a global namespace – the distinguished name (DN). In principle, a CA is not restricted from assigning any name which suitably describes an individual, however, with multiple autonomous authorities it becomes apparent that an identity in the partial X.500 namespace used in certificate based PKIs can be claimed by more than one individual. Therefore either the CAs need to share information about their subscribers' identities or they must distribute assertions corresponding to a hierarchical namespace to which each CA controls an independent proportion. Responses show that there is a fairly even spread of whether this is a policy or an implementation requirement. A significant number (17%) said that they did not require meaningful namespaces or were not sure (17%). Note that Globus-based authentication and its derivatives require a well-defined Namespace, meaning that those 17% that answered negatively (and probably some of those 17% that were unsure) are not using Globus for their grid service provisions.
- We also asked if they require that a CA issue certificates with "meaningful names" in the *commonName* field (i.e. not anonymous pseudonyms), just under two thirds of grid services felt it was important to be able to have a verifiable "Meaningful Name" asserted during access to their services. Of those who did not feel this was an important requirement, two thirds require traceability to the end user to be maintained. One respondent commented: '*We are required as CA operators to issue "meaningful names", although "meaningful names" is inherently meaningless*'. Others that answered negatively did not provide their reasons for not requiring a CA to issue certificates with meaningful names in the CN field. When asked if they would impose restrictions on elements allowed in Distinguished Name (e.g. must not use *emailAddress*). 50% responded with 'Yes', 25% with 'No' and 25% with 'Not sure'.

- *Grid authorisation mechanisms*: Respondents indicated that authorisation took place by 'Virtual Organisation' (40%), by 'lookup of locally stores X509 credentials' (20%), by 'lookup list of certificate DNs (20%), by 'External rule (e.g. time/system load)' 10%, and 10% 'by other'.

Those who control access to their grid services by Virtual Organisation were further asked if they required the VO to be associated with a legal entity. Two respondents answered this part of the questions despite previously saying they did not control access to their grid services by a VO, one of which answered positively.

Of those who did answer 'Yes' to controlling access via a VO, none require a VO to be associated with a legal entity. Those who answered positively were also asked if they used the embedded attributes for making authorisation decisions and 75% of respondents replied positively.

- A large proportion of grid service providers seem unaware or ambivalent to the impact of users' management of their identity credentials, placing little or no extra checking for GSI proxies over direct X.509 credentials (with GSI proxies being arguably a much weaker security assertion since they are stored in unencrypted form on machines and, despite generally having short lifetime (typically 12 hours), there is no actual restrictions on how long they can be valid for (apart from the lifetime of original certificate used to create the proxy)). We tried to investigate whether grid service providers limit access based on the length of the period the proxy itself is valid for, and not whether it is valid at the point of access. For example, if a proxy is valid for one month (in contrast to 12 hours which is general practice but not the rule), there is more chance an attacker can get hold of and use it. This is generally not acceptable behaviour (i.e. to have a proxy valid for more than 12 hours), but no one seems to check for it. Restrictions based on proxy lifetimes and proxy path-lengths could help services to enhance their security. Personal experience leads to a conclusion that respondents confuse these two forms of lifetime restrictions and are just verifying that the proxy certificate is within its valid lifetime, and no further checking takes place. For this reason, we have a higher number than expected of respondents who believe they are using lifetime restrictions of GSI proxies, and we are unable to distinguish between these.

5.3.4. Summary of the further community consultation

We teamed up with the related Identity Project [ID] and suggested they incorporate several LoA-related questions we had drafted into their Identity Management Survey. From their findings, it can be concluded that what institutions term as "graded authentication" is directly relevant to LoA, and that institutions clearly perceived the need for graded authentication with a score 4.31 out of 5 that was actually higher than the need for Federated Access Management (which scored 4.29 out of 5). However, as far as being able to implement graded authentication, institutions felt they were between "not very well" and "okay" (scoring 2.41 out of 5). In addition, it was reported that "the main areas where policies are not as widespread are the areas of establishing identities of visitors, graded authentication, and user authorisation.", as well as that "for graded authentication, 20% have a completed policy, 30% have a draft policy, and 44% have neither." The conclusion is that authentication LoA is recognised as being important, but policy and actual implementations are scarce.

