Electronic Identity Credential Trust Elevation Framework Version 1.0

Committee Specification Draft 01

12 December 2013

Specification URIs

This version:

http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/csd01/trust-el-framework-v1.0-csd01.doc (Authoritative)
http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/csd01/trust-el-framework-v1.0-csd01.html
http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/csd01/trust-el-framework-v1.0-csd01.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/trust-el-framework-v1.0.doc (Authoritative)
http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/trust-el-framework-v1.0.html
http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/trust-el-framework-v1.0.pdf

Technical Committee:

OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC

Chairs:

Abbie Barbir (abbie.barbir@bankofamerica.com), Bank of America
Don Thibeau (don@openidentityexchange.org), Open Identity Exchange

Editors:

Peter Alterman (peter.alterman@nih.gov), SAFE-BioPharma Assn
Shaheen Abdul Jabbar (shaheen.abduljabbar@jpmchase.com), JPMorgan Chase Bank, N.A.
Abbie Barbir (abbie.barbir@bankofamerica.com), Bank of America
Mary Ruddy (mary@meristic.com), Identity Commons
Steve Olshansky (steveo@luminagroup.com), Individual

Related work:

This specification is related to:

- *Survey of Methods of Trust Elevation Version 1.0*. Edited by Peter Alterman, Shaheen Abdul Jabbar, Jaap Kuipers, Thomas Hardjono and Mary Ruddy. 24 September 2012. Working Draft 1.3. https://www.oasis-open.org/committees/download.php/46987.

Abstract:

This document is a specification that recommends particular methods as satisfying defined degrees of assurance for elevating trust in an electronic identity credential, to assure the submitter's identity sufficiently to support elevation between each pair of assurance levels to transact business where material amounts of economic value or personally identifiable data are involved. Alternative and optional methods may be included. The description of each recommended method shall include functional definitions of the types of identity and assertion

data employed by each method, and may include specification of the data services required in each elevation, substantive data exchange patterns or models, message exchange patterns or models, and such other elements as the TC deems useful.

Status:

This document was last revised or approved by the OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at http://www.oasis-open.org/committees/trust-el/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (http://www.oasis-open.org/committees/trust-el/ipr.php).

Citation format:

When referencing this specification the following citation format should be used:

[trust-el-framework-v1.0]

Electronic Identity Credential Trust Elevation Framework Version 1.0. Edited by Peter Alterman, Shaheen Abdul Jabbar, Abbie Barbir, Mary Ruddy, and Steve Olshansky. 12 December 2013. OASIS Committee Specification Draft 01. http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/csd01/trust-el-framework-v1.0-csd01.html. Latest version: http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/trust-el-framework-v1.0.html.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction

[All text is normative unless otherwise labeled]

1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[RFC2119]**.

1.2 Normative References

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

1.3 Non-Normative References

NIST SP800-53-3 Joint Task Force Transformation Initiative, **Recommended Security Controls for Federal Information Systems and Organizations**, August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

NIST SP 800-63-1 Burr, William E., Dodson, Donna F., Newton, Elaine M., Perlner, Ray A., Polk, W. Timothy, Gupta, Sarbari, Nabbus, Emad A., **Electronic Authentication Guideline, Recommendations of the National Institute of Standards and Technology**, December 2011. http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

ITU-T X.1254 **ITU Telecommunication Standardization Sector (ITU-T) Entity authentication assurance framework**, September 2012. http://www.itu.int/rec/T-REC-X.1254/en

NIST SP 800-53-2 (Proposed text) Wilsher, R., Zygma LLC, **Detailed mapping of IS27001:2005 (requirements and controls), prepared as a potential Annex for SP 800-53 Rev2**, April 2008. http://www.zygma.biz/Pdf/NIST_SP800-53-rev2_v1-0-0_IS27001mapping.pdf

OMB M-04-04 Joshua B. Bolten, U.S. Government Office of Management and Budget, **E- Authentication Guidance for Federal Agencies**, December 2003. http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

Trust Elevation Use Case National Strategy for Trusted Identities in Cyberspace (NSTIC) Identity Ecosystem Steering Group https://www.idecosystem.org/wiki/Trust_Elevation_Use_Case

FICAM Trust Framework Solutions Federal Identity, Credential and Access Management (FICAM) http://www.idmanagement.gov/trust-framework-solutions

Federal Public Key Infrastructure (PKI) Policy Authority http://www.idmanagement.gov/federal-public-key-infrastructure-policy-authority

NISTIR 7298, R2 Richard Kissel, Editor, NIST Computer Security Division, Information Technology Laboratory, **Glossary of Key Information Security Terms,** May 2013 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

CNSS Instruction (CNSSI) 4009 Committee on National Security Systems (CNSS) Instruction No. 4009, **National Information Assurance (IA) Glossary,** April 2010 https://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

NSTIC Pilot Common Considerations 3 National Strategy for Trusted Identities in Cyberspace (NSTIC) Ri**sk Assessment Methodologies and Authentication Strength** http://nstic.blogs.govdelivery.com/2013/04/25/risk-assessment-methodologies-and-authentication-strength/

ISO/IEC 27001:2013 ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) **Information technology -- Security techniques -- Information security management systems -- Requirements** http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

CESG Good Practice Guide 44 CESG (UK National Technical Authority on Information Assurance) and UK Cabinet Office, Government Digital Services, **Authentication Credentials in Support of HMG Online Services** May 2013, Issue No: 1.2 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204447/GPG_44_-_authentication_credentials_in_support_of_HMG_online_services_issue_1.2_May_2013_1_.pdf

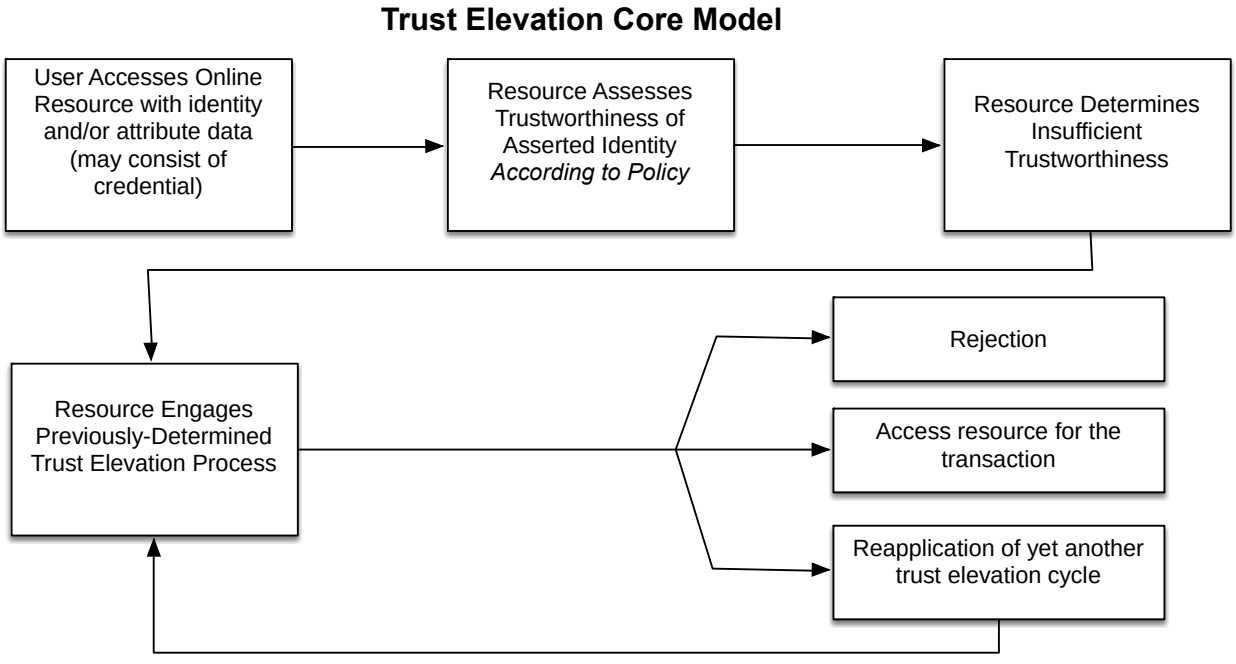
CESG Good Practice Guide 45 CESG (UK National Technical Authority on Information Assurance) and UK Cabinet Office, Government Digital Services, **Identity Proofing and Verification of an Individual**, issue 2.1, September 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204448/GPG_45_Identity_proofing_and_verification_of_an_individual_2.0_May-2013.pdf

