

The ES-LoA Project
WP3 Deliverable

*Part 2: Service Providers, Identity Providers and Grid
Community Survey on Levels of Assurance
Report on Full Survey Findings*

August 2007

Mike Jones, Ross McIntyre, Terry Morrow,
Aleksandra Nenadic, Stephen Pickles and Ning Zhang

University of Manchester

Executive Summary

This document reports the ES-LoA project full survey findings on the definitions and applications of authentication Levels of Assurance (LoAs). The survey is part of our effort to investigate LoA requirements within the UK education and research community, taking into account international standards, development and efforts on LoA definitions and specifications, and in building community consensus in the use of appropriate LoAs to achieve a fine-grained control of access to various types of resources, including grid/e-Science resources, library resources and e-learning resources.

The Full Survey was launched on May 1st 2007 through direct contacts with institutions at various events and via e-mail, through UK Higher Education IT directors' list (UCISA), JISC Middleware mailing list and National e-Science Centre Newsletter. An on-line version of the Questionnaire was also made available at the project's Web site (<http://www.es-loa.org/loa-survey>). The Full Survey Questionnaire was divided into three main sections, with questions in each section specifically designed for identity providers, service providers and grid community. A total of 30 organisations responded to the Full Survey Questionnaire, mostly from members of the UK Access Management federation but also other organisations outside the federation and the UK. The main findings from the Survey are summarised in the following:

- A vast majority of service providers (88%) and all of the responding identity providers are either adopting or planning to adopt Federated Access Management.
- Risk assessment is an important stage in adopting LoA-linked access control. Half of the service providers surveyed claim to have carried out some form of risk assessment on the consequences of an unauthorised access to their resources, and a further 12% are planning to do so.
- Damage to reputation, harm to systems, assets or public interests, and financial loss or potential legal liability were the top three risk categories perceived to have the highest impact on service providers.
- Almost all service providers (93%) require some level of confidence in an asserted user's identity, 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. 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 authenticated. Confidence in the 'reliability' of other users' attributes (i.e. attribute LoA) appears to be as important as confidence in the 'quality' of authentication (i.e. credential LoA).
- 70% of service providers agree that more valuable or sensitive resources should be matched with a stronger form of user identification and authentication mechanisms, which implies a requirement for higher level of authentication assurance.
- Almost all service providers (92%) and 83% of identity providers are willing to respect some national or international standards or guidelines on e-authentication, and a large majority (80%) would like to see medium to high levels of federation governance in place.
- 57% of identity providers claimed that they support the use of multiple authentication mechanisms, and 14% of them use different mechanisms when authenticating users for foreign services.
- Username and passwords still seem to be the authentication method of choice for the majority of identity providers. However, not a single service provider currently employs practices that would satisfy the associated NIST authentication assurance Level of 2.
- All grid community respondents place some level of sensitivity on their data, with 30% rated their resources as extremely sensitive and 20% as highly sensitive. A large proportion (80%) of the grid service providers surveyed allow user-generated code to be run on their systems and another 80% provide access to powerful compute resources, which can potentially increase the levels of risks thus requiring higher levels of authentication assurance.
- 20% of the grid respondents think current grid authentication solutions are not sufficient to support the community's e-authentication needs, largely due to the grid community's reluctance to standardise and agree on authentication mechanisms or because there is a lack of traceability between the work done on a worker node with the identity recorded at the start of the job.

- About one quarter of the grid service providers surveyed are currently in a position to authorise accesses based upon attributes presented within grid identity credentials (e.g. VOMS proxy credentials within GSI proxy credentials), while three quarters are able to accept GSI proxies.

Table of Contents

Executive Summary	2
Table of Contents	4
List of Tables	5
List of Figures	5
1 Introduction	7
2 The Survey Analysis	7
2.1 Questionnaire Section 1: General Questions.....	7
2.2 Questionnaire Section 2: Service Providers.....	8
2.3 Questionnaire Section 3: Identity Providers	16
2.4 Questionnaire Section 4: Grid Community.....	30
3 Observations and Comments on Survey Findings	41
3.1 Observations and Comments from the Service Providers' Section	41
3.2 Observations and Comments from the Identity Providers' Section.....	41
3.3 Observations and Comments from the Grid Resource Providers' Section	42
4 Conclusions	43

List of Tables

Table 1. Risk categories ordered by perceived impact.....	10
Table 2. Values for calculating whether passwords satisfy NIST Level 1 and 2 requirements	27

List of Figures

Diagram 1. Distribution of types of organisations participating in the survey	7
Diagram 2. Attitude of organisations to adopting new technologies	8
Diagram 3. Attitude towards adopting Federated Access Management	8
Diagram 4. Current status of Federated Access Management deployment among Service Providers .	9
Diagram 5. Percentage of organisations having carried our risk assessment.....	9
Diagram 6. Respondents' perception of impacts to their services as a result of unauthorised access	10
Diagram 7a. The required level of confidence in clients' identities when authentication is performed directly by the service provider	11
Diagram 7b. Perception of harm/impact to services as a result of unauthorised access for those service providers that require the highest level of confidence in identifying users	11
Diagram 8. Requirements regarding information from the authenticating party or provider of attributes when authentication is not performed directly by the service provider	12
Diagram 9. Willingness to adhere to guidelines for authentication	13
Diagram 10. Preferred level of governance by SPs.....	14
Diagram 11. Management of multiple categories of resources and the use of different authentication methods for differing categories.....	14
Diagram 12a. External vs. home users regarding authentication strength.....	15
Diagram 12b. Type of organisation agreeing that external users should be authenticated more strongly.....	15
Diagram 12c. Type of organisation disagreeing that external users should be authenticated more strongly	15
Diagram 13. The need for using stronger authentication for more valuable resources.....	16
Diagram 14. Reluctance to make resources available through a federation until there are more formal LoA guidelines.....	16
Diagram 15. Current status of Federates Access Management deployment among IdPs.....	17
Diagram 16. Distribution of services consuming authentication assertions from an IdP	18
Diagram 17a. Percentage of IdPs using multiple authentication mechanisms.....	18
Diagram 17b. Distribution of the entities allowed to choose an authentication method among multiple choices	18
Diagram 18. Percentage of IdPs using different authentication mechanisms for users in and outside their administrative domain	19
Diagram 19. Provision of authentication assertions for on and off-site users.....	19
Diagram 20. The use of the same authentication methods for on- and off-site users.....	20
Diagram 21a. The use of PKI for authentication	21
Diagram 21b. Distribution of PKI providers	21
Diagram 22. Delegation of identity vetting to Registration Authorities.....	21
Diagram 23a. Identity information collected for in-person registration	22
Diagram 23b. Identity information collected for remote registration	23
Diagram 24a. Preservation of user registration records	23
Diagram 24b. Time period registration records are preserved for	23
Diagram 25. Types of credentials used for user authentication.....	24
Diagram 26a. Imposing password validity period	25

Diagram 26b. Percentage of IdPs imposing password rules	26
Diagram 26c. Types of password rules imposed	26
Diagram 26d. Percentage imposing account lock-outs after a number of failed authentication attempts	26
Diagram 27. Types of revocations facilities for IdPs employing PKI	28
Diagram 28a. Percentage of IdPs using identity assertions	28
Diagram 28b. Common security protections for identity assertions	29
Diagram 29. Types of authentication protocols in use by IdPs.....	29
Diagram 30a. Percentage of IdPs willing to follow guidance on LoA	30
Diagram 30b. Percentage of IdPs interested to know more about LoA	31
Diagram 31. Service types exposed via grid mechanisms	31
Diagram 32. Perceived sensitivity of data exposed via grids.....	32
Diagram 33. Percentage of grid service providers allowing users to run their own code.....	32
Diagram 34. Percentage of grid service providers allowing access to large compute resources	33
Diagram 35. Adequate user identification can be achieved with current grid middleware	34
Diagram 36. Requirement for CAs to publish their CP/CPS.....	34
Diagram 37a. Percentage of grid service providers requiring adherence to CP/CPS.....	35
Diagram 37b. Enforcing adherence to CP/CPS	35
Diagram 38. Requirement for a CA to be self-signed	35
Diagram 39. Requirement for maximum certificate chain length	36
Diagram 40. Requirement for well-defined Namespace for certificate issuance	36
Diagram 41. Requirement for well-defined Namespace for certificate issuance	37
Diagram 42. Imposing restrictions of elements allowed in DN field of a certificate	38
Diagram 43. Types of access control to grid services	38
Diagram 44. Requirement for the VO to be associated with a legal entity	39
Diagram 45. Percentage of grid service providers being able to use attributes embedded in certificates for authorisation decisions	39
Diagram 46. Percentage of grid service providers accepting GSI credentials	40
Diagram 47. Distinguishing between GSI proxy credentials.....	40

Service Providers, Identity Providers and Grid Community Survey on Levels of Assurance: Report on Full Survey Findings

1 Introduction

This survey was aimed at, firstly, raising the community’s awareness with regard to authentication Levels of Assurance (LoAs) as one of the factors that can be used to quantify the degree of protection for resources with varying levels of sensitivities in federated environments; secondly, investigating potential applications of LoA to various types of resources, including grid/e-Science resources, library resources and e-learning resources; thirdly, building community consensus the use of appropriate LoA as defined by the worth of the resources; and, finally, raising resource providers’ interests in deploying a technology that can help them to achieve LoA-linked fine-grained access control.

The remaining part of this document reports the survey findings, comments, observations, and conclusions. In detail, the next section details the survey questions followed by a summary of the responses and comments. Further comments and observations are given in Section 3. Finally, Section 4 concludes the report.

2 The Survey Analysis

The questionnaire prepared for the survey consisted of four sections: (1) general questions about respondents, (2) questions for service providers, (3) questions for identity providers and (4) questions to people running or providing services on grids.

2.1 Questionnaire Section 1: General Questions

Questions in this section were mainly intended to collect contact details from respondents and help us classify respondents into categories based on their organisation's functionalities, the services they provide and their attitude towards adopting new technologies.

Diagram 1 shows the distribution of the types of services provided across all the respondents' organisations.

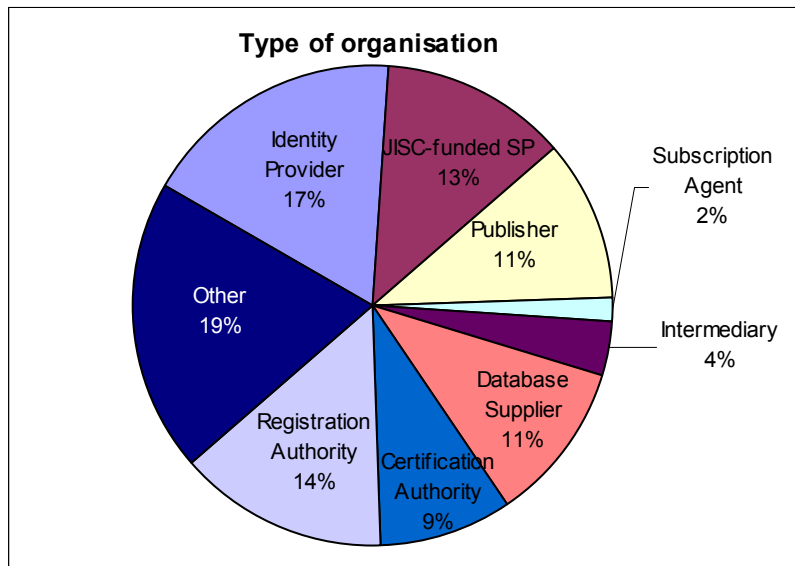


Diagram 1. Distribution of types of organisations participating in the survey

Diagram 2 depicts the attitudes of the organisations towards adopting new technologies. The respondents were asked to classify themselves as innovators, early adopters, adopting in the next development cycle, waiting for demand to be established before adopting, and those only considering new products or services. All the organisations surveyed have responded to this question, and only a small fraction of them is waiting for demand to become established.

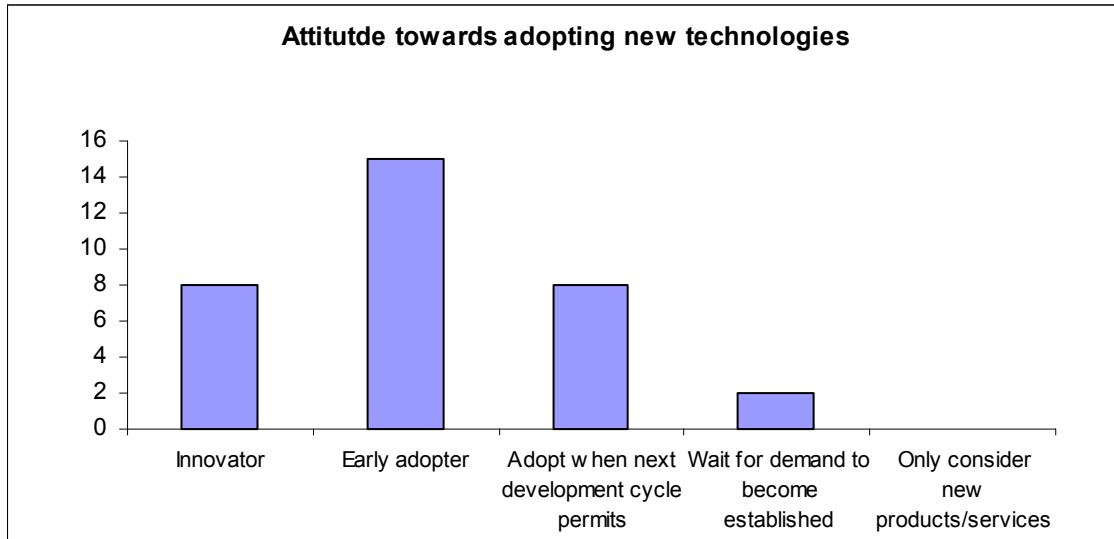


Diagram 2. Attitude of organisations to adopting new technologies

2.2 Questionnaire Section 2: Service Providers

Q2.1 Is your organisation employing, or planning to employ, Federated Access Management (e.g. using Shibboleth)?

Diagram 3 shows that a vast majority of respondents (88%) are either adopting or planning to adopt Federated Access Management. Two responded negatively, one of which is outside the UK and the other manages medical and health information.

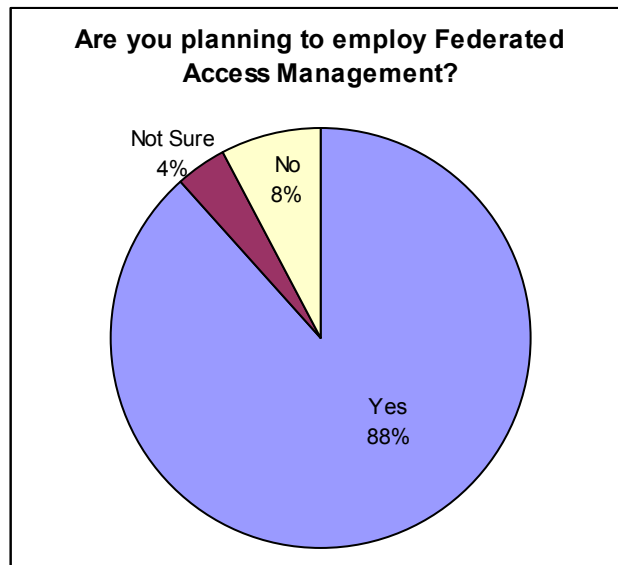


Diagram 3. Attitude towards adopting Federated Access Management

Q2.2 Of those who are adopting Federated Access Management, what is the current status of their deployment?

Four possible answers were provided:

- Fully operational
- Operational for selected services
- Currently implementing
- Being planned

The responses are summarised in Diagram 4. Roughly half of the respondents have made their services available through Federated Access Management.