During the LoA panel session held at the IAS07 conference, we raised certain questions regarding limitations of existing access control systems, practical implementations or barriers to successful adoption of LoA, etc. The response of the attendees mainly revolved around the lack of access and trust negotiation mechanisms, the lack of definitions of authorisation classes and the lack of user feedback to the introduction of LoA and how would that affect/disrupt their current authentication procedures and who would bear the cost of higher authentication LoA. Also, additional factors affecting LoA were recognised (such as trust level and organisational category) and questions were raised as to who would define and maintain the ultimate LoA across all services/institutions/institution types/countries/etc.

5.4. Publications and Dissemination Activities

The project has produced the following publications for the purpose of disseminating the project outputs:

1. Ning Zhang, David Groep, Blair Dillaway, *E-Infrastructure Security: Authentication Levels of Assurance*, presentation at the LoA BoF session, the 19th Open Grid Forum (OGF19), Chapel Hill, North Carolina, USA, January 29 – February 2, 2007, <http://www.ogf.org/OGF19/materials/561/LoA-Bof.ppt>

2. Ning Zhang and Yoshio Tanaka, the Authentication Levels of Assurance Research Group (LoA-RG) session talk, 20th Open Grid Forum (OGF20), Manchester, UK, May 9-11, 2007, <http://www.ogf.org/OGF20/materials/723/OGF20-LoA-RG.ppt>.
3. Draft LoA-RG deliverable, A Gap Analysis of Current LoA Definitions vs. LoA Requirements in e-Science/Grid Context, submitted for discussion to the 21st Open Grid Forum OGF21, Seattle, Washington, October 15-19, 2007.
4. Aleksandra Nenadic, Ning Zhang, Li Yao, and Terry Morrow, "Levels of Authentication Assurance: an Investigation", Proceedings of the Third International Symposium on Information Assurance and Security (IAS07), IEEE CS Press, ISBN: 0-7695-2876-7, August 2007, Manchester, UK, available upon subscription at <http://ieeexplore.ieee.org/xpl/periodicals.jsp>.
5. Ning Zhang, Mike Jones and Terry Morrow, Consultation slides presented at the LoA Panel, Third International Symposium on Information Assurance and Security (IAS07), 29th August 2007, <http://rpc234.cs.man.ac.uk/joomla/images/stories/ias07-loa-panel.pdf>.

5.5. Engagement with the Communities of Interest

The project team has attended the following events for the purpose of engaging with interested communities, consultation and dissemination of our results.

29 Jan - 2 Feb 2007: Four project team members attended the 19th Open Grid Forum (OGF19), where we chaired the LoA-BoF session. During the session, the current definitions of LoA and the gaps between existing LoA definitions and e-Science/Grid use cases were outlined, and a decision was made to establish a RG within OGF to address these issues.

13 Mar 2007: A project team member attended at the JISC Conference in Birmingham, where contacts were made with representatives of Ovid and the Open Group in the trade exhibition.

16 - 18 April 2007: Two project team members attended the UK Serials Group conference which was held at Warwick University, where they made short presentations during each of the JISC Federated Access Management briefing sessions. They also handed out copies of flyers along with our Brief Questionnaire, and spoke to several companies, including Blackwell Publishing, Cambridge University Press, Ex Libris, Ingenta, Institute of Physics Publishing, John Wiley, Ovid, Oxford University Press and Taylor and Francis.

19 April 2007: A project team member attended to the Library and Information Show in Birmingham and had useful conversations with British Library, Emerald Group, ProQuest, Swets Information Services, and Thomson Learning.

1 May 2007: The ES-LoA Full Survey Questionnaire was launched through direct contacts with service providers, UK HE IT directors' list (UCISA), JISC Middleware mailing list, and National e-Science Centre Newsletter.

3 May 2007: A project team member attended the JISC Identity Providers Workshop, which provided an insight to service providers' perspective. The ES-LoA project and its aims were introduced to attendees.

7-11 May 2007: Four project members attended the 20th Open Grid Forum (OGF20) and the 2nd EGEE user forum, where we chaired the LoA-RG session. During the session, detailed discussion on LoA attributes, credential issuing and security methods were discussed. Current and envisaged grid authentication use cases and architectures were suggested, and some weaknesses identified. The group concluded that there are many gaps between the NIST definitions and the LoA use cases identified. We advocated the ES-LoA project activities and surveys at the ESNW booth, at a number of OGF groups and through networking activities. Paper copies of the LoA Full Survey Questionnaires were distributed.