2 Landscape and Context

This document, the third deliverable of the OASIS Trust Elevation Technical Committee, builds on the work of the first two. To recap: the first deliverable, *Survey of Methods of Trust Elevation Version 1.0*, consists of a broad overview of current and near-future online trust elevation techniques used for (or capable of) raising a relying party's assurance that the user requesting access to its resources is actually the person he or she claims to be. The second deliverable, *Analysis of Methods of Trust Elevation Version 1.0*, evaluated how each of the identified trust elevation mechanisms operated and what threats they mitigated that added to the relying party's confidence in the identity asserted. A discussion of the methodology used to analyze the mechanisms has been included in that deliverable.

As has been the pattern for this TC's deliverables, this third one builds on the work of the first two and seeks to formulate a useful approach for enabling relying parties to implement one or more trust elevation methods in order to raise their confidence in the identity of the users requesting access to their online systems and resources to the extent necessary to adequately mitigate their risk exposures.

The third deliverable is an abstraction that helps to develop applications conforming to an accepted way of elevating trust on an electronic identity. Adopting this framework reduces research time and cost. It improves efficiency in the architectural and engineering efforts of building an electronic identity system. This will also help in the integration of systems built by various parties and may impact existing systems that are not in conformity.



2.1 A Word About Credential-Based Trust vs. Transactional Trust

The eCommerce and eGov Services cyber-world currently uses two models for secure trusted transactions. One is the credential model, in which the credential carries the trust, and its trustworthiness

comes from the credential issuer. This model presumes a user with one or more credentials of various degrees of trustworthiness using an appropriate credential to log on to a networked application. In the social media world, it's the OpenID userID/password pair. In the U.S. eGov world, it's the digital certificate. The online application (or its proxy) receives the credential, validates it, and then makes a decision about whether to grant the user access to a resource based upon an authorization determination. The credential model allows the trust and data contained in the credential to be used by many applications at many sites. In the credential model, all the applications must trust the credential issuer as much as or more than the credential user.

The other, the transaction model, is the extent to which users are deemed to be who they say they are based upon factors and tests that the application applies. To the user, this model appears very similar to the credential model: user logs on to an application with some sort of assertion of identity, explicitly (e.g., userID/password) or implicitly (e.g., RP application scans user's machine for a previously-issued cookie) but instead of validating the credential and authenticating the user into the application proper, the application starts a series of tests and challenges. The transaction model allows each application to determine trust and reliability each time the user goes to a different application, and the application (or an authentication layer at the RP) manages responsibility for that trust by creating and managing its own trust architecture (based on some risk model). Thus the extent to which users are deemed to be who they say they are depends on factors and tests that the application applies. The first deliverable of this TC summarized the types of tests and challenges currently in general use or soon to be in general use on the Internet.

While the trust elevation methods described and analyzed by this TC form the preponderance of tests and challenges in use by many online applications and services, they may be used freely in conjunction with credential-based authentication services as well. That is, some transaction-based authentication services may consume identity credentials secondarily to increase their confidence in the identity of the user at the other side of the transaction. Likewise, some credential-based authentication services may increase their trust in the identity asserted by the credential by employing one or more of the described methods secondarily. ***Therefore, the methods described in this and the prior documents apply equally to both approaches to electronic identity assertion.***

2.2 Goals of the Third Deliverable

- to identify a single set of criteria that many risk and risk mitigation models could be evaluated against,
- to array each of the models against those criteria in such a way that they could be compared to each other, and
- to create viable crosswalks between models.

Achieving these goals will make possible translation between credential-based trust models and transaction-based trust models, as well as between individual applications and Trust Frameworks, which can enable further interoperability and trust between differing domains. Note that the focus of this document is trust elevation, and not credential management.

The authors note the distinction between roles and certifications vs. data elements about the individual, and acknowledge that required attribute bundles are not fixed. The Identity Provider (IdP) makes its assertion based on its own rules/regulations or other determination, which *may* include what the Relying Party (RP) wants. Trust Elevation enables enhanced confidence in the assertion of one or more data elements that the IdP asserts.

There is a weak binding between user and device, and thus it cannot be assumed that device == user unless additional contextual factors are integrated and associated with the user-device pair. Binding user to device is often transaction-based.

Continuous authentication can be viewed as elevating trust at various points (or stages of transactions) based upon some risk value. Trust Elevation is not static, but rather it is a multi-vector process -- access control based upon a dynamic view of identity, and configurable policies.

Note: dynamic authorization and continuous authentication are becoming very important topics, and are being addressed elsewhere. Thus they are out of scope for this document.

The focus of this document is on the combination of data elements that IdPs use to assert an identity online, separate from all other data elements related to the individual or their associated device(s). Note that one of the most frequently used methods of Trust Elevation is to require additional attributes about the user requesting access, therefore Trust Elevation can occur when additional attributes extrinsic to the initial identity assertion data elements are utilized. However, we consider extended attributes to be outside of the immediate scope of this document.

The intended audience for this document is IT staff or management with a general familiarity with security concepts, threats, and risk mitigation approaches.

3 Methodology for Third Deliverable

Fundamentally, all identity assertion processes are designed to identify a user. The fact that the application requires identification in the first place demonstrates that it recognizes some degree of risk to itself, its business processes, and/or its data is inherent in engaging in online transactions. In that context, both credential-based methods for asserting identity and transaction-based methods for asserting identity aim to mitigate that perceived risk to the extent that Relying Parties are willing to engage in the online transaction with end users (with a known acceptable risk to the application owner). All methods aim to mitigate one or more understood risk vectors. This is the locus where identity management and IT security blend into one another.

There are many standards and frameworks for identifying and controlling the known set of risk vectors. Because that set is more or less common to all the standards and frameworks (only the associated analysis and controls processes differ), ***the TC chose to use the ITU-T X.1254 catalog of risk vectors as the standard list and to prune them down to only those affecting authentication risks.*** This list is the baseline against which the trust elevation methods have been arrayed. ISO/IEC 29115:2013 is equivalent to ITU-T X.1254 from a technical perspective. As there are no substantive difference between them, the TC chose to focus on ITU-T X.1254 as the framework of this document.

3.1 Threat Vectors and Trust Elevation Techniques

Trust Elevation is a process for mitigating unaddressed threats or substantially improving trust in relation to a previously mitigated threat.

Recommendation on trust elevation implementation: Based upon an assessment of the state of the art by the TC membership, trust in the transaction is increased by what may be comparable to one NIST LoA when one trust elevation technique satisfies either of the following criteria:

1. **The technique mitigates a different threat vector — e.g., implementing an additional factor which doesn't share the same vulnerability as the factors previously engaged, or**
2. **The technique leads to increase in confidence in an existing factor by enhancing a mitigation strategy that has been applied previously.**

The way in which a relying party (RP) implements any particular trust elevation method will affect the increment of trust elevation it provides. This determination is clearly a judgment call on the part of the RP and the extent to which it is interoperable with other RPs' practices is dependent upon prior shared policy and practice agreements.

