

E-Infrastructure Security:

An Investigation of Authentication Levels of Assurance (LoAs)

Prepared for OGF19 – the LoA BOF session;

Written by Ning Zhang, the University of Manchester, Manchester, UK, nzhang@cs.man.ac.uk;

Had inputs from Blair Dillaway (blaird@microsoft.com) and David Groep (davidg@nikhef.nl)

About This Document

This document outlines existing efforts on the definition of authentication Level of Assurance (LoA) guidelines and identifies gaps in applying these existing LoA guidelines to the Grid/VO context. It highlights the need for an international WG to agree on a consistent set of LoAs that are suited to a number of related federations, e.g. Grid, e-Science, InCommon (Higher Education sector), and e-Governments federations.

Copyright Notice

Copyright © Open Grid Forum (2007). All Rights Reserved.

LoA BOF Session Focus/Purpose:

Authentication Levels of Assurance (LoA) has been receiving more and more attention, with the advance of federations and authentication and authorization infrastructures.

Authentication LoA is defined as the degree of confidence in identifying an entity (an individual, a software component, or a host) to whom the credential was issued, and the degree of confidence that the entity using the credential is indeed the entity that the credential was issued to.

As more diverse resources are being incorporated into the Grid fabric, service providers (or relying parties) may require an assurance level in identifying an entity in an authentication process before an access control decision is made. For resources (data and/or services) with varying levels of sensitivity, the relying parties may specify a minimum level of authentication assurance, LoA, and require that the access is only granted should the LoA derived in an authentication instance satisfies the minimum LoA.

It is understood that the UK Government, the US Government, and NIST (US National Institute of Standard and Technology) have 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). The InCommon Federation (its mission is to support the US HE institutions in the use of their on-line credentials to manage access to external resources) and UK JISC (Joint Information Systems Committee, in support of the UK HE institutions in the use of their on-line credentials to manage access to external resources) are developing services that allow the use of LoA requirements in resource access control. It is also worth noting that the InCommon Federation is working on mapping their LoAs onto the NIST LoA guidelines, i.e. the InCommon Federation is establishing partnership with the e-Authentication Federation.

There is a significant overlap between Grid users and the users in the InCommon and e-Authentication Federations. In other words, future interoperation and trust mitigation among these

communities/federations, namely, Grid, e-Science, InCommon and e-Authentication will be inevitable. Therefore, there is a need for the Grid community to jump on the wagon to work with these communities/federations to define and/or to agree on a consistent set of LoAs that are acceptable by, and can be used consistently among, all these communities/federations.

The primary objectives of this BoF session are (1) to identify gaps in applying the NIST definition to the context of Grid/VO (hereafter referred as the Grid context), and (2) to seek consensus on how to bridge such gaps. It is anticipated that this BoF session serves as a call for an OGF WG to work on appropriate guidelines on the definition/derivation and application of LoA in securing Grid and VO resources.

Views/insights on the following questions will be sought:

- What are the existing definitions of LoA?
- Are the existing definitions suited to Grid or VO environment?
- How to apply LoA to safeguard Grid services/resources?
- Are some onerous registration requirements or special condition stipulations due to perceived inadequacies in the strength of authentication?
- Are there any limitations in terms of user accessibility, scalability and interoperability?

Session Agenda:

- The existing definitions of LoA; the major work done so far is the NIST LoA definition [NIST06].
- The gaps in applying the existing LoA definitions to the Grid/VO context.
- A proposal for LoA profile templates/guidelines for Grid/VO environments.

Session Output:

The primary output of this BoF will be a Memo that shall be a revised version of this Document containing comments, remarks, and consensus reached on the issues raised in this Document.

Document name	First draft available for comments	Revised version
Defining Authentication Levels of Assurance (LoA) in the Grid Context	December 2006	April 2007

Contents

OGF19 LoA BOF Session Description.....	Error! Bookmark not defined.
1 References for Newcomers	4
2 Preliminaries	6
2.1 What is an Authentication LoA.....	6
2.2 Factors Affecting LoAs in the Grid Context.....	6
3 Existing LoA Guidelines	7
3.1 OMB LoA Guideline	7
3.2 NIST LoA Guideline.....	8
3.3 IGTF Efforts	10
3.4 InCommon Efforts	10
4 Observations and Remarks in Using Existing LoA Guidelines in the Grid Context	10
5 Where We Go From Here	12
6 Acknowledgements	13

1 References for Newcomers

The following lists document/work in relation to the definition and application of authentication LoAs.

