

The ES-LoA Project
WP1 Deliverable

*Using LoA to Achieve Risk-Based Access Control:
A Study Report*

May 2007

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

Executive Summary

Robust electronic authentication capable of reliably identifying remote entities (human users or software components) with a certain level of assurance in authentication strength is an important prerequisite to facilitate effective user authorisation and fine-grained access control in distributed systems. In a Federated Access Management environment, users are referred back to their home or affiliated institutions (playing the role of identity providers) for authentication, and subsequently gain access to resources provided by other federation members (i.e. service providers) through the use of attributes asserted by their respective IdPs.

The separation of duties between identity providers (IdPs) and service providers (SPs) means that SPs no longer have control over the identity vetting procedures and authentication processes used to establish a user's identity. IdPs may employ dissimilar identity management policies, cross-checking procedures and authentication mechanisms, resulting in a spectrum of levels among which users are identified. More and more diverse resources are expected to join the federated environment, and they may have varying levels of sensitivity depending on their values and severity of consequences in an event of a security breach. SPs managing more sensitive resources may require a stronger form of user identification, while others having less valuable resources may not wish to subject their users to unnecessarily burdensome procedures. Increasing the level of confidence in identifying users may, on the one hand, enable more security conscious services to join a federation, but, on the other hand, inflate running costs and create a less user-friendly environment resulting in a reluctance of some providers of lower value resources to join the federation. Thus, there is a need for a more fine-grained approach to access control to replace the existing binary (grant-or-deny) solution where access control is achieved using the 'one-method-fits-all' approach regardless of the resource sensitivity and risk levels.

One way to achieve the vision of fine-grained access control is to quantify the quality or strength of an authentication process in terms of an authentication Level of Assurance (LoA), and use the LoA value as a parameter for authorisation decision making. With this approach, assurance levels and costs in identity vetting and entity authentication can be linked to the values of the assets or risk levels in the accessed environment. The higher the value or sensitivity of the assets, the more formal and stricter the identity vetting process and, thus, a higher level of assurance in the underlying authentication service will be needed. Conversely, for lower value resources, a less stringent authentication procedure may be sufficient. Different LoA values imply different types of authentication tokens being issued to users, and different tokens are required at service access time for controlling the access to resources in different sensitivity groups. Using this LoA-based access control solution will not only allow us to achieve fine-grained access control in federated virtual environments, but also allow us to strike a fine balance between the level of security protections and the level of costs incurred in federated access management.

This document reports the study of current worldwide efforts on defining LoAs and using them to achieve fine-grained access control to digital resources. The document summarises current LoA standards and specifications, in particular the work done by the US government Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) on behalf of the US government. Taking into account these international developments and efforts, we make proposals with regard to standard definitions of LoA for use within the UK education and research community.

Table of Contents

Executive Summary	2
Table of Contents	3
List of Figures	4
List of Tables	4
Acknowledgements	5
Glossary of Terms and Acronyms	6
1 Introduction	7
2 Existing Efforts in Defining and Using LoAs	7
2.1 The UK Government Initiative	7
2.2 The US Government Initiative	9
2.2.1 OMB and NIST.....	9
2.2.2 EAI	14
2.2.3 NIH	14
2.3 The European Government Initiative	14
2.4 The Australian Government Initiative	15
2.5 The Canadian Government Initiative.....	15
2.6 Industrial Sector: Liberty Alliance	16
2.7 Private Sector: E-Authentication Partnership.....	16
2.8 The US HE Federation	18
2.9 Other Worldwide HE Federations.....	18
2.9.1 UK	18
2.9.2 Switzerland.....	19
2.9.3 Denmark.....	19
2.9.4 Australia and New Zealand.....	19
2.9.5 Finland, Norway, Sweden, France.....	19
2.10 The Grid Community	20
2.11 ISO/IEC	20
3 Our Observations and Remarks	21
3.1 On LoA Definition	21
3.2 On LoA Implementation.....	21
3.3 On LoAs in Federated and Grid Infrastructures	23
4 Conclusions	24
References	25

List of Figures

Figure 1. Components influencing authentication assurance levels	23
--	----

List of Tables

Table 1: Likely values for authentication and registration levels	9
Table 2: Maximum potential impact profile mapped to assurance levels	10
Table 3: Token types allowed for each LoA	12
Table 4: Protections that protocols should provide at each LoA	12
Table 5: Authentication protocol types allowed at each LoA	13
Table 6: Additional requirements for protocols at each LoA	13
Table 7: Overview of transaction types, risks and identity assurance per LoA level	22
Table 8: LoA distribution for harm's impact/likelihood profiles	22