This table arrays threat vectors and mitigation methods for those particular threat vectors described in ITU-T X.1254. Utilize the table to identify threat vectors that the initial credential does not mitigate, and then employ one or more of the associated methods to raise the trust in the transaction. The TC arrayed the threats and controls in ITU-T X.1254 against mitigation methods described in NIST SP 800-63-1 and information security consultant Zygma LLC's analysis of controls from NIST SP 800-53-2. Any LoA or similar model can be used — the NIST LoAs used here are an example. LoA is simply one configuration, and every RP should evaluate how to calculate the difference in trust elevation based upon its own methodology. The TC is aware that all of the documents referenced are continually being revised, and so this table will need to be revised from time to time as substantive changes to the source documents are published. The latest version of this table will be referenced on the TC page: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=trust-el.

3.2 Authentication Risk Vectors and Mitigation Strategies

Legend: NIST 800-53 Controls

- AC-20 Use of External Information Systems
- IA-1 Identification and Authentication Policy and Procedures
- IA-2 Identification and Authentication (Organizational Users)
- IA-3 Device Identification and Authentication
- IA-4 Identifier Management
- IA-5 Authenticator Management
- IA-6 Authenticator Feedback
- IA-7 Cryptographic Module Authentication
- IA-8 Identification and Authentication (Non-Organizational Users)
- IA-9 Service Identification and Authentication
- IA-10 Adaptive Identification and Authentication
- IA-11 Re-authentication
- PE-3 Physical Access Control
- PE-4 Access Control for Transmission Medium
- SA-9 External Information System Services

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
1	Impersonation Some examples of impersonation are when an entity illegitimately uses another entity's identity information by using a forged driver's license or when a device registers with a network using a spoofed Media Access Control (MAC) address. *Source: ITU-T X.1254*	IdentityProofing_PolicyAdherence *Source: ITU-T X.1254*	• Strong AuthN as defined by ITU-T X.1254 • Per-service device identification (physical and logical) • KBA (time of day) • Biometric • Geolocation • Out Of Band Verification		IA-1; SA-9; AC-20	Primary: §4.2.1(b), A.5.1.1 A.6.1.1, A.11.1.1 A.11.2.1, SP53.IA.1 A.6.1.5, A.6.2.1 A.6.2.3, A.10.2.1 A.10.2.2, A.10.2.3 A.10.6.2, A.6.1.5 A.6.2.1, A.6.2.2 A.6.2.3, A.7.1.3 A.8.1.1, A.8.1.3 A.9.2.5, A.9.2.7 A.11.7.1 Secondary: §4.3.1(c), A.10.1.1 A.15.1.1, A.15.2.1, A.15.3.1, A.6.2.2
2	Impersonation (cont.)	IdentityProofing_In Person *Source: ITU-T X.1254*			IA-2 (1)(2)(3) depending on criticality; IA-3; IA-4	Primary: A.11.2.1, A.11.4.2 A.11.5.2, A.11.5.3 A.11.4.3, A.11.7.1 A.11.2.1 Secondary: A.11.1.1

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
3	Impersonation (cont.)	IdentityProofing _AuthoritativeInformation *Source: ITU-T X.1254*	Trust elevation for on-line interaction		IA-2 (1)(2)(3) depending on criticality; IA-4	Primary: A.11.2.1, A.11.4.2 A.11.5.2, A.11.5.3 A.11.2.1 Secondary: A.11.1.1

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
4	Online Guessing An attacker performs repeated logon attempts by guessing possible values of the credential. *Source: ITU-T X.1254*	• StrongPassword • Rate Limiting • DefaultAccountUse • AuditAndAnalyze *Sources: ITU-T X.1254, and demonstrated practice from industry*	• Physical Biometrics • Behavioral Biometrics Password with high entropy and other controls • KBA with transaction controls; Cookie as additional credential; HTML5 local store data; IP address • Router act as weak additional credential • Hard token • Digital certificates • Out-of-band • OTP, TOTP • Time of Access • Browsing Patterns • Context • Secure transport of credentials • Channel ID tokens (http://tools.ietf.org/html/draft-balfanz-tls-channelid-00)	• LoA 1-4 required	IA-2 (1)(2)(3) depending on criticality	Primary: A.11.2.1, A.11.4.2 A.11.5.2, A.11.5.3

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
5	Phishing An entity is lured to interact with a counterfeit verifier, and tricked into revealing his or her password or sensitive personal data that can be used to masquerade as the entity. An example is when an entity is sent an email that redirects him or her to a fraudulent website and asks the user to log in using his or her username and password. *Source: ITU-T X.1254*	How can a user know s/he is going to the right site? • DetectPhishingfromMessages • AdoptAntiPhishingPractice • MutualAuthentication *Source: ITU-T X.1254*	• Out of band verification • OTP, TOTP • CAB Forum Extended Certificate Validation Technique • Any SPAM filter that combat phishing emails • Use SSL	• LoA 3-4 required • LoA 1-2 no requirement		

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
6	Eavesdropping An attacker listens passively to the authentication transaction to capture information which can be used in a subsequent active attack to masquerade as the entity. *Source: ITU-T X.1254*	• NoTransmitPassword • EncryptedAuthentication • DifferentAuthenticationParameter *Source: ITU-T X.1254*	• Use encryption on the wire (TLS or SSL) • Physical Biometrics	• LoA 2-4 required; • LoA 1 no requirement • Establish tokens through a separate channel	IA-5, PE-4 for high system criticality; IA-4	Primary: A.11.3.1, A.11.5.2. SP53.IA.1, A.11.2.1 A.9.1.3 Secondary: A.11.5.3, A.11.1.1
7	Replay Attack An attacker is able to replay previously captured messages (between a legitimate entity and an RP) to authenticate as that entity to the RP. *Source: ITU-T X.1254*	• DifferentAuthenticationParameter, • Timestamp, • Channel Binding *Sources: ITU-T X.1254, and demonstrated practice from industry*	• Any One time factor, such as OTP • Behavioral Biometric	LoA 1-4 required	PE-3, PE-3(1) for high value systems	Primary: A.9.1.1, A.9.1.2 A.11.2.1, A.11.2.2 A.11.2.4

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
8	SessionHijack An attacker is able to insert himself or herself between an entity and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as an entity to the relying party or vice versa to control session data exchange. An example is an attacker is able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the entity. *Source: ITU-T X.1254*	• EncryptedSession • FixTCPIP_Vulnerabilities • CryptographicMutual Handshake *Source: ITU-T X.1254*	• Challenge Response using a known secret to both parties • Use a second Out of Band Channel	• LoA 2-4 required • LoA 1 no requirement	IA-7	Primary: A.15.1.1, A.15.1.6 A.15.2.1

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
9	ManInTheMiddle The attacker positions himself or herself between the entity and relying party so that he or she can intercept and alter the content of the authentication protocol messages. The attacker typically impersonates the relying party to the entity and simultaneously impersonates the entity to the verifier. Conducting an active exchange with both parties simultaneously may allow the attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other. *Source: ITU-T X.1254*	• MutualAuthentication • EncryptedSession *Source: ITU-T X.1254*	• digital certificates of sufficient strength • Out-of-band • OTP, TOTP • TLS • VPN	• LoA 1 no requirement • LoA 2-3 weak resistance only • LoA 4 strong requirement	IA-7	Primary: A.15.1.1, A.15.1.6 A.15.2.1

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
10	CredentialTheft A device that generates or contains credentials is stolen by an attacker. *Source: ITU-T X.1254*	CredentialActivation *Source: ITU-T X.1254*	• Elevate Trust through the use of MFA for example Behavioral Biometric • KBA protected from replay; cookie and IP address, HTML5 local store data • Hard token (RSA) • digital certificate protected by password or alternative • out of band; OTP w/ dynamic password • Time of Access • Browsing Patterns • Mouse Patterns • Context		IA-5	Primary: A.11.3.1, A.11.5.2. SP53.IA.1 Secondary: A.11.5.3

