A Draft Version of the OGF LoA-RG Charter

- Inviting for comments

Written by Ning Zhang, ning.zhang@manchester.ac.uk and
David Groep (davidg@nikhef.nl)

1. Brief Group Summary

Robust authentication and authorisation services are keys to the deployment of a secure virtual organisational (VO) environment where students, researchers, staff with different roles and responsibilities from different institutions are expected to share resources distributed in the Internet environment with components administered locally and independently. Authentication is the first line of defence in any secure systems, and it is particularly important in VO environments playing a critical role in the provision of a number of essential security services including authorisation, access control, auditing and accounting.

There are various methods that can be used to achieve entity identification and authentication, and different methods provide different Levels of authentication Assurance (LoA), or quality of authentication. A LoA reflects the degree of confidence in identifying the entity to which the credential was issued, and the degree of confidence that the entity using the credential is indeed the entity that the credential was issued to. All the processes and steps associated to an authentication instance influence LoA. These include the processes of identity vetting and credential issuance, during which an entity is registered with a RA (Registration Authority) and is issued with a credential that binds the entity's identity to an authentication token issued by a CSP (Credential Service Provider) associated to the RA, the type of authentication tokens (e.g. a cryptographic key, a username/password pair, an IP address, or a proxy credential) used for proving the identity, how the tokens are stored (on a smart card, inside a web browser, or in an on-line repository), and the strength of the authentication protocols/methods used by the underlying authentication service. Furthermore, a LoA is also influenced by the manner in which a claimed identity is bound to an authentication credential, the life cycle management of the credential, whether the CSP has sufficient operating procedures, processes and policy frameworks to establish the required level of trust, and the extent to which an authentication event is coupled to an authorisation event.

As more and more diverse resources are being incorporated into the Internet-based VO environments, and as more and more institutions join to form various federations, service providers (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 sensitivity and experience different levels of risks. The current certificate-based "one-method-fits-all" authentication method is no longer adequate for the diverse VO environments. Ideally, resources with a higher sensitivity level and/or managed in an environment with a higher risk level are better served by an authentication solution with a higher level of assurance, and vice versa. With this risk-based authentication approach, an SP may specify a minimum LoA depending upon the resource sensitivity and/or risk levels, and require that the access is granted only if the LoA derived from an authentication instance satisfies the minimum LoA.

Earlier efforts in defining LoA were made by the UK/US governments in their e-Government Initiatives, and as a result, the US Government and NIST (US National Institute of Standard and Technology) produced a set of operational and technical guidelines on e-Authentication LoA in the context of e-Government Federation [M-04-04, NIST06] (hereafter referred to as the e-Authentication Federation). However, these guidelines are only applicable to the use case scenario where remote human users are authenticated to IT systems; it does not cover dimensions or factors as introduced by VO/Grid contexts.

This LoA Research Group (LoA-RG) is aimed at investigating use case scenarios in the e-Science/Grid contexts, and identifying gaps in applying existing LoA definitions to such contexts.

2. Group Focus & Scope

The focus of the LoA-RG is defined by the following two proposed documents:

Document 1:

Title	A risk analysis in relation to LoA and use case gathering in an e-Science context
Abstract	This document will present a risk analysis from the prospective of relying parties (or service providers). It will address such questions as: • What is it that relying parties really need to know about an identity assertion? • What qualities do they require? • Which attributes do they 'need to know' about an assertion provider in order to decide on trust in the assertion? The document will also gather specific use cases in relation to LoA in the context.
Document Type	Memo
Editors	Mike Helm

Document 2:

Title	A gap analysis of current LoA definitions versus LoA requirements in e-Science/Grid context
Abstract	This document will give an overview of current LoA definitions and the related efforts, and identify gaps between these definitions and the potential use of LoA in the e-Science/Grid context.
Document Type	Memo
Editors	Ning Zhang, Mike Jones, and Aleksandra Nenadic

The Scope of the Group:

Other standards bodies, such as NIST and ETSI, define LoA criteria and specific LoA reference standards, but do not concern themselves with the grid-specific use cases. In particular, the impact of indirect transmission of assertions (through services or delegation) is not dealt with there. This group will clarify the gaps that separate current LoA definitions and criteria from the grid use cases, and how to address these gaps. In detail,

• The LoA-RG tackles the issues related to defining the criteria for assurance assessment, the identification of gaps between the criteria defined by other standards bodies (in particular NIST, ETSI and EU standards) and the relevant grid use cases for (identity) assertions.

- The LoA-RG will NOT pursue the conveyance of LoA assertions in authentication protocols, or the technical consumption of such assertions by software. These topics are within the remit of the OGSA-AuthN-WG (proposed)

- The LoA-RG will NOT pursue the definition of identity levels and policies, or the implementation thereof. These topics are within the remit of the grid participants, their management, regulatory bodies and coordinating groups (CAOPS-WG, IGTF, inCommon, etc).