29-30 May 2007: We attended the JISC Access Management Transition Programme Meeting, where we distributed the ES-LoA Full Survey Questionnaire.

28-30 June: We attended the CILIP Umbrella 2007 Conference at the University of Hertfordshire and contacts were made with the service providers who were exhibiting there.

29 Aug 2007: We chaired an LoA plenary session at the IAS07 conference in Manchester, UK. Our survey findings were reported in the session, and feedback was solicited.

10–13 September 2007: Two project members attended the UK e-Science All Hands Meeting, and disseminated the project outcomes via the poster and flier.

15–19 Oct 2007: A project member attended the 21st Open Grid Forum (OGF21). The LoA-RG draft deliverable on gaps between current LoA definitions and LoA requirements in an e-Science/grid context, prepared by the team members, was submitted for discussion.

Through these engagement activities, contacts with the following groups/entities have been established:

Table 2: The e-Science/Grid Group

The UK Engineering Task Force
The UK National Grid Service Operations
The UK's GridPP (Particle physics Grid)
The LHC Computing Grid
The International Grid Trust Federation
The OGF Certificate Operations Working Group
The US' SURAGrid
The US' Open Science Grid
The US' TeraGrid
The PERMIS-Users mailing list via contact with David Chadwick
Grid-Ireland / Trinity College Dublin

Table 3: The Service Provider Group

BioMed Central	OCLC PICA Ltd
Blackwell Publishing	Ovid
British Library	Oxford University Press
Cambridge University Press	ProQuest CSA
EBSCO Information Services	Royal Society of Chemistry
Elsevier	Springer
Emerald	Swets Information Services
Ex Libris Group	Taylor & Francis Group
Ingenta plc	Thomson Learning
IOP Publishing	XRefer
John Wiley & Sons Ltd	

6. Outcomes

The project has been successful in achieving a deeper understanding of the access control needs of relevant communities including identity providers, JISC-funded service providers, database suppliers, subscription agents, academic publishers, registration authorities and certification authorities.

The project team established a notable presence at both national and international levels in the LoA arena, by engaging with communities of interest at various events and via e-mail, by participating in discussion lists and through our survey questionnaires, and by organising and chairing several LoA-related events.

All the projects objectives were achieved and the planned deliverables produced. The only exception was Objective 3 where it soon became apparent that, within the community we were surveying, there were effectively no existing applications of LoA. We therefore used the survey feedback to create the recommendations for Objective 4. The outcomes of the main objectives are summarised as follows:

- *Objective 1: to investigate existing definitions of LoA at both the UK and international levels.*
Our findings are available in the WP1 report 'Using LoA to Achieve Risk-based Access Control: A Study Report' [WP1-D].
- *Objective 2: to build community consensus and make proposals with regard to standard definitions of LoA for use within the UK education and research community.*
Our recommendations can be found in the WP2 report 'A Defined Set of LoA Recommendations for the Use within the UK Education and Research Communities' [WP2-D].
- *Objective 3: to examine the current applications of LoA to various types of resources, including Grid/e-Science resources, library resources and e-learning resources.*

The findings of the surveys conducted can be found in two WP3 reports: 'Suppliers' Survey on Levels of Assurance: Report on Brief Survey Findings' and 'Service Providers, Identity Providers and Grid Community Survey on Levels of Assurance: Report on Full Survey Findings' [WP3-D] .

- *Objective 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.*

The recommendations for policy and practice are contained in this report and the WP2 deliverable report 'A Defined Set of LoA Recommendations for the Use within the UK Education and Research Communities' [WP2-D].

- *Objective 5: to identify any gaps in existing authentication and authorisation policies, procedures and infrastructure structure and processes in the use of LoA in long term in the UK education and research community.*

The gap analysis and recommendations for future work on how to bridge the gaps in federated environments are available in our interim report to JISC 'Initial Survey Findings and Recommendations for Further Work' and the WP2 report 'A Defined Set of LoA Recommendations for the Use within the UK Education and Research Communities' [WP2-D].

7. Conclusions

Through a combination of research and survey analysis, we report the following findings and observations.