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
11	Spoofing "IP spoofing" refers to sending a network packet that appears to come from a source other than its actual source. Source: NIST SP 800-48 Involves— 1) the ability to receive a message by masquerading as the legitimate receiving destination, or 2) masquerading as the sending machine and sending a message to a destination. Source: FIPS 191 Faking the sending address of a transmission to gain illegal entry into a secure system. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. 2. The deliberate inducement of a user or resource to take incorrect action. *Source: CNSSI-4009*	• CodeDigitalSignature • LivenessDetection • Cf. RFC 2827 http://tools.ietf.org/html/bcp38 *Sources: ITU-T X.1254, and demonstrated practice from industry*	• Filtering • Key Exchange		IA-4; IA-7	Primary: A.11.2.1, A.15.1.1 A.15.1.6, A.15.2.1 Secondary: A.11.1.1

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
12	Masquerading When an unauthorized agent claims the identity of another agent, it is said to be masquerading. *Source: NIST SP 800-19* A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. *Source: CNSSI-4009*		• Access List • Unicast Reverse Path Forwarding		IA-4; IA-7	Primary: A.11.2.1, A.15.1.1 A.15.1.6, A.15.2.1 Secondary: A.11.1.1
13	Masquerading (cont.)	IdentityProofing_In Person *Source: ITU-T X.1254*			IA-2 (1)(2)(3) depending on criticality; IA-3; IA-4	Primary: A.11.2.1, A.11.4.2 A.11.5.2, A.11.5.3 A.11.2.1, A.11.4.3 A.11.7.1 Secondary: A.11.1.1

	THREATS	CONTROLS	TRUST ELEVATION TECHNIQUES FROM *ANALYSIS OF METHODS OF TRUST ELEVATION VERSION 1.0, AND DEMONSTRATED BEST PRACTICE FROM INDUSTRY*	ARE CONTROLS REQUIRED BY NIST SP 800-63-1?	RELATED NIST SP 800-53-2 CONTROLS FROM ZYGMA, LLC ANALYSIS	ISO/IEC 27001 REFERENCES
14	Masquerading (cont.)	IdentityProofing _AuthoritativeInformation *Source: ITU-T X.1254*	trust elevation for on-line interaction		IA-2 (1)(2)(3) depending on criticality; IA-4	Primary: A.11.2.1, A.11.4.2 A.11.5.2, A.11.5.3 A.11.2.1 Secondary: A.11.1.1
15	General Authentication Phase Threats	• Single and any combination of contextual Multifactor • Not all MFA methods are equal. • Any technique from second deliverable can be used. • All the methods identified in the second deliverable can serve as a second factor. • Not all provide the same degree of threat mitigation	All the methods identified in the second deliverable can serve as a second factor. Not all provide the same degree of threat mitigation		IA-2 (1)(2)(3) depending on criticality	Primary: A.11.2.1, A.11.4.2 A.11.5.2, A.11.5.3

4 Risk Assessment Methodologies and Authentication Strength

Note: This clause follows the risk assessment strategy example that is located at the Identity Ecosystem Steering Group (IDESG), see http://nstic.blogs.govdelivery.com/2013/04/25/risk-assessment-methodologies-and-authentication-strength/

4.1 Background

There is a lack of standards regarding a Relying Party's (RP's) risk assessment processes and thereby the required strength in assurance of identity needed to mitigate risk in an online transaction. Current material relies heavily on OMB M-04-04 and NIST SP 800-63, which is only directly applicable to U.S. Federal government use cases.

It is expected that a Relying Party (RP) has developed an internal well-documented process that enables it to determine the risk profile of every one of its online applications and the required trust in the authentication that is needed in order to enable access to the resources that a given application provides. Once an RP has determined its required assurance strength, there needs to be a method to quantify the confidence in an asserted identity. It is the objective of this deliverable to provide a systematic process for developing such capability.

A model is needed to state objectively confidence in asserted online identity, and the confidence in the authentication mode, such as tokens, passwords and biometric technologies. NIST SP 800-63-1 provides a standard for the U.S. federal government to develop such confidence based on the assumption of human on-line authentication access. The method also should be applicable for assessing confidence in non-human assertions of identity.

It is important to note that the required degree of confidence in an individual's (or devices or groups of individuals) identity by a Relying Party can be based on its analysis of risk and business practices; alternatively, it may be pre-determined by a regulatory environment (for government, healthcare, financial, or other industries).

An early approach to risk assessment and authentication strength has been based on the degree of confidence in the individual's identity, often expressed as a required "Level of Assurance." This level of assurance defines the level of confidence in identity required by the Relying Party and can be traced back to risk assessment and risk mitigation principles (see OMB M-04-04). The term "Level of Assurance" adopted by the Canadian and US governments in the late '90s is also used to express the level of confidence provided by Identity Providers (IdPs), Attribute Providers, or by an Intermediary (by combining inputs from Identity and Attribute Providers). The success of Trust Elevation as a method for reducing risk depends on parity between the expressed requirements of Relying Parties (RPs) and the asserted or proven capabilities of Identity Providers (IdPs).

4.2 Authentication Risk Assessment

It is desirable for IdPs and RPs to be able to assess authentication risks in a similar way or to have as a common denominator a common understanding regarding risk assessment and what it involves. Otherwise, a fundamental component of interoperability across operators is missing. If RPs and IdPs assess identity risks in different ways, then they are unable to articulate their requirements using a common lexicon; deployments end up being done in an ad hoc manner; and RPs ultimately have to make ad hoc decisions about how to combine identity attributes to mitigate their risks. To avoid such

complexity, historically RPs have also been IdPs in order to control the risks inherent in online transactions. The evolution of a federated global Internet of people and things has highlighted the scalability and user problems inherent in this obsolete approach.

In most cases, identity authentication is initiated to enable access control, so the confidence in authentication can be based on control strategies. The main assumption here is that ITU-T X.1254 is used to establish the degree of trustworthiness of an asserted online identity per strategy.

4.3 Authentication Strength

In terms of mitigating identity risk, there are an increasing number of available authentication methods, as well as ways and means of combining them. A growing number of authentication technologies are being made available on mobile phones, so a combination of: device possession, location, out of band communications and biometric technologies can be used in a particular scheme where userID/password was once the only way to assert identity online.

The ability of an individual to assert a claim of identity in support of a transaction depends on the underlying confidence that a set of attributes ties them to their digital identity (*identity Proofing*), and the level of confidence that the RP or its proxies (federations, identity ecosystems, etc.) has in the credential technology and credential management (*Credential Management*). The first revision to NIST SP 800-63, SP 800-63-1, explicitly acknowledged these two discrete elements, though both had been recognized and accounted for long before NIST issued the first version of SP 800-63.

Historically, identity proofing and credential management have been provided by a single entity, in many cases the RP. However, there are an increasing number of architectural models and commercial forces driving a componentized model. As this occurs, the binding mechanisms between identity proofing and credential management become ever more important. Furthermore, the binding mechanisms need to be acceptable at the point of transaction so that the relying party has sufficient confidence that it is providing the appropriate service to the appropriate individual. The mechanism and type of binding used to create a credential also affects the potential for interoperability, or mutual recognition, of the credential by other relying parties.

Our first two deliverables have provided a well-characterized set of authentication methods and will provide more assured guidance for relying parties, thus improving the uptake of identity solutions.

4.3.1 Authentication Strength Evaluation

The main issue here is how to define an authentication technique that can be used within the context of a given transaction that yields an acknowledged reduction of risk to an RP. Authentication strength (or level of assurance) measures how hard it is for another person or entity to masquerade as the legitimate client or user. At the highest level, the authentication strength of a given method can be evaluated in terms of its raw ability to combat masquerading and session hijacking attacks such as a man-in-the-middle or man-in-the-browser attack. These two kinds of attacks draw attention to the need of a system to implement means other than a simple electronic assertion of identity to detect illegal access such as fraud detection and transaction level controls.

While on the surface, combining two or more identity assertion methods of the same kind may be thought to enhance authentication strength, the additional method would be vulnerable to the same risk vectors as the initial method. This approach is much less likely to raise assurance in the asserted identity than if the second method was not vulnerable to the same risk vector as the first method. Clearly then, care needs to be exercised when combining multiple kinds of authentication methods. Authentication strength can be enhanced only by combining methods of different kinds that do not share common vulnerabilities.