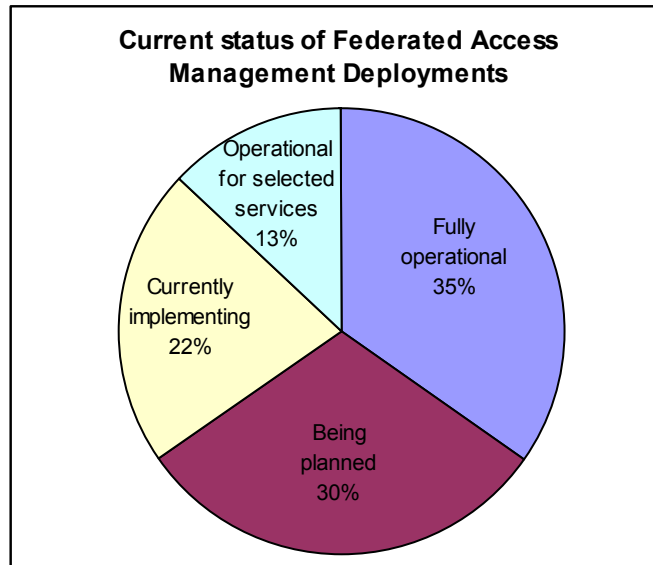


Diagram 4. Current status of Federated Access Management deployment among Service Providers

Q2.3 Have you carried out a risk assessment on the consequences of unauthorised access to your resources?

Half of the respondents claim to have carried out risk assessments, and further 12% are planning to do so, as shown in Diagram 5.

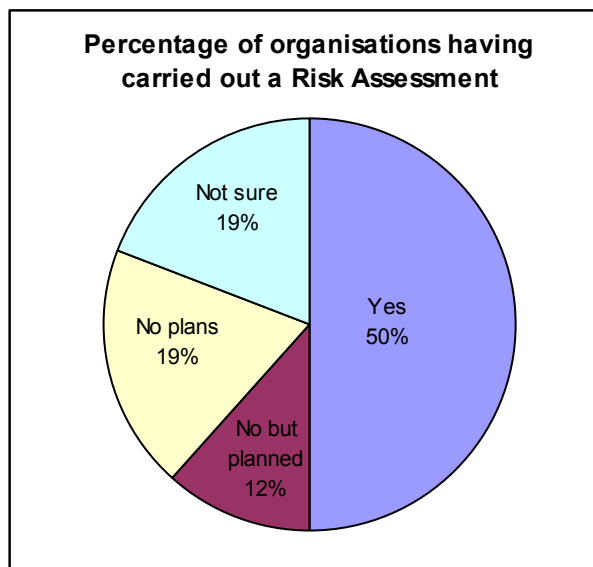


Diagram 5. Percentage of organisations having carried our risk assessment

Q2.4 Hypothetically, if an unauthorised user got access to your services (e.g. if your authentication process failed), how would you describe the potential harm or impact?

Respondents were asked to look at the impact categories listed below and rate the levels of impact of each category as 'Low', 'Medium', 'High' or 'N/A' if they do not perceive any harm from a particular impact category.

The impact categories were:

- Inconvenience, distress, or damage to the standing or reputation of your organisation (or any party involved) as a Service Provider
- Financial loss or potential legal liability
- Harm to the systems, or adverse effects on organisational operations or assets, or public interests
- Unauthorised release of sensitive personal or commercial information
- Personal safety or security
- Potential for civil or criminal legal action

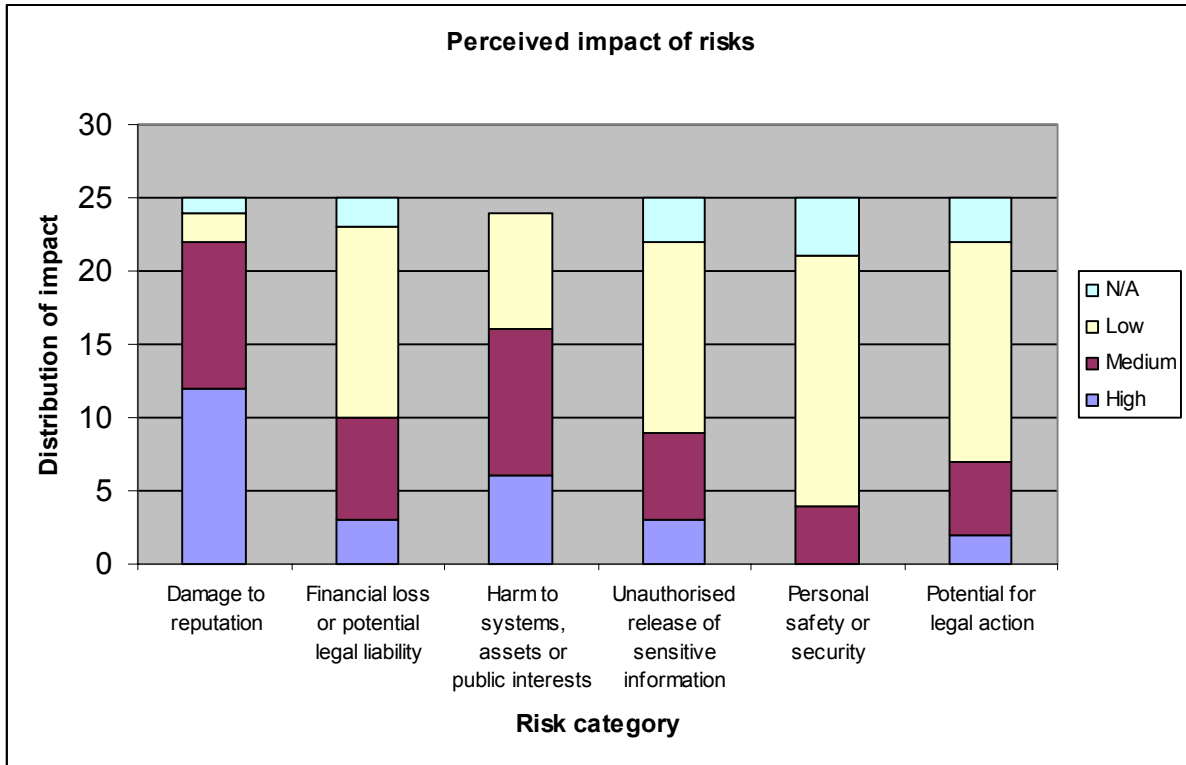


Diagram 6. Respondents' perception of impacts to their services as a result of unauthorised access

The results shown in Diagram 6 can be reordered to highlight the most important perceived impacts (i.e. classified as 'High' or 'Medium') of unauthorised access to Service Providers' resources. This is shown in Table 1.

Table 1. Risk categories ordered by perceived impact

↑	Highest	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
	Lowest	Personal safety or security

Linking the responses to this question and those of question Q2.1, a relation can be drawn that for respondents who are not or are not sure about employing Federated Access Management, their overall perceived impact of risks was high to medium in the four most important categories (top four in Table 1). This leads us to conclude that there are 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 proportion of service providers not willing to join a federation is minimal and the majority of those are from outside the UK.

Q2.5 When dealing with requests to access your resources from a remote site, which of the following is true?

In case 1, where respondents authenticate their remote users directly (i.e. not via an identity provider), we offered the following options:

- The remote user’s personal identity is unimportant (Level 1)
- I need some confidence in identifying the remote user (Level 2)
- I require a high level of confidence in identifying the remote user (Level 3)
- It is essential to have very high level of confidence in identifying the remote user (Level 4)
- Not sure

In case 2, where a remote user is authenticated by a third party identity provider, and the identity provider subsequently sends the service provider a security assertion with user’s attributes, respondents were offered the following options:

- I do not care about how the remote user is identified and authenticated
- I would like to know how the remote user is identified and authenticated, e.g. the authentication token type and authentication protocol used in the authentication process
- I would like to know the assurance level of the remote authentication process.
- I would like an indication of the reliability of the attributes of the remote user as presented by the Identity Provider
- Not sure

In both cases, respondents were allowed to tick more than one option, as in case 1, they may have resources with different requirements with regard to user authentication, and in case 2, they may wish to know more than one characteristic of an authentication process. Diagrams 7 and 8, respectively, depict the responses for direct authentication and authentication via a third party.

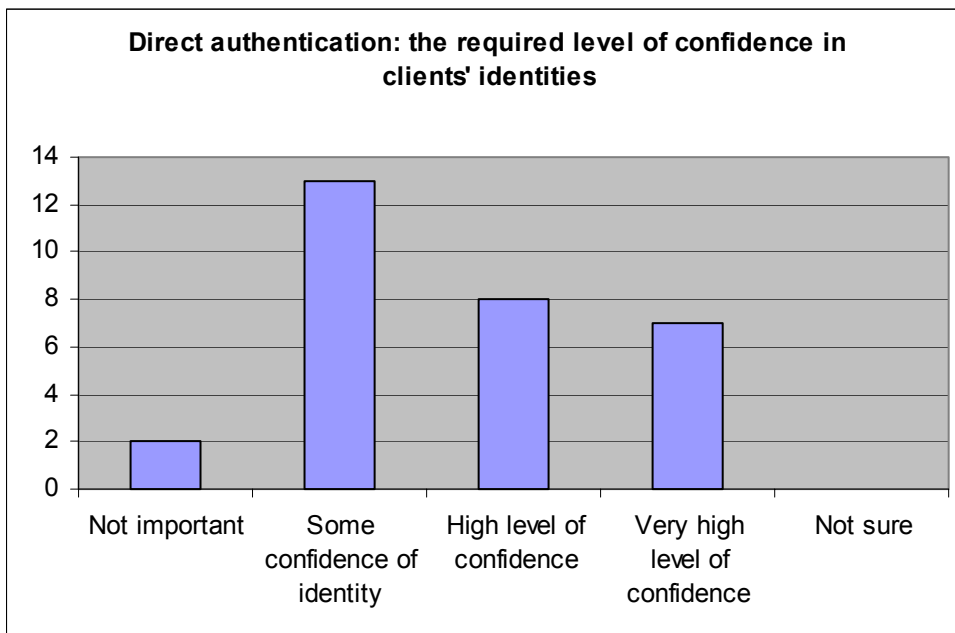


Diagram 7a. The required level of confidence in clients' identities when authentication is performed directly by the service provider

Diagram 7a shows that almost all service providers require some confidence in the asserted users'

identities, and 27% claim to have resources that would require the highest LoA. There appears to be a correlation between service providers requiring the highest LoA and those perceiving risk impacts as stronger. This correlation can be seen when comparing Diagram 7b with Diagram 6.

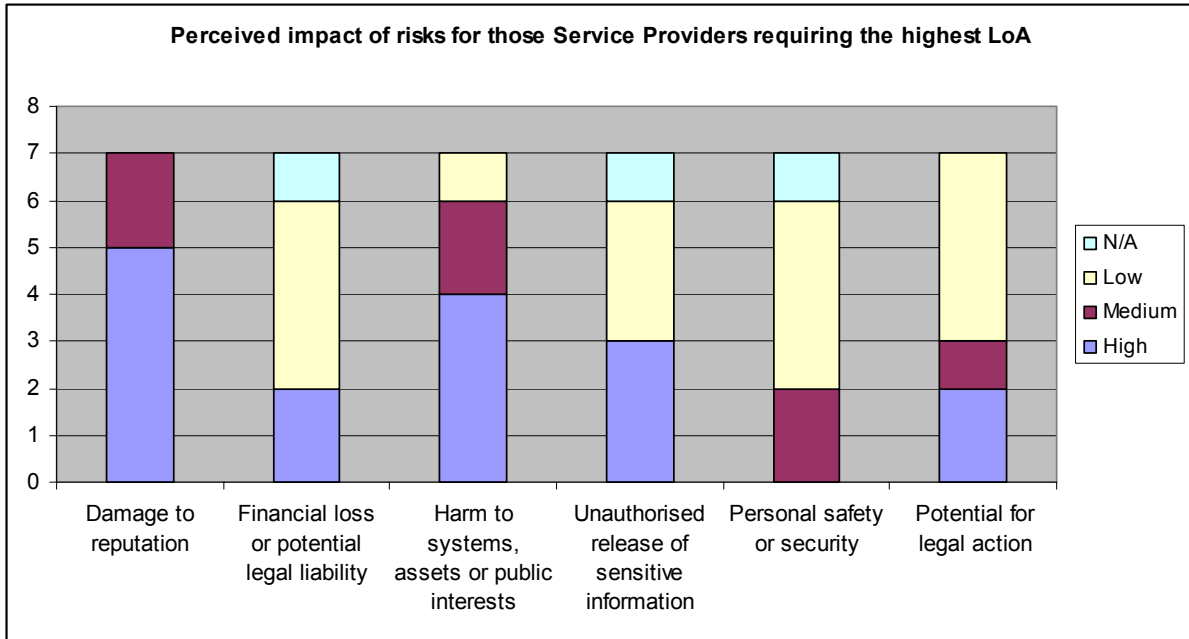


Diagram 7b. Perception of harm/impact to services as a result of unauthorised access for those service providers that require the highest level of confidence in identifying users

Also, there seems to be no significant correlation between service providers not willing to adopt Federated Access Management and those requiring a higher value of LoA.

Diagram 8 shows that almost all service providers wish to know the mechanism by which a user is authenticated when the authentication is performed by a third party identity provider. About one third were ambivalent towards the use of LoA. Furthermore, the confidence in asserted attributes appears to be more important than confidence in LoA, although by a small margin.

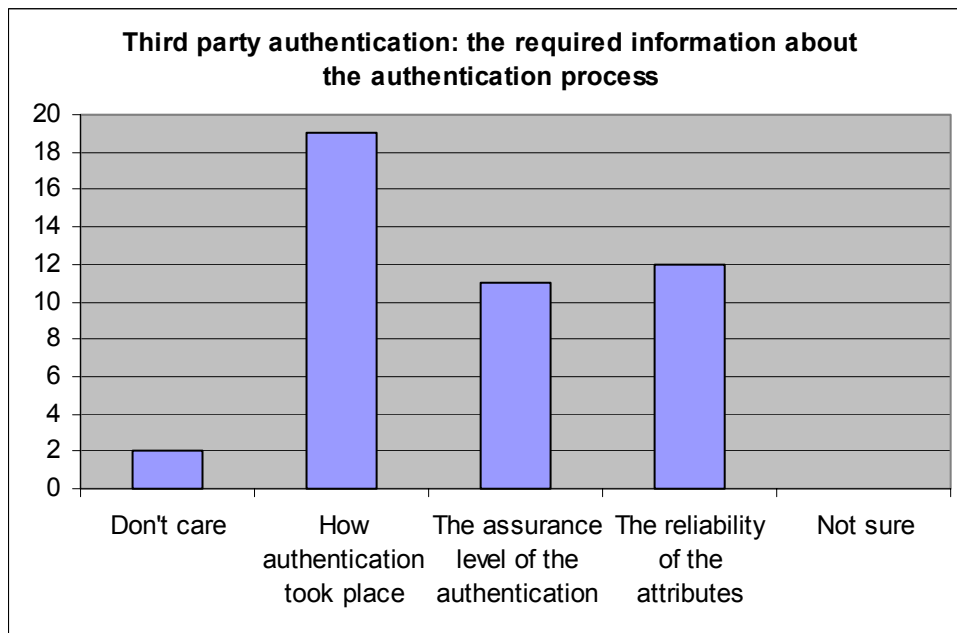


Diagram 8. Requirements regarding information from the authenticating party or provider of attributes when authentication is not performed directly by the service provider

Q2.6 Would you be willing to take steps to adhere to some national or international guidelines on e-Authentication in order to interoperate with other federations or to make your resources accessible to users from a wider community?

Almost all respondents (92%) said that they would be willing to adhere to some form of standards or guidelines on e-authentication (see Diagram 9).