Authentication LoA Related References:

- [eGov] e-Government Authentication Framework, Version 2, Sept 2002, available at http://www.cabinetoffice.gov.uk/csia/documents/pdf/Assurance_V2_Sept_2002.pdf. This was the first such effort in defining and applying authentication LoAs, and was made by the UK government. It specifies Registration and Authentication e-Government Strategy Framework Policy and Guidelines.
- [FAME] <http://www.fame-permis.org/index.html>; a project sponsored by the UK JISC (Joint Information Systems Committee) funding body. It develops middleware extensions in the Shibboleth infrastructure to support authentication LoAs linked fine-grained access control.
- [Groep] The Grid – Virtual organisations and their support via federation; presented by David Groep at EuroCAMP 2006; slides available at <http://www.terena.org/activities/eurocamp/october06/day2/groep-Grid-Federation-Eurocamp-20061018.ppt>. This talk emphasised the need for having more than one levels of LoA in the Grid/VO context. The slides also describe Grid authentication and authorisation use case scenarios.
- [Kling] LOA Mapping, presented by **Ken Klingenstein** at EuroCAMP 2006; slides available at <http://www.terena.org/activities/eurocamp/october06/day1/klingenstein-panel2-loa.ppt#257.2.LOA>. Briefly mentioned authentication LoAs.
- [IGTF-1] Profile for Traditional X.509 Public key Certification Authorities with Secured infrastructure, version 4; available at <http://eugridpma.org/guidelines/IGTF-AP-classic-20050930-4-0.doc>. This authentication profile of the International Grid Trust Federation describes the comprehensive security requirements on traditional X.509 PKI CA services (i.e. with regard to the issuance of CRLs, and issuance and revocation of long-term PKI credentials to end entities). The profile covers the aspects of identity vetting rules, operational requirements, site security, publication and repository responsibilities, and audits.
- [IGTF-2] Profile for Short Lived Credential Services X.509 Public key Certification Authorities with Secured infrastructure, version 1; available at <http://www.tagpma.org/files/IGTF-AP-SLCS.doc>. This authentication profile of the International Grid Trust Federation describes the minimum requirements on a Short Lived Credential Service (SLCS) X.509 PKI CAs.
- [InCom-1] <http://www.educause.edu/ir/library/powerpoint/EDU06288.pps#257>; this talk describes the InCommon federation's vision of integration of multiple trust fabrics, including federal government and HE based InCommon federations, and proposes to map the InCommon LoA levels to NIST LoA levels.
- [InCom-2] http://209.85.135.104/search?q=cache:n8lrq8OI2ikJ:www.incommonfederation.org/docs/E-Auth/InCommon_GSA_EAF_RFI_Submittal.pdf+incommon,+Bronze,+Silver&hl=en&gl

=uk&ct=clnk&cd=5; this document gives the justification for the InCommon Federation Partnership with the E-Authentication Federation. An implication of this, i.e. the integration of these two Federations, is the need for LoA definition integration. Do we (i.e. the Grid community) want to be left out?

- [M-04-04] e-Authentication Guidelines for Federal Agencies, available at: <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>. The guidelines are built upon the guidelines specified by the UK government [eGov], and are produced as the result of the US government's e-Authentication Initiative. The document defines a framework for determining the levels of authentication assurance needed for e-Government transactions.
- [NIST06] Electronic Authentication Guideline, NIST Special Publication 800-63, Version 1.0.2, April 2006; available at http://72.14.209.104/search?q=cache:nDcR4B5YKugJ:csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf+NIST+800-63&hl=en&gl=uk&ct=clnk&cd=1. This NIST guideline is supplementary to the guidelines defined in [M-04-04]. It provides technical authentication requirements for the four levels of LoA defined in [M-04-04].
- [SLCS] The talk slides by Tony J. Genovese, from Lawrence Berkeley National Laboratory; it describes the SLCS profile; available at www.es.net/pub/esnet-doc/Short-Lived-Credential-Service.pdf.

Other Related References:

- [GFD-I.12] Security Implications of Typical Grid Computing Usage Scenarios, by Marty Humphrey and Mary R. Thompson, published in the Journal of Cluster Computing, Volume 5, Number 3, July, 2002, Springer Netherlands, ISSN: 1386-7857 (Print) 1573-7543 (Online), pp. 257-264.
- [OGSA23] OGSA Security Profile 1.0 - Secure Channel: https://forge.gridforum.org/sf/docman/do/downloadDocument/projects.ogsa-wg/docman.root.working_drafts.security_profile_1_0/doc13560/23.
- [OGSA-hpc] OGSA HPC cluster usecase for reference Model v.02, by Hiro Kishimoto Oct. 22, 2006.
- [SAMLv2] OASIS SAMLv2, available at <http://www.oasis-open.org/specs/index.php#samlv2.0>. SAMLv2 supports the passing of some of the attributes determining authentication LoA.