Note: For a useful reference, also see NIST SP 800-63 Table 7 "Assurance Levels for Multi-Token E-Authentication Schemes."

5 Conformance

An entity that institutes a trust elevation process that incorporates the principles described in this document, *Electronic Identity Credential Trust Elevation Methods Framework Version 1.0,* in both policy and practice may be said to be elevating trust in conformance with the findings of this TC.

Appendix A. Use Case Example

Mitigation of high risk can be achieved in a transaction, but this doesn't have to be based solely on the credential or the authentication method.

One prevalent use case for this is when a financial institution is transferring funds at a customer's request, e.g. between accounts (whether within the same system or to an external system). The user logs in with username and password, or perhaps includes a second factor, but the financial institution engages in trust elevation techniques (transactional methods) (i.e. knowledge-based authentication — KBA) outside the user's view, and without the user's involvement, before executing the transaction. This might vary based upon the perceived risk in a particular transaction, e.g. when it is to an external entity or above a certain value, and may include:

- DNS — evaluating whether the source IP address and destination is consistent with past usage patterns; and if the IP address varies from past transactions, whether it is located in a suspicious geographic area, etc.;
- Examining the cookie(s) for evidence of past contact appropriate to the transaction being requested; or
- user access through TOR (The Onion Router), which disguises source IP address.

Strategies for elevating transactional trust can vary based on the access methods and devices. For example in the mobile space, strong device identification including validation of number and geolocation can be used in order to identify the device first. Binding the device to a particular user can then be done based on criteria such as time of day, location, type of transaction being performed and knowledge of expected behavior of the user. A password or biometric authentication can then be used to validate the prediction of the user and as such approving requested transaction.

A.1 Use Case Example of Trust Elevation

When active duty personnel complete their term of military service, the Department of Defense (DoD) reclaims their PIV/CAC cards and issues them a userID/password pair to be used to log in to DoD online services post-duty. The PIV/CAC card satisfies both Federal Bridge High Assurance and NIST LoA-4 and, as the antecedent for issuance of the userID/password pair, satisfies NIST LoA-3 requirement for identity proofing. Thus, the userID/password pair is a NIST LoA-2 credential.

The US Department of Veterans Affairs web portal, which serves as a front-end to many of its online services for former military personnel, has been designed to consume and validate these userID/password pairs so former active duty military personnel, now veterans, may be authenticated to these services. Because of risk assessment determinations regarding some of their online services, however, the VA requires LoA-3 credentials for authentication to those applications, as when the application provides access to a veteran's personally-identifiable information. In these cases, the program managers at VA may choose to enable trust elevation at the portal to allow the veteran to gain access to the LoA-3 application.

The VA portal knows what LoA is required to authenticate to each application it services and whether trust elevation has, by policy, been approved for that application. Assuming trust elevation has been approved, a trust elevation scenario plays out as follows:

- The application receives a login request with an LoA-2 userID/password pair and hands it off to an authentication service at or connected to the portal;
- The authentication service validates the LoA-2 credential;
- The authentication service determines that an LoA-3 credential is required for access to the application and sees that trust elevation has been approved for that application;
- The authentication service engages the user in a real-time transaction with a trust elevation method that has been predetermined by policy to add sufficient additional trust in the identity of the user to

satisfy the risk mitigation requirements of the application's cybersecurity requirements. In this hypothetical case, the service decides to check the user's computer for a cookie that it has placed there during a previous session;

- Assuming the cookie is found, the authentication service decides that a validated second factor ("something you have") has been added to the first factor presented by the initial credential ("something you know") and that these two factors are sufficiently trustworthy to satisfy the application's risk mitigation policy;
- The authentication service returns a valid LoA-3 message to the application, which then authorizes the user to access its resources and transact business.

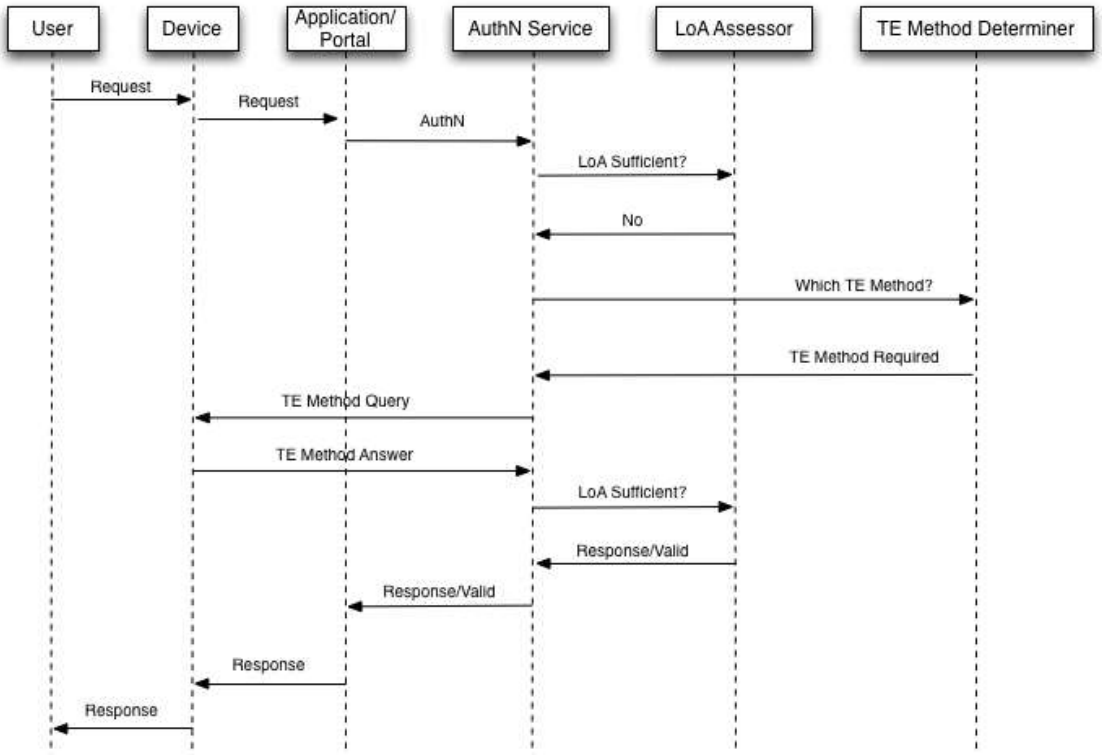


Figure 1. Trust Elevation Use Case Process Flow

Appendix B. White Paper: E-Authentication Partnership Policy On Levels Of Assurance Of Identity For Authentication Of Electronic Identity Credentials

Prepared for the CS-AL Work Group of the E-Authentication Partnership

Version 1.0

Principal Authors: Peter Alterman, Ph.D.; Noel Nazario, Chris Louden

Table of Contents

Acknowledgement

The primary authors wish to acknowledge with gratitude the invaluable assistance of our colleagues on the Credential Assessment - Assurance Level workgroup, especially Kim Cartwright, Donna Dodson, Yuriy Dzambasow, Chris Daly, Richard Wilsher, R.J. Schlecht and Von Harrison.

Executive Summary

The purpose of this paper is to examine the issues surrounding electronic authentication and credentialing of the identity of individual human beings presented during electronic commerce or electronic government transactions. A future document will address issues surrounding electronic authentication and credentialing of machines, computer code, etc.

In order to engage in secure e-commerce and e-government both, online applications often need to know the identity of the individual on the other side of the Internet. This entity may be new to the application and the application often needs to be confident of the identity of the business partner in order to grant him or her authorization to access the system or service. The way identity is presented to online applications and services is through presentation of some kind of identity credential.

