

The ES-LoA Project

WP2 Deliverable

**A Defined Set of LoA Recommendations for the Use within the
UK Education and Research Communities**

October 2007

*Aleksandra Nenadić and Ning Zhang
School of Computer Science
University of Manchester*

Executive Summary

The ES-LoA project, funded by the UK Joint Information Systems Committee (JISC) under its e-Infrastructure Security Programme, investigates current and future needs among UK research and education community for a more fine-grained access control, which allows service providers to take into account of the levels of confidence in identifying a remote entity requesting for service access. Such a fine-grained access control scheme can be attractive to service providers offering resources with varying levels of sensitivity or wishing to tailor their security protections based upon risk levels. Service providers may wish to restrict access to more sensitive resources only to those who have gone through a more stringent authentication process, or given the same remote entity, require the use of a stronger authentication token should the access request come from a more risky environment. In this way, the quality of an authentication instance, expressed as an authentication Level of Assurance (LoA), becomes one of the parameters used in access control decision making.

The project has investigated existing LoA definitions at both national and international levels, and examined the suitability of these definitions when being applied for use in UK education and research communities, and identified gaps in existing authentication and authorization policies, procedures and infrastructure structure and processes in the use of LoA in long term in the UK education and research community. Our research has revealed that the most notable and widely used LoA regime is the one produced by the US government (the OMB Memorandum M-04-04 and NIST SP 800-63 E-Authentication Guideline), which proposes a 4-level LoA model (with Levels 1 to 4). The OMB/NIST 4-level LoA model is being used, or being referenced, by several initiatives, including the US e-government, e-commerce and a number of international federations and research initiatives. A critical mass of institutions adopting and implementing this regime seems to have been established. Through our community consultation with the UK education and research community in terms of LoA definitions and applications, taking into account issues such as interoperability with other international federations and communities, we are able to recommend the community to use the OMB/NIST LoA regime, while addressing the gaps identified when applying this model to federated access management environments based on the Shibboleth technology.

This document gives recommendations with regard to concrete steps for the UK education and research community to take in order to implement the OMB/NIST LoA regime, and highlight further work necessary when applying this regime to the federated access management environment. The document should be read in conjunction with the ES-LoA project WP1 deliverable 'Using LoA to Achieve Risk-Based Access Control: A Study Report' and 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', which contain a more detailed coverage of existing LoA definitions and efforts at both UK and international levels, and our survey findings that lead to these recommendations and gap identifications, respectively.

Table of Contents

Executive Summary	2
Table of Contents	3
List of Figures	4
Acknowledgements	5
1 Introduction	6
2 Background	6
3 Recommendations to JISC	7
4 Gap Analysis	8
4.1 Gaps in LoA Definitions	8
4.2 Gaps in LoA Policies	9
4.3 Gaps in LoA Implementation	10
5 Conclusions	11
References	12

List of Figures

Figure 1. Distribution of LoAs vs. resource sensitivity/risk levels and IdM costs	7
Figure 2. Factors affecting the LoA in a Shibboleth environment.....	9

Acknowledgements

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

A Defined Set of LoA Recommendations for the Use within the UK Education and Research Communities

1 Introduction

The document, the WP2 deliverable of the ES-LoA project, serves two of the ES-LoA project objectives as defined in the original project proposal, i.e. (1) to build community consensus and make proposals with regard to the standard definition of LoA and the number of these levels for use within the UK education and research community, and (2) to identify any gaps in existing authentication and authorization policies, procedures and infrastructure structure and processes in the use of LoA.

