A Gap Analysis of Current LoA Definitions vs. LoA Requirements in e-Science/Grid Context

1 Introduction

In an environment where authentication and authorisation processes are performed by separate administrative entities (e.g. identity providers are responsible for authentication and service providers for authorisation), there is a need to provide a way to quantify the 'strength' of an authentication process. The separation of duties means that a service provider (SP) may no longer have control over how the identity of a remote user is established (identity vetting), an electronic credential is bound to the identity (credential issuance), and the credential is verified when an access request is made (authentication protocol) before a decision on the access request is made (authorisation). Different identity providers (IdPs) may use different policies, procedures and processes for identity vetting, credential issuance and management, and entity authentication, thus resulting in a spectrum of quality or confidence levels in user identification and authentication.

In addition, an SP may manage classes of resources with varying levels of sensitivity. For example, electronic catalogue services typically have a lower sensitivity level than subscribed electronic resources such as e-journals and e-learning materials, whereas these are less sensitive than personal health records. Similarly, raw patient datasets uploaded into a central repository for anonymisation are much more sensitive than the processed datasets that have already had private and sensitive personal information removed. Clearly, there should be a minimum agreed level of trust between a user and their IdP and between the IdP and an SP for the granting of, and access to, resources with varying levels of sensitivity. A determining factor in this trust level derivation is the strength, or Level of Assurance (LoA), of the underlying authentication systems used to express the level of confidence in a user's claimed identity. In other words, to provide a fine-grained access control to resources, there is a need to link access privileges to the authentication LoA derived based upon the credential used to identify the user and the underlying access management system used by the IdP.

This document reports the study of current worldwide efforts on defining LoA and applying it to achieve fine-grained access control to digital resources. It first summarises current LoA standards and specifications, in particular the work done by the US government's Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) on behalf of the US government. Next, we look into current frameworks that support the use of LoA and implementations of LoA-based systems. Finally, we identify potential gaps for the use of these LoA definitions in grid environments.

2 Existing Efforts in Defining and Using LoAs

The idea of using an authentication LoA as a determining factor to control the level of protection applied to electronic resources was first proposed by the UK government in its e-Government Authentication initiative [UK-AuthFram]. This idea was then followed-up by the US government, the US industrial public and private sectors, the US High Education (HE) Federation, the US National Institutes of Health (NIH), as well as governments and HE federations in several other countries.

2.1 The UK Government Initiative

In 2000, as part of the initiative for modernising government by moving towards the electronic delivery of services, the UK government introduced the concept of authentication assurance levels for the first time. In their 'e-Government Authentication Framework' [UK-AuthFram], four distinctive authentication assurance levels, ranging from 0 to 3, were identified in terms of the sensitivity and importance of transactions. The framework also gave guidance to service providers on how to classify transactions into different groups based on potential impact due to authentication errors, and how to allocate an applicable assurance level to each group. The identified transaction classes and the related authentication assurance levels as defined in the guidance are summarised below.

- **Level 0:** *Informal transactions*. A transaction is categorised as Level 0 if no trust is placed on the identities claimed by users. In other words, misappropriation of identity or repudiation of transaction would not result in inconvenience to the identity holder, risk to their personal safety, or financial loss or distress to any party.
- **Level 1:** *Personal transactions*. At this level, users will need to identify themselves by presentation of a credential and demonstration of the knowledge of a secret, which can be a username/password pair. With personal transactions that may contain personal but non-sensitive information, a mistaken identity would have a minor impact to one or more of the involved parties. Misappropriation of identities or repudiation of transactions would not result in major inconvenience to the identity holder, risk to their personal safety, or financial loss or distress to any party.
- **Level 2:** *Transactions with financial or statutory consequence*. With this class of transactions, misappropriation of identity or repudiation of transaction might result in substantial inconvenience to the identity holder (but not risk to their personal safety), significant financial loss or distress to any party. It also might assist in commissioning a serious crime or hinder its detection and materially damage the reputation of the identity holder. To access Level 2 transactions, users will have to identify themselves by presentation of a credential, which would preferably be a digital certificate, and demonstrate the right to that credential by proving the possession of both the corresponding private key and a password or biometrics used to access the encrypted private key. The validity of a credential must be time-bound and the revocation status of the credential must be checked at the time of transaction.
- **Level 3:** *Transactions with substantial financial, statutory or safety consequence*. At this level, misappropriation of identity or repudiation of transaction might result in substantial inconvenience to the identity holder and risk to their personal safety, significant financial loss or distress to any party. For a Level 3 transaction, users will have to identify themselves by presentation of a digital certificate that will preferably be stored in a secure hard token, and demonstrate the right to that certificate by proving the possession of both the corresponding private key and a password or biometrics to unlock the private key from the token. Face-to-face user registration is required at the time of obtaining a credential and, similar to Level 2, the validity of the credential must be time-bound and the revocation status of the credential must be checked at the time of transaction.

In September 2002, the UK government published a follow-on document, 'e-Government Strategy Framework Policy and Guidelines: Registration and Authentication v3.0' [UK-RegAuth]. This document builds on the previous Authentication Framework and further specifies that the assurance level in identifying a client should be defined in terms of trust acquired during both the client's *registration* and *authentication* processes. Registration is defined as a complex process consisting of the following steps: identity registration, identity validation, identity verification, credential issuance, logging for audit purposes, and credential withdrawal. Authentication is a process of requesting an identity and verifying it. The document specifies four levels of registration assurance and four levels of authentication assurance, which are appropriate for, and can be mapped to, the four identified transaction classes. In addition, the document also defines four categories of *identification* with their implied registration and authentication levels as follows:

- **Anonymous or pseudo-anonymous**: neither real-world nor the electronic identity is required to complete the transaction (registration level: 0; authentication level: 0).
- **Anonymous or pseudo-anonymous with electronic identity**: the real-world identity of the client is not required to complete the transaction, but the electronic identity enables service provider to recognise the client in repeated transactions (registration level: 0; authentication level: 1, 2, or 3).
- **Anonymous or pseudo-anonymous with electronic identity and traceable**: the real-world identity of the client is not required to complete the transaction, but the electronic identity enables service provider to recognise the client in repeated transactions and could be used to trace the real-world identity via the Registration Authority that has registered the client (registration level: 1, 2, or 3; authentication level: 1, 2, or 3).

- **Real-world identity established**: the real-world identity of the client needs to be established to some degree before the transaction can be performed (registration level: 1, 2, or 3; authentication level: 1, 2, or 3).

Table 1 gives a summary of the likely combinations of the registration and authentication levels that may be assigned to different classes of transactions. From the table, it can be seen that some combinations do not make much sense. For example, there is not much point to have a transaction that has registration level 3 (i.e. extensive verification of real-world identity) but requires authentication level 0 (i.e. essentially unrestricted access).

Table 1: Likely values for authentication and registration levels*

x unlikely combination √ likely combination		Authentication level			
		0	1	2	3
Registration level	0	√	√	√	√
	1	x	√	√	√
	2	x	x	√	√
	3	x	x	x	√

* Source [UK-RegAuth]

The UK government's efforts have laid the cornerstone for all subsequent efforts on defining and using LoAs. However, these guidelines have only addressed two aspects of LoAs, i.e. registration and authentication. Technical and operational requirements on how to achieve a given level of assurance were missing from the guidelines.