2 Preliminaries

2.1 What is an Authentication LoA?

Authentication is a process of confirming an entity's identity. An authentication level of assurance (LoA) is defined as the strength of authentication required for a relying party to be assured that an entity is indeed the claimed entity. It reflects the degree of confidence in an authentication process that an identifier refers to a claimed entity (an individual, a software component, or a hardware device) which the credential was issued to, and the degree of confidence that the entity using the credential is indeed the entity that the credential was issued to [M-04-04].

2.2 Factors Affecting LoAs in the Grid Context

An authentication LoA is affected by all the steps of an authentication process, namely, identity proofing, credential issuance, remote authentication using the credentials, which, in turn, includes the types/strengths of authentication credentials and protocols and how/where the authentication credentials are stored, record keeping and auditing. In the Grid/VO context, the effecting factors also include authentication depth (note: the weakest link principle applies here - the step providing the lowest assurance level may compromise the others), credential delegation, the use of on-line credential repositories, and validity durations of assertion messages.

- A. Identity proofing: the processes of registering one's identity with a RA (Registration Authority), and obtaining a credential which binds the identity to an authentication token issued by a CSP (Credential Service Provider) associated to the RA.
- B. Types/strengths of authentication tokens (e.g. a cryptographic key and the minimum key length, a password, or a proxy credential) for proving the identity, and their storage devices (hardware token, software token, or credentials stored in an on-line repository).
- C. Authentication protocols or methods used by the underlying authentication services and their strengths.
- D. An assertion mechanism used to communicate the result of a remote authentication performed by an IdP (Identity Provider), or a verifier, to a relying party, and validity durations of assertion messages.
- E. The life cycle management of the credentials:
 - The manner in which a claimed identity is bound to an authentication credential, and record keeping and auditing of such bindings.
 - Whether the CSP has sufficient operating procedures, processes and policy frameworks to establish the required level of trust. In other words, the CSP's issuance and maintenance policy should also be assessed to make sure that it conforms to the required level of authentication assurance [page 13, M-04-04].
- F. The extent to which an authentication event is coupled to an authorisation event.

Most of the A-F above have been addressed in [M-04-04] or [NIST06] except for those Grid context related factors. In other words, there aren't any (consistent) guidelines or agreement on authentication LoAs versus the factors specific to the Grid/VO context, e.g. authentication depth, delegated credentials, assertion message validity periods, and the use of on-line credential repositories. In addition, there does not seem to be any standards on LoAs versus the process and manner by which the assertion messages are generated and transported, and on how LoA effecting factors/attributes are conveyed to relying parties in a trusted manner.

3 Existing LoA Guidelines

3.1 OMB LoA Guidance [M-04-04]

This guidance document provides US Federal government agencies with the criteria for determining authentication LoAs required to identify citizens when they access on-line services provided by the agencies. Four levels of authentication assurance, 1 to 4, are defined in terms of the consequences of the authentication errors and misuse of credentials with respect to defined potential impact categories. In other words, authentication errors with potentially worse consequences require a higher value of LoA. The four assurance levels are defined as follows [M-04-04]:

- **Level 1:** Little or no confidence in the asserted identity's validity.
- **Level 2:** Some confidence in the asserted identity's validity.
- **Level 3:** High confidence in the asserted identity's validity.
- **Level 4:** Very high confidence in the asserted identity's validity.

Table 3.1: Maximum potential impact profile mapped to assurance levels [M-04-04]

Potential impact categories for authentication errors	Level 1	Level 2	Level 3	Level 4
Inconvenience, distress, or damage to reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorised release of sensitive information	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low	Mod	High

The guidance recommends the following steps in managing e-authentication:

- Conduct a risk assessment of an e-authentication system in terms of potential impacts and likelihood of the impacts.
- Map identified risks to the applicable assurance levels using the Profile.
- Select technology based on NIST Technical E-authentication Guidance [NIST06].
- Validate that the implemented system has achieved the required LoA.
- Periodically reassess the system to determine technology refresh requirements.