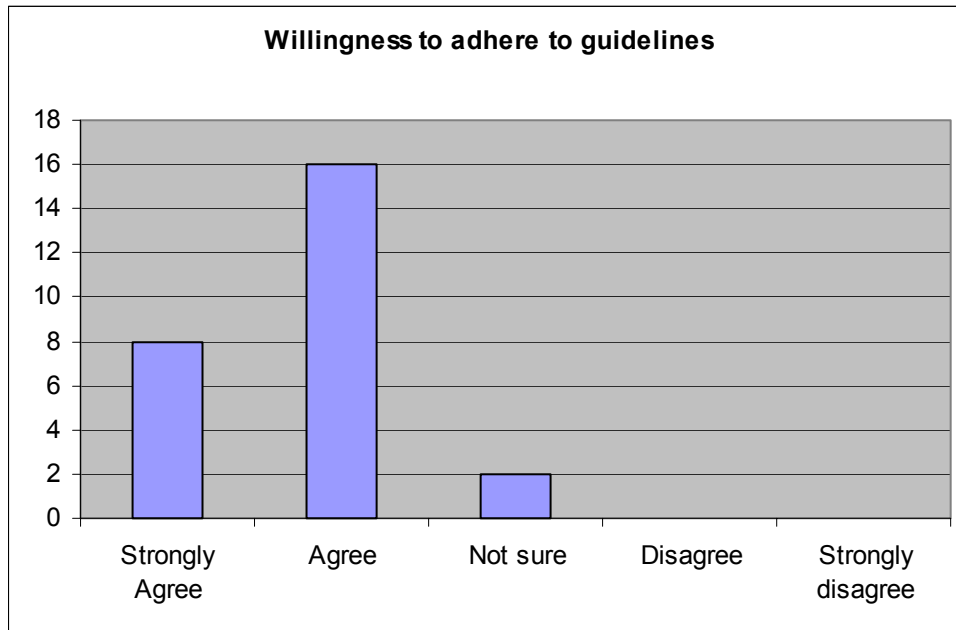


Diagram 9. Willingness to adhere to guidelines for e-authentication

Q2.7 If you are a service provider in a federation, then users accessing your resources may be identified and authenticated by another institution (a third party Identity Provider) in the federation.

In this case what level of governance should be in place to make sure that the users are identified with a certain degree of confidence before they are allowed to access your resource?

Respondents were offered the following options:

- A high level of governance (proactive governance, e.g. regular auditing, Service Level Agreements with the federation)
- A medium level of governance (passive governance, e.g. peer review against published Service Level Descriptions with procedures in place for dispute resolution)
- A low level of governance (minimal governance, e.g. self assertion by an IdP of their practices and policies)
- No governance
- Not sure

Diagram 10 shows that a large proportion of the service provider community surveyed (80%) would like to have a medium to high level of governance to help them ensure that the users are identified with a certain degree of confidence. Only a small number (4%) were against any form of governance regarding the use of LoA.

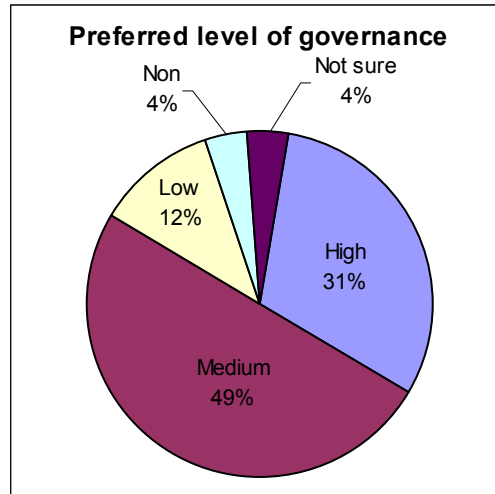


Diagram 10. Preferred level of governance by SPs

Q2.8 Do you manage multiple categories of resources with different sensitivity levels?

Suggested answers were:

- Yes, we divide resources into different categories; some are more sensitive than the others.
- No, all our resources are of the same sensitivity level
- Not sure

Those, who answered positively, i.e. said that they manage resources with varying sensitivity levels, were further asked whether they use the same authentication service to identify users accessing different categories of resources.

In Diagram 11, the first bar indicates those who manage resources with varying sensitivity levels, whereas the second and third bars represent those who do not manage resources with varying levels of sensitivity and those who are not sure, respectively. Among those who do have different resource groups (i.e. the first bar), 61% uses the same authentication method to identify users regardless of resource group they are accessing, while 39% claim they impose different authentication requirements for different resource groups.

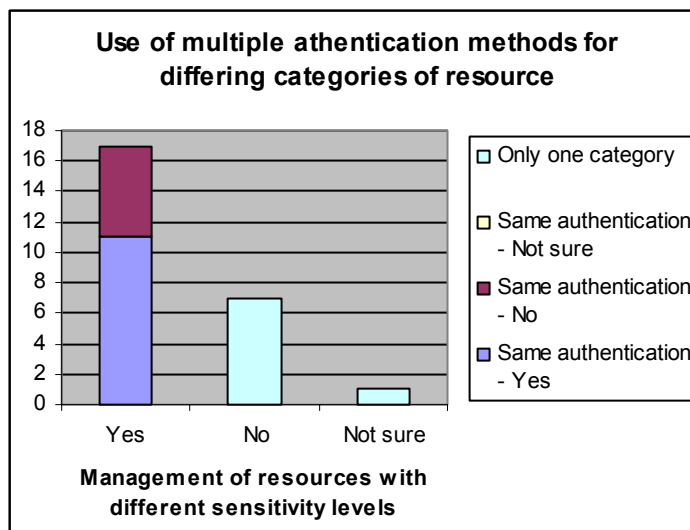


Diagram 11. Management of multiple categories of resources and the use of different authentication methods for differing categories

Q2.9 Rate the following statement: “an external user (or an off-site user) should be identified with a stronger authentication method than a local user”.

As shown in Diagram 12a, 52% of the service provider respondents disagree, while 32% believe external or off-site users should go through a more rigorous authentication process than internal or on-site users.

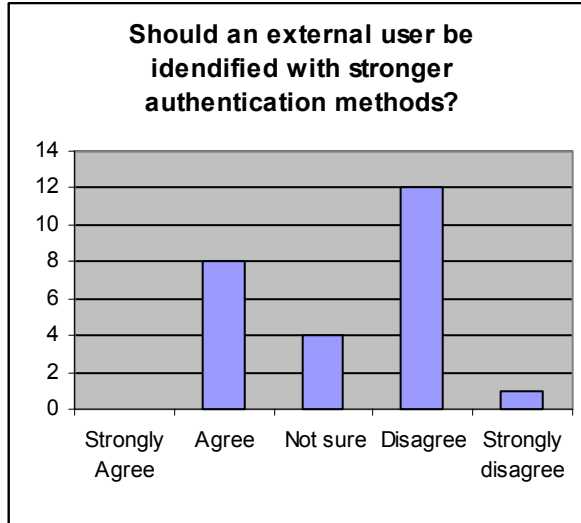


Diagram 12a. External vs. home users regarding authentication strength

Diagrams 12b and 12c show the distributions of service types that are in agreement and in disagreement with the statement in Q2.9, respectively.

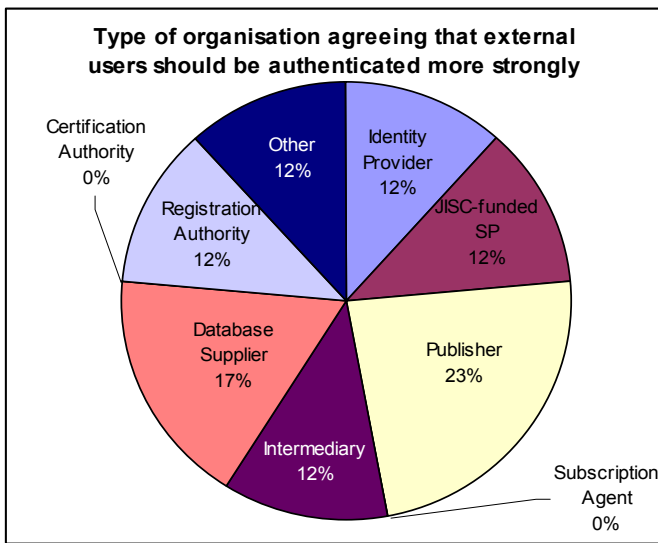


Diagram 12b. Type of organisation agreeing that external users should be authenticated more strongly

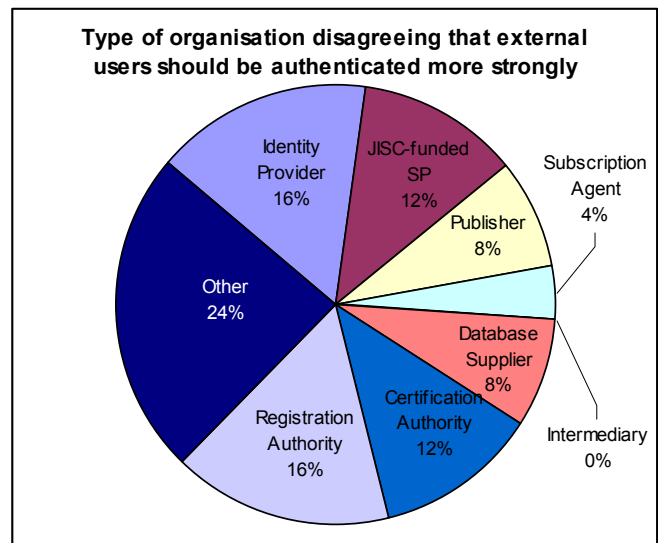


Diagram 12c. Type of organisation disagreeing that external users should be authenticated more strongly

Q2.10 Rate the following statement: “We would like to be able to use a stronger form of user identification and authentication for some of our more valuable or sensitive resources”.

As shown in Diagram 13, 70% of service providers either agree or strongly agree that more valuable or sensitive resources should be matched with a stronger form of user identification and authentication process.

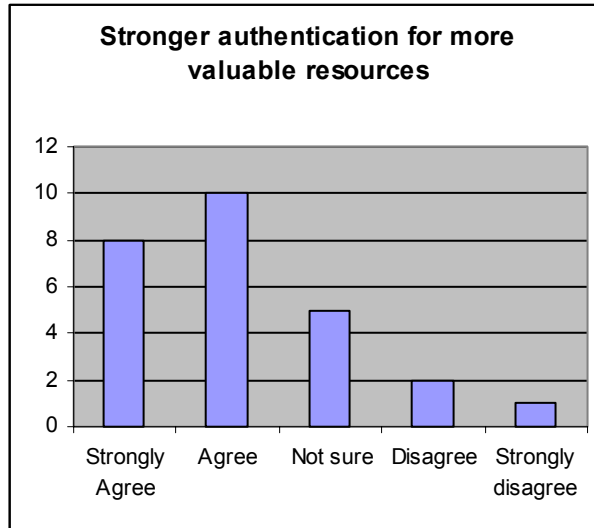


Diagram 13. The need for using stronger authentication for more valuable resources

Q2.11 Rate the following statement: “We, as a service provider in the federation, would be reluctant to put our services or data into the federation pool until appropriate policies and procedures regarding assurance levels are established”.

As shown in Diagram 14, 77% of respondents believe that putting some formal LoA guidelines into practise within a federation would make them more willing to share their more valuable or sensitive resources, and only 7% think that imposing LoA guidelines would make no difference.

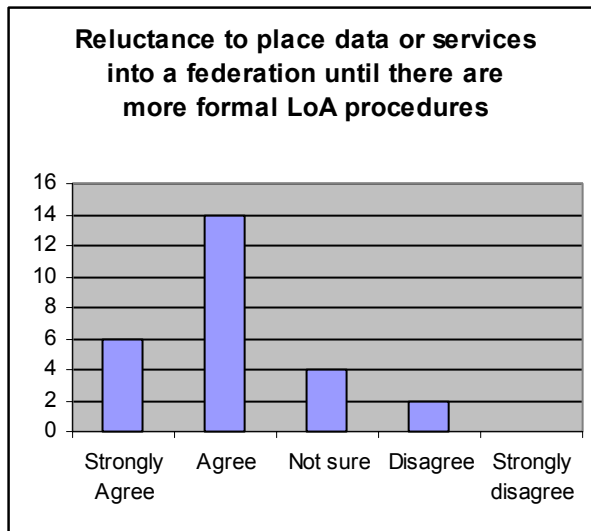


Diagram 14. Reluctance to make resources available through a federation until there are more formal LoA guidelines

2.3 Questionnaire Section 3: Identity Providers

Q3.1 What is the current status of Federated Access Management deployment in your institution?

Diagram 15 shows that no identity provider appears to be opposed to employing Federated Access Management.

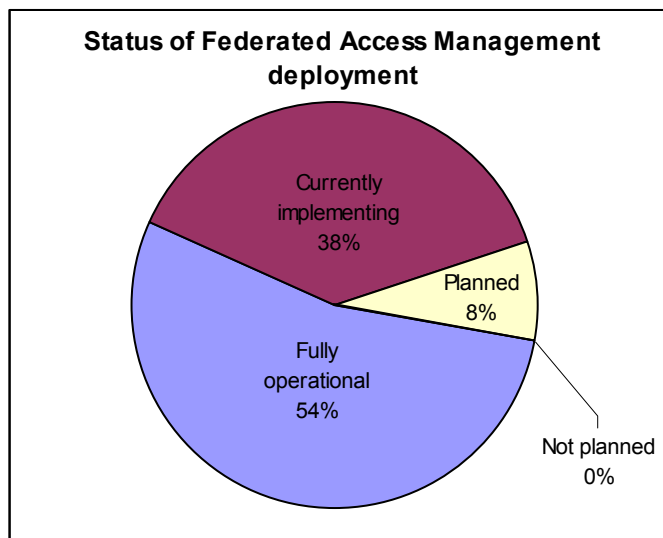


Diagram 15. Current status of Federates Access Management deployment among IdPs

Q3.2 Who uses the authentication assertions you issue?

The suggested answers included:

- One service
- Services within the same administrative domain as the Identity Provider
- Services within the same federation as the Identity Provider
- Services within the same country as the Identity Provider
- External commercial services
- External academic services
- External governmental services
- External health services

Diagram 16 shows the overall distribution of services that consume identity assertions generated by identity providers (where one identity provider may issue assertions to multiple services). Federations appear to be the biggest consumers of identity assertions - 86% of the identity providers issue identity assertions to institutions in the same federation. However, none of the identity providers are currently issuing identity assertions for accessing governmental services.

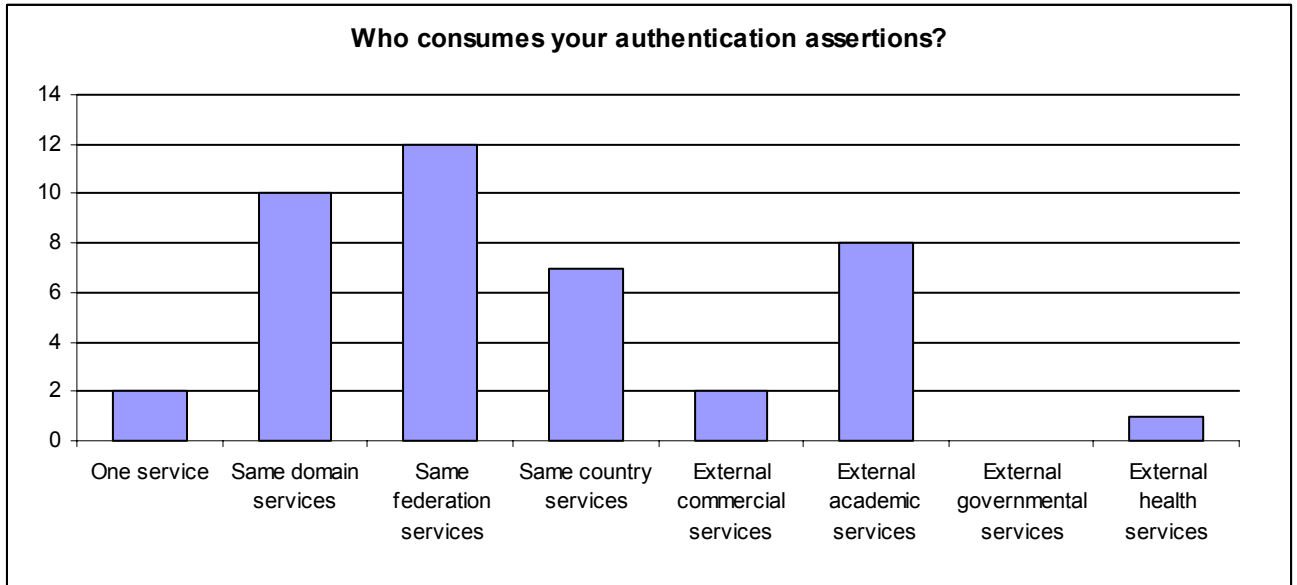


Diagram 16. Distribution of services consuming authentication assertions from an IdP

Q3.3a Do you allow individuals to authenticate using multiple mechanisms (e.g. username/password, biometric device, PKI, hardware device, one time password)?