Acknowledgements

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

Glossary of Terms and Acronyms

Terms

Grid	A Grid is the technology that enables resource virtualization, on-demand provisioning, and service (resource) sharing among organizations through the use of a set of open standards and protocols. The Grid technology enables users to gain access to applications, data, processing power, storage capacity and a vast array of other computing resources over the Internet.
LoA	An authentication Level of Assurance (LoA) is used to quantify the level of certainty in an authentication process, with which a verifying party can be assured of the identity of an authenticated entity.
Shibboleth	Shibboleth is an open-source, standards and Web-based inter-institutional architecture that enables federated resource sharing and identity management. In the Shibboleth architecture, a user's authentication is performed by the user's home institution or identity provider (IdP) and the authorisation is managed by a resource or service provider (SP) based on the user's attributes asserted by the IdP using Shibboleth protocols.
SSO	Single Sign-On (SSO) is a specialised form of authentication which enables a user to authenticate once and subsequently gain access to resources to different systems at multiple sites during one access session.

Acronyms

CA	Certification Authority
CSP	Credential Service Provider
GSA	General Services Administration
HE	Higher Education
IdP	Identity provider
LoA	Level of Assurance
OMB	US Federal Government Office of Management and Budget
RA	Registration Authority
SAML	Security Assertions Markup Language
SP	Service provider
NIST	The US National Institute of Standards and Technology

1 Introduction

Electronic authentication is a process by which a relying party establishes the identity of an entity, e.g. a person or a software component, when the entity requests access its services or performs an electronic transaction with the relying party. Authentication is the first line of defence of any information system. It is typically immediately followed by authorisation, the goal of which is to determine the identified entity's access rights or permissions in the system accessed. As more and more diverse resources (including data, applications and services) are being incorporated and delivered electronically in the federated digital world, service providers will increasingly need to consider the sensitivity levels of resources when making access control decisions. A service provider may specify a minimum level of authentication assurance (LoA) and require that the access is only granted should the assurance level derived in an authentication instance satisfy this minimum value. This LoA-based fine-grained access control approach allows service providers to classify their resources into different groups each with a different sensitivity/risk level, map this risk level to an appropriate authentication LoA, and to filter access to these resources according to the confidence in identifying a remote entity in addition to the usual access control attributes such as subjects' identities, their roles, operations and objects.

The authentication LoA represents the degree of confidence in an electronic identity of a claimant presented to a verifier (e.g. a relying party) by means of a credential. It reflects the degree of confidence in identifying an entity whom 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. The LoA value is affected by all the steps directly or indirectly involved in an authentication process, namely, identity proofing, credential issuance and remote authentication using the credential, which, in turn, depends on the types and cryptographic strengths of authentication credentials and protocols used, how and where the authentication credentials are stored, and how and where events and records are logged and audited. In a federated environment, the factors also include credential delegation, the depth of delegation, the strength and reliability of assertion messages, and where and how users' attributes are managed.

Access to resources with varying levels of sensitivity should be governed by varying levels of assurance in the requester's asserted identity. The required levels of assurance are determined by the levels of risks and the severity of consequences that may arise due to an authentication error or misappropriation of credentials: the more severe the consequences or higher the risk experienced by an SP, the higher level of assurance in an asserted identity will be required from the requester to access the resource managed by the SP. For example, when a client reads or downloads publicly available information from an SP's Web site, a zero or a low level of assurance in identifying the client's identity may be required. On the other hand, accessing patients electronic health records, that are associated with a high sensitivity level, would require a higher assurance level as determined by very stringent security checks and verification of the client's identity.

This document reports our study of national and international efforts and activities in defining authentication levels of assurance and specifying requirements for the identified levels. Through this study and community consultation, we aim to make proposals with regard to definitions of LoAs for the use within the UK education and research community.

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]. The idea was then followed-up by the US Government, the US industrial and private (e-commerce) sectors, the US High Education (HE) Federation, the US National Institutes of Health (NIH), and the international grid community, as well as governments and HE federations in several other countries in the world.

2.1 The UK Government Initiative

In 2000, as part of the initiative for modernising government by moving towards the electronic delivery of its 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 gives the 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*.** Misappropriation of identity or repudiation of transaction would not result in inconvenience to the identity holder, risk to their personal safety, financial loss or distress to any party. An authentication service is categorised as Level 0 if no trust is put in the identities claimed by clients.
- **Level 1: *Personal transactions*.** Mistaken identity would have a minor impact to one or more of the involved parties as information involved is personal but non-sensitive. Misappropriation of identity or repudiation of transaction would not result in major inconvenience to the identity holder, risk to their personal safety, financial loss or distress to any party. For a Level 1 authentication service, users will identify themselves by presentation of a credential, which can be a username, and demonstrate the knowledge of a related secret, which can be a password.
- **Level 2: *Transactions with financial or statutory consequence*.** 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. For a Level 2 authentication service, users will 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. 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*.** 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 authentication service, users will 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. 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 in the guidelines.

2.2 The US Government Initiative

2.2.1 OMB and NIST

While the UK government guidelines define LoAs 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 measured in terms of potential impacts of authentication errors and the likelihood of their occurrence.