The U.S. Federal government has posited four levels of assurance of identity (LOA), from minimal assurance of identity through high assurance of identity, and has linked them to levels of risk of harm. The question the EAP Assurance Level Sub-workgroup has addressed is whether this model is acceptable for use by the private sector in e-commerce implementations or whether a different scheme is preferable.

In reviewing relevant documents and systems rules, the following issues stood out:

- Assurance of identity in electronic transactions is based partly upon identity proofing, which is a mature process with well-known rules and procedures;
- Assurance of identity in electronic transactions is based partly upon credential management, which encompasses the manner in which a proofed identity is bound to an electronic credential and the extent to which the credential is trustworthy, including the reliability of the credential service provider, the token technology that contains the credential, and the life cycle management of the credential and token.
- The extent to which an authentication event is coupled to an authorization event is an important condition, running the gamut from very tight to very loose; that minimal assurance of identity can lead to authorization to high risk applications when coupling is loose and other factors are present sufficient to satisfy the risk equation.
- It may be possible to develop an algorithmic method for determining LOA that is objective rather than arbitrary.

The Assurance Level Sub-workgroup has recommended that the EAP adopt the U.S. Government's Four (4) Levels of Assurance of Identity as an interim standard for authenticating identity for online business transactions.

It furthermore recommends that work be initiated to develop a comprehensive algorithmic model for determining LOA based upon the work presented in this document, as a potential candidate for a final standard.

Introduction

The purpose of this document is to identify the issues underlying issuing electronic identity credentials for use in online business transactions and to develop a common agreement whereby electronic identity credentials may be categorized as satisfying discrete Levels of Assurance based upon the extent to which the identities presented in the credential can be trusted to actually belong to the entities represented, and the extent to which the electronic credential can be trusted to be a proxy for the entity named in it, including the extent to which the electronic credential can be trusted to be utilized by the individual named within it and not someone else.

This paper specifically addresses electronic authentication and credentialing of the identity of individual human beings presented during electronic commerce or electronic government transactions. A future document will address issues surrounding electronic authentication and credentialing of machines, computer code, etc.

The Federal Government has published guidelines describing four (4) Levels of Assurance, known as LOA, for use in authenticating electronic identity credentials for use in providing government services electronically. The question for private industry is whether the Federal government's approach, and its recommended four LOA, satisfies the requirements for e-commerce, and whether it, or an alternate approach, should be adopted by the private sector generally. In order to address this fundamental question, the E-Authentication Partnership has been constituted as an advisory body on behalf of all private industry, broadly defined, in the U.S.

Complicating the question of trusting electronic identity credentials is the sometimes subtle distinction between authenticating an identity and authorizing that identity to access resources or services electronically. The relationship between these two functions may be less than straightforward. A key point in resolving the question of how Authentication (AuthN) and Authorization (AuthZ) are related is understanding that they can be coupled tightly or loosely.

As the attached bibliography demonstrates, much attention has been paid to each of these issues, and this paper hopes to codify and present key issues in a coherent manner. In order to do so, the paper is organized as follows:

- A discussion of Authentication and Authorization, emphasizing the relative functions of each in e-commerce and e-government and emphasizing the concept of "coupling" whereby an authenticated identity is authorized access to a resource or service. A discussion of risk is included.
- Recommendations for private industry for addressing the question of determining LOA.
- Two Appendices that present an in-depth discussion of the elements that go into creating an electronic identity and in authenticating that identity, including identity management and credential management.
- An Appendix that presents an approach to generating an "objective" model for determining LOA.

Levels of Assurance of Identity (LOA)

The commonly-held meaning of the term "Level of Assurance" (LOA) is that it describes the degree to which a relying party in an electronic business transaction may be confident that the credential being presented actually represents the entity named in it, and may be confident that the represented entity is actually engaging in the electronic transaction. LOA are discrete assurance indicators used to quantify the degree of protection afforded by the controls that an information system implements to manage security risk. LOA are creatures of convenience defined so we can compare dissimilar systems in terms of the protection they provide. LOA are hierarchical and defined in the context of some set of policies, regulations, best practices or guidelines.

LOA, then, are based on the following factors:

- The extent to which the identity presented in an electronic credential can be trusted to actually belong to the entity represented. **This is generally handled by identity proofing.**
- The extent to which the electronic credential can be trusted to be a proxy for the entity named in it. This is generally known as identity binding, and is *directly related to the trustworthiness of the credential technology, the processes by which the credential is secured to a token, the trustworthiness of the system that manages the credential and token and the system available to validate the credential.* This includes the reliability of the credential service provider responsible for the system. **These elements are collectively known as credential management.** The extent to which the electronic credential can be trusted to be utilized by the individual named within it and not someone else is a direct outcome of this factor.

However, an authentication event in isolation is meaningless. Anyone can claim to be anyone else in isolation without consequences of any sort. It is only when John Smith claims to be Mary Jones in a transaction that a problem arises. That is, the legal system only cares that John Smith is claiming to be Mary Jones when he tries to assert her identity fraudulently for some purpose. In other words, authentication of identity is only necessary when an authorization event, or attempted authorization event, follows.

This leads to an important point: ***that LOA are primarily useful or required when an authentication event leads to an authorization event***. It is for this reason that the Federal Government based its guidance on determining LOA on degrees of risk (see OMB M-04-04 and FIPS 199). In fact, the OMB guidance document was carefully aligned with the risk levels in NIST FIPS 199.

Higher LOA are required to mitigate higher levels of risk. LOA are measures of the authentication trustworthiness required to authorize access to services or resources, so ***LOA exist as a function of the relationship between authentication and authorization events.*** This is why it is hard to talk about LOA without addressing authorization, even though LOA is a characteristic of authentication.

Any company engaged in e-commerce may choose to assess risk any way it wishes. FIPS standards are mandatory for U.S. Federal entities only and advisory for others. FIPS 199 is only one of several risk assessment and risk analysis schemas, although it may be considered the most complete and technically accomplished of the lot. Particular industries may apply more stringent or less stringent criteria. The financial industry as a whole, for example, may have to answer to business-specific requirements of governments in addition to technology-specific issues. In other words, different business sectors may weight risk factors differently. Keep in mind that risk assessments and risk analyses are essential to authorization decisions, rather than authentication decisions.

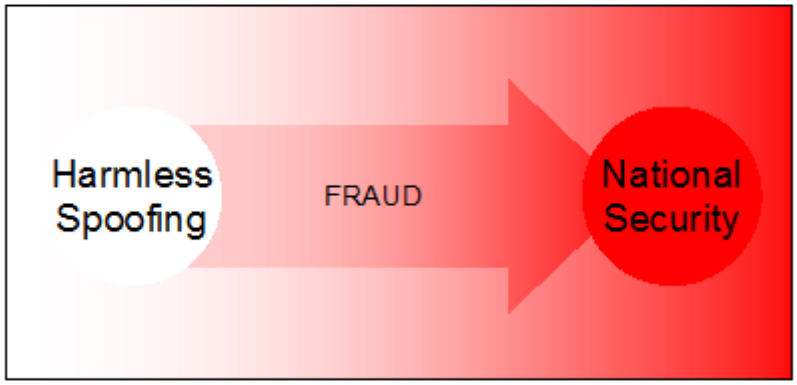
Risk and Risk Mitigation

Authentication is the process of establishing with a certain level of confidence or assurance in the veracity of a claimed identity. Authorization is the act of granting access to a certain resource based on the results of an authentication process. In information systems, risks and potential harm are Authorization issues, i.e., authorization deficiencies or failures open the door to potential harm. The effect of deficiencies in the Authentication process is therefore only indirectly related to system risk. Without the risk of improper Authorization, the LOA of the Authentication process not an issue. That is, there is no risk from someone asserting a fraudulent identity until that person tries to gain improper Authorization to access a system resource. Therefore, risk is a term related to Authorization, not Authentication.