The document is produced based on the outcomes of two ES-LoA project tasks, the investigation of existing definitions of LoA at both the UK and international levels, and community survey and consultation with the UK education and research community, commercial service providers, and e-science/grid community with regard to appropriate definitions and applications of LoA in achieving fine-grained access control of various types of resources. It should be read in conjunction with two other ES-LoA project deliverables, WP1 deliverable 'Using LoA to Achieve Risk-Based Access Control: A Study Report' [WP1-D] and WP3 deliverable Part 2 'Service Providers, Identity Providers and Grid Community Survey on Levels of Assurance: Report on Full Survey Findings' [WP3-D]. The document is structured as follows. Section 2 summarises current efforts in defining and using LoA to achieve fine-grained control of access to networked resources and electronic transactions. Section 3 recommends an LoA model for the use within the UK education and research community, while Section 4 identifies the gaps, challenges and areas of further work if the community is to adopt the recommended LoA model in the federated access management environment. Finally, Section 5 concludes the document.

2 Background

The OMB/NIST LoA specification, produced by the US Government as part of its e-government initiative, is by far the most complete and comprehensive LoA specification to date. The specification comprises two companion documents: the Office of Management and Budget's (OMB) Memorandum 'E-Authentication Guidance for Federal Agencies' [OMB-M0404] and the National Institute of Standards and Technology's (NIST) SP 800-63 'Electronic Authentication Guideline' [NIST-SP800-63]. They define four levels of authentication assurance in terms of potential impact of authentication errors and misuse of credentials. Level 1 gives the lowest and Level 4 the highest degree of certainty that an identifier presented by a user indeed refers to the user's identity. The OMB Memorandum specifies a set of guidelines for organisations to assess risks associated with authentication errors, to classify resources and transactions into four classes based on the severity and impact of the identified risks, and to assign appropriate authentication assurance levels to each resource class. The complementary document, the NIST E-Authentication Guideline, specifies the necessary technical requirements for implementing the OMB's levels of authentication assurance.

The NIST LoA specification (see Figure 1) allows the use of a wide range of authentication methods often seen in networked applications, and assigns assurance levels to these methods as follows:

- Authentication methods using username/password pairs provide single-factor authentication, and can only achieve assurance Levels 1 and 2. At Level 1, password challenge-response protocols are allowed, while Level 2 requires passwords to be sent through an encrypted channel, e.g. through a TLS/SSL tunnel.
- Authentication methods using soft cryptographic tokens and one-time password devices can achieve Levels 1 to 3. At Level 3, however, a token must be activated (unlocked) with the use of another factor, e.g. a password, a PIN or a piece of biometric.
- Authentication methods using hard cryptographic tokens that are activated by a password, a PIN or biometrics can achieve the maximum NIST LoA Level 4. In other words, only multi-factor authentication methods are allowed at NIST LoA Levels 3 and 4.

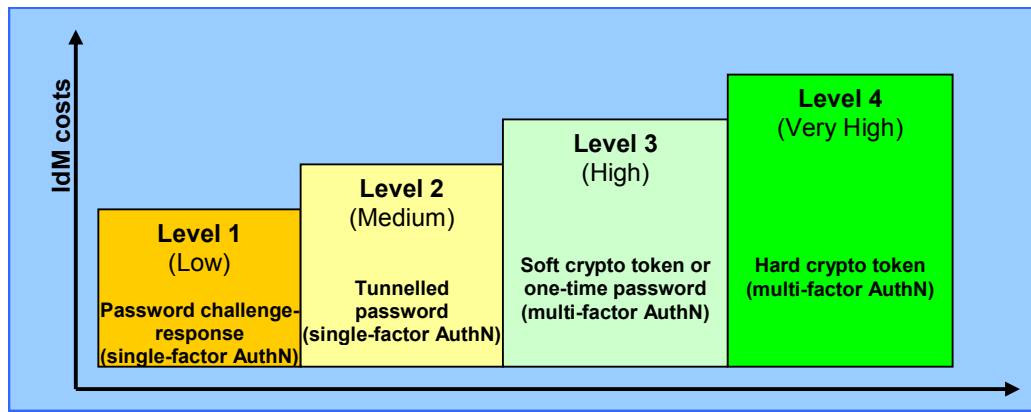


Figure 1. Distribution of LoAs vs. resource sensitivity/risk levels and IdM costs

In addition to the technical requirements on authentication token strengths and types, the NIST LoA specification also gives technical guidelines for achieving the four assurance levels in terms of user registration and identity proofing, credential management, authentication protocols, and assertion message validity periods. More details with regard to the OMB/NIST LoA model are given in [WP1-D].