2.2 The US Government Initiative

2.2.1 OMB and NIST

While the UK government guidelines define LoA in terms of the sensitivity levels and importance of transactions, the US government's Office of Management and Budget (OMB), in its memorandum, 'The E-Authentication Guidance for Federal Agencies' [OMB-M0404], defines levels of authentication assurance in terms of the consequences of the authentication errors and misuse of credentials. This memorandum specifies four assurance levels (Level 1 to 4), to help and direct US federal agencies in reviewing e-government transactions, determining their authentication needs, and ensuring that the authentication process satisfies the minimum LoA given the risk level of the transaction.

The OMB-defined four assurance levels are as follows:

- **Level 1:** for transactions requiring little or no confidence in the claimed identity.
- **Level 2:** for transactions requiring some confidence int the claimed identity.
- **Level 3:** for transactions requiring high confidence in the user's claimed identity.
- **Level 4:** for transactions requiring very high confidence in the user's claimed identity.

According to the OMB, the risk from an authentication error can be measured in terms of (1) potential *harm* or *impact* and (2) *likelihood* of its occurrence. Harm or impact are of the following categories:

- Inconvenience, distress, or damage to reputation;
- Financial loss or agency liability;
- Harm to agency programs or public interests;
- Unauthorised release of sensitive information;
- Personal safety;
- Civil or criminal violations.

For each impact category, three impact values, *low*, *moderate* and *high,* are recognised. These values can be mapped to the four LoA levels using an example impact profile shown in Table 2.

Table 2: Maximum potential impact profile mapped to assurance levels*

	LoA impact profiles			
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

* Source [OMB-M0404]

The OMB recommends the following steps in managing e-authentication in accessing e-government services:

(1) Conduct a risk assessment for all the transactions performed on an underlying system to assess the severity of potential harm and likelihood of their occurrence in each impact category.
(2) Determine the required assurance level using Table 2.
(3) Select the necessary technology to achieve the determined LoA based on the NIST 'Electronic Authentication Guideline' [NIST-SP800-63].
(1) Validate the system to confirm that it has achieved the required LoA.
(2) Periodically reassess the system to verify that the technology applied corresponds to the refreshed requirements.

The OMB recognises that each step of an e-authentication process influences the overall conformance to the desired LoA, and each should be as strong and robust as the next. Otherwise, the principle of the 'weakest link' applies - the step that provides the lowest LoA in the process affects all the others, regardless of how strong they are. The following LoA-affecting processes and procedures have been identified by OMB:

i) Registration and identity proofing: initial enrolment with a Registration Authority (RA) and obtaining a credential and subsequent visits to the RA;
ii) Credential management: issuance, maintenance, suspension, revocation, re-issuance of credentials;
iii) Strength (in cryptographic sense) of the credential and the token in which it stored;
iv) Verification of an identity credential: the use of a credential to proof one's identity using an authentication protocol;
v) Transaction management: from both technical and administrative perspectives;
vi) Audit and record keeping;
vii) Periodic system re-assessment.

The technical requirements for achieving each of the four OMB levels, as indicated in step (3) above, have been specified in a complementary document published by the US National Institute of Standards and Technology (NIST) - 'NIST SP 800-63: Electronic Authentication Guideline' [NIST-SP800-63]. The NIST guideline provides guidance to federal agencies on how to implement authentication systems that comply with the four OMB's LoA levels.

The NIST guideline provides technical guidance on e-authentication aspects outlined below:

(1) Registration and identity proofing ((i) from above);
(2) Credential management ((ii) from above);
(3) Tokens used for proving identity ((iii) from above);
(4) Remote authentication as a combination of cryptographic protocols, credentials and tokens used to establish the identity of the claimant ((iv) from above); and
(5) Assertion mechanisms used to communicate the results of an authentication instance to other interested parties (not mentioned by the OMB Memorandum).

(1) *Registration and identity proofing*: the process of registering one's identity with a RA, and obtaining a credential from a Credential Service Provider (CSP) associated with the RA. Requirements that different LoAs should satisfy can be summarised as follows:

- **Level 1**: At this level, names are not verified (i.e. names are always assumed to be pseudonyms) and anonymous credentials are allowed. There are no LoA-specific requirements at this level.
- **Level 2**: At this level, credentials and identity/attribute assertions must specify whether the name is real and verified or a pseudonym. In-person or remote registration is permitted.
- **Level 3**: At this level, real names must be verified. In-person or remote registration is permitted.
- **Level 4**: At this level, real names must be verified. Only in-person registration is permitted.

(2) *Credential management*: the measures used for the management of long term secrets, credential and token lifetime, status and revocation.

- **Level 1**: There are no stipulations about revocation or lifetime of credentials. Long-term secrets may be revealed to verifiers. Files with shared secrets should not contain plaintext passwords and should be protected by discretionary access control that limits access to administrators and only those applications that require access. For instance, passwords should be hashed before storing them in a password file. Password strength, expressed as the probability of successfully breaking a password without any *a priori* knowledge of it, shall not exceed 1 in 1024 (i.e. 2^{-10}) over the lifetime of the password.
- **Level 2**: CSP should provide a mechanism, such as a signed revocation list or a status responder, to allow verifiers to check that credentials are still valid. CSP should have mechanisms to revoke credentials within 72 hours after being notified that the credential is no longer valid. Long-term secrets should never be revealed to verifiers or to any other party except for the CSP and the owner themselves. Files with shared secrets should not contain plaintext passwords and should be protected by discretionary access control that limits access to administrators and only those applications that require access. For instance, passwords should be concatenated with salt and then hashed before storing them in a password file. Password strength, expressed as the probability of successfully breaking a password without any *a priori* knowledge of it, should not exceed 1 in 16384 (i.e. 2^{-14}) over the lifetime of the password.
- **Level 3**: CSP should provide a mechanism, such as a signed revocation list or on-line validation servers, to allow verifiers to ensure that credentials are still valid. CSP should have mechanisms to revoke credentials within 24 hours after being notified that the credential is no longer valid. Long-term secrets should never be revealed to verifiers or to any other party except for CSP and the owner themselves. Files of shared long-term should be protected by discretionary access control that limits access to administrators and only those applications that require access. For instance, such files should be encrypted with a key held in FIPS 140-2 Level 2 or higher validated hardware cryptographic module or FIPS 140-2 approved Level 3 or higher cryptographic module.
- **Level 4**: The same as for Level 3.

(3) *Token strengths*: NIST recognises four kinds of authentication tokens:

- Password token: a secret memorised by a claimant and linked to their username.
- Soft token: a cryptographic key that is typically stored on disk or some other media. The key can be stored in encrypted form, in which case it is activated by a user-known password.
- One-time password (OTP) device token: a personal hardware device that generates OTPs for authentication purposes. An OTP generated by the device has a limited life-time and is manually entered by the user to the verifier as a password, typically

tunnelled via a TLS/SSL session. This kind of a device may or may not have an integrated entry keypad or a biometric reader that can be used to activate the device.