Respondents who answered positively to Q3.3a (i.e. authenticate users using multiple authentication mechanisms) were further asked about how the decisions were made with regard to the choice of authentication mechanisms:

- At the individual's request
- At the Identity Provider's choice
- At a relying party (Service Provider's) request

Diagram 17a shows the percentage of identity providers using multiple authentication mechanisms when authenticating users, and Diagram 17b shows who makes the decision about what authentication method is used, among those who do.

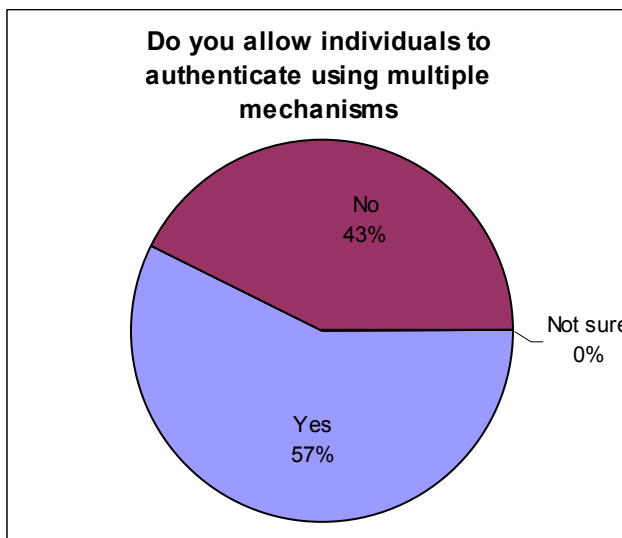


Diagram 17. Percentage of IdPs using multiple authentication mechanisms

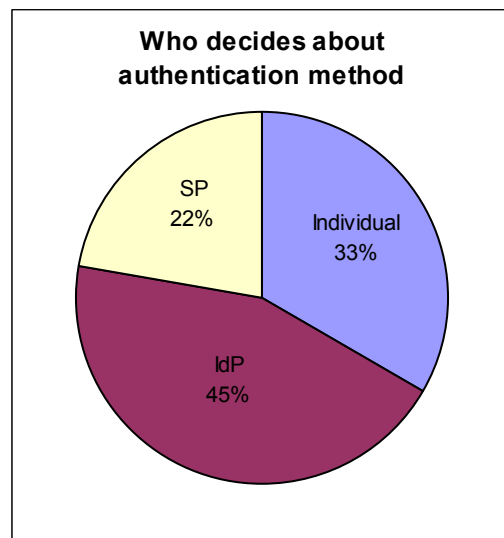


Diagram 17b. Distribution of the entities choosing an authentication method among multiple choices

Q3.3b If you do make use of multiple authentication mechanisms and you provide authentication assertions to entities both inside and outside your administrative domain, do you impose different authentication methods when identifying individuals?

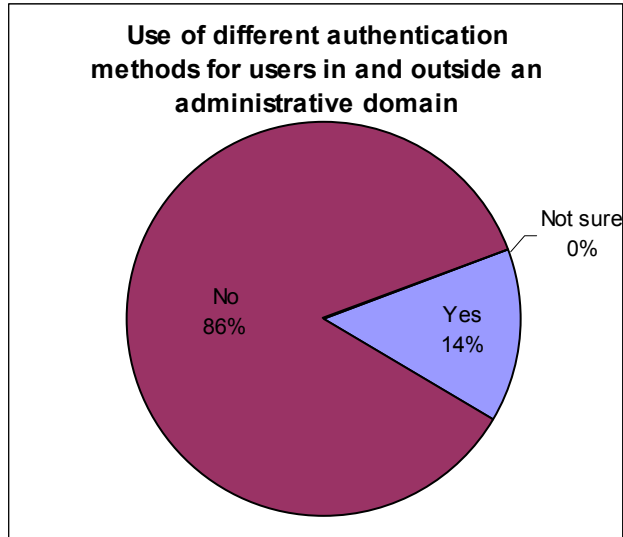


Diagram 18. Percentage of IdPs using different authentication mechanisms for users in and outside their administrative domain

Diagram 18 shows that 86% of organisations that do have different authentication mechanisms do not differentiate between assertion consumers in their own domain and those from outside their domain.

Q3.4a Do you provide authentication assertions for off-site as well as on-site users?

The suggested answers included:

- Yes
- No (on site only)
- No (off site only)
- Not sure

As can be seen from Diagram 19, a large proportion of institutions (92%) authenticate users that are both on and off-site. Note that outsourced IdPs have not been contacted as part of the survey, hence the result for off-site users is 0% in the diagram below.

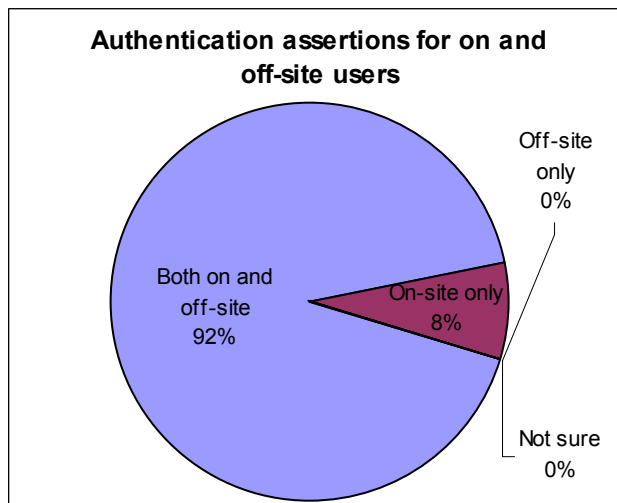


Diagram 19. Provision of authentication assertions for on and off-site users

Q3.4b In case you provide authentication assertions for both on and off-site users, is the same authentication method used for both?

The suggested answers included:

- Yes (it is a requirement)
- Yes (it is sufficient)
- No
- Not sure

In cases where an institution authenticates both on and off-site users, Diagram 20 depicts the proportion of institutions where the same authentication method is required, is sufficient, or different methods are required (i.e. institutions impose different authentication methods for on an off-site users).

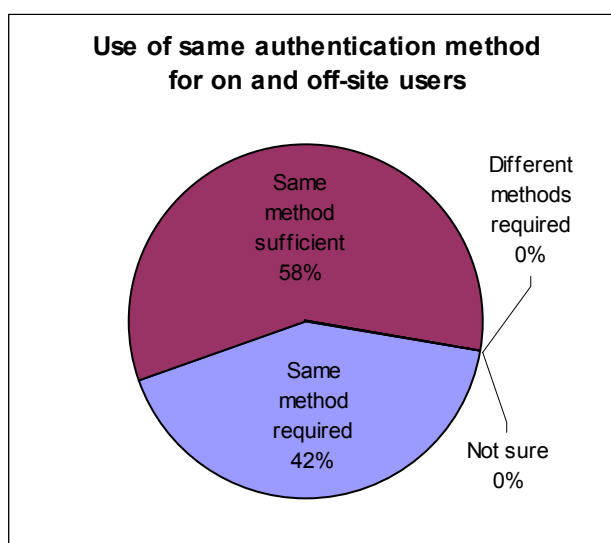


Diagram 20. The use of the same authentication methods for on- and off-site users

Q3.5a Do you make use of a PKI for identifying your users?

Respondents who answered positively were asked to indicate their PKI providers by ticking all that apply from the following options:

- We rely on externally operated PKIs (e.g. Thwart, Verisign, UKeScience)
- We rely on PKI operated within the same federation as the IdP
- We rely on PKI operated within the same administrative domain of IdP
- We operate our own PKI

Diagram 21a shows the proportion of institutions making use of a PKI, and Diagram 21b shows how or by whom the PKI is provided. It can be seen from Diagram 21b that a large proportion of institutions have invested time in setting up a PKI themselves.

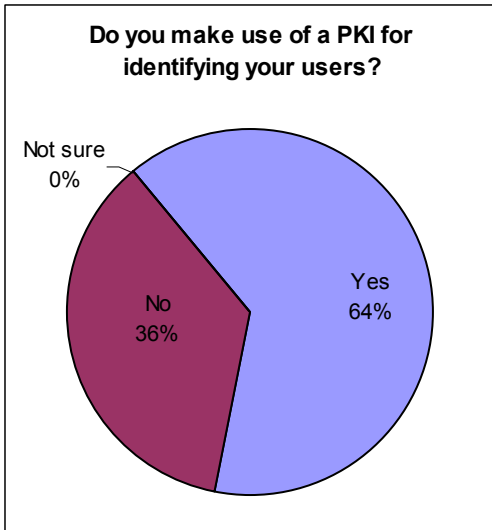


Diagram 21a. The use of PKI for authentication

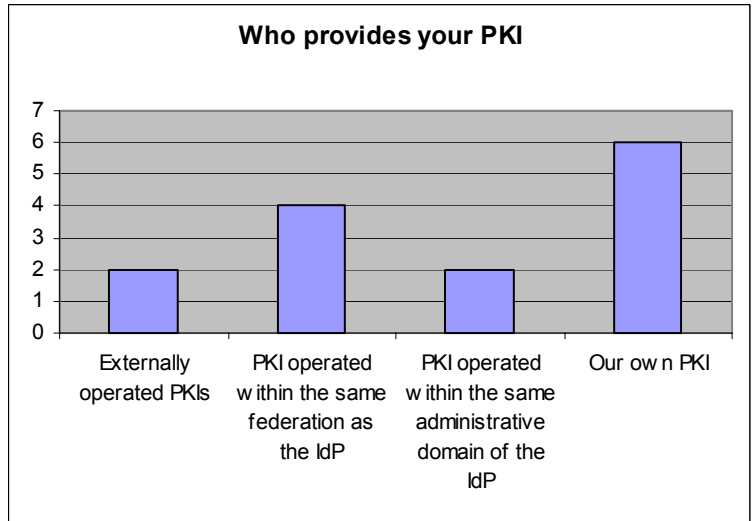


Diagram 21b. Distribution of PKI providers

Q3.5b If you operate your own PKI, do you delegate the identity vetting to Registration Authorities?

Diagram 22 shows that a large proportion of identity providers make use of Registration Authorities for identity vetting.

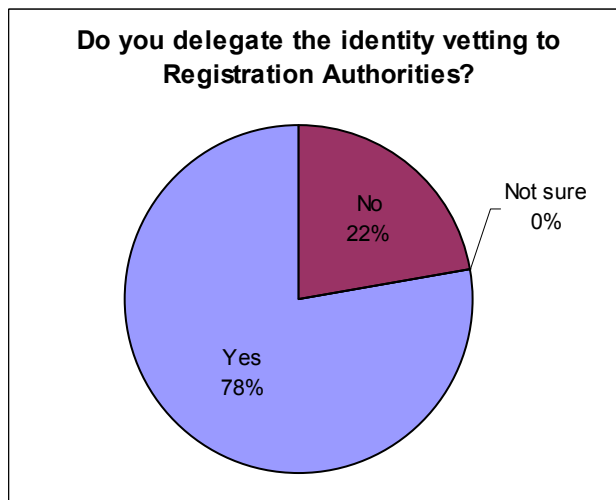


Diagram 22. Delegation of identity vetting to Registration Authorities

Q3.6 Identity proofing and registration refer to a procedure by which a user's identity information is checked by the RA before an authentication credential is issued to the user. Which of the following do you require for user registration?

For in-person registration, respondents were asked to select from the following:

- A name or a pseudonym which is accepted without verification
- A full legal name (Collected or Collected and verified¹)
- Date and place of birth (Collected or Collected and verified)

¹ This can be verified via documentation such as a recent bank statement or a utility bill.

- Current home address (Collected or Collected and verified)
- The user proves the knowledge or possession of a previously issued credential
- The user provides his/her picture ID issued by the Government (e.g. passport or driver's licence)
- Other

Diagram 23a shows the types of identification information collected from users at the time of in-person registration. Other types of information used for identity vetting by the respondent institutions are student matriculation cards, personal knowledge of the individuals, payroll, and attribute assertions from other trustworthy departments.

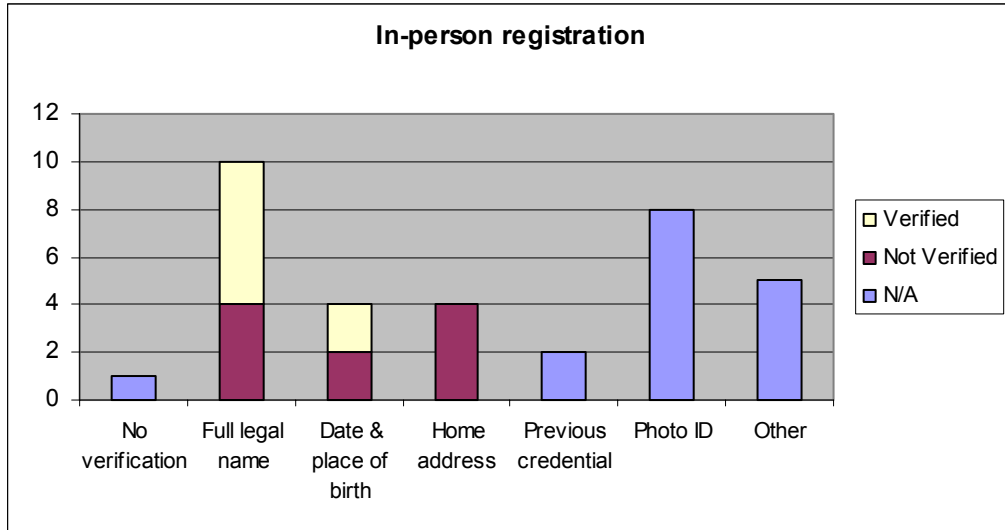


Diagram 23a. Identity information collected for in-person registration

For remote registration (e.g. via email or post), respondents were asked to select from the following:

- A name or a pseudonym which is accepted without verification
- User's full legal name, verified with, e.g. a valid credit or bank card
- User proves the knowledge or possession of previously issued credential
- User's postal address, verified by sending an authenticator to the address
- User's telephone number, verified by requiring a call from or to the number
- Other

Diagram 23b shows the types of identification information requested from users when registration is performed remotely. Other types of information include valid matriculation card numbers, telephone communication with the individual concerned, payroll, and attribute assertions from other trustworthy departments.