Following the US government's e-authentication initiative that resulted in the OMB/NIST LoA specification, a number of organisations and federations worldwide have also made efforts in defining and using LoA to protect digital resources. These include the governments of Australia, Canada and EU, Higher Education (HE) federations of the US [inCommon], Australia and New Zealand [AAF], Switzerland [Switch], Finland [HAKA], Norway [Feide], Sweden [Swami], Denmark [DK-AAI] and France [CRU], the US National Institutes of Health [NIH], the US government's Electronic Authentication Federation [EAF] and industry-led Electronic Authentication Partnership [EAP], and the global body Liberty Alliance [LA]. However, all these efforts are related to the OMB/NIST model; they either adopt the OMB/NIST guidelines, or specify their LoA definitions based upon the OMB/NIST guidelines, or make their proposals compatible with the OMB/NIST guidelines. For example, the OMB/NIST specification has been implemented by the US government's E-Authentication Initiative [EAI] and the E-Authentication Federation [EAF] (a partnership between the US federal agencies and private sector organisations). The EAF has also struck an inter-federation interoperability partnership with the US InCommon HE federation [InCommon] and the US NIH (National Institutes of Health) [NIH], and have agreed on a common LoA vocabulary. The US HE federation InCommon has defined a set of two authentication profiles, called Bronze and Silver, which can directly be mapped onto NIST Levels 1 and 2.

3 Recommendations to JISC

Owing to the fact that the OMB/NIST LoA specification gives the most comprehensive set of guidelines for LoA definitions and applications in the context of electronic resource access, and that it is, by far, the most recognised LoA specification among international bodies and organisations, we translated the OMB/NIST LoA guidelines and technical requirements into a set of survey questions [WP3-D], and used the questions to consult with the UK academic and research community to investigate and examine the community's needs with regard to LoA definitions and applications. Some of the findings from this survey are very interesting (for more detailed discussions, please refer to our project deliverable [WP3-D]): almost all the service providers (93%) require some level of confidence in an asserted user's identity (i.e. NIST Level 2), while 46% claimed to have resources that would require a high or very high LoA (i.e. Level 3 or 4). On the identity providers' side, a vast majority (92%) employ username/password-based authentication method that can potentially achieve NIST Levels 1 and 2, 42% use soft certificate tokens with the maximum achievable LoA of Level 3 and 25% use hard certificate tokens capable of achieving NIST Level 4.

Based upon our findings from both research and community consultation, we are able to make the following recommendation:

Recommendation 1

Using the OMB/NIST 4-level approach as a starting point, and taking into account UK e-Government initiatives in this area, and in the light of the (surprisingly) wide consensus

uncovered by our survey, start drafting a set of LoA definitions/profiles that are appropriate to the UK academic and research community.

Survey results back-up the adoption of four assurance levels; some service providers have expressed the need for the highest LoA (i.e. Level 4), although for the majority of the respondents Levels 1, 2 and 3 would suffice.

There are a number of benefits for the UK academic and research community to adopt the OMB/NIST LoA model. Firstly, the model addresses direct user-to-system authentication, which is the most commonly seen use case scenarios in the UK HE federation. Secondly, the OMB/NIST guidelines cover most aspects of user-to-system authentication and risk-based access control, so it would be more cost-effective for JISC to adopt this model while addressing the gaps in applying it to the federated access management infrastructure used by the community. Thirdly, using the OMB/NIST LoA model would make it easier for the UK HE federation to interoperate with those federations that already use, or plan to use, the OMB/NIST LoA regime. Compatibility and interoperability with other federations are important for inter-federation partnerships and seamless sharing of federated resources across federation boundaries.