The OMB-defined four assurance levels are as follows:

- **Level 1:** Little or no (minimal) confidence in the asserted identity's validity for transactions requiring little or no confidence in the claimed identity.
- **Level 2:** Some (moderate) confidence in the asserted identity's validity for transactions requiring some confidence that the claimed identity is accurate.
- **Level 3:** High (substantial) confidence in the asserted identity's validity for transactions requiring high confidence in the user's claimed identity.
- **Level 4:** Very high confidence in the asserted identity's validity for transactions requiring very high confidence in the user's claimed identity.

According to the OMB, a risk from an authentication error can be expressed as a function of two factors: (1) potential *harm* or *impact* and (2) *likelihood* of its occurrence. Risk impacts of e-authentication errors are classified into the following impact 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 are mapped to the four LoA levels using an impact profile, as shown in Table 2. To determine the minimum required LoA for a given transaction or resource, a service provider should perform a risk assessment to identify all possible risks, and, for each of the risks, create an impact profile by assigning impact values to each of the impact categories that influence the risk based on the consequences of authentication error to the transaction or the business process. The minimum LoA for a particular risk is then identified by having the impact profile meet or exceed the potential impact for every impact category identified for that risk.

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

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

* Source [OMB-M0404]

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

- (1) Conduct a risk assessment of each transactions of an e-Government system in terms of potential impacts and likelihood of their occurrence.
- (2) Map the identified risks to an appropriate assurance level using Table 2.
- (3) Select the necessary technology to achieve the required LoA based on the NIST 'Electronic Authentication Guideline' [NIST-SP800-63].
- (4) Validate that the implemented system has achieved the required LoA.
- (5) Periodically reassess the system to determine that the technology applied corresponds to the refreshed requirements.

The OMB Memorandum 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. According to the OMB, the steps influencing an authentication process are:

- 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.

To satisfy each of the assurance levels as specified by the OMB Memorandum, appropriate authentication technologies should be identified, implemented and regularly assessed. The complementary document from the US National Institute of Standards and Technology (NIST), 'NIST

SP 800-63: 'Electronic Authentication Guideline' [NIST-SP800-63], identifies the necessary technologies and provides guidance to implement the OMB's levels of authentication assurance. In addition, NIST also maintains two related standards: NIST FIPS 140-2 [FIPS140-2] and NIST FIPS PUB 199 [FIPS199]. FIPS 140-2 specifies security requirements for the design and implementation of cryptographic modules, and classifies such modules into security levels according to their strengths. FIPS PUB 199 provides security categorisation of federal information and information systems to help government agencies with risk analysis and assessment tasks.

The NIST's E-Authentication Guideline is a comprehensive document covering all the stages of an authentication process as outlined in (i)-(vii) above by the OMB. It states specific technical requirements for each of the four Levels of Assurance in the following areas:

- (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**: Names are not verified; names are always assumed to be pseudonyms. Anonymous credentials are allowed. There are no LoA-specific requirements at this level.
- **Level 2**: 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**: Real names must be verified. In-person or remote registration is permitted.
- **Level 4**: Real names must be verified. Only in-person registration is permitted.

(2) *Credential management*: protection 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.

These token types along with assurance levels they can be mapped to are summarised in Table 3.

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) *Authentication protocols:* An authentication protocol is defined as a sequence of messages exchanged between a claimant and a verifier, which enables the verifier to verify that the claimant is indeed in control of a valid token so as to establish their identity. Protocols are classified into LoA categories according to specific attacks and threats that they are resistant against, as shown in Tables 4 and 5. The 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*: Assertion mechanisms are used to communicate the results of a remote authentication to a relying party (e.g. a service provider) by a verifier (i.e. an identity provider). Assertions are particularly important in environments where the tasks of authentication and authorisation are performed by different organisational or administrative entities, in which case the user authenticates to one entity (usually the user's home organisation or identity provider), and the user's attribute assertions are then sent to the other entity (usually a service provider), and authorisation and access control are performed by the service provider based upon the assertions by the identity provider. Examples of assertions include signed SAML [SAML] assertions and cookies or unsigned assertions from a trusted directory or database. A relying party (i.e. service provider) trusts an assertion based on the source, the time of creation and attributes associated with the claimant. NIST Electronic Authentication Guideline states 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.

Note that NIST levels of assurance are inclusive in the sense that qualification for any of the higher levels requires compliance with all the criteria defined for the levels below.

2.2.2 EAI

The US government's E-Authentication Initiative (EAI) [EAI] aims to provide a trustworthy and secure standards-based authentication architecture to support US federal e-government applications. The main objective is to provide a uniform process for establishing identities electronically so as to eliminate the need for each application to develop its own authentication solution. It is also aimed at enabling citizens and businesses to use non-government issued credentials to conduct transactions with the government.

