

The ES-LoA Project
WP3 Deliverable

*Service Providers, Identity Providers and Grid Community
Survey on Levels of Assurance*

Part 1: Report on the Brief Survey

August 2007

Terry Morrow, Mike Jones,
Aleksandra Nenadic and Ning Zhang

University of Manchester

Executive Summary

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' document and the accompanying 'Brief Questionnaire' were designed for these communities to gauge their knowledge and interest in the topic. This report contains the Brief Survey findings.

A total of 24 publishers and intermediaries were contacted, and 19 responses were received. Four of the contacted organisations completed the more detailed Full Survey instead. Seven organisations completed both the Brief and Full Survey.

The results 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.

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 'LoA Briefing' document plus a self-selecting body of respondents.

Five service types were identified by respondents as areas where they would like to be able to require higher LoAs before granting access: financial, sensitive content, account maintenance and administration, author/editor/reviewer access to pre-publication material, and membership privileges. However, one major publisher expressed concern that adopting the LoA technology could possibly make their site more difficult to use than competitors'.

Table of Contents

Executive Summary	2
Table of Contents	3
1. Introduction	4
2. The Responses	4
3. Conclusions	7
3.1 Federated access management deployment.....	7
3.2 Understanding of the subject of LoA.....	7
3.3 Applications of LoA.....	8
3.4 Reasons why LoA might not be applicable	8

Suppliers' Short Survey: Report on Findings

1. Introduction

At the start of the project, it was not clear to what extent commercial organisations such as academic publishers, subscription agents, database suppliers and similar organisations were 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, a short survey form containing eight simple questions was drafted, including two inviting free-text answers. 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.

The 24 publishers/intermediaries were contacted. In addition four European federations, in Norway, Finland, Denmark and Switzerland, were invited to complete either the short or long questionnaire.

By the close of the survey 19 responses to the short questionnaire were received. Three organisations completed the more detailed, full questionnaire instead of the short questionnaire.

A breakdown of the responses to the 19 returns follows.

2. The Responses

Q1: Is your organisation employing, or planning to employ, Federated Access Management (e.g. using Shibboleth)?

Answer	#	%
Yes	17	89%
No	2	11%
Not sure	0	-

Of the two that answered No, one appeared to be using their own mechanisms for delivering levels 1 to 3. The other said they are purely conducting research into the subject at the moment.

Q2: If your answer is Yes, what is the current status of its deployment?

Answer	#	%
Fully operational	3	14%
Operational for selected services	4	19%
Currently implementing	4	19%
Being planned	8	38%
N/A	2	10%

The reason why there are 21 replies from 19 respondents with that one of the respondents (a European federation) checked all three of Fully Operational, Operational for selected services and Currently Implementing. They said this was because their federation covers a range of organisations at different stages. It is clear the great majority are either operating now, or in the process of planning or implementing, a federated access management system.

Q3: Do you understand the concept of Levels of Assurance in the context of authentication for network services?

Answer	#	%
Yes	17	89%
No	1	5%
Not sure	1	5%

Perhaps surprisingly, all but two of the respondents claimed that they did understand the concept of LoA. And of these two, one (a commercial respondent) did come up with a plausible reason why support for LoA might be useful.

Q4: How well informed do you believe your company or organisation is on this subject?

Answer	#	%
Well informed and up to date	6	33%
Has some knowledge and understanding	5	28%
Is aware of the subject and would like to know more	6	33%
Is aware of the subject but doesn't think it is relevant	1	6%
Has no knowledge or awareness	0	-

One respondent didn't mark an answer to this question. All remaining respondents stated that their organisations had at least some awareness of the topic and an encouraging one third claimed their organisation was well informed and up to date.

Q5: Has your organisation considered or investigated the possible application of Levels of Assurance (LoA) to any of your networked services?

Answer	#	%
Yes	9	56%
No	6	38%
Not sure	1	6%

Two organisations didn't check this box and one didn't seem to be sure.

Questions 6 and 7 invited free text responses.

Q6: If "Yes", can you give examples of services where you think you would like to be able to require higher levels of assurance before granting access?

Seven of the respondents from the publisher/intermediary group gave an answer to this question.

One *publisher* suggested that allowing institutional payment for open access publications, would perhaps require more assurance than granting access to a subscription resource.

A national *library* commented that they currently provide services which fit levels 1 to 3, but they don't use the same terminology.