The focus here is on the access of e-government information systems/services, and on risks associated with each of the information systems.

The **scope** of the definition:

- The guidance only applies to remote authentication of human users of IT systems; it does not apply to the authentication of servers, or other machines or networked components.
- The guidance does not address issues associated to agency use of authentication credentials as

electronic signatures as in the case of cross-domain authentication or attribute assertions.

- LoA definition is given based upon the assessment of risks associated with each step of a user-to-system e-authentication process, including identity proofing, credentialing, technical and administrative management, record keeping, and the use of the credential. It has not taken into consideration of the risks or scenarios as seen in Grid/VO environment.
- LoA values are not fed into the authorisation decision process.
- The guideline does not identify technologies that should be used by agencies to implement the given levels of authentication assurance, and this issue has been addressed by the NIST guideline [NIST06]. In other words, the two pieces of work presented in 3.1 and 3.2 in this Document are complementary.

3.2. NIST LoA Guideline [NIST06]

The NIST Guideline, NIST SP800-63 [NIST06], is supplementary to the guideline defined in [M-04-04]. NIST SP800-63 provides technical authentication requirements for authentication LoAs defined in [M-04-04].

The LoA definition (from technical aspects) is comprehensive, and here gives a summary:

- A. Identity proofing: the process of registering one’s identity with a RA, and obtaining a credential which binds the identity to a token from a CSP associated with the RA.
- Level 1:** names are not verified; names are always assumed to be pseudonyms;
- Level 2:** credentials and assertions must specify whether the name is a verified name or a pseudonym;
- Levels 3 and 4:** names must be verified.
- B. Type of tokens for authenticating a claimant’s identity: the NIST guidance recognises four kinds of tokens: hard token (a hardware device that contains a protected cryptographic key), soft token (a cryptographic key that is typically stored on disk or some other media), one-time password (OTP) device token (a personal hardware device that generates OTPs for use in authentication) and password token (a secret memorised by a claimant for authentication).

Table 3.2: Token types allowed at each authentication LoA [NIST06]

Token types	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password (OTP) device	√	√	√	
Soft crypto token activated by a password or biometric (two factor authentication is required)	√	√	√	
Signed assertion with an expiry duration of 2 hours ¹	√	√	√	
Signed assertion with an expiry duration of 12 hours	√	√		
Passwords & PINs	√	√		

¹ This is particular important in an environment where the separation of AuthN and AuthZ are allowed.

Table 3.3: Required protections [NIST06]

Protection against	Level 1	Level 2	Level 3	Level 4
On-line guessing	√	√	√	√
Reply	√	√	√	√
Eavesdropper		√	√	√
Verifier impersonation			√	√
Man-in-the-middle attack			√	√
Session hijacking				√

Table 3.4: Authentication protocol types [NIST06]

Protection against	Level 1	Level 2	Level 3	Level 4
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
Tunnelled or Zero knowledge password	√	√		
Challenge-response password	√			

Table 3.5: Additional required properties [NIST06]

Protection against	Level 1	Level 2	Level 3	Level 4
Shared secrets not revealed to third parties by verifiers or CSPs		√	√	√
Multi-factor authentication			√	√
Sensitive data transfer authenticated				√

- C. Authentication protocols or methods used by the underlying authentication service; **see Table 3.4.**
- D. Assertion mechanisms (e.g. SAML assertions, cookies) used to communicate the results of a remote authentication to a relying party by a verifier. A relying party trusts an assertion based on the source, the time of creation, and attributes associated with the claimant. – **see Table 3.2.**
- E. How credentials are managed; - **also defined in [NIST06].**

The **scope** of the definition:

- The guideline only addresses traditional widely implemented methods for e-authentication based on secrets. It does not cover knowledge based authentication, and the use of biometrics is only considered in the process of registration and for unlocking keys.
- It does not address machine-to-machine authentication; it does not address credential delegation, n-tier authentication, or the use of on-line credential repository.
- It does not address the requirements for authentication credential/token issuance to machines or servers.
- It only addresses identity authentication; it does not address attributes, authorisation, or access control.

3.3. IGTF Efforts

As part of its work on Grid authentication, the **IGTF** (International Grid Trust Federation) WG has produced a list of authentication profiles and come out with two LoAs, Classic and SLCS (Short Lived Credential) services. The Classic X.509 profile is maintained by EUGridPMA [IGTF-1], whereas the SLCS profile is maintained by TAGPMA [IGTF-2, SLCS].