- Hard token: a hardware device that contains a protected cryptographic key and requires an entry of a password or a biometrics to activate the key stored in the device.

Password tokens can satisfy the assurance requirements for Levels 1 and 2, which provide single-factor authentication. Constraints imposed on password tokens are that the probability of guessing a password without any a priori knowledge of it should not exceed 2^{-10} (for Level 1) and 2^{-14} (for Level 2). Passwords are not allowed at Levels 3 and 4, which require multi-factor authentication according to the NIST guideline. Soft cryptographic tokens and OTP devices can be used with proof-of-possession protocols at assurance Levels 1 to 3. At Level 3, however, they must be activated (unlocked) with the use of a password, a PIN, or a piece of biometric. Hard cryptographic tokens, which are always activated by a password, a PIN or biometrics, can be used at assurance Levels 1 through 4.

Table 3: Token types allowed for each LoA*

Token type	Level 1	Level 2	Level 3	Level 4
Hard cryptographic token	√	√	√	√
OTP device token	√	√	√**	
Soft cryptographic token	√	√	√**	
Password token	√	√		

* Source [NIST-SP800-63]
** Must be activated by a password, PIN or biometrics at Level 3.

(4) *E-authentication protocols*: A claimant, through the execution of an e-authentication protocol, proves to a verifier that they are indeed in control of a valid token so as to establish the claimant's identity. According to NIST, e-authentication protocols can be assigned a LoA category according to specific attacks and threats that they are resistant against, as shown in Tables 4 and 5. Different threats and attacks recognised by the NIST guideline include: password guessing, replay attacks, eavesdropping, verifier impersonation, man-in-the-middle attacks and hijacking of authenticated sessions. Other mentioned threats (not directly related to the protocol itself) include: fooling claimants to use an insecure protocol or accepting unverified servers' certificates, obtaining tokens out-of-band in some other manner such as social engineering or shoulder-sniffing, or by penetrating the verifier's or the CSP's system.

Table 4: Protections that protocols should provide at each LoA*

Protection against	Level 1	Level 2	Level 3	Level 4
Password guessing	√	√	√	√
Replay	√	√	√	√
Eavesdropping		√	√	√
Verifier impersonation			√	√
Man-in-the-middle attack			√	√
Session hijacking				√

* Source [NIST-SP800-63]

Table 5: Authentication protocol types allowed at each LoA*

Protocol type	Level 1	Level 2	Level 3	Level 4
Private key Proof-of-Possession (PoP)	√	√	√	√
Symmetric key Proof-of-Possession (PoP)	√	√	√	√
Tunnelled or zero-knowledge password	√	√		
Challenge-response password	√			

* Source [NIST-SP800-63]

Table 6: Additional requirements for protocols at each LoA*

Required property	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				√

* Source [NIST-SP800-63]

(5) *Assertion mechanisms*: An assertion mechanism is used by an identity provider (i.e. the entity performing the authentication) to communicate the result of an e-authentication process to a relying party (e.g. a service provider). Assertions are particularly important in federated environments where the tasks of authentication and authorisation are performed by different organisational or administrative entities. In such environments, a user authenticates to one entity (usually the user's home organisation), while the authorisation decision is made by the other entity managing the resources based on the outcome of the user's authentication and possibly the user's additional attributes passed in the form of an assertion. Signed SAML [SAML] assertions and cookies are most commonly used to carry assertions. A relying party may trust an assertion depending on the origin and the time of generation of the assertion. The NIST guideline recommends that relying parties may accept assertions that are either:

- Digitally signed by a trusted entity (e.g. a verifier), or
- Obtained directly from a trusted entity using a protocol where a trusted entity is authenticated to the relying party using a secure protocol (e.g. TLS) that also protects the confidentiality of an assertion.

Authentication assertions are treated differently at the four defined assurance levels:

- **Level 1**: Assertions with no expiration time are accepted.
- **Level 2**: Assertions are accepted up to 12 hours from the time of creation.
- **Level 3**: Assertions are accepted up to 2 hours from the time of creation.
- **Level 4**: Authentication assertions are not allowed at Level 4; i.e. at this level, a user must authenticate directly to the relying party.

2.2.2 EAI

The E-Authentication Initiative (EAI) [EAI] from the US government is aimed to provide a secure and standards-based authentication architecture to support US federal e-government applications. Their main objective regarding e-authentication is to provide a uniform process for establishing identities of their clients electronically so as to eliminate the need for each application to develop its own authentication solution. They also want to enable citizens and businesses to use credentials issued by non-governmental bodies (such as universities) to conduct transactions with the government.

In order to achieve its goal, the EAI has adopted the risk-based and LoA-linked approach to authentication and access control and implemented a system fully compliant with the OMB/NIST e-authentication guidelines. To help them with the risk assessment, the EAI has produced the Electronic Risk and Requirements Assessment (E-RA) tool [ERA], and has also established the Interoperability Lab [EA-Lab], run by the US General Services Administration (GSA) and with the involvement of the NIST, to help federal agencies with testing and certifying their interoperability and compliance with the OMB/NIST guidelines. So far, the EAI has published the Federal Trust List of Approved Credential Service Providers [CSPList] and Approved E-Authentication Technology Provider List [TPList], containing all trusted CSPs and certified interoperable vendor suites for the use in the implementation of EAI-adopted schemes.

In May 2007, the EAI has revised its architecture [EA-Arch] to incorporate the SAML v2.0 specification in order to provide richer syntax for expressing authentication and identity assertions and better meet the authentication needs of its members. The EAI's authentication

architecture functions in the similar way to Shibboleth [Shibboleth]: SAML messages are exchanged between endpoints - a Credential Service Provider and a relying party - resulting in delivery of an identity assertion conveying authentication outcome along with additional attribute information about an authenticated end-user.

As part of the EAI, the E-Authentication Federation (EAF) [EAF] has been established to help the US government's agencies to form a trust federation between the agency's service and identity providers, and as of July 2007 the EAF has 46 members [EAI-News-July07]. According to the EAF rules, the LoA value is a compulsory attribute that must be present whenever a SAML authentication assertion is issued between federation members. The EAF has defined a special URI (us:gov:e-authentication:basic:assuranceLevel) to uniquely identify the LoA attribute, and the attribute can only have values of 1, 2, 3, 4 or 'test'.

2.2.3 NIH

The US National Institutes of Health [NIH] has adopted the OMB/NIST LoA approach as well, and, together with the US InCommon HE federation (see section 2.8), are making an inter-federation pilot [NIH-pilot] that will allow users from the HE sector to access NIH resources based on their authentication LoAs. The LoA attribute will be conveyed in a SAML assertion under the formal name of 'authnLoa'. The value of the attribute will most probably be a URI under the MACE-Dir namespace similar to 'urn:mace:dir:constant:nist-sp-800-63:1', to signify the LoA value in the NIST SP 800-63 scheme.

2.3 The European Government Initiative

The IDABC (Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens) [IDABC] is a programme of European government that supports the use of information and communication technologies to encourage the delivery of cross-border public sector services to citizens and enterprises in Europe, and to facilitate the interoperability of e-Government services at pan-European level.