One *publisher* thought that if they made highly sensitive content, such as exam papers, available online this would be an appropriate application.

A major *academic publisher* reported that users of two of their services can have "administrative privileges", meaning that they are able to manage account settings on their institute's behalf. Aside from providing a username and password, these administrative users currently have to be using an IP address belonging to their institute in order to get access to administrative functionality. Also, they are looking at future integration of AuthN/AuthZ for their author and editor services, which will probably require the use of different levels of assurance.

An *intermediary* suggested that in a situation where a personal user is authenticated via Shibboleth and has stored credit card details on their service, it is possible that they may want to insist on a higher level of assurance for access to that information than for, e.g. subscription access to content.

A *society publisher* suggested three scenarios where LoA might come into play: (1) Librarian (or site contact) might be able to maintain their customer record remotely. (2) Student member - who might have access to member-specific content/benefits. (3) Editorial Board Members - who might have certain access privileges.

Another *major academic publisher* also suggested several scenarios where LoA might have a role. (1) Authors and/or reviewers collaborating on pre-publication material or partners collaborating on pre-

release products or service - unique and assured author id would be useful in many contexts (2) Students taking certification exams - examiners of such papers (3) Institutional Customers who have purchased a premium service for a small group within a larger institution[for example a service which might be purchased for use by surgeons within a complex of medical schools allied to a university. (4) Society members who may be entitled or required to access something but do not share a geographical location or are not members of the same academic or corporate institution - so a Society member at an institution may be entitled to access something no-one else at the institution is. All of these scenarios can be handled by requiring username/password plus secret code or similar but this requires the user to remember yet another set of codes and numbers.

There were also responses to this question from a grid service provider, a European State Library, a European federation operator, and from a Greek research organisation.

The *grid service operator's* response expressed a point of view that if they were to offer a more finely grained authentication scheme by employing LoA's, people might be prepared to offer more resources to the Service and thereby encourage its adoption. They added the viewpoint that existing resources would benefit from the availability of higher LoA's.

The *state library* suggested the following possible applications of LoA: 1) services with money transactions included; 2) services where you have access to other people's personal data. They added here that they run the national web-archive (where they harvest all national web-pages). From this material it is possible to find personal data by doing a thorough search of the archive, implying that it needs a higher level of protection; 3) Services where the user can make changes to their account. E.g. get a new password.

The *federation operator* suggested the following: 1) Requirements from the central government on government services. 2) Specific services with either financial transactions or strong privacy requirements (for example health research).

However, they added that the complexity of adding LoA is not something they want to venture into unless there is clear demand from the user community. In practice they are more likely to add separate authentication schemes for each LoA, keeping the current federation at level 2. They added that a policy discussion on this had started, but has not yet reached a conclusion.

The *Greek research organisation* completed the short questionnaire. They are currently carrying out research on managing untrusted Grid Storage Services. One proposed approach is "policy-based", where a quantitative "security level" is obtained and this is then used to provide the user with access to the resource. They report that this is based on previous work at the Technical University of Catalonia on policy-based Grid validation. They point out that this work is purely research based as they think a production implementation in Hellas Grid could take sometime.

Q7: If you have heard of LoA, but not considered it applicable to your services, can you give a reason or reasons why?

Nine respondents answered this question.

One *publisher* stated that most of their content is open access so institutional authentication is not a primary concern. However individual identity verification could be very relevant.

Another *academic publisher* said that they haven't yet had time to consider this in detail.

Another *publisher* said that this would currently be considered a possible enhancement in future development of their website. They added that they would be interested in obtaining further information about LoA .

Another *publisher* stated that they don't believe that their applications and services need a high level of assurance at this time. However, if/when they do offer personalisation or e-commerce type services, then this might create a requirement for higher levels of assurance.

A *subscription agent* pointed out that security for their networked services has always been a major focus point for their organisation. On the one hand to protect their own company critical data and IT

systems, on the other to protect their customers' data and to prevent misuse of their accounts. They therefore already employ different levels of security based upon the risk that they run of it being compromised. They didn't elaborate on how they implement this.