4 Gap Analysis

When applying the OMB/NIST LoA guidelines to a federated access management environment such as the Shibboleth infrastructure, we are able to identify a number of gaps which can be classified into the following areas: (1) LoA definitions, (2) policy aspects of enforcing the use of LoA in HE federations, and (3) actual implementation of LoA-based systems.

4.1 Gaps in LoA Definitions

Identity and attribute assertions are recognised by the NIST LoA specification, which is necessary to support third party based authentication. According to the NIST LoA definitions, third party based authentication can only achieve assurance Levels 1 through 3. Level 4 is only achievable by users directly authenticating themselves with the service provider managing the requested resources. In a federated Shibboleth infrastructure, a user is always directed to their home institution that serves as a third party identity provider (IdP). Upon successful authentication, the IdP will issue an attribute assertion to convey the user's identity information along with attributes to the service provider, which then makes an access control decision to allow or deny the user to access the requested resource. Thus, due to this restriction imposed by the NIST LoA specification, the Shibboleth federation can only achieve authentication assurance levels of 1, 2 and 3. However, as our survey has uncovered, a quarter of the surveyed service providers claim to have resources that would require the highest LoA (i.e. Level 4), so more research is needed to look into the procedures, policies and algorithms that are necessary in order to implement an authentication assurance level beyond 3 in the Shibboleth infrastructure. For example, the UK HE federation may want to consider defining a new LoA level, called Level 3* (i.e. a level between NIST Levels 3 and 4) with appropriate identity vetting, and attributes management and assertion procedures and policies to accommodate this LoA need.

Recommendation 2

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

There is also a perceived gap in applying the NIST LoA specification to e-science/grid environments, as it only caters for direct user-to-service authentication or authentication via a third party IdP, while delegation of (a subset of) access rights is outside the scope of the specification. Delegation via GSI proxy credentials is a basic mean of authentication in grids, and proxies can be used to create other subordinate proxies allowing for n -tier delegation and authentication. This process (the level of delegation), as well as the manner in which proxy certificates are stored (remote or locally) and managed (file systems or MyProxy servers), introduces certain consequences to the LoA value. These consequences and new issues need further study and investigation.

Recommendation 3

Investigate the consequences of applying an LoA model to grid scenarios and draft a set of LoA definitions for grid environments, addressing proxy credentialing and delegation.

4.2 Gaps in LoA Policies

According to the OMB/NIST LoA specification, the following steps should be performed in order to implement a LoA-linked fine-grained access control system.

Step 1: Risk assessment or classification of services/resources into different groups of sensitivity levels.

At this step, service providers perform a risk assessment of resources under their management and identify risks. For each of the identified risk categories, service providers estimate (1) the impact to its services should the risk be materialised, and (2) the likelihood of its occurrences. The OMB guidance gives a detailed recommendation with regard to how this process may be performed.

Step 2: Mapping risks/impact levels to authentication LoA

Once the risks are identified and their impacts and likelihoods are assessed, an appropriate level of assurance is selected to match the resource in question using the impact/likelihood profile. The OMB guidance has given a profile table for this purpose. However, the profile table only considers the potential impact of the risks as an underlying parameter for the mapping; it does not take into account the likelihood of the risks being materialised. We have proposed an improved profile for this purpose, in which each of the identified harm categories is evaluated along two axes – i.e. in terms of *impact* and *likelihood* of its occurrence (more details can be found in [WP1-D]).

Step 3: Select appropriate authentication technologies based upon the NIST guidance to achieve the level of assurance determined at Step 2.