One of its projects, the eIDM Interoperability [eIDM], works on secure means of electronic identification across the EU member countries and aims to build an European eIDM (Electronic Identity Management) framework by 2010 based on interoperability and mutual recognition of national eIDMs. They made plans for building a pan-European multilevel authentication mechanism [EU-LoA] based on the NIST four-level approach and using risk assessment as proposed by the OMB. Their future plans involve creating a mapping of existing authentication mechanisms reported in the national profiles of member states to the recognised four authentication levels, following the NIST guidelines for the registration process, authentication process and credential/token types. Provisional work has been done, but this effort is still at an early stage. They are also planning to prepare draft recommendations on encouraging the uptake and practical use of this proposal and implementing a large scale eIDM pilot.

2.4 The Australian Government Initiative

The Australian government has defined an authentication policy in its e-Government initiative to boost confidence in on-line transactions involving government bodies. The outcome of this initiative is the establishment of the Australian government's e-Authentication Framework (AGAF) [Aus-AF], which, similar to the NIST guideline, recommends the use of a risk-based and LoA-linked authentication approach to on-line transactions. It uses the four authentication assurance levels as defined by NIST:

- **Level 1**: Minimal risk and little requirement for e-authentication.
- **Level 2**: Low risk and some requirement for e-authentication.
- **Level 3**: Moderate risk and moderate requirement for e-authentication.
- **Level 4**: High risk and high requirement for e-authentication.

Similarly to the US government's OMB, the Australian government identifies risk categories for government and businesses. They are not intended to be prescriptive; organisations are free to modify the lists to suit their particular circumstances.

For the government, they have identified: financial loss; damage to standing or reputation; personal safety; release of personal or commercially sensitive information to third parties; inconvenience; distress caused to any party; threats to government's agencies' systems or capacity to conduct business; assisting crime or hindering its detection as the major risk categories. For businesses, the identified risks are: financial loss; damage to standing or reputation; health and safety; impacts on confidentiality of business or privacy of individuals; threats to the business' productivity or usability of its services; impacts resulting in disciplinary actions; impacts that adversely affect the business' regulatory compliance; impacts that cause legal penalties.

2.5 The Canadian Government Initiative

The Government of Canadian British Columbia has also recommended the LoA-linked authentication approach for on-line governmental transactions [Canada-LoA]. The recommendation is based on the UK Government's "Framework Policy and Guidelines" [UK-RegAuth]. Four trust levels, from 0 to 3, are recommended linking authentication requirements to four types of transactions, and the reference profiles for each of the trust levels are also specified. The mappings between the four trust levels and the four types of transactions are as follows:

- **Level 0:** *Anonymous transactions* - Transactions that do not require the transaction initiators to be identified or transactions that require the protection of the identities of the transaction initiators.
- **Level 1:** *Pseudonymous transactions* - Transactions that do not require the transaction initiators to be identified, but do require means for further contacts for follow-up services, etc.
- **Level 2:** *Identified transactions* - Transactions that require the identification or confirmation of a transaction initiator, e.g. name, address, birth date, etc. or the linkage between the initiator and the transactions, e.g. invoice number, personal health number, etc.
- **Level 3:** *Verified transactions* - Transactions that require the initiator to be specifically identified and the integrity of the transactional data verified. Sufficient evidence indicating that the initiator has indeed performed the transactions should be generated.

According to the recommendation, once an Authentication Profile is established (on a scale 0 - 3), risks and consequence of authentication errors related to each of the transaction groups should be assessed. The level of trust assigned to a business process based on the Authentication Profile should adequately address the concerns of the risk assessment. The identified categories of risks are similar to those specified by the governments of UK, US and Australia, i.e. financial loss; damage to standing or reputation; personal safety; release of personal or commercially sensitive information to third parties; inconvenience; distress caused to any party; threats to government's agencies' systems or capacity to conduct business; assisting crime or hindering its detection.

2.6 Industrial Sector: Liberty Alliance

The Liberty Alliance [LA] is a global body working to establish business, policy and technical standards for digital identity management and SAML-based identity framework using Web Services.

The Identity Assurance Expert Group (IAEG) within the Liberty Alliance is the main driving force behind the adoption of identity and authentication assurance services. The IAEG's goal is to achieve interoperability between different e-authentication systems and provide both public and private sector organizations with uniform means of relying on digital credentials issued by a variety of identity providers (or credential service providers) in order to advance trusted identity federation. To achieve this goal, the IAEG provides a forum for identifying and resolving the market acceptance and commercial obstacles to broad deployment and adoption of LoAs. The group is aimed to develop a global standard framework for validating trusted identity providers and certifying them as compliant to common policies and business rules in order to help avoid any confusion about the meaning of LoA value delivered.

The work of IAEG began by consolidating the work done by several bodies, including the Trust Framework of the Electronic Authentication Partnership (EAP, see section 2.7) [EAP], the US government's E-Authentication Federation (EAF, see section 2.2.2) and other public and private industry contributors. The goal is to produce a standard that consist of an identity credential policy, business procedures and rules and minimal baseline commercial terms (e.g. liability allocation) framework supporting mutual acceptance, validation and lifecycle maintenance across different identity federations. This will help realise the vision of inter-federation collaborations on a global scale. To help with achieving their vision, the group formed the Liberty Trust Framework (LTF) that encompasses a set of concepts, such as business rules, procedural and technical trust criteria for identity providers, and assessment methodologies for determining conformance to the defined trust criteria.

2.7 Private Sector: E-Authentication Partnership

The International Collaborative Identity Management (I-CIDM) WorkGroup (WG) was formed in 2004 as a result of a multi-industry partnership working on the vital task of interoperability for electronic authentication in public and private sectors. The WG recognises that the interoperability is essential to cost-effective and secure operations of electronic systems in the sectors. The I-CIDM involves members from governments with PKI initiatives (US, UK, Canada, the Netherlands), industry organizations involved in operating rules and best practice (NACHA, MasterCard, Visa, American Express), PKI bridge providers (US Federal and Higher Education Bridges, Commercial Bridge), major aerospace and defence companies with PKI initiatives (EADS/Airbus, Boeing, Lockheed Martin, Northrop Grumman), standards organisations (ISO, NIST, IETF), etc.

The I-CIDM Bridge-to-Bridge (BB) sub-WG has prepared a white paper, 'E-Authentication Partnership Policy on Levels of Assurance of Identity for Authentication of Electronic Identity Credentials' [EAP-e-com], for the CS-AL (Credential Standards and Assurance Levels) WG of the E-Authentication Partnership [EAP]. The EAP is working on enabling interoperability for electronic authentication among private and public sector organisations with a vision of having multiple interoperable federations across different industries and governments. The document examines issues surrounding e-authentication of human users in e-commerce transactions. It recognises the four LoAs introduced by the NIST and their linkage to risk levels when engaging in e-government transactions and investigates whether this model is acceptable for the use in the private (e-commerce) sector.

The EAP LoA Policy recommends the four levels of authentication assurance as defined by the NIST as an interim standard for electronic authentication of entities in on-line business transactions. It further recommends that more work is necessary to develop a comprehensive mathematical model and an algorithm for determining LoA based on the factors recognised by the CS-AL WG, as a potential candidate for a final standard. The factors recognised by CS-AL as influential for e-authentication include: (1) identity proofing, (2) credential management, and (3) the extent to which authentication is coupled with an authorisation.