IGTF-Classic:

- This is an authentication profile describing the minimum requirements on traditional X.509 PKI CAs with regard to the issuance of CRLs, and issuance and revocation of long-term PKI credentials to end entities. The profile covers the aspects of identity vetting rules, operational requirements, site security, publication and repository responsibilities, and audits.

IGTF-SLCS:

- A SLCS mainly caters for credential/ID translation - a user's Grid DN in a short-lived certificate is translated from (linked to) one and only one local site ID.
- In SLCS, the task of the user's local site ID verification is delegated to his/her local authentication service - possible local site service candidates: Kerberos, Windows Domain, LDAP user Account DB, One Time Password and long-term certificate based credentials.
- A SLCS does not apply to Grid host or service identities. These identities types require a long term certificate identity.
- The use of MyProxy credential stores is to be addressed in future profiles.

The IGTF profiles mainly focus on the operational aspects of CAs (traditional CAs and short-lived credential services). In the IGTF approach, LoAs are classified into two groups in terms of long-term (classical) and short-term credentials. Other LoA related parameters, such as the consequence of authentication errors, authentication token types/strengths and authentication protocols/services used by the end entities, and assertion validity periods are not considered as parameters in the LoA classification.

3.4. InCommon Efforts [InCommon-1/2]

Recently, the InCommon federation has proposed the idea of inter-federation with the U.S. Government's e-Authentication Federation. The idea is to map InCommon LoAs to federal levels of assurance, 1 and 2, i.e. InCommon Bronze = NIST Level 1, and InCommon Silver = NIST Level 2.

4 Observations and Remarks in Using Existing LoA Guidelines in the Grid Context

Observation 4.1: The NIST LoA definition is specified in the context of federal IT client-server systems. In a Grid context, this definition may work if we assume that every user registers respectively with every relying party, and if credential delegation is not allowed (or proxy credentials are not used).

Observation 4.2: In the Passport (authentication) and Visa (authorisation) model described by [Groep], the use of LoAs in authorisation decision making is more important, as access control decisions should be linked to the confidence level in identifying a user.

Observation 4.3: In Grid community, relying parties are persuaded to 'trust' the AuthN assertions sent by IdPs. There is no clear guideline on the procedures and issues determining the LoAs of assertion messages.

Observation 4.4: There is a lack of synergy between the two sets of LoA definitions; the NIST definition that is defined for e-government context vs the IGFT definition that is defined for the Grid community. However, can we really separate the two communities? For example, the NIST definition resembles HE (Higher Education) scenarios more than IGTF definition. Do we expect the interoperation and integration of different trust fabrics, (e.g. HE, e-Research, e-Government, and Grid applications)? If so (certainly in UK, there is a trend towards national federation – the integration of Shibboleth based HE, and PKI based e-science and Grid fabrics), then we need a consistent or unified set of LoAs, which is suited for both communities. It is worth emphasising here that the InCommon federation has already started the process of becoming partnership with the e-Authentication Federation that uses the NIST LoA definition. Do we (the Grid community) want to be left out?

Questions for discussion:

Question 1: Should we impose a limitation on the lifetime of passwords for LoA Level 2?

Observation 4.6: the NIST Level 2 requires that on-line guessing attacks are prevented, which implies that the lifetime of a password should be restricted. Have we got any guideline on this? Should we impose a limitation on the lifetime of passwords for LoA Level 2?

Question 2: Is the NIST guideline suited to current Grid security infrastructure that is characterised by global authentication trust fabric, the separation of authentication (performed by an IdP) and authorisation (performed by an replying party that is typically different from the IdP), and the use of assertions?

Observation 4.7: The NIST definition states [page 29, NIST06] “In general, at assurance Levels 2, 3, and 4, independent verifiers must not be given long-term shared secrets by CSPs”. This requirement may create uncertainty if password (or symmetric key) based authentication methods are used and if the verifying party and the CSP are not the same entity.

Observation 4.8: The NIST guideline states [pages 33 and 36, NIST06] “**For level 2**, assertions generated by a verifier shall expire after 12 hours and should not be accepted by thereafter by the relying party”, and “**For level 3**, assertions generated by a verifier shall expire after 2 hours and should not be accepted by thereafter by the relying party”. Can we, i.e. the Grid Community, take this assertion validity requirement? If the answer is ‘No’, then are we happy to only have a LoA value of Level 1?