The authentication model in the Shibboleth federated environment can be summarised using Figure 2 below. According to the NIST LoA specification, an authentication process encompasses the following procedures, all of which affect the LoA in an authentication instance:

- *Registration and Identity Vetting.* In this process, a user registers with a Registration Authority (RA) and proves his identity (e.g. by means of a photoID).
- *Credential Issuance.* In this process, a user is issued with an authentication credential/token.
- *Entity Authentication:* during this process, the user uses the authentication token to authenticate him/herself to an IdP.
- *Attribute Assertion.* If the authentication is not performed directly to the service provider (SP) but via a third-party IdP. Upon the user's successful authentication to the IdP, the IdP sends an assertion message to the SP to assert the user's identity and/or other attributes.

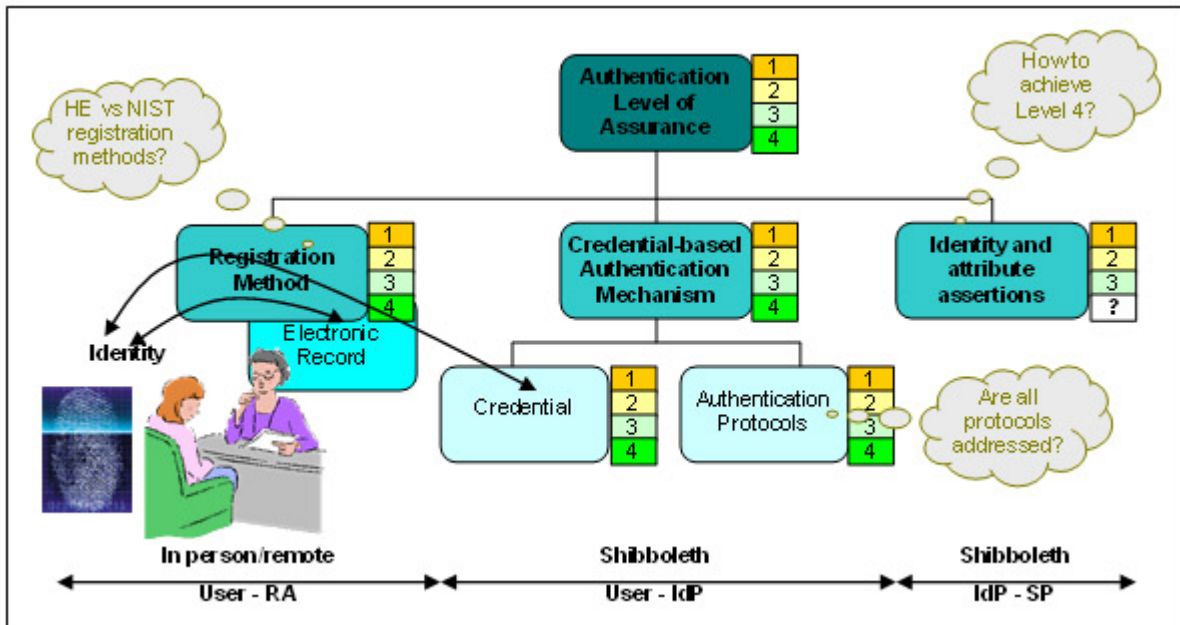


Figure 2. Factors affecting the LoA in a Shibboleth environment

Step 4: Validation and periodical assessment of the LoA implementation.

Validation and periodical assessment should be performed on an LoA compliant access control system by a specialist body to ascertain that the implemented authentication system indeed achieve the required LoA and the identity policies and procedures implemented at the IdP indeed compliant with the NIST specification. For example, an institution (Interoperability Lab [E-AuthLab] of the US federal E-Authentication Initiative [EAI]) has already been established in the US for this purpose.