Identity proofing refers to the extent to which the identity named in a credential can be trusted to actually belong to the entity using the credential. Credential management refers to the extent to which a credential can be trusted to be the proxy for an entity named in it. The influential factors are the trustworthiness of the credential technology and the system that manages credentials and tokens, how the credential is secured to a token, and the trustworthiness of the system validating the credential. Finally, CS-AL has also noted that a LoA is only useful or required when an authentication event leads to an authorisation event. So, even though a LoA is a characteristic of an authentication process, it cannot be discussed without addressing authorisation which is closely related to risk levels (a higher LoA is required to mitigate a higher level of risks) and which, in turn, are determining factors for LoA (according to the OMB/ NIST guidelines).

The workgroup argues that risks are defined as the potential harm or damage arising from inappropriately authorising access to a system or a resource. Thus, risk assessment and mitigation are essential to authorisation decisions. They attempt to use a LoA as a discrete indicator to quantify the degree of protection that an information system implements to mitigate or eliminate these risks. The primary risks associated with identity assertion are from identity fraud, with identity theft being the most common form. However, there is a whole

spectrum of risks of fraud, ranging from harmless spoofing to breaches of national security. Each e-commerce service provider must conduct its own risk assessment and perform risk-to-harm mapping as part of its risk mitigation process. Harm typically occurs when authorisation is improperly granted (false positive) or withheld (false negative) in a business transaction. Therefore it is the job of an authorisation event to determine a LoA that is required for authenticating a requesting entity.

Authentication and authorisation events can be tightly or loosely coupled. An exemplar loosely coupled case is on-line purchase with a credit card – the assurance of an identity is less important here because a merchant is willing to go ahead with the transaction as long as the credit card issuer authorises it. This enables, for instance, a child to use the parent's credit card for authorised purchases even if the child is not the cardholder. An exemplar tightly coupled authorisation and authentication case is when accessing one's bank account details on-line. In this case, establishing the client's identity is crucial to the service access. The LoA is just one of the determining factors in making authorisation decisions for e-commerce transactions. Other factors include, for instance, payment history, purchase/spending patterns, transaction amount involved, etc. The implication of the relationship between authentication and authorisation events is that the more tightly they are coupled, the more important LoA becomes and the less important other factors are.

The CS-AL workgroup recognises that the four levels of authentication assurance recommended by the NIST reflect the spectrum of authentication assurance, but argues that there is no objective metrics associated with the derivation of an assurance level. So they propose to develop a mathematical model to describe all the factors involved in identity proofing and credential management and an algorithm to precisely calculate a LoA. In their proposal, each effecting factor is assigned with a weight based on the degree it contributes to an authentication process. Different factors may not necessarily have the same weight – a factor with a higher weight should have more impact. The overall LoA value is calculated based on all the contributing factors and is expressed as a percentage of confidence. This approach can be easily mapped to the US Gov/NIST LoA scheme and made interoperable with it in the following manner:

- Under 25% confidence in an authentication event is mapped to US Gov/NIST Level 1
- 25-50% confidence in an authentication event is mapped to US Gov/NIST Level 2
- 50-75% confidence in an authentication event is mapped to US Gov/NIST Level 3
- 75-100% confidence in an authentication event is mapped to US Gov/NIST Level 4.

Since July 2007, the Trust Framework of the EAP merged with the Liberty Alliance to form the Identity Assurance Expert Group (IAEG). The members in the group are developing the Liberty Trust Framework by initially extending contributions from the EAP and the US government's EAF. This effort will be an important step to remove a major barrier to global inter-federation deployments: the complexity of assessing the level of identity assurance among all organizations participating in federated relationships.

2.8 The US HE Federation

The InCommon federation, an access management federation of US HE institutions, uses the Shibboleth [Shibboleth] authentication and authorization system to enable cost-effective, privacy-preserving and federated identity management among its community of participants.

In its draft document, 'Bronze and Silver Credential Assessment Profiles' [InComm-CAP], InCommon recommends two classes of authentication services to be used by the federation's IdPs, and defines two Credential Assessment Profiles (CAPs), namely Bronze and Silver. The Profiles contain the assessment criteria for IdPs wanting to be qualified for providing the Bronze or Silver services. The InCommon Bronze and Silver Profiles only recognise password-based authentication systems. The Profiles neither recognise PKI certificate-based authentication systems, nor systems that use passwords in conjunction with hard (physical) tokens or other specialised hardware or proprietary client software. The reason for this is that campuses across US HE mainly support the use of password-based authentication services, and, currently, they do not have any plan for broad adoption of PKI. This is why InCommon have only concentrated on defining profiles compliant with OMB/NIST Levels 1 and 2 (note that certificate-based authentication is a prerequisite for Levels 3 and 4).

InCommon has made their Bronze and Silver CAPs fully compatible with the NIST specification used by the US EAI/EAF. The Bronze CAP maps directly onto the NIST Level 1 and the Silver CAP onto Level 2. Although currently InCommon members have not explicitly expressed the need for different LoAs, InCommon has drafted their informal proposal for inter-federation interactions with EAF that already has an established infrastructure and has very stringent LoA requirements. The inter-federation collaboration looks inevitable as the InCommon HE community represents a large pool of potential users for the US government and EAF applications. The need for the interoperability between the two federations (and other federations in general) has driven InCommon to draft their Profiles to be conformant with the ones adopted by the EAF.

Though InCommon currently recognises only password-based authentication systems in its CAPs, which can at best be mapped to Level 2 of the NIST LoA Guideline, it does leave room for defining the so-called Gold and Platinum profiles. These would presumably allow for PKI certificate-based authentication and offer assurance levels higher than Level 2.

2.9 Other Worldwide HE Federations

2.9.1 UK

There are current efforts (through the JISC-funded ES-LoA [ES-LoA] and Identity [Id] projects) to investigate the needs and requirements for adopting risk-based access control and federated identity management among the UK's HE community. The ES-LoA project is currently investigating the possibility of adopting the NIST four Levels of Assurance, and to assess whether they are sufficient to cover the application use case scenarios for both federated and grid environments.

2.9.2 Switzerland

The Swiss HE Federation, SWITCH, has published an informal proposal for using authentication assurance levels on their Web site [Switch-AAI]. The Federation funded a pilot project to examine the opportunities and limitations of using LoAs and multi-factor authentication in the Shibboleth infrastructure. The proposal recommends the four-level approach as recognised by the US Government, NIST, E-Authentication and InCommon federations:

- **Level 1** (Bronze)
- **Level 2** (Silver)
- **Level 3** (Gold)
- **Level 4** (Platinum)

It also further specifies the requirements for each of the four levels in terms of the following authentication aspects:

- Registration procedure
- Identity proofing
- Credential delivery
- Authentication security
- Authentication session validity
- Credential validity.