The E-Authentication Federation (EAF) [EAF] has been part of the EAI established to help the US Government agencies to form a trust network between the agency applications (i.e. service providers) and credential service providers (i.e. identity providers). As of July 2007, the EAF has 46 members [EAI-News-July07].

The EAI implements, and is fully compliant with, the OMB/NIST e-authentication guidelines, and adopts the risk-based approach to authentication and access control. With this approach, as discussed above, the risks associated with user authentication are first identified, and then, based on the risk assessment, authentication requirements are defined in terms of LoAs. To help with the risk assessment, the EAI has produced the Electronic Risk and Requirements Assessment (E-RA) tool [ERA], which is fully comply with the OMB and NIST guidelines. The EAI 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 List [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..

Recently (in May 2007), the EAI has revised its architecture [EA-Arch] to incorporate the SAML v2.0 specification to better meet the authentication needs of federal agencies. They have adopted the 'SAML 2.0 Single Sign-On (SSO) Profile Using HTTP POST' [SAML2.0-Profiles] in the ASC (Authentication Service Component) of the architecture. The ASC functions in the similar way as the Shibboleth: SAML messages that are exchanged between the 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. According to the EAF rules, the LoA value is a compulsory attribute that must be present whenever a SAML authentication assertion is issued. 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 also adopted the OMB/NIST LoA approach, and, together with the US InCommon HE federation (see section 2.7), 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 recognised across the EU and aims to build an European eIDM (Electronic Identity Management) framework by 2010 based on interoperability and mutual recognition of national eIDM. 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 in order to boost confidence in on-line transactions involving government bodies. The outcome from this initiative, the Australian Government's e-Authentication Framework (AGAF) [Aus-AF], aims to enhance trust in government on-line transactions by mapping the level of risks involved in a transaction to an appropriate e-authentication mechanism. It provides guidance for: (1) government, (2) businesses and (3) individuals. It recognises that different transactions may need different e-authentication mechanisms depending on the degree of risk involved, and adopts the four risk and assurance levels as defined by the 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.

The identified risk categories follow closely those specified by the UK and US governments. In detail,

For businesses:

- 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.

For government:

- 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.

The above risk categories are not intended to be prescriptive; organisations are free to modify the lists to suit their particular circumstances.

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 in terms of authentication requirements for particular types of transactions are defined, and reference profiles for each of the trust levels are also specified. The proposed trust levels 0 – 3 are mapped to four different groups of transactions:

- **Level 0:** *Anonymous transactions* - access provided for transactions that do not require a person to be identified or transactions which require protection of a person's identity.
- **Level 1:** *Pseudonymous transactions* - access provided for transactions that do not require a person to be identified but do require means for further contact to deliver a product or service. For example, a note from someperson@internet.ca cannot be readily translated into an

individual's name, but it may be sufficient to request information, to provide some services, or an on-going follow up.

- **Level 2: Identified transactions** - access provided for transactions that require that a person be specifically identified. The nature of the transaction may require confirmation of a person's identity (e.g. name, address, birth date, etc.) or data linking the person to a transaction (e.g. invoice number, personal health number, etc.).
- **Level 3: Verified transactions** - access provided for transactions that require the person to be specifically identified and verification of the integrity of the data exchanged, and the creation of sufficient evidence to indicate that the person agreed to be bound by the transaction. For example, a digitally signed note provides sufficient evidence that a specific person intended to conduct a transaction.

Once the 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. Ideally, the level of trust assigned to a business process based on the Authentication Profile should adequately address these concerns. However, if the risks and consequences of a transaction do not appear to correlate to the identified level of trust, the decisions made in the Authentication Profile should be re-evaluated. The identified categories of risks are similar to those specified by the governments of UK, US and Australia:

- 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) is driving the work within the Liberty Alliance of fostering the adoption of identity and authentication assurance services. The IAEG's goal is to achieve interoperability of 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 (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 will develop a global standard framework for validating trusted identity providers and certifying them as compliant to common policies and business rules and help to avoid any confusion about the meaning and substance of LoA value delivered.

The work of IAEG will begin by consolidating the Trust Framework of the EAP (Electronic Authentication Partnership, see section 2.6) [EAP], the US government's E-Authentication Federation (EAF, see section 2.2.2) and other industry contributions. The produced standard will 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 identity federations. Its goal is to foster inter-federation on a global scale. To accomplish this goal, the group will form the Liberty Trust Framework (LTF) that will encompass a set of concepts such as business rules, procedural and technical trust criteria for identity providers, and assessment methodologies for determining conformance to trust criteria. The LTF will be based on the EAP's Trust Framework, the EAF's Credential Assessment Framework, and input from both public and private industry stakeholders with relevant experience and contributions to this effort.

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]. 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.