The NIST specification is specifically designed for direct user-system interactions, and deploying it in a federated access management environment has left some open issues that need further research and investigation (particularly regarding *Step 3* and *Step 4* above). These include:

- Registration and identity vetting procedures in HE institutions differ from those specified by NIST; the latter were defined for federal agencies. For example, the NIST guidelines require the verification of a government-issued photoID document, which may prove to be difficult in the HE sector. Some modifications of the original NIST LoA guidelines may be necessary in this aspect.
- The NIST LoA specification does not cover all the authentication methods that are used by the UK HE institutions. More work is necessary to accommodate these authentication methods in the LoA regime.
- Currently there is no auto-negotiation mechanism involving the user (e.g. depending on what credentials the user has access to), the IdP (e.g. depending on the level of LoA it is accredited to), and the SP (e.g. depending on the access control policy of the resource being requested).
- An overwhelming majority (92%) of service providers we surveyed saw the need for medium to strong governance to give them confidence that third party IdPs are carrying out their roles effectively. Also, 77% of service providers believed that putting formal LoA policies and procedures into practice within a federation would make them more willing to pump their more valuable or sensitive resources into the federation. On the other hand, 83% of the IdPs said they would be willing to follow technical guidance on e-authentication so as to achieve the required level of authentication assurance. Thus, there is a need for a federation with appropriately defined LoA policies and procedures, and the means for enforcing them.

Recommendation 4

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

4.3 Gaps in LoA Implementation

As part of our survey on the use of LoA, we investigated the authentication systems currently in use. The survey revealed that all the respondent IdPs using username/password based authentication systems fail short of achieving even the lowest NIST LoA level, Level 1. Even among password-based authentication systems, a multitude of different practises are in place. Thus, policies and guidelines on passwords selections and management would be beneficial as well as measures to enforce the policies and guidelines. There should be more guidance provided to institutions on how to implement LoA-compliant systems, and bodies for validating and certifying compatibility with certain LoA Levels.

Recommendation 5

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

Attribute assertions in a Shibboleth infrastructure are typically implemented using the OASIS SAML standard [SAML]. SAML messages are exchanged between the endpoints – an IdP and a service provider, resulting in the delivery of an identity assertion containing the outcome of the authentication and additional attribute information about an authenticated end user. In SAML v2.0 (supported by the latest Shibboleth v2.0 release), an LoA value can be conveyed in one of the two ways: (1) as one of the attributes in a SAML assertion, or (2) as part of an Authentication Context. Authentication

Contexts are a new feature of SAMLv2.0 and can be used to present a service provider with detailed information about an authentication process performed by an IdP, such as the identity vetting process used to verify a user's identity, credential management and storage, authentication method, mechanisms used for protecting the credentials, credential renewal frequency, etc. These pieces of authentication contextual information can be used by service providers to calculate a level of authentication assurance themselves and put it into a risk-aware authorisation decision making process.

The implications of choosing one of the two methods mentioned above are as follows: conveying the LoA value as an attribute in an assertion is simpler, easier to implement and more cost-effective to operate, but the decision with regard to at which assurance level the user should be authenticated is left to the IdP (unless there is a policy at the federation level to govern this). Using Authentication Contexts, on the other hand, is slightly more complicated, but it gives the service provider more flexibility in using the information to achieve fine-grained access control. The international community is yet to agree on which method should be used for LoA conveyance. The UK HE federation should make a stand on this issue.

Recommendation 6

Engage in international and trans-sector discussions and investigate the issues of LoA value conveyance in federated environments.

In addition to the assurance level of a user's identity (i.e. credential LoA), assurance in user's other attributes (i.e. attribute LoA) appears to be as important according to the results of our survey. Attribute LoA is dependent on the ways by which the attributes are stored, managed, accessed, and conveyed between an IdP and a service provider.

Recommendation 7

Define specifications and vocabularies for describing assurance levels of attributes in federated access management environments.

The absence of any reference implementation was commented on by respondents of our survey. The project strongly recommends that the most effective way to widen understanding and to show the effectiveness and relevance of the LoA concept is to develop a demonstrator, covering a small number of differing use cases. The demonstrator would allow us to highlight issues related to the real-life deployment of LoA linked fine-grained access control.