2.9.3 Denmark

The Danish HE federation, DK-AAI, has only just been formed. It has not yet published any official or non-official documentation on the LoA issues. In its draft Federation Agreement [DK-AAI-FedAgr] produced in February 2007, it stated that 'IdP's MUST have an identity management system and procedures complying with at least Level 2 of the NIST E-Authentication Guideline'.

2.9.4 Australia and New Zealand

The Australian HE federation, AAF (Australian Access Federation) [AAF], plans to build on the existing DEST-funded work in the first phase of the e-Security Framework project (based at the University of Queensland) [eSec] and the MAMS (Meta Access Management System project, based at the Macquarie University) [MAMS]. MAMS has established a test Shibboleth federation with three levels of assurance, as reported at the 7th TF-EMC2 (Task Force on European Middleware Coordination and Collaboration) meeting, October 2006, in Malaga, Spain [TF-EMC2-min]. The system was not operational at the time of this writing, and no official documentation on the assurance levels has been published to date. However, a LoA working group under the auspices of AAF has been recently established to propose a set of LoAs for adoption among the Australian and New Zealand HE communities. From the informal communication with the AAF community, we have learned that their proposal will be partially based on the Australian Financial Transaction Reports Act 1988 [FTRA88] and the Financial Transaction Reports Regulations 1990 [FTRR90]. The approach assigns points to various identity documents, e.g. passport=70pts, driving licence=40pts, etc., and a final score is derived by aggregating the points. These accumulated points from the identity documents are then combined with the four-level approach proposed by the US Gov/NIST in the following manner: if an entity presents identifying documents that collectively give less than 100 points then he will be assigned with Level 2; for more or equal 100 points - Level 3; for more or equal 100 points plus an additional background check – Level 4.

2.9.5 Finland, Norway, Sweden, France

Other international HE federations that have adopted the Federated Identity Management and Shibboleth infrastructure include Finish HAKA [HAKA], Norwegian FEIDE [Feide], Swedish SWAMI [SWAMI] and French CRU [CRU]. At the time of this writing, none of these federations have officially announced their standing about authentication assurance levels. Finish HAKA currently uses only one authentication method (username and passwords) and thus one LoA. However, they are planning to introduce PKI with smartcards and OTP devices and are waiting for the Shibboleth 2.0/SAML 2.0 that has a richer support for LoAs [HAKA-slides].

2.10 ISO/IEC

The Sub-Committee SC27 of the ISO/IEC Joint Technical Committee (JTC) on Information Technology has made a proposal for the 'New Work Item on Authentication Assurance' standard [ISO-LoA], which was scheduled to be submitted in March 2007. The standard is intended to improve the trust and confidence in authentication by providing objective and vendor-neutral guidelines on how the strength of authentication (i.e. authentication assurance) can be measured. Relying on the work previously done by the US government (OMB and NIST), the committee plans to establish metrics for quantifying risks that an entity attempting to gain access to a resource is not the one whose identifier has been presented. The criteria for the authentication metrics will include:

- Authentication tokens,
- Authentication protocols,
- Characteristics and location of a PC or a device used to access a resource (a PC inside an organisations' area with properly certified operating system with latest patches vs. a PC located in a public area, such as Internet cafe, with unverified software), and
- Type of the communication network (e.g. wireless, open wired, commercial leased lines, etc.).

2.11 Grid Community

In general, grid authentication is based on X.509 PKI certificates (standard long-term and short-term proxy ones). However, in recognition of the increasing need to allow IdPs to leverage their existing non-PKI identity management systems to provide their users with grid access, the IGTF has formally specified the requirements for operating a particular type of authentication service in the form of three Authentication Profiles:

- 'Authentication Profile for Classic X.509 Public Key Certification Authorities' [IGTF-Class],
- 'Authentication Profile for Short Lived Credential Services (SLCS) X.509 Public Key Certification Authorities' [IGTF-SLCS], and
- 'Profile for Member Integrated X.509 Credential Services (MICS) with Secured Infrastructure' [IGTF-MICS].

The Profiles define a comprehensive set of rules for the CAs operating the issuance of grid credentials (i.e. certificates), covering aspects of identity vetting, certificate expiration, renewal and re-keying, operational requirements (CA's key size, hardware requirements, CRLs, revocation, etc.), the physical security of the CA's site, audit and disaster recovery procedures. All three credential services (Classic, SLCS and MICS) provide users with X.509 certificates which are later on used to produce users' proxy certificates for accessing grids.

The Classic Profile describes the security requirements and operation procedures for CAs offering traditional X.509 PKI services and issuance of long-term X.509 certificates with the maximum lifetime of 1 year and 1 month. The SLCS Profile describes similar requirements for CAs that issue short-term X.509 certificates and leverage the existing local authentication systems to produce a short-lived grid identity. The SLCS-produced certificates are standard X.509 certificates, the only difference being that they are short-term – the maximum lifetime of such certificates is around 11 days (1000000 seconds). The MICS Profile describes requirements for the X.509 CAs that issue long-term credentials that are fully compatible with the Classic profile but to end-users that are authenticated by a federation or a large organisation using their native authentication systems. The SLCS and MICS Profiles can be based on any primary authentication system, which does not necessarily have to be (and usually is not) certificate-based, to produce the X.509 credential and a grid identity for the user upon their successful authentication. The generated X.509 credential is consequently used by the user to access grid services in a usual manner (i.e. the X.509 credential is used to generate short-term proxy certificate for grid access). Because of this 2-tier authentication (to the primary authentication system using original credential and then to a grid service using the grid credential), any LoA definition in a grid context would have to take this into account and to evaluate the LoA of both authentication processes separately. Attaching a LoA value to any of the grid Authentication Profiles would also have to address the issue of credential delegation, which is currently specific to grids only.

3 Existing LoA Middleware

So far, several worldwide projects have either developed middleware support for LoAs or have extension capabilities though which the LoA attribute can be passed and used, for example SAML, Shibboleth, FAME-PERMIS, SHEBANGS, ES-LoA and GridSite.

3.1 SAML

SAML [SAML] is an XML-based framework developed by OASIS that enables requesting, creating and exchanging security assertions between entities. It enables identity providers to make assertions regarding the identity, attributes and entitlements of a subject (an entity that is often a human user) to service providers. SAML has been adopted by many security frameworks (e.g. Shibboleth, E-Authentication Federation and Liberty Alliance) for communicating security and identity information, and LoA value can be conveyed as part of one of the attributes in a SAML assertion. In addition, the latest SAML v2.0 supports the use of Authentication Contexts as an optional part of an authentication assertion. Authentication Contexts can be used to present a service provider with additional information about an authentication process performed by an identity provider, such as identity vetting process that was used to initially associate a subject and their identity, credential management and storage, authentication method, mechanisms for minimising compromise of credentials, credential renewal frequency, etc. Such rich information about the authentication process can be used by the service provider to put the level of authentication assurance into a risk-management context. Thus, there are currently two approaches to how LoA information can be represented in SAML v2.0: either as an attribute or using an Authentication Context. Internet2 together with OASIS and Liberty Alliance are currently discussing which of the two approaches is the best (see mace-dir mailing list [mace-dir]). It is quite possible that both

approaches would be accepted and the decision would be left to assertion creators and consumers.