- The LoA-RG will NOT define any standards or recommendations under this charter.

3. Exit Strategy:

LoA-RG Deliverables: The two proposed documents will be submitted to the OGF.

Knowledge sharing: We will be helpful if asked to share our knowledge even after the research work is completed.

Appendix: The Seven Questions and Answers

1. Is the scope of the proposed group sufficiently focused?

Yes. The focus is defined by the two proposed documents of the research group:

1) "Overview of current LoA criteria and the relation to the risk analysis by relying parties in an e-Science context". Specific use cases will be gathered as part of this work.

What is it that relying parties really need to know about an identity assertion, what qualities do they require, and which attributes do they 'need to know' about an assertion provider in order to decide on trust in the assertion?

2)"gap analysis of reference definitions by current LoA standards and the requirements of grid and e-Science use cases for identity assertions".

Current LoA definitions are intended for direct validation by a service provider and are mostly based on planned government and defence uses and on client-server electronic transactions. This work will identify the gaps between these definitions and the potential use of LoA in the grid context.

2. Are the topics that the group plans to address clear and relevant for the Grid research, development, industrial, implementation, and/or application user community?

A review of related activities (although mainly in the e-Science domain) shows a significant interest in LoA. As more diverse resources get integrated in production grid infrastructures, LoA is seen as a way of providing qualified access to these resources.

This group will clarify the gaps that separate current LoA definitions and criteria from the grid use cases, and how to address these gaps.

3. Will the formation of the group foster (consensus–based) work that would not be done otherwise?

Although many groups and forums are used to discuss LoA issues, there is no single focal point for these discussions. This group can provide that focal point. There is currently no other proposal to do this focussed work elsewhere.

4. Do the group's activities overlap inappropriately with those of another OGF group or to a group active in another organization such as IETF or W3C?

Has the relationship, if any, to the Open Grid Services Architecture (OGSA) been determined?

The demarcation between the proposed LoA-RG and the relevant groups in OGF has been defined as such:

- The LoA-RG tackles the issues related to defining the criteria for assurance assessment, the identification of gaps between the criteria defined by other standards bodies (in particular NIST, ETSI and EU standards) and the relevant grid use cases for (identity) assertions.

- The LoA-RG will NOT pursue the conveyance of LoA assertions in authentication protocols, or the technical consumption of such assertions by software. These topics are within the remit of the OGSA-AuthN-WG (proposed)

- The LoA-RG will NOT pursue the definition of identity levels and policies, or the implementation thereof. These topics are within the remit of the grid participants, their management, regulatory bodies and coordinating groups (CAOPS-WG, IGTF, inCommon, etc).

- Other standards bodies, such as NIST and ETSI, define LoA criteria and specific LoA reference standards, but do not concern themselves with the grid-specific use cases. In particular, the impact of indirect transmission of assertions (through services or delegation) is not dealt with there.

Although the proposed LoA-RG will of course consider the OGSA use cases in the gap analysis, the work itself is orthogonal to the architecture. As the RG will not be involved in the transmission of assertions (that is deferred to the OGSA-AuthN-WG (proposed)), it does not conflict with the Architecture.

The RG will not define any standards or recommendations under this charter.

5. Are there sufficient interest and expertise in the group's topic, with at least several people willing to expend the effort that is likely to produce significant results over time?

The BoF session was attended by 18 people, all of whom have a known interest in this topic and are likely to contribute to group discussions and critically review documents. The spread of people over different background is such that appropriate

representation of the various interest groups is ensured (IGTF, TERENA, US Internet2, US Higher Education CA efforts, UK JISC, UKERNA).

Two documents have been proposed during the BoF session, and for both documents the editors and contributors have been identified.

6. Does a base of interested consumers (e.g., application developers, Grid system implementers, industry partners, end-users) appear to exist for the planned work?

The evaluation of LoA criteria is timely, and many groups such as the IGTF, and the OGSA-AuthN-WG is waiting on the results of this RG before starting work on the protocols to convey LoA. The UK JISC has funded a project to study the LoA definitions and applications, and to reach community consensus on the use of LoA in the Shibboleth infrastructure.

The use of LoA is becoming increasingly more important as diverse resources are integrated into production infrastructures. Non-OGF workshops in the e-Science domain, such as those organised by TERENA and I2, have a strong focus on LoA and will consume the analysis of the LoA-RG (proposed). Other LoA consumers include UK JISC (the UK Joint Information Systems Committee) community, a body supporting UK higher education and research, UK NGS, UKERNA, GridSite, and some UK biomedical research communities.

7. Does the OGF have a reasonable role to play in the determination of the technology?

The use of indirect and transitive assertions is unique to the grid use cases, and has not and will not be dealt with by other bodies. The use of LoA in other e-Science use cases is being addressed also in the educational federations supported by, e.g., Internet2, GEANT2 and TERENA, but today falls short of addressing these more grid-like cases. It is will within the OGF scope to address these specific issues.