Observation 4.9: At Level 3 and over, the NIST guideline requires (1) multi-factor authentication (although a soft token locked by a password is of this category, but in the case of myProxy where a PKI credential is stored in a central repository and the access to credential is activated with a password, this category could not be classified as a two-factor authentication according to the principle of the weakest link); (2) the system should be resistant to *verifier impersonation* and *man-in-the-middle attacks* (this goes against the use of any third party verifiers, e.g. the case where IdP and relying parties are played by separate entities). In other words, these Grid security practices have effectively ruled out NIST LoA Levels 3 and 4.

Question 3: What is the LoA value when credential delegation is used, i.e. programs and services acting on your behalf through the use of proxy credentials?

Observation 4.10: The NIST definition does not address the delegation scenario, which is an integral part of the Grid architecture! Or in other words, based upon the NIST definition, a proxy

credential is only good enough to achieve NIST Level 1, at most. A proxy credential is usually valid for 12 hours [GFD-I.12].

5. Where We Go From Here

More questions:

- (1) Do we (the Grid community) need a set of LoAs for fine-grained access control?
- (2) If yes to (1), should the Grid LoAs be consistent (or unified) with the NIST definition which has already been used by the e-Authentication and InCommon federations?
- (3) If yes to (2), then more work is required to plug the gaps, to unify Grid LoAs with NIST LoAs, or to map Grid LoAs to NIST ones.

In addition, the following table summarises the factors expected to affect LoAs in the Grid context (this list may not be complete – it needs your contribution!), and further highlights the gaps between what has currently been defined and what has not been defined.

Grid/VO Authentication LoA Definition Template and Gaps:

LoA Profile Matrix	Existing definitions/guidelines
Identity vetting procedures	Defined in [NIST06] and by IGTF; more work is required to ensure the two LoA Profiles are consistent.
CAs operational procedures	Defined by both NIST and IGTF; more work is needed to ensure LoA Profile consistency.
Authentication token types/strengths	Defined in [NIST06]; see Table 3.2. But some Grid specific tokens should be considered and included too. In addition, should we also consider the implications of cryptographic token strength (e.g. key sizes, algorithms, password entropy)? Should we specify guidelines on minimum key sizes, password strength and validity duration, etc?
Authentication token storage devices: software tokens, hardware tokens, MyProxy (a credential store)	Mostly defined in [NIST06], except for remote on-line credential repository (MyProxy).
Authentication protocol types	Defined in [NIST06]; see Table 3.4.
Inter-domain authentication assertions: Cookies and SAML assertions	Briefly mentioned in [NIST06]; Consultation is required in Grid community in terms of management, type and storage of credentials used in generating assertions and assertion validity periods versus LoA. The current assertion validity periods define by NIST for levels 2 and 3 can not satisfy what is required by a Grid job – “Each job last several seconds to several days” [OGSA-hpc].
Use of proxy credentials, and n-tier authentication	In the NIST definition, the delegation of credentials is prohibited [page 30, NIST06]; IGTF SLCS covers short-lived certificate

	<p>certification and issuance issues; more work is required on the derivation of LoA when n-tier authentication is involved, and on the unification of NIST and IGTF profiles.</p> <p>Additionally, when using delegation credentials, would the LoA be different wrt: 1) establishing the entity using entity's identity; and 2) authenticating the entity based on the delegation credential.</p>
On-line credential repository stored long-term credentials	Not addressed so far; what is the LoA value when locked using different authentication schemes?
Credential translation service?	IGTF-SLCS [SLCS] covers this allowing the translation of a local site's native ID to a Grid ID. More work is needed in terms of consistency with the NIST definition.
Credential revocation and CRL issuance procedures	<p>At NIST Level 1, there are no stipulations about the revocation or lifetime of credentials.</p> <p>At NIST Level 2, credential revocation facility is required – “CSPs shall revoke credentials and tokens within 72 hours after being notified that a credential is no longer valid”.</p> <p>At NIST Levels 3 and 4, “revocation must be done within 24 hours”.</p> <p>At the IGTF-Classic Level, “The CA must react as soon as possible, but within one working day, to any revocation request received”.</p> <p>At the IGTF-SLCS Level, the revocation of short lived certificates is may not be necessary.</p>
Algorithm for calculating aggregated LoA when more than one issues mentioned above co-exist.	No standard method or guideline available; and more work is required. For example, in the scenario where a claimant authenticates to a verifier using a Level-3 token, and the verifier sends a signed SAML assertion (with validity period of 24 hours to a relying party – then which LoA value should we grant? (according to NIST guideline, we can only grant Level 1)
Standard methods for passing LoA attribute values from an IdP to RPs in a trustworthy manner	When relying on multi-stage processes to obtain the credentials needed to access a particular resource. In such cases RPs may want to understand the chain of authentications and credentials used so they can perform 'weakest-link' analysis. Have we defined any standards for how to pass such information in a trustworthy manner?
Audit and separation of duties	Audit is a requirement for both Classic and SLDS services.
The application of LoAs to safeguard Grid resources?	
Any other factors?	