Recommendation 8

Fund a pilot project to demonstrate the real-life implementation and application of LoA-based access control.

5 Conclusions

As more and more institutions and organizations may be interested in joining federated access management environments, and some of them (e.g. government agencies, financial and higher educational institutions, commercial organisations, health care providers, and third party data providers) may manage resources (including data, systems and services) with varying levels of sensitivities or experience varying levels of risks, the current 'grant or deny' approach to authentication and authorisation is no longer adequate. Therefore, we are looking forward to using an LoA-based fine-grained access control approach where resources with a higher sensitivity or risk level will be served by an authentication solution with a higher level of assurance. With this approach, a service provider may specify a minimum LoA depending upon the resource sensitivity or risk levels, and require that the access is granted only if the LoA derived from a user's authentication instance satisfies this minimum LoA.

Upon research and community consultation with the UK academic and research community, taking into account international development and efforts in the area, we are able to propose that the OMB/NIST LoA regime is the most comprehensive and appropriate one for the use by the community. However, there are a number of gaps when applying the existing OMB/NIST LoA guidelines to federated authentication and authorization environments, and more work is necessary to address

these gaps before we could realise the vision of LoA linked fine-grained access control within the UK HE community.

References

- [WP1-D] ES-LoA Project WP1 Deliverable, Using LoA to Achieve Risk-Based Access Control: A Study Report, <http://www.es-loa.org/images/stories/wp1-loastudyreport-v1.0.pdf>.
- [WP3-D] ES-LoA Project WP3 & WP4 Deliverables: "Full Questionnaire" – full community survey questionnaire targeting at a wide range of institutions, available at <http://www.es-loa.org/images/deliverables/wp3-fullquestionnaire-v2.0.pdf>; 'Part 1 - Suppliers' Survey on Levels of Authentication: Report on Brief Survey Findings', available at <http://www.es-loa.org/images/deliverables/wp3-part1-supplierssurveyreport-anonymous.pdf>; 'Part 2 - Service Providers, Identity Providers and Grid Community Survey on Levels of Assurance: Report on Full Survey Findings', available at <http://www.es-loa.org/images/deliverables/wp3-part2-identityandserviceproviderssurveyreport-anonymous.pdf>.
- [OMB-M0404] Office of Management and Budget (OMB), Memorandum M-04-04: E-Authentication Guidance for Federal Agencies, Dec. 2003, <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>.
- [NIST-SP800-63] National Institute for Standards and Technology, Special Publication 800-63: Electronic Authentication Guideline v1.0.2, April 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
- [EAI] US Government's E-Authentication Initiative, <http://www.cio.gov/eauthentication/>.
- [EAP] Electronic Authentication Partnership, <http://eap.projectliberty.org/>.
- [LA] The Liberty Alliance, <http://www.projectliberty.org>.
- [InCommon] US HE Federation, <http://www.incommonfederation.org/>.
- [Switch] Swiss HE Federation, http://www.switch.ch/edu/educ_orgs.html.
- [AAF] The Australian Access Federation, <http://www.aaf.edu.au/>.
- [HAKA] HAKA, Finnish HE Federation, <http://www.csc.fi/english/institutions/haka>.
- [Feide] Feide, Norwegian HE Federation, <http://rnd.feide.no/>.
- [DK-AAI] Danish HE federation, <http://www.dk-aa.dk/>.
- [SWAMI] SWAMI (Swedish Alliance for Middleware Infrastructure), Swedish HE Federation, <http://www.swami.se/>.
- [CRU] French HE Federation, <http://federation.cru.fr/cru/index-en.html>.
- [E-AuthLab] E-Authentication Interoperability Lab Concept of Operations, <http://www.cio.gov/eauthentication/documents/LabOPS.pdf>.
- [SAML] SAML V2.0 OASIS standard specification set, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20.
- [FAME-PERMISS] The FAME-PERMISS project, <http://www.fame-permiss.org>.