Risk is defined as the potential for harm or damage (including perceived harm or damage) arising from inappropriately authorizing access to a system or resource, or from failure to allow access to a properly authorized entity. In terms of identity assurance, these risks are: improper authorization based on misrepresentation of identity, and failure to properly authorize based on misinterpretation of identity. The risk of misrepresentation may be for attributes as well as for identities, especially as an entity's identity may be represented as an aggregate of all its attributes, or aggregates of subsets of attributes, such as those associated with a person's professional identity as distinguished from his or her personal identity.

The overall goal of an information system's "Risk Equation" is to equal zero. Experience tells us that goal is not achievable in practical terms, but it helps frame and model our analysis. To equal zero, such equation must account for both all system risks and sufficient countermeasures to mitigate or "eliminate" those risks. The set of mitigation strategies implemented on a given system define the LOA for that system. Our goal is to define discrete, meaningful, and practical LOA.

The primary risk associated with identity assertion is fraud, and the current most popular version of fraud is identity theft. However, there is a spectrum of risk of fraud, running from harmless spoofing to catastrophic breach of national security. The extent to which the risks of fraud require mitigation is based upon the potential harm caused by someone gaining access to secured resources.

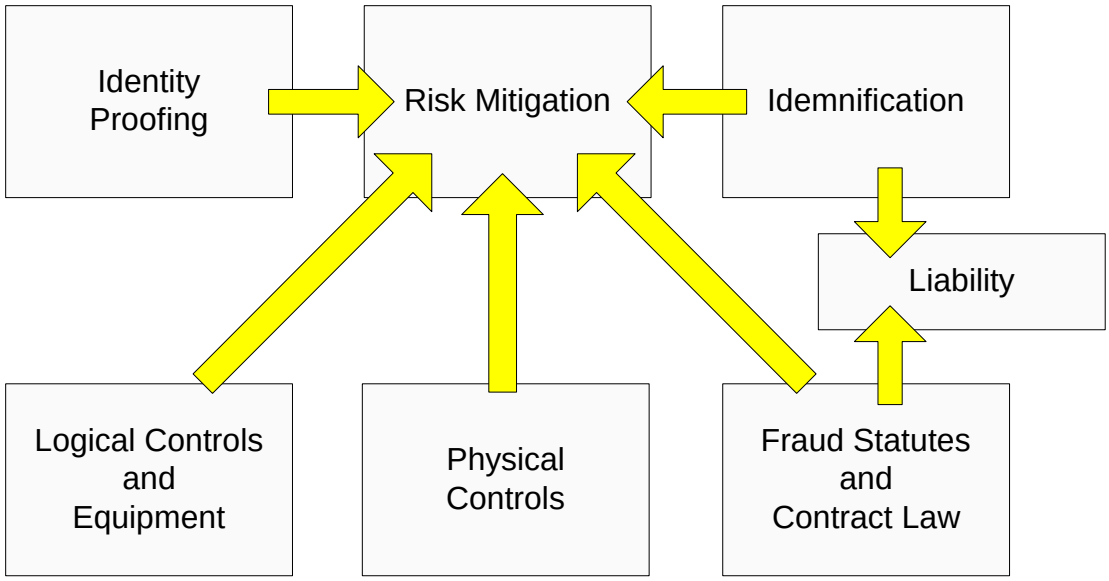


Spectrum of Risk = Spectrum of Harm

Every application owner must make his or her own risk to harm mapping. This is usually called “risk assessment” and results in creation of risk mitigation plans. There are a number of generally-accepted models and standards for performing systems risk analyses. Among the results of a risk analysis is a determination of risk mitigation requirements, and within the context of identity management, that means identifying the identity authentication requirements for authorizing system access.

Elements of risk mitigation include the following elements. Complete sets of elements are addressed in the American Bar Association PKI Assessment Guide; ANSI X9.79; AICPA WebTrust and others.

- Identity proofing, only to the extent that authentication of identity is linked to authorization (see following section);
- Logical controls and equipment;
- Physical controls and personnel management procedures;
- Indemnification;
- Liability agreements;
- Fraud statutes and contract law;
- Civil recourse when authorization is withheld inappropriately and harm results.



Identity proofing runs the spectrum from none to the establishment of identity through the use of breeder documents, biometric identification, and data aggregation. As for all mitigation strategies, even the most cumbersome procedure is not problem-free. Identity is an aggregation of personal attributes and no single source can establish identity on its own. Furthermore, individuals have multiple valid identities in the real world, some with little overlap. These properties of "identity" may not be relevant, but must be recognized in developing ID proofing strategies.

The last two categories, Laws and Regulations, and Indemnification are closely related mitigation strategies for certain types of risk. Laws, Regulations and Indemnification tend to be more significant than assurance of identity as business enablers in a given risk environment. They may not help prevent system compromise, but they would enable prosecution of perpetrators and compensate for losses due to subversion or misuse of system resources. Indemnification and fraud/contract law together underpin the key determinants of liability.

In summary, then, harm can only occur in a business transaction or a government-citizen interaction when authorization is improperly granted or withheld. Thus, there are properly no risks associated with improper authentication of identity, or improper assertion of identity through an electronic credential, unless authentication of identity is part of an authorization event. It is the requirement of the authorization event, determined by risk analysis and risk mitigation design, that determines the LOA required for authentication of identity in an electronic credential.

Here is an excellent summary of the authentication-authorization issue:

> "Find out if Sonny wants to see this guy," the fat guy said.
>
> The guy in the sandals went inside. The fat man had dropped his arm, but stood with his body shielding the entrance. If I wasn't supposed to go in and he let me, Sonny would have his ass. If I was supposed to go in and he didn't let me, Sonny would have his ass. We waited. Hawk seemed to be enjoying it. Vinnie didn't seem to know it was happening. The other guy came back out.
>
> "Okay," he said to the fat guy.

From Parker, Robert B., *Back Story*, Berkley Books, 2003, p. 82.

Coupling Authentication and Authorization

Authentication is the process of establishing with a certain level of confidence or assurance the veracity of a claimed identity. Authorization is the act of granting access to a certain resource based on the results of an authentication process. In information systems, risks and potential harm are Authorization issues, i.e., authorization deficiencies or failures open the door to potential harm. The effect of deficiencies in the Authentication process is therefore only indirectly related to system risk. Without the risk of improper Authorization, the LOA of the Authentication process not an issue. That is, there is no risk from someone asserting a fraudulent identity until that person tries to gain improper Authorization to access a system resource. Therefore, risk is a term related to Authorization, not Authentication.

There are many instances where authorization decisions are based solely and directly on presentation of identity. If a bank authenticates an individual's identity, that individual is generally entitled to access to his or her accounts. A name present on the access control list (ACL) of an automated system may be the simplest example of this identity to authorization linkage, and the more sensitive the data in the system, the higher the degree of assurance of identity, or LOA, necessary before access may be authorized.

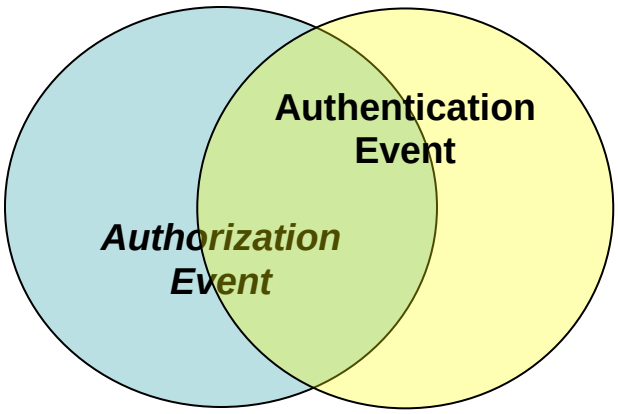
There are many cases, however, where assurance of identity is not as important to authorizing access to a system. Buying goods or services online with a credit card is a useful model of a transaction where assurance of identity is less important. In this case, the merchant is willing to accept the transaction due to the credit card issuer authorizing the electronic transaction based not on an individual identity but on the history of payment by the cardholder, patterns of purchasing, etc. Additionally in this example, liability and recourse are well-defined. In fact, a child may use his or her parent's credit card and so long as the bill is paid, the company might never know that the individual using the token was not the individual whose name is embossed on it. In this model, factors other than authentication of identity are central to the authorization event.