As far as delegation goes, SAML profiles are restricted to an exchange between a single identity provider and a single service provider, i.e. there are no SAML-specified means to support situations where a service provider may need to access additional services at other service providers on behalf of the user (i.e. delegation).

3.2 Shibboleth

Shibboleth [Shibboleth] is standards-based, open source middleware which provides an infrastructure for inter-institutional resource sharing and SSO across organizational boundaries. To enable this, the Shibboleth technology defines a federation of two types of institutions - identity providers and service providers. Inside the federation, Shibboleth enables locally authenticated users to access remote resources provided by various SPs. The task and the means of identifying a user is left to the user's home institution (IdP) and authorisation decision making to the SP that manages the resource the user is making access to. Shibboleth defines a set of protocols for exchanging SAML assertions for confirming a user's identity and secure assertion of the user's attributes between an IdP and a SP, based on which access control by the SP is made later on. Using the SAML attribute assertion, the LoA value for the user's current Shibboleth session (assigned to them by their IdP at the time of authentication) can easily be conveyed to the SP as one of the user's attributes. Alternatively, information about an authentication process could be represented by a SAML v2.0 Authentication Context, from which an SP would infer the LoA value.

Shibboleth people have also drafted a set of SAML v2.0 profiles [SAML-del] for enabling SSO with constrained delegation that would allow an SP to act as a proxy on behalf of authenticated user in order to access services on other SPs. In the proposed draft, delegation of duties to the SP would be based on the user's assertion issued by their IdP that contains certain delegation extensions. This feature, however, will not be part of the Shibboleth v2.0 or SAML v2.0. There are other proprietary and open source proposals (e.g. by Liberty Alliance and SAML TC) to address this issue by defining various SAML v2.0 profiles. How this is going to affect the LoA concept is an open issue.

3.3 FAME-PERMIS

The FAME-PERMIS (Flexible Access Middleware Extensions to PERMIS) project [FAME-PERMIS] has developed an extension (FAME) to a Shibboleth IdP that controls user authentication using a variety of authentication methods and implements authentication-method-to-LoA mapping as specified by the NIST 'Electronic Authentication Guideline'. The PERMIS authorisation decision engine, deployed at a Shibboleth SP, has been extended to include LoA in its decision making process. In this way, using the FAME-PERMIS assembly, an authorisation decision is made based on (*Subject, Target, Action, LoA*), rather than the traditional (*Subject, Target, Action*) attributes. When a user attempts to access a resource at a PERMIS-protected SP they are redirected to their home FAME IdP where they can choose from a variety of authentication methods supported by their institution. A user can have multiple identification tokens, all of which are mapped to the same identity once authentication if performed, but which can have different LoA values .

3.4 SHEBANGS

The SHEBANGS (Shibboleth Enabled Bridge to Access the National Grid Service) project [SHEBANGS] developed the Credential Translation Service (CTS), which forms a bridge between authentication methods in a Shibboleth environment and those used in a grid environment, and provides the ability to convey the strength of the authentication performed and calculated by the FAME IdP through the use of four different CAs to issue credentials for each of the four possible LoA values.

3.5 ES-LoA

As a follow-up to the FAME-PERMIS project, the ES-LoA (E-infrastructure Security: Levels of Assurance) project [ES-LoA] was set out to investigate existing worldwide LoA definitions and applications and needs for LoA in the UK HE. The project consulted with the UK education and research communities with regard to standard definitions of LoA and their appropriate uses as defined by the worth of the resources, and was set out to identify any gaps in existing authentication and authorisation policies, procedures and infrastructures regarding the long-term use of LoA in the UK education and research community.

3.6 GridSite

The GridSite project [GridSite] developed a piece of middleware to provide a community or VOs with secure access to and management of webpage content using X.509 credentials. The GridSite middleware has evolved over time to become a generic file server and various security mechanisms have been incorporated into the system allowing it to interoperate with FAME, PERMIS, Shibboleth, PKIs and VOMS. Access control is specified using either the GACL [GACL] or XACML [XACML] languages on a per directory basis, within which a minimum LoA requirement may be specified for accessing a specified directory on the file server. By interacting with the FAME authentication module, GridSite is now able to delegate authentication and accept users authenticated with credentials other than PKI X.509 certificates.

3.7 Other LoA ApplicationsApart from the US government and US NIH, several members of the US HE federation InCommon have considered and implemented passing the LoA value as one of the Shibboleth attributes,

4 Gap Analysis

Most of the institutions and organisations that are adopting the risk-based and LoA-linked approach to access control are going for a variant of the OMB/NIST-proposed four-level approach (with some modifications in the definition of transactions on each level and risk categories based on their particular operational environments and security needs). However, the OMB/NIST proposal has not been specified having grids in mind, and therefore there are some gaps for the adoption of this approach among grid environments.

Many grid applications achieve security through the use of a PKI (Public Key Infrastructure) or the GSI (Grid Security Infrastructure)[GSI], where entity identification and authentication are based upon X.509 credentials. Every entity (a user or a service) within such a grid has an X.509 certificate (containing all information vital to identifying the entity) and a private key associated to the public key certified in the certificate. The GSI extends the PKI by providing a single sign-on (SSO) environment and identity delegation for its non-network entities (the users). It does this by the creation of GSI proxy certificates.

A GSI proxy credential is similar to an X.509 credential, the main difference being that an end-entity certificate and its corresponding key (in the case of SSO) or a GSI proxy certificate and its key (in the case of delegation) can be used to sign subordinate GSI proxy certificates. These subordinate certificates tie the same identity (i.e. that of the owner of the original certificate) to an additional public/private key pair, thus increasing the number of certificates in the chain between the trust anchor (the CA) and the public/private key pair used during network security handshakes.

During a security handshake most relying parties that recognise GSI proxy credentials perform validation checks that are essentially the same as those performed on the X.509 credentials. However a GSI proxy key pair and certificate are generated under the control of the client alone, thus there are no CP/CPS style regulations in force. The way the certificate is stored and secured on disk, its key size and key entropy pool, etc. are not known by a relying party and consequently the value of the identity assertion is somewhat lessened when GSI proxy credentials are used. The GSI currently relies upon default behaviour of the client's security software: a proxy will usually have a short lifetime (12 hours), though it may have any lifetime (validity then being limited by the other certificates in the chain). A proxy certificate is

assumed to be stored on a local disc with appropriate file system access control attributes; however there is nothing to stop keys being copied or moved.

To cater for different authentication scenarios being deployed by grid IdPs, the IGTF has identified the following Authentication Profiles:

1. Classic X.509 PKI
2. Short Lived Credential Services (SLCS)
3. Member Integrated Certificate Service (MICS).

Each of the specified profiles can potentially have a LoA value attached to them – the question is how to calculate this value. In cases when users leverage their existing accounts with their home institutions to access the grid (e.g. SLCS, MICS), they obtain signed SAML assertions from their IdPs and subsequently a specialised body translates their identity from the assertion onto their grid identity/account and help them create proxy certificate to access the grid in the usual way. SAML assertion from the IdPs could contain LoA values to indicate the level of assurance of the original authentication method. However, the overall user's LoA can only be the lower of the LoA value of the actual authentication method and the LoA value of the proxy certificate. For on-line X.509 credential repositories, from which users can obtain their proxy certificates on-demand, the LoA value would depend on the strength with which the user authenticates when accessing their credential from the store, and the way certificates are stored and managed. Another process that may potentially influence the LoA value, and is only specific to grids, is the depth of the delegation process when parent job generates another proxy certificate for a subordinate job and so on.