- The project researched and identified existing standard definitions of LoA suited for use within the communities concerned.
- It identified some gaps in existing authentication and authorisation policies, procedures and infrastructure that need attention if the JISC is to attract more resources and service providers into the UK federation.
- Among the communities surveyed there does appear to be a significant interest in, and demand for, a viable, fine-grained access control framework. Such a framework needs to support the tailored protection of resources with varying levels of sensitivities in order to achieve an optimum balance between Identity Management costs and the risks of any security breaches.
- One way of achieving this is to use LoA-linked fine-grained access control. That is, for higher value assets, or resources with a higher sensitivity level, a higher LoA should be required. The values of LoA are governed by the identity vetting and authentication policies and procedures, and the authorisation process should take the LoA as a decision parameter.
- In order to investigate issues related to the real-life deployment of the LoA-linked fine-grained access control solution in a federated environment, and to provide a demonstrator for those who want to achieve better understanding of the concept, the project has concluded that there would be significant value in the creation of a working demonstration system employing LoA concepts.

The following is a more detailed summary of the major conclusions to be drawn from the study.

Existing LoA Definitions

- The OMB/NIST 4-level LoA model has been widely accepted by e-government, e-commerce and a number of research initiatives. A critical mass of institutions adopting this approach has been established.

Service Providers

- Respondents involved in service provision completed either the Brief Survey or the Full Survey or both. The vast majority of these have either adopted or are planning to adopt a Federated Access Management (FAM) system.
- The great majority of service providers claimed to understand LoA concepts.
- Five areas were suggested by SPs as potential applications of LoA: financial transactions, sensitive content, account maintenance, controlling access to pre-publication material, and membership privileges.

- Half of respondents claimed to have carried out a risk assessment of unauthorised access to their resources.
- Damage to reputation, harm to systems, assets or public interests, and financial loss or legal liability were perceived to be the top three risk categories for unauthorised access.
- 93% of service providers require some confidence in a user's identity.
- 70% of service providers think that more valuable/sensitive resources should be protected by a stronger form of user identification/authentication. Currently 61% use the same authentication procedure for all resources.
- Almost all respondents are willing to respect national or international standards on e-authentication. The great majority want medium to high levels of federation governance.

Identity Providers

- All respondents have implemented, are implementing, or are planning to implement FAM.
- Unsurprisingly, username/password pairs seem to be the authentication method of choice for the majority of IdPs. However, many other mechanisms are also in use. 57% claim to support multiple authentication methods.
- 86% do not use different methods for home and foreign users.
- The majority of IdPs do not differentiate between on-site and off-site users.
- In terms of user registration, identity vetting and record keeping, IdPs current practices were checked against the current NIST requirements. 67% do not even satisfy minimum record keeping requirements for Level 2.
- In neither in-person registration nor remote user registration was NIST Level 2 being met. However the NIST specification was designed for federal agencies which have different procedures and databases for cross-checking. 75% of IdPs preserve user registration records, though only 8% keep them for more than 7years and 6 months (the NIST LoA standard for Level 2).
- The criteria for password selection, periods of validity, and the number of unsuccessful attempts allowed were investigated. None of the respondents could satisfy even the minimal requirements for NIST Level 1. The survey revealed a multitude of different practices.
- 83% of respondents would be willing to follow some technical guidance on LoA and 92% would be willing to adopt a risk-based access control approach incorporating LoA.

e-Science/Grid Community

- A wide variety of service types are exposed via grid mechanisms including resource brokers, computer applications and collaborative environments.
- All respondents attributed some level of sensitivity to their data, fairly evenly distributed across the levels from Level 1 (20%) to Level 4 (30%).
- 80% of grid service providers allow user-generated code and/or access to powerful compute resources.
- All respondents require users to be identified with some level of certainty and 90% use a PKI and one or more certificate authorities.
- Work involving sensitive medical data requires user identification at a higher level than currently provided by grid middleware.
- 75% of grid service providers require a CA to publish Certificate Practices/Certificate Policy Statements (CP/CPS) and 84% require the CA to adhere to these. However half of them do not have mechanisms to ascertain this.
- The majority of grid service providers (66%) require a well-defined namespace.
- Just under two thirds of grid services said it was important to have a verifiable "Meaningful Name" asserted during access to their services.

- Authorisation mechanisms in use include: 40% by 'Virtual Organisation', 20% by 'lookup of locally stored X509 credentials', 20% by 'lookup list of certificate DNs', and 10% by 'external rule'.
- A large proportion of grid service providers seem unaware or ambivalent regarding users' management of their identity credentials.

Additional consultations

The JISC-funded Identity Project, which ran in parallel, included several LoA related questions in their survey. The following summarises these results.