We welcome your views, comments and insights on these questions:	Are some onerous registration requirements or special condition stipulations due to perceived inadequacies in the strength of authentication? Are there any limitations in terms of user accessibility, scalability and interoperability?
--	--

6. Acknowledgements

We would like to gratefully acknowledge the funding support by UK Joint Information Systems Committee.

Some useful correspondence

-----Original Message-----

From: philopro@gmail.com [mailto:philopro@gmail.com] **On Behalf Of** Jessica Bibbee

Sent: 04 January 2007 23:05

To: mace-dir@internet2.edu

Cc: Caskey, Paul; Steve Olshansky; Keith Hazelton; Soldi, Miguel; Nate Klingenstein; RL 'Bob 'Morgan; Jim Lowe; Brendan Bellina

Subject: Re: [3] LOA - proposed call times

Level of Assurance Discussion

December 15, 2006

Attendees

Keith Hazelton, U. Wisconsin-Madison

Jim Lowe, U. Wisconsin-Madison

Miguel Soldi, U.T. System, Austin

Paul Caskey, U.T. System, Austin

Brendan Bellina, USC

R.L. "Bob" Morgan, U. Washington

Nate Klingenstein, Internet2

Steve Olshansky, Internet2

[Jessica Bibbee, Internet2 (scribe)]

Agenda – Questions surrounding LoA space

1. What problem(s) are you trying to solve?
2. What's your general plan (high-level sketch)?
3. What's your next milestone?
4. What might we do to help each other work through LOA issues?
5. What changes in middleware layer anticipated?
6. What changes in business process anticipated?

Discussion

The purpose of today's call is to discuss current ideas and practice regarding level of assurance on campus, with the intent of stimulating discussion among others to contribute back to best practices and additional work that will help this work move forward. In addition to these notes, please see Keith's summary appended below[0].

{Jim} shared the current situation from the perspective of U. Wisconsin-Madison, which is dealing with state-wide pressures to increase security. In particular, they are looking at level of assurance for restricted information. A couple of the issues center around 1) moving away from internal identifiers used at universities across Wisconsin and moving towards campus credentials, and 2) ensuring that some level of assurance and identity proofing is done on the more than 13 different identity stores around the state. They would like to follow suit as InCommon has done with a CAFing process (Credential Authentication

Framework), such that campuses can self-audit and be assured that they have answered questions and know where their credential stores are at.

One driver is to move the financial system to a shared system, instead of the current credential systems in which credentials are assigned and stored in the application itself. See the draft LoA document that {Jim} has floated to the list.

Another example of restricted data refers to notification/identification, PHI data, HIPAA Law, while the focus for the near future will be on the latter and Wisconsin state law. {Jim} stressed the importance of requiring a higher level of assurance if you are accessing, not your own but, another's SSN, for example. Perhaps a hardware token would be required, as stated in {Jim's} document. A general assurance around login ID and password, but a higher level of assurance if accessing others' PHI information. Beginning with the roll out (next year?), these few people will be required to have meet two- factor authentication (T-FA).

{Paul} stated that the benefits application will not require level 3, but level 2, down the road. He also mentioned that there is an immediate need for the GRID folks – with much debate around whether everything in GRID space would require T-FA or just that which satisfies the campus.

Another resource is the InCommon Credential Assessment Profile; see "InCommon Bronze/Silver Draft" at: <http://www.incommonfederation.org/docs/drafts/> (cf. Keith's email, 3-Jan).

{Bob} explained how U. Washington has used T-FA for access to administrative mainframe, but at one point, was decided incapable of supporting encrypted connections. All applications using a username/password and doing secureID were migrated to the web. These have been decided at a per-web-application basis, but the question now points to when it should be required. There is no need to expand from 4K users to more than 20K, without any sort of risk analysis. However, there is a situation moving in the opposite direction, where expansion of identity holders is desired. LoA is particularly important when dealing internally to the enterprise, but the same concern may not exist when dealing with applications relevant to e.g., alumni only.