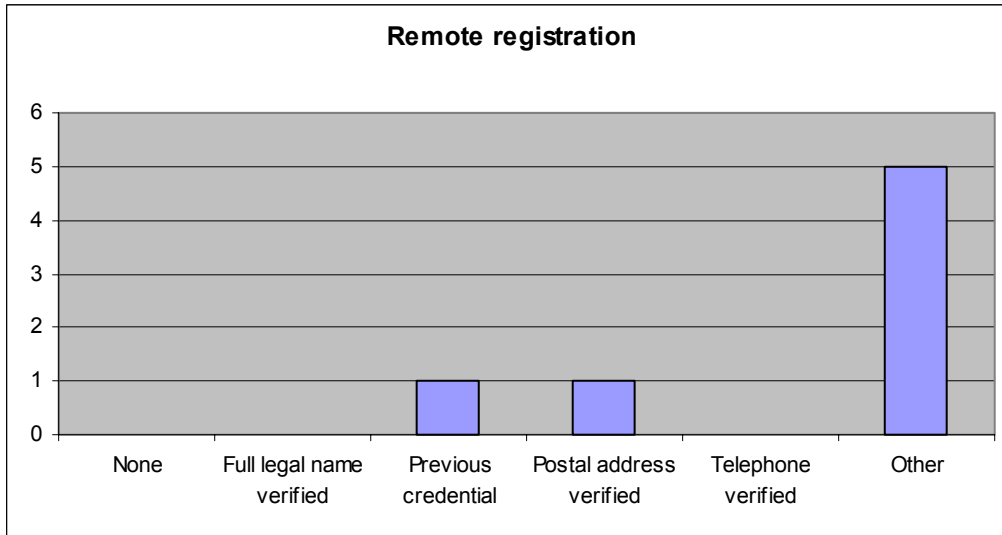


Diagram 23b. Identity information collected for remote registration

Q3.7 Do you preserve user registration records?

Respondents that retain registration records were also asked about the minimum period they retained registration data beyond the expiration or revocation of a credential, and were offered the following answers:

- 7 years and 6 months beyond the expiration
- 10 years and 6 months beyond the expiration
- Other

This question was asked to ascertain whether identity providers already satisfy the requirements for retaining user identification records as specified in the NIST LoA standard (NIST SP 800-63). It can be seen from Diagram 24b that many identity providers (67%) currently do not even satisfy the record retaining requirement for Level 2 (which is 7 years and 6 months).

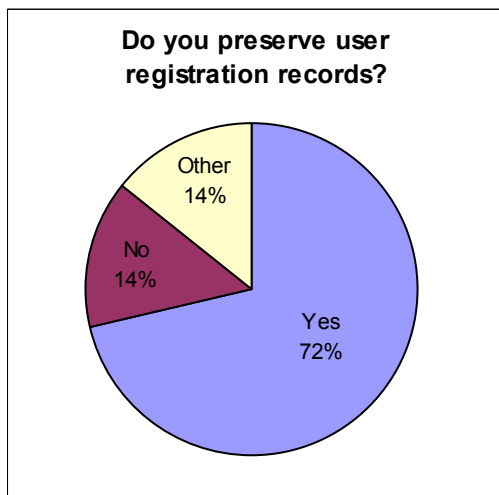


Diagram 24a. Preservation of user registration records

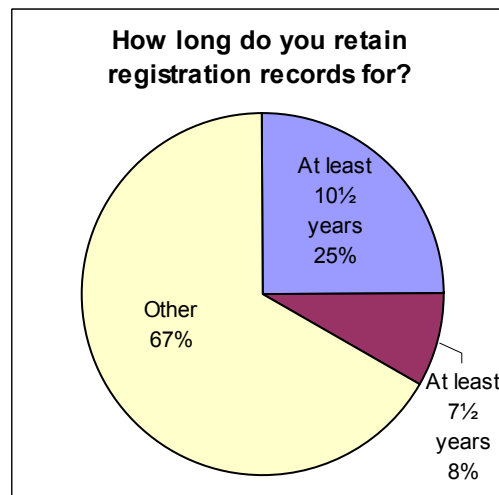


Diagram 24b. Time period registration records are preserved for

Q3.8 What type of credentials do you use for user identification and authentication?

The suggested answers were:

- Username/password pairs
- PKI credentials uploaded in users' browsers

- PKI credentials stored on a hard token (e.g. an USB token or a smartcard)
- PKI credentials stored on a hard token that is activated by a PIN/password/biometrics
- One-time password hard tokens
- Credentials stored in a remote repository access controlled through the use of passwords
- Proxy credentials (or delegated credentials)
- Group or membership type of credentials
- Other

Diagram 25 shows the distribution of the types of authentication credentials used by the respondent institutions. Among 'Other' credential types mentioned in the survey responses were PKI certificates stored on a file system and Kerberos tickets.

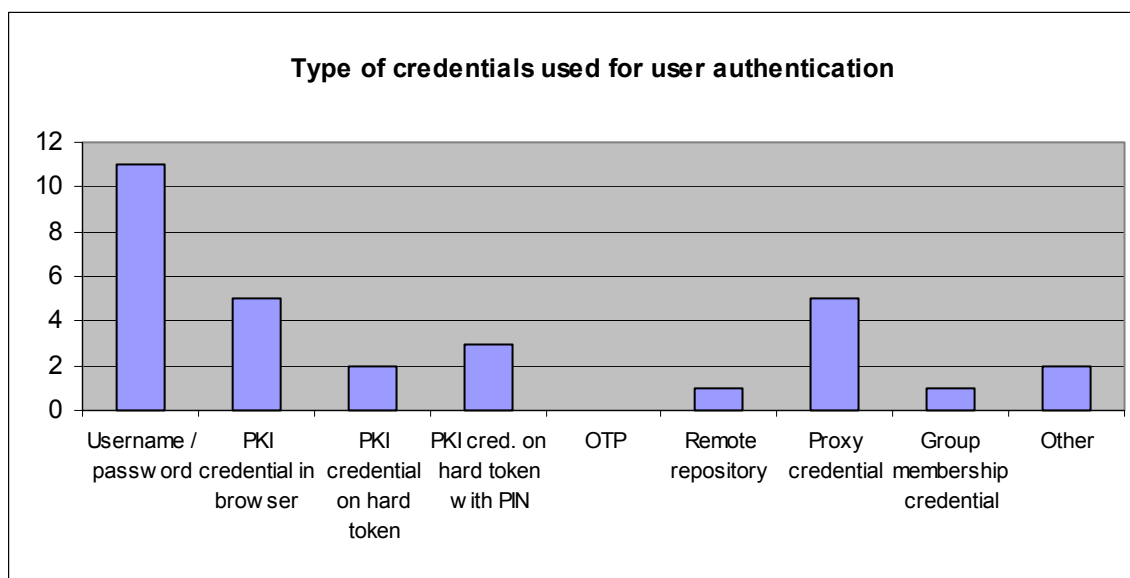


Diagram 25. Types of credentials used for user authentication

For those respondents that use more than one credential type, they were further asked to give details in terms of resource types for which (or other circumstances under which) each of the credential types is required. Here is a summary of their responses:

One UK eScience establishment uses a combination of username/passwords and proxy credentials; the latter are used for NGS and GSI applications.

One international science laboratory uses a combination of username/passwords and PKI credentials stored in both browsers and smartcards; smartcard credentials locked with PINs are used for highly secured experiments.

One foreign national eScience centre currently uses username/passwords, but is also experimenting with PKI/smartcards. The latter option is not yet in production use, and the centre is waiting for the release of Shibboleth 2.0 with the SAML 2.0 support.

One foreign national identity federation currently uses username/passwords and PKI credentials from browsers and smart tokens. The PKI credentials are just used as an additional authentication service; they are waiting for applications that require the use of a higher LoA.

One UK University Computing Services unit uses username/passwords and proxy credentials; they also use forwardable Kerberos tickets for some backend services (e.g. IMAP).

A member of Grid Ireland uses PKI credentials stored in browsers for accessing Web pages (such as Wikis); PKI and proxy credentials stored in a filesystem are used to access grid resources (such as Resource Brokers, Computing Elements, Storage Elements); PKI credentials stored in a hard token may be used via browser to access Web resources or to generate a proxy to access grid resources.

A US based national laboratory controls access to CA operations through the use of hard-tokens. It is worth noting that most organisations accept multiple credential types.

Q3.9 If your authentication system uses username/password pairs, complete this question.

3.9.1 Do you impose any validity period for passwords?

Respondents imposing validity periods were asked to further specify the period:

- Users are forced to change their passwords at least every 6 months
- Users are forced to change their passwords at least every 12 months
- Other

Diagram 26 shows the distribution of organisations imposing password validity periods. The first ('Yes') bar (representing those who do impose password validity periods) also shows durations of the periods.

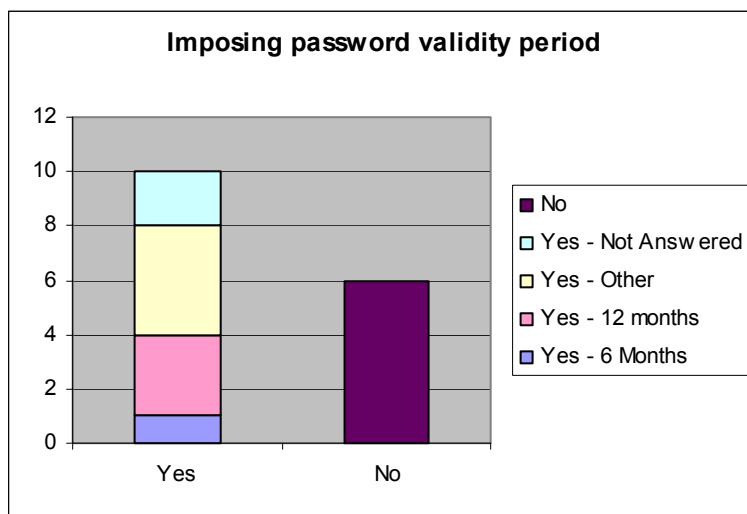


Diagram 26a. Imposing password validity period

3.9.2 Do you impose any criteria for the selection of passwords by your users?

Respondents who impose criteria for password selections were further asked to detail their criteria. They were offered to choose from the following provided answers or detail their criteria in the 'Other' box:

- A minimum of 8 characters, selected from an alphabet of 94 printable characters
- To include at least one upper case letter, one lower case letter, one number and one special character
- Not to use common dictionary words or permutations of user names
- Other

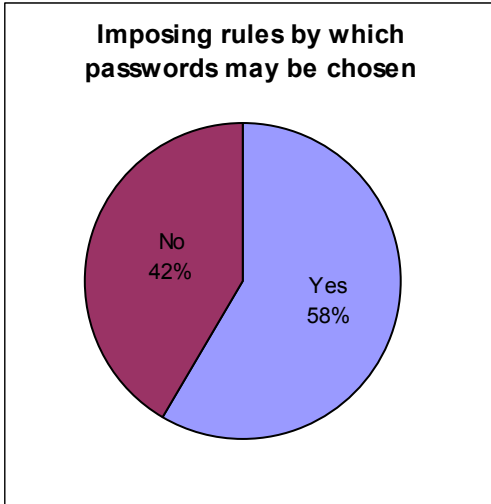


Diagram 26b. Percentage of IdPs imposing password rules

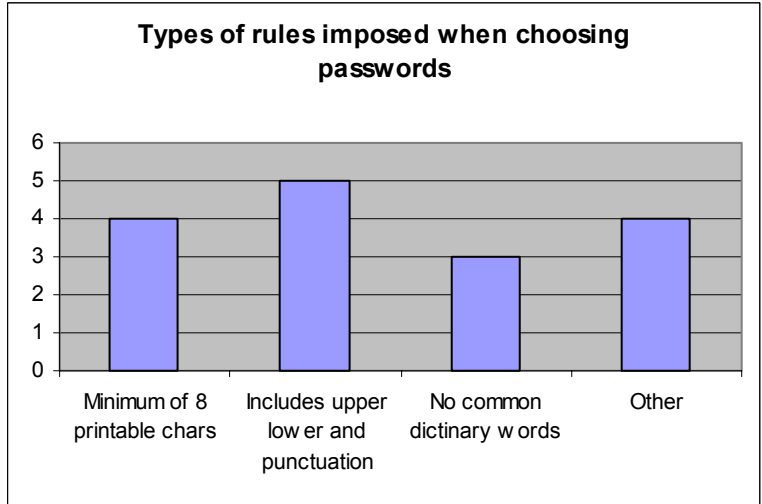


Diagram 26c. Types of password rules imposed

3.9.3 Does your system lock out password authentication attempts for x minutes after y unsuccessful trials?

Respondents imposing account lock-outs were further asked to specify values for x and y.

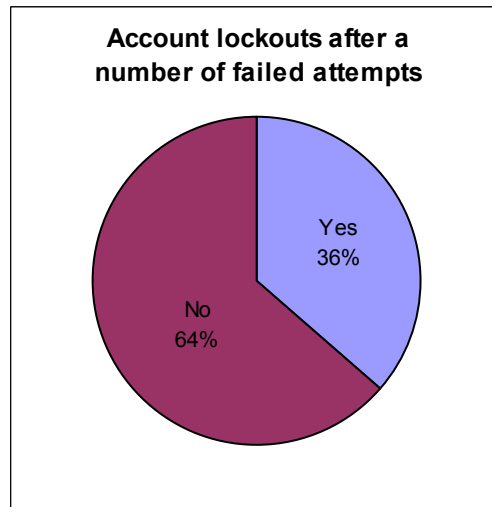


Diagram 26d. Percentage imposing account lock-outs after a number of failed authentication attempts

The rationale behind Q3.9 was to try to investigate whether, and if so, to what extent, identity providers actually satisfy the NIST SP 800-63 LoA recommendations for Levels 1 and 2. In order to determine this, we needed to estimate password entropy (E) from the responses, along with other parameters, i.e. the number (N) of unsuccessful trials allowed within a given time period (T) and the permitted lifetime of a password (L).

$Att = N * L / T$ gives the maximum number of trials an attacker may attempt during the lifetime of a password.

$PBr = Att / 2^E$ gives the probability that a password of entropy E will be broken given a number Att of attempts.

NIST LoA standard stipulates that, in order to achieve Level 1, probability P that an attacker with no *a priori* knowledge of a password can successfully crack a password, should not exceed 2^{-10} (i.e. $P < 2^{-10}$). For Level 2 this probability should not exceed 2^{-14} .

This means that, in order to satisfy the NIST LoA Level 1 and Level 2 requirements when using the username/password authentication method, the probability PBr should be less than this probability P (2^{-10} for Level 1 and 2^{-14} for Level 2).

In case of Level 1, the above formula becomes $Att / 2^E < 2^{-10}$.

In case of Level 2, the above formula becomes $Att / 2^E < 2^{-14}$.

Table 2. Values for calculating whether passwords satisfy NIST Level 1 and 2 requirements

	Estimated password entropy ² E	N° of trials N	Lockout period T	Password lifetime L	Max number of attempts during password lifetime $Att = N * L / T$	Upper limit to probability of password compromise $PBr = Att / 2^E$
UK University	Unrestricted (~0)	7	½ hour	90 days	$7 * 90 * 24 / (1/2) = 30240$	<input type="checkbox"/> 100%
International Laboratory	24	500	¼ hour	365 days	$500 * 365 * 24 / (1/4) = 17520000$	<input type="checkbox"/> 100%
Foreign National eScience centre	18	N/A	N/A	N/A	N/A	N/A
Foreign University	30	N/A	N/A	365 days	N/A	N/A

Only four respondents answered this question, and two out of the four (as shown in the first two rows in Table 2) provided enough information for us to estimate whether their practices satisfy the NIST SP 800-63 LoA Levels 1 and 2 requirements. The UK University which responded to these questions limits the number of trials to 7 within half an hour and requires users to change their passwords every 90 days. However, they do not impose any rules on the size or character base for password selection, therefore we cannot estimate a lower limit of the entropy E . In order to achieve the NIST LoA Level 1, they would have to achieve password entropy of at least 25. This can be done, for example, by imposing a 7 character password from a 94 character alphabet (requiring at least one special character) and checking for dictionary collisions. To achieve Level 2, an entropy value of 29 must be achieved (e.g. by increasing the password length to 8 characters). The international laboratory, has an estimated probability of password compromise 2^0 , which does not even satisfy Level 1. However, if they were, for example, to reduce the number of attempts N from 500 to 5 and to impose dictionary collision checks (and thereby increasing the estimated entropy E to 30), then they would satisfy NIST LoA Level 1. In order to achieve NIST LoA Level 2, they could in addition reduce L to 90 days and increase T to half an hour. After a follow-up consultation with them, we were told that they chose N to be 500 (which was a bit peculiar) in order to avoid too many helpdesk calls when users are forced to change their passwords, as some email clients (mostly Outlook in IMAP mode) ignore the 'Wrong Password Error' and keep on retrying dozens of times, leading to an account lockout.