In 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 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 that employ Web browsers on the client side. 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 credentials. This is why InCommon have only concentrated on defining profiles compliant with US Gov/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 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 - even though they have not officially adopted them yet. It is more cost-effective for the InCommon federation to be in partnership with the EAF and achieve inter-federation interoperability, than to require its members to also join the EAF.

Though InCommon currently recognises only password-based authentication systems for 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 is 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, drivers 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 The Grid Community

Many grid applications achieve security through the use of the GSI (Grid Security Infrastructure)[GSI], in which entity identification and authentication are based upon PKI credentials. Every grid entity (a user or a service) is expected to have a PKI credential consisted of a private key and public-key certificate (which contains information vital to identifying the entity) and a private key associated to the public key certified in the certificate. The GSI also provides a delegation capability through the use of proxy credentials. A proxy credential consists of a proxy certificate (with a new proxy public key in it) and a related proxy private key. It is signed by its owner rather than by a CA. A proxy credential has a much shorter lifetime than the original long-term PKI credential from which it is spawned (typically shorter than 24 hours). It is usually generated to perform a specific task or to execute a specific job on a grid. The use of proxy credentials allows single sign-on (SSO) when a job involves the use of services provided by multiple Grid entities – the user only has to key in the pass-phrase for his (original) private key once (during the proxy lifetime), i.e. at the time when the proxy key pair is generated. Thereafter, the proxy credential is used to authenticate the user (i.e. the user's job). In the GSI environment, a proxy credential can further be used to generate other proxy credentials thus achieving the so called *n*-tier delegation.

The IGTF (International Grid Trust Federation) has published two Authentication Profiles - the 'Authentication Profile for Classic X.509 Public Key Certification Authorities' [IGTF-Class] and the 'Authentication Profile for Short Lived Credential Services (SLCS) X.509 Public Key Certification Authorities' [IGTF-SLCS]. The Classic profile describes the comprehensive security requirements and operation procedures for CAs offering traditional X.509 PKI services and issuance of long-term certificates. The SLCS profile describes the similar requirements for the X.509 CAs that issue short-term (e.g. proxy) credentials to end-users, who themselves control the key pair. The SLCS allows a user's identity within a local organisation, once confirmed by means of the local organisation's authentication system, to be translated onto the user's grid identity. The SLCS can be used in conjunction with a number of local authentication systems, which do not have to be certificate-based. In the case where a user does not possess a grid credential, the user may authenticate to a local authentication system, and obtain a short-lived certificate-based grid credential. Due to this 2-tier authentication (to the local authentication system using original credential and then to a grid service using grid credential), any LoA definition in the SLCS context would have to take into account, and to evaluate the LoA of, both authentication processes collectively.

The two Authentication Profiles defined by the IGTF define a comprehensive set of rules for the CAs operating the issuance of credentials, covering aspects of identity vetting, certificate expiration, renewal and re-keying, operational requirements (CA's key size, hardware requirements, CRLs, revocation procedures, etc.), the physical security of the CA's site, audit and disaster recovery procedures. They also define two different types of credentials - the long-term (traditional) and the short-lived one, both of which can be further used for delegation and creation of another short-term (proxy) credentials. With some modifications, the rules and credentials specified by the Profiles can be mapped onto the NIST LoA definitions. Furthermore, by their very nature, proxy credentials can only be stored in soft tokens, and therefore cannot achieve NIST Level 4. In addition, the act of delegation and *n*-tier authentication introduces certain implications to the derivation of LoA values, which need further examination and investigation. In addition, the manner in which proxy certificates are stored and managed (locally or remotely) should also be looked into.

2.11 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) may be measured. Relying on the work previously done by the US Government and NIST, the committee plans to establish metrics for quantifying risks in an authentication process. The criteria for the metrics 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.).

3 Our Observations and Remarks

3.1 On LoA Definition

To date, the OMB/NIST LoA specification remains the most comprehensive set of guidelines for implementing authentication assurance levels. It is also the most widely used; a number of worldwide sectors or bodies have either adopted these guidelines or have made their proposals compatible with the OMB/NIST LoA specification. These sectors and bodies include governments of Australia, Canada and Europe, HE federations of the US [inCommon], Australia and New Zealand [AAF], Switzerland [Switch], Finland [HAKA], Norway [Feide], Sweden [Swami], Denmark [DK-AAI] and France [CRU], the US National Institutes of Health [NIH], the US government's Electronic Authentication Federation [EAF] and industry-led Electronic Authentication Partnership [EAP], global body Liberty Alliance [LA], the US health sector NIH, etc.

The OMB/NIST 4-level approach has already been deployed by the US government's EAI and EAF (a partnership between the US federal agencies and private sector organisations). A subset of the defined levels has been adopted by the US HE InCommon federation in their Bronze and Silver Profiles (equivalent to NIST Level 1 and 2 respectively) in order to achieve inter-federation interoperability with the EAF. The US National Institutes of Health (NIH) together with the US InCommon HE federation are deploying an inter-federation pilot that will allow users from the HE sector to access NIH resources based on their authentication LoAs.