References

[UK-AuthFram] Office of the e-Envoy, Authentication Framework v1.0, Dec. 2000, http://archive.cabinetoffice.gov.uk/e-envoy/resources-pdfs/$file/authentic.pdf.

[UK-RegAuth] Office of the e-Envoy, e-Government Strategy Framework Policy and Guidelines: Registration & Authentication Framework v 3.0, Sept. 2002, http://archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication/$file/Registration-AuthenticationV3.0.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.

[FIPS140-2] National Institute for Standards and Technology, FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 2001, http://csrc.nist.gov/cryptval/140-2.htm.

[FIPS199] National Institute for Standards and Technology, FIPS PUB 199: Standards for Security Categorization of Federal Information and Information, Feb. 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[SAML] SAML V2.0 OASIS standard specification set, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20.

[EAI] US Government's E-Authentication Initiative, http://www.cio.gov/eauthentication/

[EAF] US Government's E-Authentication Federation, http://www.cio.gov/eauthentication/MembershipDocuments.htm.

[EAI-News-July07] http://www.cio.gov/eauthentication/documents/FederationNewsletterJULY2007.pdf

[ERA] US Government's E-Authentication Initiative: Electronic Risk and Requirements Assessment (e-RA) Tool, http://www.cio.gov/eauthentication/era.htm.

[EA-Lab] E-Authentication Interoperability Lab Concept of Operations, http://www.cio.gov/eauthentication/documents/LabOPS.pdf.

[EA-Arch] US Government's E-Authentication Federation: The Architecture, http://www.cio.gov/eauthentication/documents/EAuthFederationArchitectureInterfaceSpec.pdf.

[LA] The Liberty Alliance, http://www.projectliberty.org.

[SAML2.0-Profiles] Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

[NIST-WB-talk] William Burr, NIST E-Authentication Guidance SP 800-63 and Biometrics, a talk at the 2004 Biometrics Consortium Conference, Sept. 2004, http://www.biometrics.org/bc2004/Presentations/Conference/2%20Tuesday%20September%2021/Tue_Ballroom%20B/2%20NIST%20Session/3%20Burr_presentation.pdf.

[eOffer] eOffer, http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=15775&noc=T.

[eRule] eRulemaking, http://fdms.gov.

[Aus-AF] Australian Government Information Management Office (AGIMO), e-Authentication Framework for Individuals Overview and Principles, June 2006, http://www.agimo.gov.au/__data/assets/pdf_file/51341/Australian_Government_e-Authentication_Framework_for_Individuals_-_Overview_and_Principles.pdf.

[Canada-LoA] Canadian Government of Columbia, Determining Authentication Levels, March 2002, http://www.mser.gov.bc.ca/privacyaccess/main/authv1.doc.

[EAP-e-com], Draft E-Authentication Partnership Policy on Levels of Assurance of Identity for Authentication of Electronic Identity Credentials v1.0, http://tscp.org/ICIDM/BBWG/AL%20Policy%20Document%20v1.0.doc.

[InCom-CAP] InCommon, Bronze and Silver Credential Assessment Profiles v0.3, June 2006, http://www.incommonfederation.org/docs/drafts/InC_Bronze_CAP_0.3.doc.

[ES-LoA] The ES-LoA project, http://www.es-loa.org

[Id] The Identity project, http://www.identity-project.info/.

[Switch-AAI] Switch Pilot Assurance Levels Definition, https://aai-wiki.switch.ch/bin/view/AAIHomeOrgs/AssuranceLevels.

[TF-EMC2-min] Minutes from the 7th TF-EMC2 meeting, Malaga, Spain, Oct. 2006, http://www.terena.org/activities/tf-emc2/meetings/7/emc2-minutesv0.4.pdf.

[DK-AAI-FedAgr]DK-AAI Federation Draft Agreement, Feb. 2007, http://www.dk-aai.dk/2007_02_01_dk-aai_agreement-draft_ENG.pdf.

[AAF] The Australian Access Federation, http://www.aaf.edu.au/.

[eSec] eSecurity Framework Project, University of Queensland, Australia, http://www.esecurity.edu.au/.

[MAMS] Meta Access Management System, Australian Testbed HE federation, http://www.federation.org.au/FedManager/jsp/index.jsp.

[FTRA88] Financial Transaction Reports Act 1988, February 2004, http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200403474?OpenDocument.

[FTRR90] Financial Transaction Reports Regulations 1990, Office of Legislative Drafting, Australia, March 2003, https://www.imolin.org/pdf/imolin/Astlft90.pdf.

[HAKA] HAKA, Finnish HE Federation, http://www.csc.fi/english/institutions/haka.

[Feide] Feide, Norwegian HE Federation, http://rnd.feide.no/.

[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.

[HAKA-slides] Federations round table: Haka Federation of Finland, http://www.terena.org/activities/eurocamp/april07/slides/eurocamp_helsinki_haka.ppt.

[GSI] Grid Security Infrastructure, http://www.globus.org/security/overview.html.

[IGTF-Class] EUGridPMA, Authentication Profile for Classic X.509 Public Key Certification Authorities with Secured Architecture v4.1, Dec. 2006, http://eugridpma.org/guidelines/IGTF-AP-classic-4-1.pdf.

[IGTF-SLCS] TAGPMA, Authentication Profile for Short Lived Credential Services X.509 Public Key Certification Authorities with Secured Architecture v1.1, Nov. 2006, http://eugridpma.org/guidelines/SLCS/IGTF-AP-SLCS-20051115-1-1.pdf.

[IGTF-MICS] TAGPMA, Profile for Member Integrated X.509 Credential Services (MICS) with Secured Infrastructure v1.0, July 2007, http://www.tagpma.org/files/IGTF-AP-MICS-1.0.pdf.

[OGF] Open Grid Forum, http://www.ogf.org/.

[ISO-LoA] ISO/IEC JTC 1/SC 27, New Work Item Proposal on Authentication assurance, Dec. 2006, http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/755080/1054034/2541793/JTC001-N-8446.pdf?nodeid=6023594&vernum=0.

[mace-dir] MACE-Dir mailing list, https://mail.internet2.edu/wws/info/mace-dir.

[SAML-del] http://shibboleth.internet2.edu/docs/draft-cantor-saml-sso-delegation-01.pdf.

[Shibboleth] The Shibboleth Project, Internet 2, http://shibboleth.internet2.edu/.

[FAME-PERMIS] The FAME-PERMIS project, http://www.fame-permis.org.

[SHEBANGS] The SHEBANGS project, http://www.rcs.manchester.ac.uk/research/shebangs.

[GridSite] The GridSite Project, http://www.gridsite.org/.

[GACL] The GridSite Grid Access Control Language, http://www.gridsite.org/wiki/GACL.

[XACML] The XACML Committee, http://www.oasis-open.org/committees/xacml/.