{Miguel} pointed out that another area not being adequately addressed is awareness of the Identity Management lifecycle. A person enters an institution as a Student, but the affiliation may evolve to Staff and later Faculty. This leaves much room for revision and reassessment as the application changes, but these needs are not being met. Another example is the person who, as an applicant, has a low level of assurance, but once they are on campus, they move directly to a need for a higher level of assurance. At a base level, there are implicit levels of assurance depending on the affiliation.

{Bob} reminded the group of the impressive work lead by Mike Conlon at U. Florida. He compiled an analysis entailing their system of multiple password policies and how they required a level of assurance for their applications, complete with population set requirements. You can view his presentation (3-June-05) at <http://www.educause.edu/ir/library/powerpoint/CMR0555.pps>.

At U.T. System, one motivator may end up being shared services, as centralized applications are not standard there. So, then the question is which applications and who would benefit from these shared

services or federations to leverage what is being done. The Grid is one such example.

{Bob} shared another tool, the Electronic Risks and Requirements Assessment (e-RA), that is a part of the E-Authentication work: <<http://www.cio.gov/eauthentication/era.htm>>. While it is not intended to assess levels 1-4 directly, it still takes a subjective approach that asks about the risk level regarding X application. It might provide something more concrete for auditors to look at.

The LoA discussion will continue on the MACE-Dir mailing list and the next MACE-Dir Working Group call, scheduled for Monday, January 15, 2007 at 4:30pm EST.

[0] Keith's Summary of the LoA call

Does your campus face the need to handle different levels of assurance in different usage scenarios and/or for different populations of users?

As a kick-start for the discussion, here are notes from a call in mid-December from a few institutions moving in this direction.

Quick summary followed by additional excerpts from the call:

U Washington, UT System, U Wisconsin all being driven to support multiple levels of assurance.

id/password and associated identity proofing is the baseline (call it NIST 800-63 level 2); new populations, new apps and new data protection policies are pushing us toward things weaker than level 2 (applicants, "parents") and stronger (some grid resources, access to restricted/sensitive information)

We're handling in a variety of ways, but all are based on knowing which apps, which affiliations, which authentication method etc. are involved in a given usage scenario, and hand-wiring the appropriate pieces together or controlling through a policy chokepoint (U Fla).

We can imagine a world where a service provider could get richer authentication context information at run time, about how authenticated identity was vetted, what kind of credential was used to authenticate, etc., but that is a way off yet.

Jessica Bibbee, Technical Analyst

Internet2

jbibbee@internet2.edu

mobile: +1-734-255-6644

Wishing you an inspired and innovative 2007.

<http://www.internet2.edu/greetings/newyears2007/>

Electronic Risk and Requirements Assessment (e-RA):

Background

To provide authentication services that can be used across government, the E-Authentication project must first identify the full range of authentication requirements for the electronic Government Initiatives and projects. The E-Authentication Initiative teamed with the Software Engineering Institute (SEI) at Carnegie Mellon University to develop a risk-based approach to authentication requirements, called the Electronic Risk and Requirements Assessment, or e-RA. This approach identifies the Risks associated with insufficient authentication of users, and it forms the basis for the definition of authentication requirements. The tool is fully aligned with OMB M-04-04 E-Authentication Guidance.

The e-RA Tool

The e-RA tool is available to anyone through the E-Authentication Initiative to assess authentication risks of its customer's environment.

In response to feedback from e-RA users and the E-Authentication Program Management Office, the e-RA tool has been improved. The current database version is 1.5 (November 2005). The new version provides the following enhancements:

- Improved end user interface
- Added functionality to capture transactions by user type
- Added more comment areas
- Added enhanced reports

Click on the appropriate link to download the version of the e-RA tool that will work for you.

Electronic Risk and Requirements Assessment Guide e-RA Activity Guide v1.5

Please refer to the [E-Authentication e-RA Tool Activity Guide](#) before using the e-RA tool; particularly (Section 2.2, page 4)

Important Note: When downloading the e-RA tool and opening the application, you may receive Security Warnings. These warnings may be ignored (**click "open" to ignore the warning and begin using the tool**).

Download the Tool

- If you have MS Access 2002/2003 loaded on your PC, you may download [eRA2003v15.mde - 2.10 MB in size](#)

- If you have MS Access 2000 loaded on your PC, you may download [eRA2000v15.mde - 1.96 MB in size](#)

- If you do not have MS Access loaded on your PC, you may download [eRA v15install.zip - 34.2 MB in size](#)