Q3.10 If you are an Identity Provider supporting the use of PKI credentials, check any of the following that are true in your case:

- There is an on-line facility for verifying that the credentials are still valid (e.g. revocation lists or on-line validation servers)
- PKI credentials are revoked within 24 hours after being notified that the credential is no longer valid.
- PKI credentials are revoked within 72 hours after being notified that the credential is no longer valid.
- We do not have any revocation facility
- PKI credentials automatically expire after 24 hours
- PKI credentials automatically expire after 72 hours
- PKI credentials automatically expire after one year
- PKI credentials remain valid for more than 18 months if not otherwise revoked.

² Estimated entropy was calculated according to the Appendix A of the NIST e-authentication standard SP 800-63.

- Other

Results are displayed in Diagram 27.

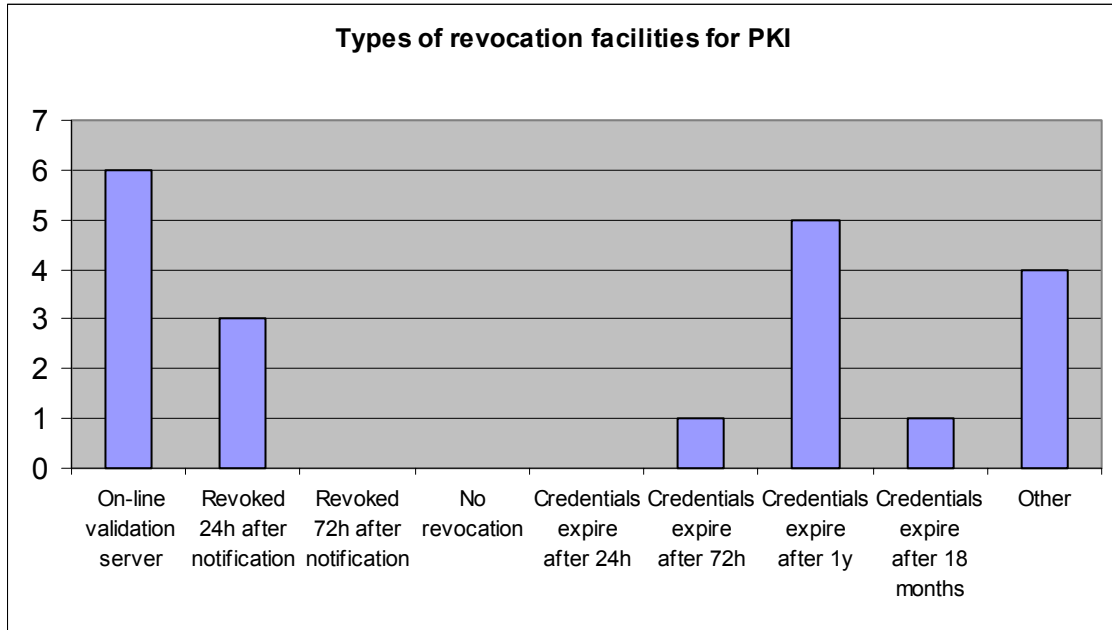


Diagram 27. Types of revocations facilities for IdPs employing PKI

Q3.11 As an identity provider, do you support the use of identity assertions?

Respondents using identity assertions were asked to further provide more information about their assertions by selecting all that apply to them from the following:

- Assertions are digitally signed
- Assertions are sent over an authenticated and secure channel using protocols such as SSL
- Assertions expire 12 hours after their generation, and are not accepted thereafter
- Assertions expire 2 hours after their generation, and are not accepted thereafter
- Other

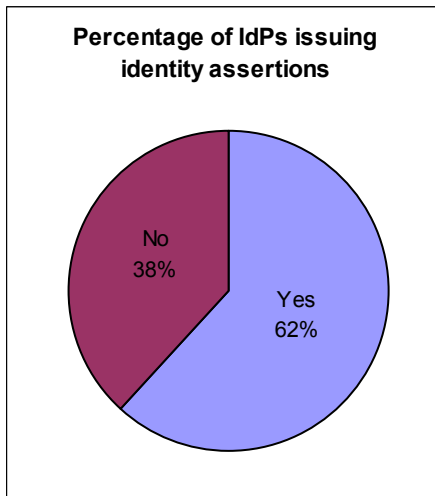


Diagram 28a. Percentage of IdPs using

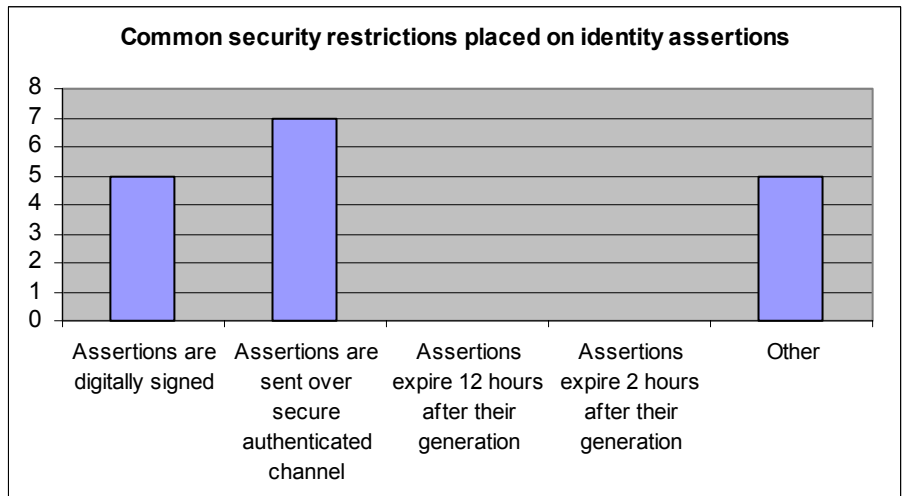


Diagram 28b. Common security protections for identity assertions

identity assertions

Q3.12 What is the average time from a user leaving your institution to disablement of his/her account?

Most identity providers disable user accounts within 24 hours from the last day of an employment or the last day of a student card's validity. One UK University disables student accounts nine months, and staff accounts 4 months, after the last day of the employment/enrolment, to leave room in case they may be contacted for survey or statistics purposes. Most foreign institutes and federations disable accounts within one to two weeks upon the termination of employment/enrolment.

Q3.13 What type of authentication protocols do you use?

The suggested answers were:

- Plaintext passwords sent unencrypted over the network
- Password challenge-response protocol
- Passwords sent over a secure channel using Secure Socket Layer (SSL) / Transport Layer Security (TLS)
- Full Kerberos (using tickets)
- Browser-based Kerberos (using passwords)
- Other

Diagram 29 shows that username/password over SSL is by far the most widely used authentication method. According to NIST SP 800-63, this method achieves a maximum of assurance Level 2.

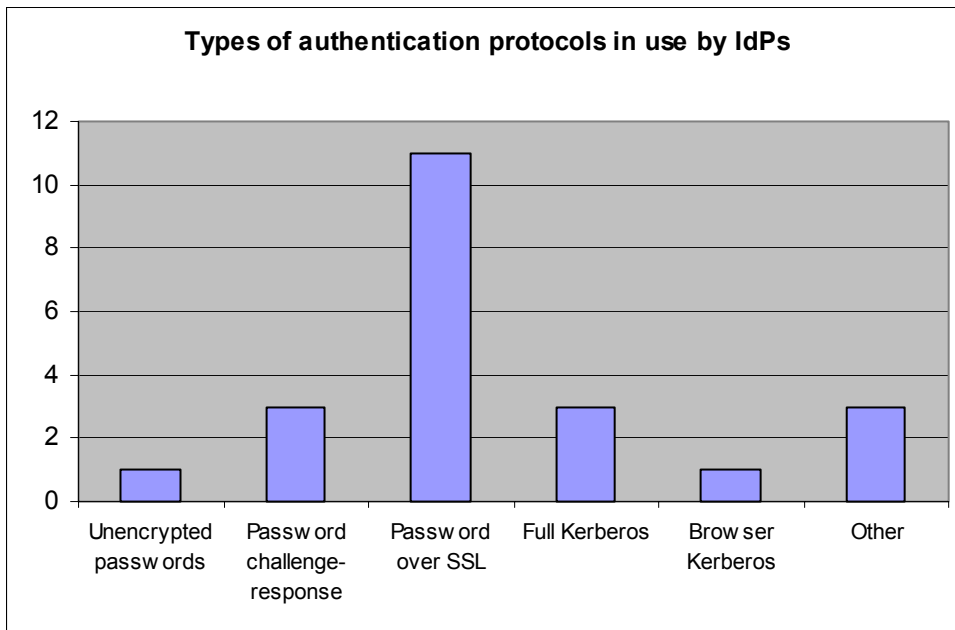


Diagram 29. Types of authentication protocols in use by IdPs

Q3.14 Service providers may require a certain level of assurance in your authentication system/process used to identify your users, which is governed by the sensitivity levels of their resources.

3.14.1 Would you be willing to follow some technical guidance for e-authentication under governance so as to achieve the required level of authentication assurance?

Diagram 30a shows that a resounding majority of identity providers would be willing to follow some technical guidance on LoA, if there were any.

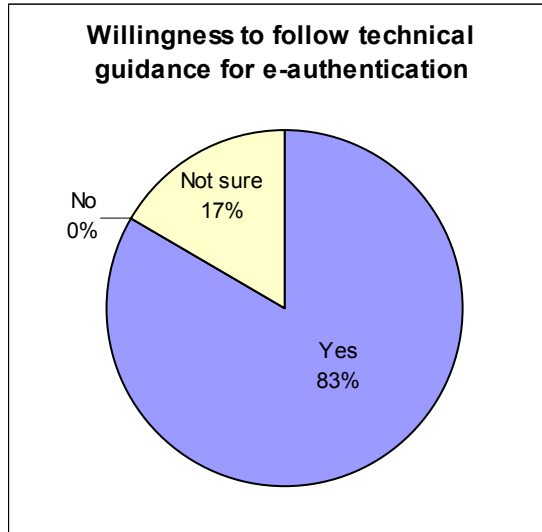


Diagram 30a. Percentage of IdPs willing to follow guidance on LoA

3.14.2 Would you be interested in being informed about the levels of authentication assurance and risk-based authentication approach?

Diagram 30b shows that 92% of identity providers would be willing to adopt the risk-based approach to authentication that incorporates LoA.

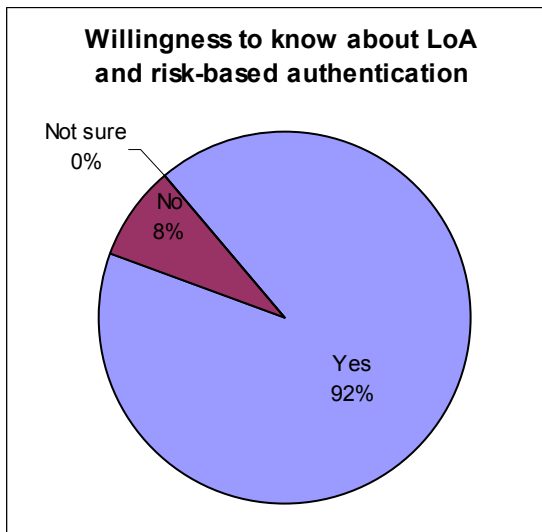


Diagram 30b. Percentage of IdPs interested to know more about LoA

2.4 Questionnaire Section 4: Grid Community

Questions Q4.1 – Q4.5 were designed to investigate service types in grids and potential applications of LoA to safeguard the grid services.

Q4.1 What kind of services do you expose via grid mechanisms?

The suggested answers were:

- Databases
- Data sets

- Data storage
- Computer terminal access
- Computer application
- Application hosting
- Visualisation
- Collaborative environment
- Resource broker
- Credential translation (e.g. KCA, GSSKLOG)
- Other

Diagram 31 presents the distribution of different types of services that are made available through grids.

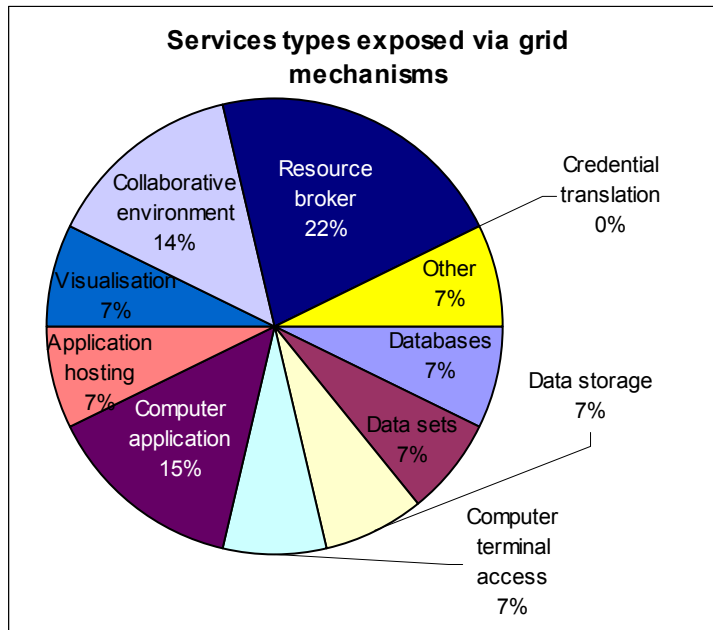


Diagram 31. Service types exposed via grid mechanisms

Q4.2 How would you rate the levels of sensitivity of the data your users can potentially access through your grid services?

Respondents were asked to rate the sensitivity levels of their resources with a value of 0, 1, 2, 3 or 4 (4 being extremely sensitive and 0 being the least sensitive). Results are shown in Diagram 32. All respondents placed some level of sensitivity on their resources. It can be noted that there is a fairly even distribution across the range of sensitivity levels.

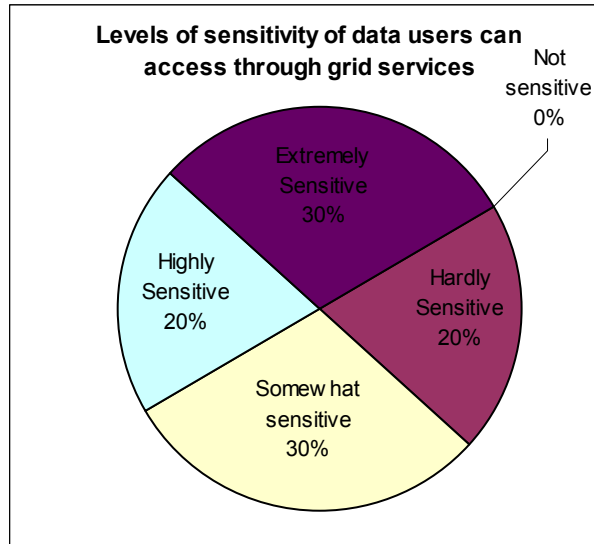


Diagram 32. Perceived sensitivity of data exposed via grids

Q4.3 Do your grid services allow users to run their own code?

Diagram 33 shows that 80% of the grid service providers surveyed do allow user-generated code to be run on their services. By allowing this, these grid service providers potentially experience greater risks and perhaps should consider employing more stringent access control approaches, e.g. LoA-linked access control approach.