3.2 On LoA Implementation

In order to implement a system that is compliant with the OMB/NIST LoA guidelines, institutions should broadly perform the following two steps:

- (1) Service providers (relying parties) should carry out a risk assessment of the transactions, resources and services that are subject to access by external or home users. Based upon the assessment, LoA requirements are determined and appropriate LoA levels are identified. Service providers are free to define their own risk and harm categories during the risk assessment stage (i.e. they do not have to use the categories defined by the NIST and can specify categories to suit their particular operational environments and security needs) and have their own mappings to the four LoA levels.
- (2) Identity providers (credential service providers) should implement, manage and execute their authentication services according to the LoA requirements, e.g. as defined in the NIST 'Guidelines on E-Authentication', if they are to be accredited to a certain authentication assurance level. Once a LoA level is accredited to an IdP, the IdP may be allowed to provide authentication services and issue authentication assertions, with an assurance level up to (i.e. not higher than) the accredited LoA. In addition, the IdP should be regularly audited and assessed to make sure that the IdP's operational procedures and processes satisfy the requirements defined for that LoA level. It is worth pointing out that this accredited LoA refers to the maximum LoA level at which an IdP would be allowed to operate. For example, if an IdP is accredited with a LoA value of 2, then the IdP should be allowed to authenticate users at LoA levels, 0, 1, and 2. Of course, in this case, the IdP is expected to satisfy all the operational procedures and LoA implementation requirements as defined for Level 2, which by default are inclusive of those for Level 1 and 0.

In the following, we look into the above two steps in more detail.

(1) Service providers' tasks

According to the OMB/NIST guidelines, SPs should classify their transactions into four categories - transactions that experience *minimal*, *moderate*, *high* and *very high* risk and therefore respectively require *minimal*, *moderate*, *high* and *very high* requirements for authentication assurance (see Table 7 below).

Table 7. Overview of transaction types, risks and identity assurance per LoA level

	LoA profiles for transactions			
Level of Assurance	Level 1	Level 2	Level 3	Level 4
Risk vs. transaction type	Minimal risk (informal transactions)	Moderate risk (personal transactions)	High risk (transactions with financial or statutory consequences)	Very high risk (transactions with high financial, statutory or safety consequences)
Required identity assurance	Little or no assurance in identity	Moderate assurance in identity	High assurance in identity	Very high assurance in identity
Identity assurance vs. transaction type	Anonymous transactions	Pseudo-anonymous (pseudonym with real identity traceable)	Identified transactions (real identity established)	Verified transactions (real identity established and transaction signed)

In order to perform the classification of their transactions, institutions should carry out a risk assessment of all transactions available to users electronically. Risk can be defined and assessed by considering the following harm categories:

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

Institutions are free to modify the above harm categories to suit their business requirements.

Each of the identified harm categories should be evaluated along two axes – i.e. in terms of *impact* and *likelihood* of its occurrence. During this risk assessment, the values of *low*, *moderate* and *high* is assigned to each of the two properties for every identified harm category. The following table can be used to determine which Level of Assurance should be used to mitigate the risks caused by the given harm.

Table 8: LoA distribution for harm's impact/likelihood profiles

HARM	Impact		
Likelihood	<i>Low</i>	<i>Moderate</i>	<i>High</i>
<i>Low</i>	Level 1	Level 2	Level 3
<i>Moderate</i>	Level 2	Level 3	Level 3-4
<i>High</i>	Level 3	Level 3-4	Level 4

During the risk assessment, this process should be repeated for every identified harm category. Institutions are free to define their own distributions of LoAs along the harm's impact and likelihood axes, and are free to use more fine-grained values for impact and likelihood (for instance, instead of using values *low*, *moderate* and *high*, values such as *low*, *moderate*, *high* and *very high* can be used).

When analysing a potential risk, all possible direct and indirect harms should be examined (based on the above harm categories), and for each of the harm, a LoA should be determined based on the impact/likelihood profile defined for the harm. If a single risk can cause harm in more than one category – the highest LoA of all categories analysed must be taken. For example, if an identified risk requires the use of Level 2 to mitigate the potential harm to the organisation's reputation and Level 3

to mitigate its financial loss impact, then to counter this risk the overall assurance Level 3 should be chosen for the system to authenticate its users.