- Institutions clearly perceive the need for "graded authentication" (ie LoA) with a score of 4.31 out of 5. This was rated even more highly than the need for Federated Access Management (4.29 out of 5).
- Institutions were, however, not at all confident about being able to implement graded authentication (2.41 out of 5).
- Authentication LoA is recognised as being important, but policy and actual implementations are scarce.

A presentation on the project was given at the IAS07 Conference followed by a discussion. The following issues were raised.

- There is currently a lack of access and LoA negotiation mechanisms.
- There is concern about how LoA would affect/disrupt current authentication procedures, and potential costs.
- There was also concern about who would define and maintain LoA across various domains including services, institutions, countries, etc.

8. Gap Analysis and Recommendations to JISC

The report titled 'Initial Survey Findings and Recommendations for Further Work', delivered to JISC in July 2007, gave our initial observations and recommendations for follow-up work on LoA. A more detailed and a final set of recommendations and gaps are contained in the WP2 report 'A Defined Set of LoA Recommendations for the Use within the UK Education and Research Communities' [WP2-D]. Here we summarise the recommendations and identify potential gaps that would benefit from additional work.

The US OMB and NIST have already contributed a large body of work regarding defining LoAs and the risk-management aspects of access control, and these specifications have been accepted by various communities (most notably government agencies and the HE community). The JISC-supported UK HE federation should ideally be compatible and interoperable with other international federations and with the UK/US e-Government initiatives.

Compatibility with other federations will make it easier to build inter-federation partnerships and for members of one federation to access resources from the other. In particular, LoA compatibility would mean that users authenticated by an institution from one federation would receive the same treatment or level of service at the other federation, knowing that they have passed a certain level of identity checking. Our survey results also back-up the adoption of four different levels; some service providers have expressed the need for the highest LoA (i.e. Level 4), although for the majority of the respondents Levels 1, 2 and 3 would suffice.

Recommendation 1

Using the OMB/NIST 4-level approach as a starting point, and taking into account UK e-Government initiatives in this area, and in the light of the (surprisingly) wide consensus uncovered by our survey, start drafting a set of LoA definitions/profiles that are appropriate to the UK academic and research community.

Certain gaps have been identified for the use of the OMB/NIST LoA model in federated and grid environments, in terms of (1) LoA definitions, (2) policy aspects of enforcing the use of LoA in a HE federation, and (3) actual implementation of LoA-based systems.

(1) Gaps in LoA definition:

- Level 4 allows only for direct user-to-service authentication and prohibits the use of identity and attribute assertions, which are the cornerstone of the Shibboleth technology used to implement federated access. Thus, more work is needed on how to achieve Level 4 in such environments. In addition, if a user authenticates to an IdP using a smart token, even though this authentication method is 'stronger' than any of the Level 3 methods, the user cannot achieve Level 4 in a federated environment since, as mentioned previously, the use of authentication assertions is prohibited. It is perhaps of interests for federation members to investigate the introduction of a 'Level 3*' (which is lower than NIST Level 4) authentication assurance to accommodate such cases.

Recommendation 2

Investigate how to achieve Level 4 in a federated access management environment.

- The NIST LoA specification caters only for direct user-to-service authentication or authentication via a third party IdP, while delegation of (a subset of) access rights is outside the scope of that specification. Delegation via proxy credentials is a basic mean of authentication in grids, and proxies can be used to create other subordinate proxies allowing for *n*-tier delegation and authentication. This process, as well as the manner in which proxy certificates are stored and managed, introduces certain consequences to an LoA value that need to be further addressed.

Recommendation 3

Investigate the consequences of applying an LoA model to grid authentication.

(2) Gaps in policies:

- Who makes the final decision on the LoA value for a user's current session – is this up to an IdP or does the decision rest with an SP? Could we have an auto-negotiation mechanism involving the user (e.g. depending on what credentials the user has access to), the IdP (e.g. depending on the level of LoA it is accredited to), and the SP (e.g. depending on the access control policy of the resource being requested).
- Identity proofing procedures in HE institutions differ from those proposed by the NIST for federal agencies (e.g. to verify the photoID number issued by the government and confirm the user's full name, date of birth and address) - what measures for identity proofing ought to be established for a HE federation and how would they map to the NIST Levels?
- The federation infrastructure for governing, certifying federation members and enforcing LoA procedures should be established. Would there be four different HE federations, each operating at a certain Level or, or just a single federation with members certified to provide services up to a certain Level?
- Defining LoA vocabularies to describe the LoA specifications.
- To facilitate inter-federation interoperability, consideration should be given to matching LoA vocabularies and policies from different federations.