A *major academic publisher* suggested that there are three reasons for authenticating users on their products and gave reasons why they thought LoA is not highly relevant to them at the present time. (1) to change contact details and other personalisation preferences. They consider this to be sensitive information but would not require the user to do anything more than any other site the average user visits eg Amazon, eBay. There are no credit card details stored so a low level of assurance would be acceptable. (2) to access subscribed content. There is no content on their website that is considered more sensitive than any other content. They therefore don't require different levels of assurance to different content. The customer, the librarian, is keen to see their users have the easiest and least frustrating access to content possible therefore a low level of assurance is all that is required unless the standard in the industry were to change. (3) to make a purchase. At the point of making a purchase we acknowledge that a greater level of assurance is required, but ecommerce validation provides this assurance. They would not want to make using their site more complex than other sites, either within or outside the industry.

Another *publisher* thought that current authentication mechanisms (IP address, Referring URL, Username/Password, Cookies, Athens, Shibboleth, Patron Identifier, etc.) provide an "authenticated and authorized" flag for all subscribed to services. Within their current business model the need for LoA is not deemed necessary. Future services might well require LoA implementation.

There were also responses to this question from a European federation operator, and from a Greek research organisation.

The *federation operator* pointed out that LoA adds complexity and would require changes to the federation specifications. This would create issues with backwards compatibility. In other words, at the moment they see the disadvantages outweighing the advantages.

The *Greek research organisation* said that they have suggested that if a site does not comply with the minimum "trust level" (maybe achieved through PMA's evaluation), then it should not be part of the Grid. Other approaches are also being considered for their research (i.e. point-2-point security). On the other hand, they thought that changing the AA infrastructure for a production Grid (i.e. Hellas Grid) does not seem like a task to perform in the short term.

Q8: Would you be willing to be contacted by the research project to answer additional questions?

An encouraging 18 out of 19 answered Yes to this question. 13 of these have been sent longer questionnaires, of whom 9 have sent back completed copies. One organisation said that they would be happy to answer any specific follow-up questions, but they would prefer not to fill in the longer questionnaire.

3. Conclusions

3.1 Federated access management deployment

A remarkable 17 out of 19 were either implementing or planning to implement a Federated Access Management regime such as Shibboleth. The only two respondents who were not are arguably outside the mainstream of this survey (a national library and a Greek research group).

Having said that, only 3 claimed a fully operational service with 8 of the 19 still at a planning stage.

3.2 Understanding of the subject of LoA

A quite remarkable 89% of respondents claimed they understood LoA concepts, and the only one who answered No did provide a plausible reason why LoA support may be useful to them (which suggested they did after all understand the concept).

Reinforcing this, nearly two thirds (61%) claimed to be well informed and up to date, or at least have some knowledge and understanding. No-one claimed no knowledge or awareness. This of course

may have been self-selecting. It is possible that people who knew nothing about the subject didn't see the point of responding to the questionnaire and demonstrating their ignorance.

3.3 Applications of LoA

Nine of the 16 respondents who answered question 5 said they had considered possible applications of LoA and gave examples. These can be divided into 5 areas:

3.3.1 Financial

Several respondents suggested that transactions involving money require higher levels of assurance. Examples include institutional payment for open access and stored credit card details. A national library and a European federation operator mentioned financial transactions as a possible application of LoA.

3.3.2 Sensitive Content

Another area where a higher level of assurance might be required is access to sensitive content such as examination papers (two publishers mentioned this) or health information where personal privacy should be protected.

3.3.3 Account maintenance and administration

Several respondents included account maintenance and administration (eg changing/resetting passwords) as a function perhaps requiring a higher level of assurance.

3.3.4 Author/editorial board/reviewer access to pre-publication material

This was also regarded as a sensitive area where a higher LoA would be useful. It was mentioned by three publishers.

3.3.5 Membership privileges

Several respondents suggested that special privileges such as those derived from society membership status or who have purchased premium services would be a useful area to employ LoA technology. These suggestions came from two publishers,

These responses suggest that there is a latent demand for a Levels of Assurance infrastructure. Once such a thing is in place, it would seem likely that organisations would step forward to make use of it.

3.4 Reasons why LoA might not be applicable

Question 7 asked respondents to say why, if they had looked at LoA but decided it didn't apply to their services, what their reasons were.

One academic publisher said they hadn't yet considered the issue. Four organisations said that, although they don't see a current need, they could envisage a requirement in the future.

One subscription agent stated that they already employ different levels of security but didn't explain how they do this.

One of the larger academic publishers gave a lengthy answer which can be summarised as saying that they were very keen not to make their site or services difficult to use. The only example they gave where they acknowledged a greater level of assurance was required is online purchasing of content, but they seem happy with current e-commerce systems for this.