(2) Identity providers' tasks

Once the required LoA is determined through the risk assessment stage as described above, then the next step is to determine how the required assurance level can be achieved by the underlying authentication system. This second step involves the consideration of several factors:

- The underpinning registration process should follow appropriate procedures, in terms of:
 - Registration and identity proofing
 - Credential management (credential issuance, delivery, storage, maintenance, revocation)
 - Audit and record keeping
- Credentials with appropriate strengths should be used, based on:
 - Type of a token where a cryptographic key is stored
 - Soft, hard or OTP device
 - The use of a password, PIN or biometric to unlock tokens at Levels 3 and 4
 - The length of a cryptographic key
 - Password entropy and resistance to known password-cracking attacks
 - Password alphabet and forcing the use of special characters
 - Password updating frequency
 - Maximum number of unsuccessful trials allowed
 - Account lockouts for a predefined time period after maximum number of unsuccessful trials
- Appropriate authentication protocols should be chosen, based on:
 - Security of the protocol (in terms of which attacks it can counter, what information is revealed to verifier, etc.)
 - The use of authentication assertions, how they are conveyed to relying parties and the authenticated session validity duration

Figure 1 below depicts the factors that should be considered by IdPs when attempting to implement a system that meets a certain LoA. The principle of the 'weakest link' applies – the LoA of the weakest point in a chain determines the overall LoA of the system.

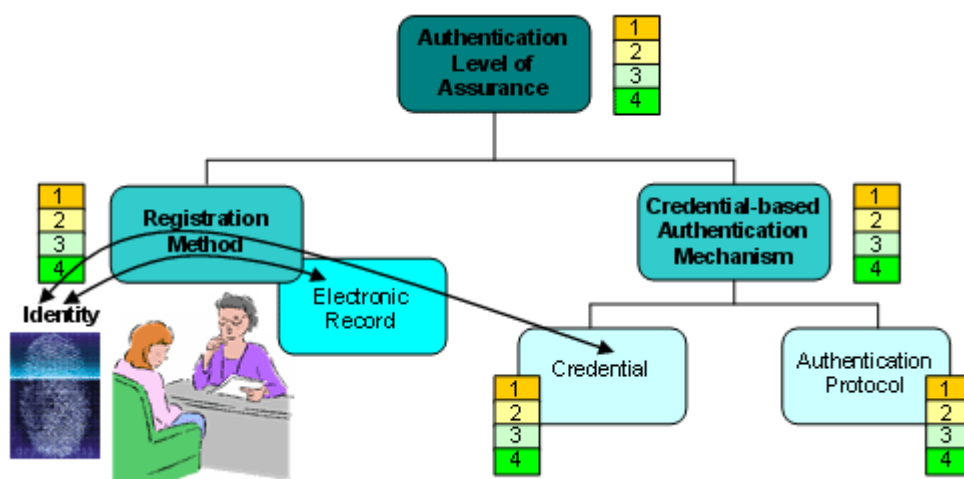


Figure 1. Components influencing authentication assurance levels

3.3 On LoAs in Federated and Grid Infrastructures

In Shibboleth-based federations, an identity provider uses an attribute assertion message to convey the identity information and attributes of an authenticated user to a SP which then makes an access control decision. The Shibboleth attribute assertion messages are implemented using the OASIS SAML standard, and have a short lifetime that falls under the NIST-imposed restrictions on the lifetime of assertion messages. That is, using Shibboleth assertions, Levels 1, 2 and 3 are achievable.

Since the use of attribute assertions are prohibited at Level 4 according to the NIST specification (only direct authentication with a service provider is allowed at Level 4), this Level cannot be achieved with the current Shibboleth technology. However, it is widely accepted that Levels 1-3 may be sufficient to cater for the access requirements of the HE community, which largely uses usernames and passwords (i.e. up to Level 2 authentication) in most cases.

SAML v2.0 seems to be the technology of choice when it comes to conveying user's confirmed identity and attributes. There are two approaches based on SAML that can be utilised for this purpose: (1) LoA information represented as a SAML attribute or (2) embedded in a SAML Authentication Context. Both of the approaches may have their pros and cons. Authentication Contexts are more complicated and difficult to create and understand but are more appropriate to convey additional information about authentication process (and not just single value) that might be useful for service providers for their access control decision making. From the discussions seen on the various mailing lists, it appears that both options may be supported in the future and the decision as for which one should be used is left to the federation. In any case, both will be able to convey the LoA value and the LoA regime defining LoA specification/standard/profile/vocabulary the LoA value conforms to.

For example, the US InCommon HE federation might specify the following two URIs as globally unique identifiers for their Silver and Bronze Authentication Profiles:

```
urn:mace:incommon:loa:bronze.
urn:mace:incommon:loa:silver.
```

The US government may define similar identifiers as:

```
urn:usgov:nist:loa:1
urn:usgov:nist:loa:2.
```

The US NIH may decide to use identifiers:

```
urn:mace:dir:constant:nist-sp-800-63:1
urn:mace:dir:constant:nist-sp-800-63:2
```

The above identifiers contain both the LoA value (bronze, silver, 1, or 2) as well as specifications (InCommon or NIST) to which the values conform to. The identifiers may then be used in either Authentication Context elements or in simple attribute assertions with the same semantics. The most important thing then is to define the interoperability mappings between different specifications, e.g. the InCommon, NIH and NIST profiles. For example, urn:mace:incommon:loa:silver matches urn:usgov:nist:loa:2 which in turn matches urn:mace:dir:constant:nist-sp-800-63:2.