Recommendation 4

Review the policies and infrastructure necessary for the implementation of an LoA regime; and establish a governing body at the federation level to offer guidance on LoA policies and procedures and to enforce them through verification and certification of federation members.

(3) Gaps in implementation:

- Not a single IdP respondent to our survey currently employs practices that can satisfy the minimal NIST Level 1. There should be more guidance available for institutions on how to implement LoA-compliant systems, and bodies for checking and validating that the systems implemented has operationally achieved the required Levels.

Recommendation 5

Draft and circulate guidance to IdPs on how to implement LoA compliant systems and how to ensure compliance with the required LoA levels.

- Conveyance of an LoA value and/or LoA effecting attributes: current proposals include (1) conveying LoA as an attribute of a SAML v2.0 authentication assertion, or (2) using Authentication Contexts (a new feature of SAML v2.0) to describe the LoA vocabulary it refers to and the LoA value. The level of assurance in a user's other attributes effecting the user's

access rights also appears to be an important issue, i.e. the so-called attribute LoA issue. More work is required to investigate factors affecting the value of attribute LoA.

Recommendation 6

Investigate the issues of LoA value conveyance and attribute LoA in federated identity management environments.

Recommendation 7

The absence of any reference implementation was commented on by respondents. The project strongly recommends that the most effective way to widen understanding and show the effectiveness and relevance of the concepts would be via a demonstrator, covering a small number of differing use cases. It would highlight issues related to the real-life deployment of LoA based fine-grained access control.

9. References

- [Shib] The Shibboleth Project, <http://shibboleth.internet2.edu/>.
- [eInf] UK HM Treasury, Science & innovation investment framework 2004-2014, http://www.hm-treasury.gov.uk/media/6/C/spend04_sciencedoc_4a_090704.pdf.
- [eGov] Cabinet Office e-Government Unit, http://www.cabinetoffice.gov.uk/government_it.aspx.
- [UK--AuthFram] Office of the e-Envoy, Authentication Framework v1.0, Dec. 2000, [http://archive.cabinetoffice.gov.uk/e-envoy/resources-pdfs/\\$file/authentic.pdf](http://archive.cabinetoffice.gov.uk/e-envoy/resources-pdfs/$file/authentic.pdf).
- [UK-RegAuth] Office of the e-Envoy, e-Government Strategy Framework Policy and Guidelines: Registration & Authentication Framework v3.0, Sept. 2002, [http://archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication/\\$file/Registration-AuthenticationV3.0.pdf](http://archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication/$file/Registration-AuthenticationV3.0.pdf).
- [OMB-M0404] US Office of Management and Budget, Memorandum M-04-04: E-Authentication Guidance for Federal Agencies, Dec. 2003, <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>.
- [NIST-SP800-63] National Institute for Standards and Technology, Special Publication 800-63: Electronic Authentication Guideline v1.0.2, April 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
- [NIH] The US National Institutes of Health, <http://www.nih.gov/>.
- [NIH-Pilot] The National Institutes of Health (NIH) Pilot, <https://spaces.internet2.edu/display/macedir/NIH+Pilot+Notes+on+Levels+of+Assurance>.
- [EAI] US Government's E-Authentication Initiative, <http://www.cio.gov/eauthentication/>.
- [EAP] Electronic Authentication Partnership, <http://eap.projectliberty.org/>.
- [LA] The Liberty Alliance, <http://www.projectliberty.org>.
- [inCommon] US HE Federation, <http://www.incommonfederation.org/>.
- [Switch] Swiss HE Federation, http://www.switch.ch/edu/educ_orgs.html.
- [AAF] The Australian Access Federation, <http://www.aaf.edu.au/>.
- [HAKA] HAKA, Finnish HE Federation, <http://www.csc.fi/english/institutions/haka>.
- [Feide] Feide, Norwegian HE Federation, <http://md.feide.no/>.
- [DK-AAI] Danish HE federation, <http://www.dk-aa.dk/>.
- [SWAMI] SWAMI (Swedish Alliance for Middleware Infrastructure), Swedish HE Federation, <http://www.swami.se/>.
- [CRU] French HE Federation, <http://federation.cru.fr/cru/index-en.html>.
- [FAME-PERMISS] The FAME-PERMISS project, <http://www.fame-permiss.org>.
- [SAML] SAML V2.0 OASIS standard specification set, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20.