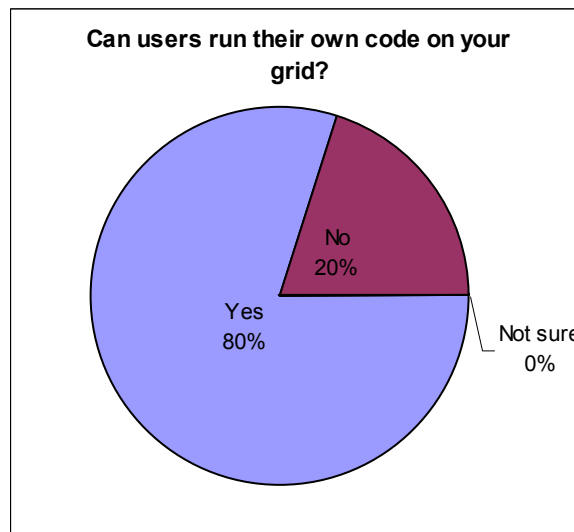


Diagram 33. Percentage of grid service providers allowing users to run their own code

Q4.4 Do your grid services provide access to large compute resources (please do not count resource brokers here)?

Diagram 34 shows that the majority of the grid service provider respondents provide access to powerful compute resources. Again, similar to question Q4.3, providers of large computing resources are in a greater risk from authentication errors as consequences of misuse of their resources can be more costly.

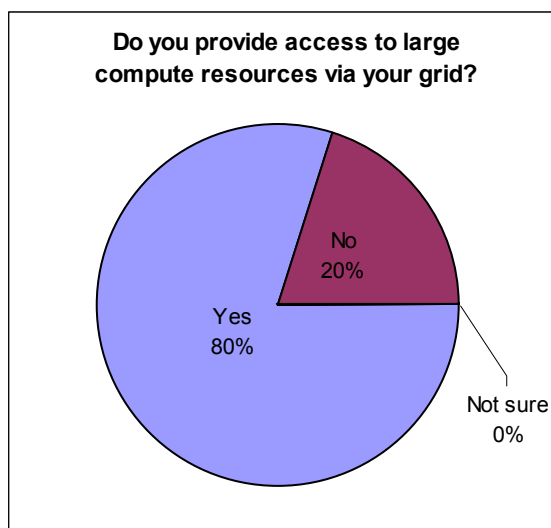


Diagram 34. Percentage of grid service providers allowing access to large compute resources

Q4.5 In exposing your service is there a requirement that you identify users who access it with any level of certainty?

All of the 10 respondents answered positively to this question. They were then further asked (Q4.5.a-c) to specify how they achieve this required level of certainty when authenticating users, and were offered with the following options:

- By selecting specific (individual or group) Certificate Authorities (CAs)
- By exchanging public keys/certificates directly (i.e. without relying on a CA infrastructure)
- By any other means

90% of respondents said that 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. One respondent (from the health sector) elaborated: *"Given the scope of access, we used to physically meet and exchange keys that way. We do not use any networked collaboration at the moment."*

Finally, respondents were asked (in Q4.5d) if they felt that they were able to achieve adequate user identification with current grid middleware, and if not, to elaborate. Diagram 35 shows that 80% believe they are able to achieve a sufficient level of authentication assurance on grids. Those 20% that think the current grid authentication provision is not sufficient feel that this is due to the grid community's reluctance to standardise/agree on mechanisms, or due to the fact that there is a lack of traceability between the work done on a worker node with the identity (e.g. certificate's subject DN) recorded at the start the job. In addition, one grid provider within the area of research involving medical records noted that there are unique and complicated requirements for identification of users in 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. To bridge the gap, more work is needed to address the requirements themselves, along with the support from the grid middleware.

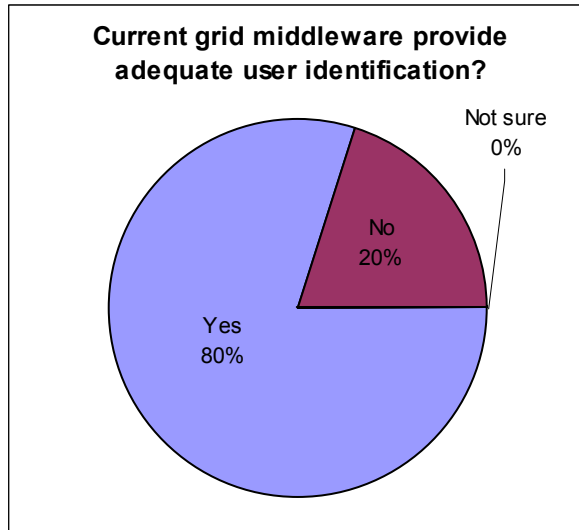


Diagram 35. Adequate user identification can be achieved with current grid middleware

Questions Q4.6-Q4.7 were about Certificate Practices/Certificate Policy Statements (CP/CPS), and their verification and enforcement.

Q4.6 Do you require that a CA publish a CP/CPS?

As shown in Diagram 36, three quarters of grid service provider respondents require a CA to publish CP/CPS documents.

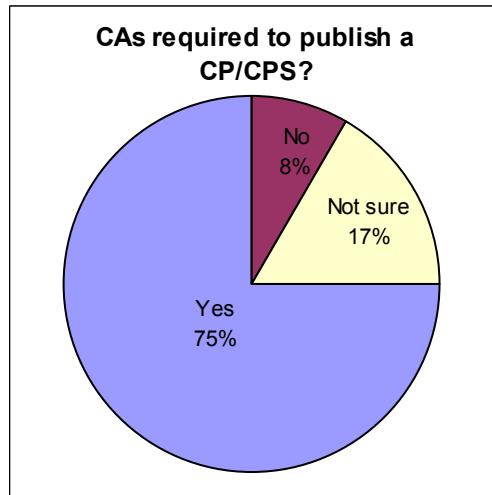


Diagram 36. Requirement for CAs to publish their CP/CPS

Q4.7 Do you require that a trusted CA adheres to their CP/CPS?

Respondents who required their trusted CAs to adhere to the CAs' CP/CPS were further asked how they enforced the requirement:

- By auditing the CAs they trust
- By relying on a third party to accredit CAs
- By trusting the CAs to run according to its CP/CPS

Diagrams 37a and 37b show that 84% require that a CA follows its own guidelines. However, less than 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 rôle to the federation in Federated Access Management).

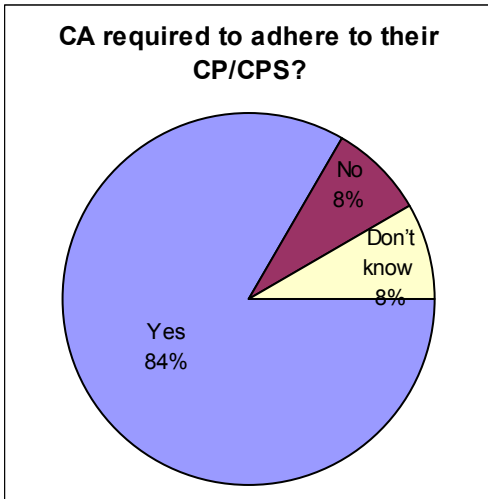


Diagram 37a. Percentage of grid service providers requiring adherence to CP/CPS

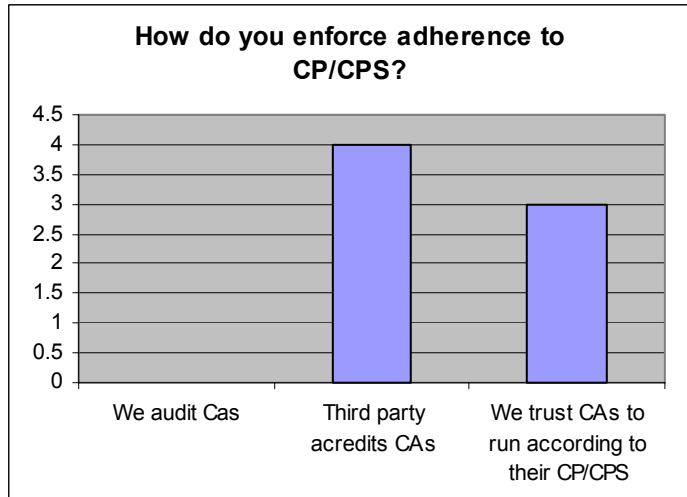


Diagram 37b. Enforcing adherence to CP/CPS

Questions Q4.8- Q4.9 were about Certificate Chains.

Q4.8 Do you require that a CA be self signed?

Those who answered positively were further asked to specify if this was:

- Policy driven
- Software implementation driven
- Driven by both

Only two respondents provided answers to the second part of this question – one was driven by policy and the other was driven by both policy and software implementation.

The purpose of this question is to gain some understanding about how middleware enabled or restricted authentication. Given that there were only 2 survey responses to this question, we cannot draw any meaningful conclusions.

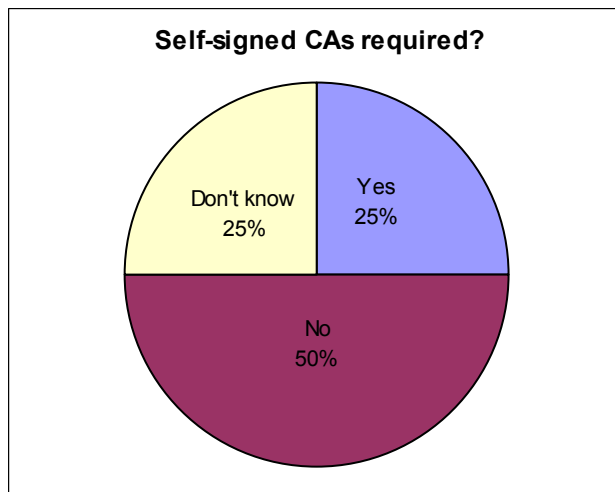


Diagram 38. Requirement for a CA to be self-signed

Q4.9 Is it necessary to impose a maximum length on a certificate chain?

Those answering positively were further asked if this was:

- Policy driven
- Software implementation driven
- Driven by both

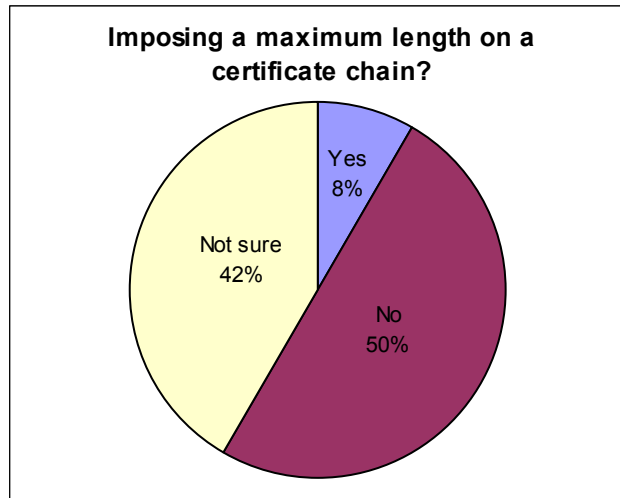


Diagram 39. Requirement for maximum certificate chain length

Only one respondents answered positively and said this was driven by both policy and software implementation. Current grid implementations, such as the Globus Toolkit, require all CAs in a chain to be present in a trusted directory, whereas a Web-based middleware, such as Apache, allows users to supply additional CA certificates to make up the chain.

Questions Q4.10- Q4.12 were designed to investigate about Namespaces.

Q4.10 Do you require that the CA issues certificates within a well defined Namespace?

Those answering positively were again asked whether this was:

- Policy driven
- Software implementation driven
- Driven by both

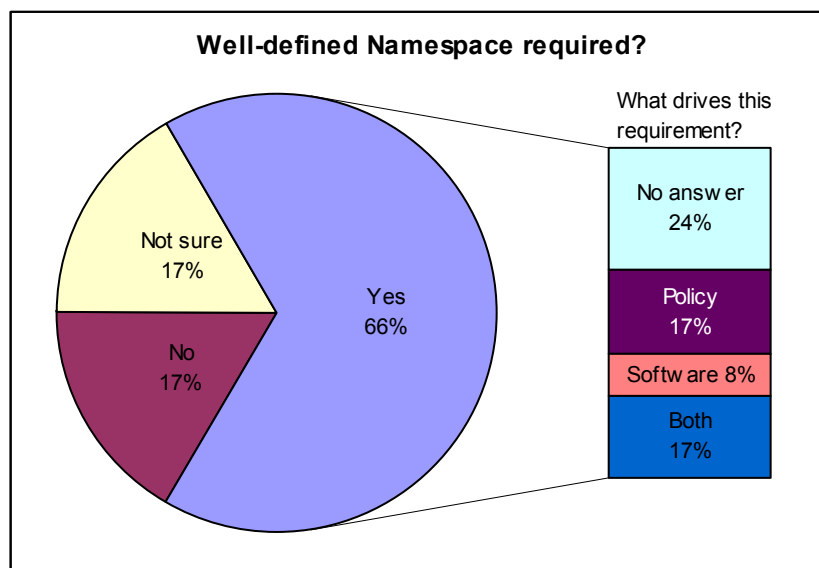


Diagram 40. Requirement for well-defined Namespace for certificate issuance

While the majority of respondents answered positively, a significant number responded negatively or were not sure. 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.

The purpose of this question was to highlight the split between the PKIX community's idea of authorisation based upon X.509 certificates and the grid communities. If authentication is based on a mixture of CAs from both communities then it is difficult to see how any confidence in the authorisation process can be maintained.

Q4.11 Do you require that a CA issue certificates with "meaningful names" in the *commonName* field (i.e. not anonymous pseudonyms)?

The suggested answers included:

- Yes
- No (but the CA must be able to provide a trace back to the individual possessing the corresponding private key)
- No (please give your reasoning)

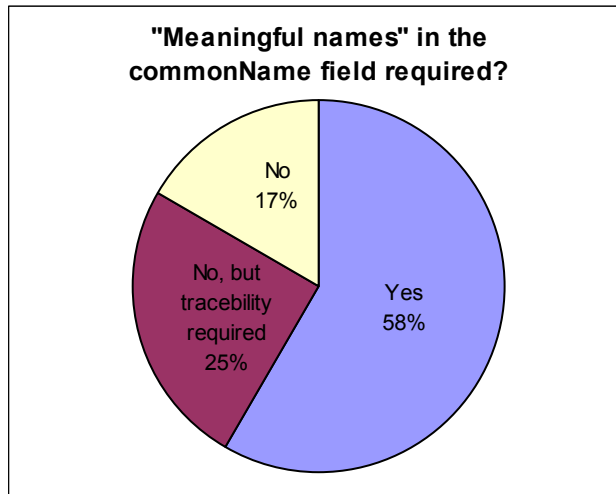


Diagram 41. Requirement for well-defined Namespace for certificate issuance

One respondent commented: *'We are required as CA operators to issue "meaningful names", although "meaningful names" is inherently meaningless'*. Others (those that answered negatively) did not provide any reasons for not requiring a CA to issue certificates with meaningful names in the CN field.

The survey results show that just under two thirds of grid services felt it was important to be able to have a verifiable "meaningful Name" asserted when 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.

Q4.12 Do you impose restrictions on elements allowed in Distinguished Name (e.g. must not use *emailAddress*)?

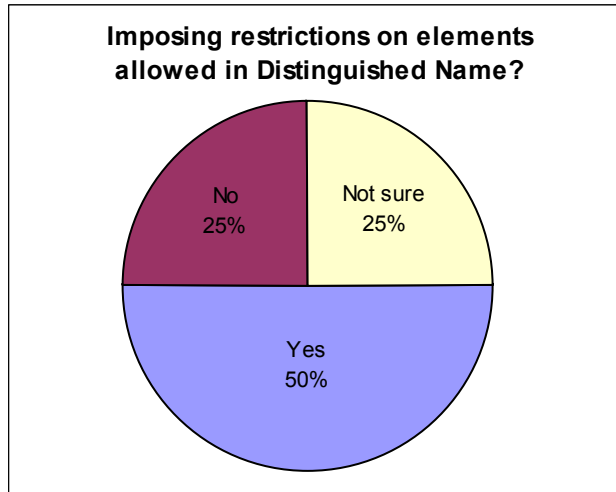


Diagram 42. Imposing restrictions of elements allowed in DN field of a certificate

Questions Q4.13- Q4.14 were about authorisation.

Q4.13 How do you control access to your grid services?