There is a need to establish a governing body at a federation level to evaluate and accredit federation members (most notably identity providers) with certain assurance levels upon inspecting their authentication systems, policies, practices and operational procedures. Similar authorities have already been established in the US (e.g. the US federal Interoperability Lab). One way of doing this may be to establish a PKI hierarchy of 'levelled' CAs, where each CA would have its own associated LoA, and that CA could issue accreditations to IdP in the form of "*Operates/Accredited at NIST Level x*", upon inspection of the IdP's practices. An IdP with a NIST Level x can then issue authentication assertions with an assurance Level not higher than x.

Grid community does not have an official standing on the LoA issue yet, but the LoA-RG [LoA-RG] has been established under the OGF [OGF] to address this problem and identify potential gaps in using the NIST standard for the grid context. The NIST specification in particular does not address the issue of delegation of (a subset) of an authenticated entity's rights, which is the main concept in grid environments. The NIST specification only concerns with direct user-to-system authentication.

4 Conclusions

There is significant interest across various communities, most notably governments and HE, in using levels of authentication assurance as a qualifier of the strength of an authentication process and then feeding it back to authorisation process in order to achieve risk-based access control to resources with varying levels of required security protections. LoAs are assigned to transactions or resources based on the risks of unauthorised use due to authentication errors, which are identified during a risk assessment phase carried out by service providers. LoA values are then translated into detailed

authentication requirements that should be satisfied by identity providers through the implementation of technical solutions and operational procedures.

The most notable LoA specification is the one defined and implemented by the US Government (through NIST, OMB and EAI). The specification encompasses comprehensive guidelines in two areas: the guidelines for agencies to conduct the risk assessment of their systems and to map the identified risks to an appropriate level of assurance (OMB), and technical guidelines on how to implement the required level of assurance (NIST). The OMB/NIST guidelines were fairly well received by network security professionals and cryptographers [NIST-WB-talk], and a new version is currently being drafted for release sometime in 2007.

The E-Authentication Initiative (EAI) has successfully deployed the approach through its E-Authentication Federation (EAF), and there are two operational deployments of the solution – eRulemaking [eRule] and eOffer [eOffer]. They have established an Interoperability Lab to test the systems' conformance to the proposed standards. The EAF has struck inter-federation collaborations with industry (via Liberty Alliance and E-Authentication Partnership), US National Institutes of Health (NIH pilot) and US HE InCommon federation. Thus, there is already a critical amount of work done and critical mass of institutions that have adopted, or are planning to adopt, the OMB/NIST approach. For this reason, it may be fruitful for the UK HE federation to go along the same road from the standpoint of interoperability with other federations, provided that the OMB/NIST guidelines satisfy the authentication requirements of the UK HE community (as to be confirmed through our consultation with the UK HE community).

In federated infrastructures (such as Shibboleth) where an identity provider uses an attribute assertion message to convey the confirmed identity and attributes of an authenticated user to a service provider or relying party, it is not possible to achieve the highest OMB/NIST Level 4. The reason for this is that attribute assertions are simply not allowed at this level, and the end user must authenticate directly to the relying party using a credential stored on a hard token that is activated through the use of a password or biometrics. More work is required to investigate whether there is a need for Level 4 in federated environments, and how it can be achieved using Shibboleth technology.

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](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](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.

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

[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.

[SAML] E. Maler et al., Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML), OASIS Document ID oasis-sstc-saml-core-1.1, Sept. 2003, <http://www.oasis-open.org/committees/security/>.

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

[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>.

[CSPList] The EAI's Trusted Credential Service Providers List, <http://www.cio.gov/eauthentication/documents/TCSP.pdf>.

[TPList] The EAI's Trusted Technology Providers List, <http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm>.

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

[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>.

[NIH] The US National Institutes of Health, <http://www.nih.gov/>.

[NIH-pilot] The National Institutes of Health (NIH) Pilot, <https://spaces.internet2.edu/display/macedir/NIH+Pilot+Notes+on+Levels+of+Assurance>.

[IDABC] IDABC, Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens, <http://ec.europa.eu/idabc/en/home>.

[eIDM] IDABC' eIDM Interoperability Workshop: Roadmap, <http://ec.europa.eu/idabc/en/document/7208>.

[EU-LoA]] IDABC's Pan-European Multilevel Authentication Mechanism, <http://ec.europa.eu/idabc/servlets/Doc?id=29292>.

[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>.

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

[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] Electronic Authentication Partnership, <http://eap.projectliberty.org/>.

[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://rmd.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>.
- [LoA-RG] Levels of Assurance Research Group, <http://forge.ogf.org/sf/projects/loa-rg>.
- [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>.
- [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>.