[OASIS-SAML-TC] The OASIS SAML Technical Committee, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

[OGF] The Open Grid Forum, <http://www.gridforum.org/>.

[Internet2] The Internet2 Consortium, <http://www.internet2.edu/>.

[WP1-D] ES-LoA Project WP1 Deliverable, “Using LoA to Achieve Risk-Based Access Control: A Study Report”, available at <http://www.es-loa.org/images/stories/wp1-loastudyreport-v1.0.pdf>.

[WP2-D] ES-LoA Project WP2 Deliverable, “A Defined Set of LoA Recommendations for the Use within the UK Education and Research Communities”, available at <http://www.es-loa.org/images/deliverables/wp2-recommendationstojisc.pdf>.

[WP3-D] ES-LoA Project WP3 Deliverables, consisted of a set of documents, “LoA Briefing Document”, “Brief Questionnaire”, “Full Questionnaire”, and a two-part report on survey findings “Part 1: Suppliers' Survey on Levels of Authentication: Report on Brief Survey Findings” and “Part 2: Service Providers, Identity Providers and Grid Community Survey on Levels of Assurance: Report on Full Survey Findings”, all are available at <http://www.es-loa.org/images/deliverables>.

[LoA-RG] OGF's Levels of Authentication Assurance Research Group (LoA-RG), <http://forge.ogf.org/sf/projects/loa-rg>.

[IAS07] International Conference on Information Assurance and Security, <http://www.ias07.org>.

[ISO-LoA] ISO/IEC JTC 1/SC 27, New Work Item Proposal on Authentication assurance, Dec. 2006, <http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/755080/1054034/2541793/JTC001-N-8446.pdf?nodeid=6023594&vernum=0>.

[Quest-Full] ES-LoA Project's Full Questionnaire, <http://www.es-loa.org/images/deliverables/wp3-fullquestionnaire-v2.0.pdf>.

[LoA-Brief] ES-LoA Project's “LoA Briefing Document”, <http://www.es-loa.org/images/deliverables/wp3-fullquestionnaire-v2.0.pdf>.

[Quest-Brief] ES-LoA Project's Brief Questionnaire, <http://www.es-loa.org/images/deliverables/wp3-briefquestionnaire.pdf>.

[ID] The Identity project, <http://www.identity-project.info/>.

Appendix A: Workpackage 1 Deliverable

Workpackage 1 deliverable: “Using LoA to Achieve Risk-Based Access Control: A Study Report” [WP1-D]; available at <http://www.es-loa.org/images/deliverables/wp1-loastudyreport-v2.0.pdf>.

Appendix B: Workpackage 2 Deliverable

Workpackage 2 deliverable: “A Defined Set of LoA Recommendations for the Use within the UK Education and Research Communities” [WP2-D]; available at <http://www.es-loa.org/images/deliverables/wp2-recommendationstojisc.pdf>.

Appendix C: Workpackages 3 & 4 Deliverables

Workpackage 3 and 4 deliverables are combined and are consisted of the following reports:

- “LoA Briefing Paper” and the accompanying “Brief Questionnaire” used to investigate the interest and awareness of the publishing community regarding LoAs [WP3-D]; available at <http://www.es-loa.org/images/deliverables/wp3-loa-briefing-document.pdf> and <http://www.es-loa.org/images/deliverables/wp3-briefquestionnaire.pdf> respectively.
- “Full Questionnaire” – full community survey, targeting at a wide range of institutions [WP3-D]; available at <http://www.es-loa.org/images/deliverables/wp3-fullquestionnaire-v2.0.pdf>.
- “Suppliers' Survey on Levels of Authentication: Report on Brief Survey Findings” [WP3-D]; available at <http://www.es-loa.org/images/deliverables/wp3-part1-supplierssurveyreport-anonymous.pdf>.

- “Service Providers, Identity Providers and Grid Community Survey on Levels of Assurance: Report on Full Survey Findings” [WP3-D]; available at <http://www.es-loa.org/images/deliverables/wp3-part2-identityandserviceproviderssurveyreport-anonymous.pdf>.