The suggested answers included:

- By Organisation
- By Virtual Organisation
- By lookup list of certificate DNs
- By lookup of locally stores X509 credentials
- External rule (e.g. time/system load...)
- Other

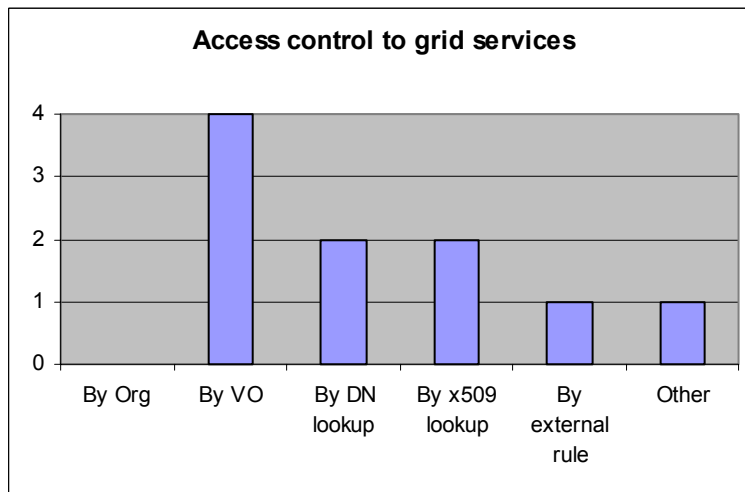


Diagram 43. Types of access control to grid services

The respondent that answered ‘Other’ qualified their answer by saying that they used SAML assertions.

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 required a VO to be associated with a legal entity.

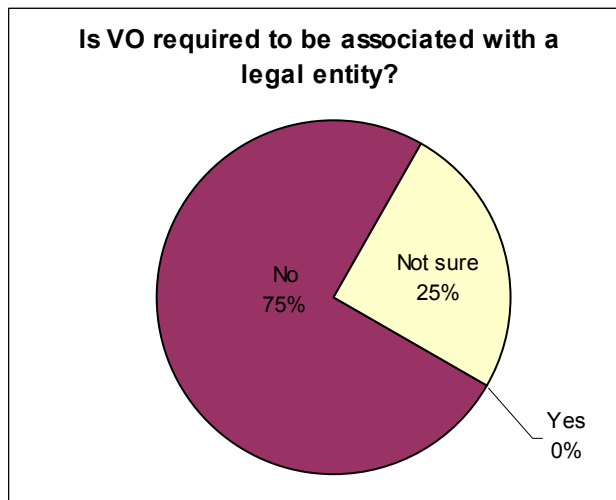


Diagram 44. Requirement for the VO to be associated with a legal entity

Q4.14 Is your service able to use authorisation attributes embedded within an entity's authentication credential?

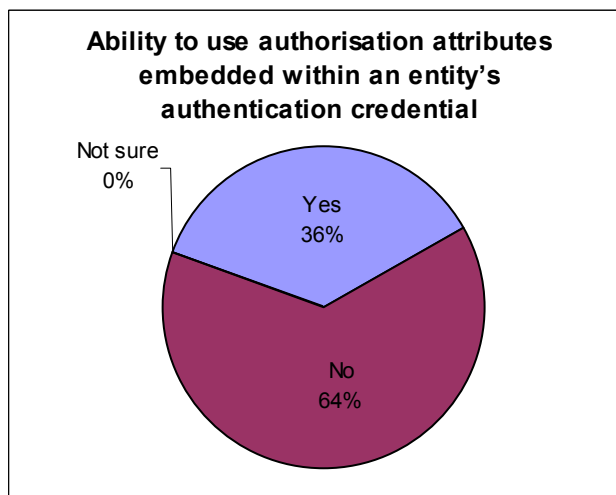


Diagram 45. Percentage of grid service providers being able to use attributes embedded in certificates for authorisation decisions

Those who answered positively were also asked if they used the embedded attributes for making authorisation decisions and 75% of respondents replied positively.

Questions Q4.15- Q4.16 were about GSI Proxies.

Q4.15 Do your services accept GSI proxy credentials?

Diagram 46 shows that the majority of respondents are able to accept GSI proxy credentials for authentication. The implication of this question is that, since these credentials are stored in unencrypted form on machines and, despite generally having short lifetime (typically 12 hours), there are no actual restrictions on how long they can be valid for (apart from the lifetime of original certificate used to create the proxy), this will certainly affect the maximum LoA level that can be achieved.

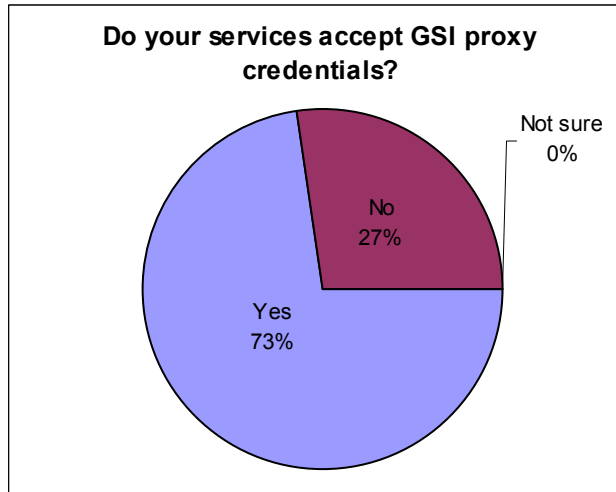


Diagram 46. Percentage of grid service providers accepting GSI credentials

Q4.16 Do you make any distinctions between different types of GSI proxy credentials?

Those who answered positively were asked to specify the restrictions as:

- Lifetime restriction
- Path length restriction
- Accept specific types (legacy, pre-rfc, rfc) of proxies
- Other

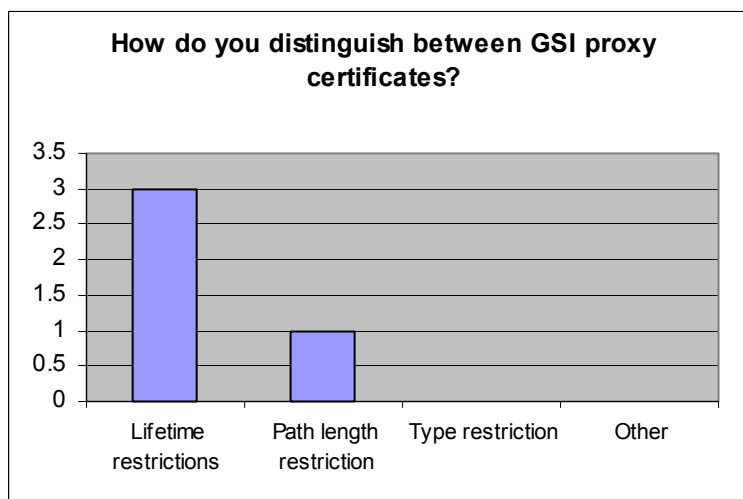


Diagram 47. Distinguishing between GSI proxy credentials

The purpose of this question was to see whether people 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 a general practice but not a rule), then there are more chances for an attacker to get hold of and use it. This is generally not an acceptable behaviour (i.e. to have a proxy valid for more than 12 hours), but no one seems to check for this. Restrictions based on proxy lifetimes and proxy pathlengths could help services to enhance their security.

Personal experiences lead 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 two.

3 Observations and Comments on Survey Findings

The following summarises our observations made from the survey results, and point out the most interesting findings.

The survey had 30 respondents and a good spread of different types of organisations – identity providers, service providers, publishers, Certification and Registration Authorities, etc. Surprisingly a large number of respondents (23 out of 30) thought they were innovators or early adopters.

3.1 Observations and Comments from the Service Providers' Section

A large proportion of service providers (88%) are adopting or planning to adopt Federated Access Management. About half of them are operational (partly or fully).

Risk assessment is an important stage for adopting LoA-based access control; half of the service providers surveyed have done risk assessments, another 12% is planning to do so, and 19% are not sure about performing risk assessment.

Regarding damage and consequences to their assets or services due to unauthorized access – most service providers were concerned about reputation or system security. Also, those reluctant to adopt Federated Access Management thought there was a high or medium levels of risks associated with joining a federation.

Nearly all of the service providers surveyed required some confidence in users' identities, and 27% of them required the highest level (i.e. Level 4 on a scale 1 - 4). These 27% also seem to correlate with service providers perceiving risk impact to their services as stronger. That is, those wanting the highest LoA are the ones most concerned about damage to reputation or system security. There seems no correlation between the willingness to join a federation and those wanting a high value of LoA.

Almost all of the service providers surveyed wanted to know how users were authenticated. The confidence in the 'quality' of the users' attributes asserted by a third party identity provider (i.e. attribute LoA) is rated as important as the confidence in the 'quality' of authentication (i.e. credential LoA).

Almost all service providers would be willing to respect some national or international standards or guidelines on e-authentication, and a large majority 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.

Many (68%) of the service providers surveyed agreed that some of their resources were more sensitive than others. However, a smaller majority (61%) of them use the same authentication procedure for all resources (perhaps because they do not have any alternatives).

With regard to authenticating on and off-site users, a majority of service providers believed that the same system should be used for both user groups. The exception seemed to be commercial service providers (publishers, subscription agents, etc.), the majority of whom believed that external users needed a stronger form of authentication.

Unsurprisingly, 70% of the service providers wanted a stronger form of authentication for more sensitive/valuable resources.

There are potential services not yet available via the federation because some service providers surveyed implied that they were waiting for more formal LoA procedures before placing their more valuable resources into the federation pool.

3.2 Observations and Comments from the Identity Providers' Section

All of the identity providers surveyed have implemented, are implementing or are planning to implement Federated Access Management.

The majority of authentication assertions issued by identity providers are being used by services within the same federation and/or within the same country. Academic and/or commercial services

external to the federation of the identity providers concerned are also using the assertions. However, there currently seem to be no government services consuming the assertions.

More than half of the identity providers surveyed use multiple authentication mechanisms; the decision as to who is supposed to choose a particular authentication mechanism during service access is split between an identity provider (45%), individual (33%) and service provider (22%). A large majority (86%) use the same authentication method for users from inside and outside an administrative domain.

Nearly all (92%) of the identity providers provide assertions for both on-site and off-site users. For these identity providers, the same authentication mechanism is deemed either necessary or sufficient in all cases.

Two thirds of identity providers make use of a PKI for identifying users and use a variety of PKI providers. More than three quarters delegate identity vetting to a Registration Authority. All respondents supporting PKI credentials have some sort of verification/revocation/expiration mechanism.

Full legal name, place/date of birth, home address and a photoID were the most common requirements for in-person user registration. However, not all of them actually verified the supplied documents. A variety of methods were used for remote registration verification; typically student card numbers were required or a proof of possession of a previously issued credential.

Three quarters of identity providers retain users' registration records. However, among these, only 8% keep them for more than 7 years and 6 months, which is the NIST LoA registration requirement for Level 2.

While username/password pairs seem to be the major authentication method used by 92% of identity providers, many other authentication mechanisms are also supported and used in various combinations (Kerberos tickets, PKI credentials, proxy credentials, etc.). Around half (57%) of identity providers accept multiple credential types. When the username/password-based authentication method is used, the most commonly used authentication protocol is tunnelling passwords over TLS/SSL channels, which achieves at most NIST LoA Level 2.

Among those respondents using username/password pairs for authentication, a slight majority (62.5%) impose some sort of validity period while the rest do not impose any. A small majority (58%) have rules about password selection including minimum password length, mixed case or no common dictionary words requirements. Only a third of respondents lock out users after a number of failed attempts. In other words, none of the respondents actually imposes all these rules at the same time. Thus, we can conclude that no one among those surveyed that use the password authentication method can actually achieve NIST LoA Level 2. However, two among the respondents came very close to achieving Level 2 (and would be able to achieve Level 2 provided that they impose a slight change in their password management procedures).

Nearly two thirds of the identity providers surveyed supply identity assertions (i.e. they assert the identity of an individual in addition to any other attributes supplied).

Most identity providers disable users' accounts within 24 hours from the last day of their employment or the last day of students' cards validity periods, and some maintain the accounts for a longer period upon termination of employment/enrolment.

3.3 Observations and Comments from the Grid Resource Providers' Section

Similar to the surveyed service providers, a great majority (83%) of identity providers would be willing to follow some guidance on e-authentication. In addition, 92% would like to be informed about the LoA developments and risk-based approach to authentication.

The grid service providers surveyed rated the sensitivity levels of their resources fairly evenly along the scales 1-4, and none rated their services to have a sensitivity level of 0.

A large proportion (80%) of grid service providers allow users to run their own code which will potentially increase the levels of risks imposed to the service provider, and this may affect the LoA value required. The majority of these grid service providers (80%) also provide access to large compute resources, which further increases risk levels.

80% of the grid service providers surveyed said they were satisfied with current grid authentication provisions. Those that feel otherwise came from the health sector and national laboratory. The grid service providers from the health community tend not to use on-line key exchanges for establishing trust.

Three quarters of grid service providers require a CA to publish and adhere to their CP/CPS; however, 30% of them allow CAs on their system without checking the CA's adherence to its CP/CPS.

Certificate chain length is not perceived as important to the majority of grid resource providers; however, a large number were unsure. The majority of grid service providers require a well defined namespace and there is a fairly even spread of whether this is a policy or an implementation requirement. 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.

A fair number (40%) of grid services grant a VO the authority to access their resources, and three quarters of them do not require the VO to be linked to a legal entity. This is in contrast to the position of the current UK Identity Management Federation and may be related to the strict identity policies available through trusted Certificate Authorities and the subsequent traceability of the individuals via their identity and not their VO membership.

A relatively few (about one quarter) grid services surveyed are currently in a position to authorise access based upon attributes presented within grid identity credentials (i.e. GSI proxy certificates), despite about three quarters of grid service providers being able to accept proxies.

A large proportion (50%) of grid service providers using GSI proxy credentials for authentication 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).

4 Conclusions

The information gathering process for this survey mainly targeted at identity providers and service providers within the UK academic and research community, of which a fair number responded. Given the current size of the UK federated management initiative we estimate that this sample covers between 10% and 20% of this community.

We are able to report that the early adoption of federated access management is good.

There is a clear requirement for the level of assurance of an authentication credential to be evaluated before access to certain services and the community as a whole is beginning to factor in some levels of authentication assurance into their services' risk assessments. However, this appears to be approached without reference to standards, which will become difficult to re-evaluate should the service become part of a federation.

There is a discrepancy between commercial services and non-commercial services in that the commercial sector wishes external users to be authenticated more strongly than internal users. This suggests the reliance upon other security mechanisms within those organisations e.g. a physical presence or access via VPNs, etc.

Should the UK Access Management Federation adopt LoA guidelines based upon, e.g. NIST SP 800-63, the majority of Identity providers surveyed would fail to achieve even the most minimal standard of authentication assurance. In most cases it would be trivial for the identity providers to create policies which elevated their maximum permitted LoA to level 2 at a minimum cost. However, most IdPs do not employ technologies which would allow for a higher LoA.

The demand for higher LoAs is apparent with roughly 25% of respondents showing a need for a LoA higher than most IdPs are capable of achieving, assuming that a "very high level of confidence" in clients' identities maps onto NIST LoA Levels 3 or 4.

Should we wish to embrace the medical sector, and the commercial sector we need to

1. encourage the provision of more secure authentication methods; in many cases the plain username/password method is the most commonly used but often insufficient;
2. in cases where username/password authentication methods are used, appropriate identity management and operational policies should be in place in order to achieve NIST LoA Levels up to 2;
3. provide a secure infrastructure within which these attributes can be moved; and
4. provide guidance and/or governance.

Most grid technologies already provide access based upon PKI credentials and the infrastructure is established. It is felt that this is a currently sufficiently high level of authentication for the types of services deployed. However, we note again that there is a general avoidance of grid computing by the commercial and medical sectors. This may change if-and-when Federated Identity Management takes on the role of Registration Authority within the Grid PKIs.