It should be clear, then, that the relationship between authentication event and authorization event is variable. In some cases, the two events are ***tightly coupled***, as in the first example. In other cases, authentication of identity is but one of several criteria that go into an authorization event and in this case authentication and authorization may be said to be ***loosely coupled***.

Tight Coupling: Identity = Authorization

Loose Coupling: Identity + Payment History + Pattern of Buying + Transaction Amount + Indemnification + Legal Recourse = Authorization

Keep in mind that in these examples the term "identity" includes both identity proofing and credential management (type of credential, token, system safeguards, etc.). Appendices A and B discuss in some detail the technical issues underlying identity proofing and credential management.



Coupling may also be thought of as the degree to which the authorization event overlaps the authentication event.

It is not always assurance of identity that mitigates risk. Other factors may be as important as, or more important than identity when determining authorization. The corollary is that the tighter the coupling between Authentication and Authorization, the more important LOA becomes. There is no one to one relationship between LOA and authorization. ***Depending on the degree of coupling, a low LOA may be sufficient for a high risk authorization.***

Because it is possible to identify every factor that contributes to an authorization event, it is theoretically possible to calculate a metric for degree of coupling. The formula for that calculation would be:

$$\text{Degree of Coupling} = \frac{x+y+z+..}{x}$$

where x = Authentication confidence (see Appendix C) and

y, z, etc. = confidence in other factors, such as business history, indemnification, etc.

It is the responsibility of the application or service owner to determine the factors required to authorize access to resources or services, as well as the LOA, if any, that may be required for the transaction.

Validating the Credential: the Role of the Relying Entity

So far, the discussion of the trustworthiness of an electronic identity credential has focused on the issuer. There is another factor that needs to be considered, however, and that is the ability of the entity relying on the identity credential to validate that credential. Each application or system that relies on an identity credential as part (or all) of its authorization process must have in place a strategy for validating the presented credential. That process can be null, that is, no validation of presented credential – or it can, and should, be consonant with the LOA that the authorization process requires.

In this document, the distinction between an electronic identity credential and an identity token may be described as follows: an electronic identity credential is an electronic proxy for an individual composed of one or more related strings of code. The form factor used to present the code to an application or service is known as a token. Tokens may be hardware-based or software-based. Strictly speaking, all electronic identity credentials reside on tokens, therefore it is common usage to use the two terms interchangeably. However, the term "token" also is used commonly to refer specifically to a hardware device that houses code that serves as a proxy for an identity and "credential" is used to refer specifically to the code. Usually, context distinguishes which meaning of "credential" or "token" is being used.

While weak or absent credential validation processes do not change the intrinsic LOA of the identity credential, they may compromise the system they are designed (or not designed) to protect. A poorly-designed or poorly-implemented validation process may not be able to discriminate between a valid identity credential and an invalid one, or between a low assurance credential and a high assurance one. This invalidates the usefulness of higher-assurance level identity credentials in that instance and sabotages the overall security of the system.

In summary, then, if a system requires a high assurance of identity (leave that undefined for the moment), then the process for validating the identity credential should satisfy the requirements for a credential management system operating at that same level of assurance. Another way to say that is that ***the credential validation process should be as rigorous as the credential issuance process for the LOA required for authorization.*** Specifics of credential management system design are recognized elements and are presented in Appendix B, following.

How Many Levels Of Assurance?

The U.S. Federal Government Approach: The U.S. Office of Management and Budget, following the lead of the Federal PKI Policy Authority (which in turn followed the lead of the Government of Canada PKI and the U.S. Department of Defense PKI) has established four (4) LOA: minimal assurance of identity; moderate assurance of identity; substantial assurance of identity and high assurance of identity. These levels are arbitrary in that no objective metrics are associated with them. They do, however, summarize the spectrum of assurance.

The technical guidance designed to help government agencies determine which LOA a particular credential is issued at addresses the two general categories of identity proofing and credential management largely in terms of how well any particular implementation mitigates risk. It is instructive to note that the identity proofing requirements for Federal LOA Three are the same as Federal LOA Four. The differences between these two levels are in the types of credentials that assert the identities and in the credential management systems behind them.

In all fairness, though, the four LOA called out by the Federal government are not unreasonable, and certainly cover the vast majority of circumstances likely to be met in real world implementations of e-commerce and e-government, spy thriller movie scenarios notwithstanding.

An Algorithmic Approach: There is an alternative to positing an arbitrary number of LOA, whether two, four, five or seventeen. That is to develop an algorithm that (more or less) accurately models the factors involved in identity proofing and credential management. The output of the algorithm is a number that represents Assurance of Identity for each instance of credential issuance for all degrees of identity proofing and credential management. The spectrum in identity proofing would run from no assertion of identity all the way to absolutely validated assertion of identity along a continuous scale using "threshold windows." All credentials, from self-selected UserID/password pairs through biometrically-protected, hardware tokenized digital certificates, fall along a spectrum of reliability.

Both identity proofing and credential management are familiar activities, for which the requirements are well-understood. In general, auditing standards address requirements for both, and the bibliography to this document references many of them. (See Appendices A and B for detailed discussions of these requirements.) It should therefore be possible to build an algorithm to generate "objective" scores for all instances of identity proofing and all instances of credential management and to use those range of scores to develop a mathematical model that describes an "objective" set of LOA with numeric ranges. At the very least, it would allow credential providers to self-assert particular LOA for their credentials, citing a standard methodology for comparison.

An initial effort to developing just such an algorithmic approach is documented in Appendix C. At first blush, this approach looks to have great potential. Unfortunately, however, such an algorithmic approach requires more analytical work, done by staff with specialist skills and knowledge, in order to deliver a useful, viable model. The current AL workgroup has neither the resources nor the time necessary to build such a model. Furthermore, algorithmic models gain credibility from historical data, which does not currently exist.

Recommendation of the AL Work Group

While an "objective" methodology for determining LOA for a given credential is clearly the desirable choice, the practical reality is that, until a viable alternative method for determining LOA is available, the Federal government approach of summarizing LOA into four broad categories is the only currently viable alternative. The reasons for that are as follows:

1. The Federal Four (4) LOA model fits the government's E-Authentication architecture that controls how identity is managed in e-government. Any private sector entity doing business electronically with the U.S. Federal government will be driven to adopt or adapt to this model. With national defense and law enforcement in the government mix, a very large number of business transactions, both national and international, are affected.
2. There are no conflicting LOA models operational in the e-commerce space at the present time, although there are a number of competing schemes for implementing authentication and authorization events.
3. The Federal Four (4) LOA model is compatible with other governmental schemes, notably T-Scheme in the U.K., the Canadian Government PKI model and the Australian Gatekeeper model.
4. Adoption of an alternate LOA scheme based on yet another arbitrary parsing of the identity assurance spectrum would at the very least require private sector entities to map their LOA to the Federal Four, in some as-yet undefined manner, and could possibly cause massive confusion as citizens / customers try to negotiate multiple e-business experiences. Such confusion would not advance the growth of e-commerce or e-government.

Therefore, the Assurance Level Work Group recommends that:

1. **The E-Authentication Partnership adopt the Federal Four levels of assurance of identity as an interim standard for e-commerce, and**
2. **The E-Authentication Partnership support development of the Algorithmic Approach as a candidate for final standard for defining levels of assurance of identity for e-commerce.**

Bibliography

a. Common Criteria
b. FIPS 199
c. OMB M-04-04
d. ANSI/ASC X9.79
e. NECCC Identity Management White Paper
f. NECCC Enterprise Identity and Access Management: The Rights and Wrongs of Process, Privacy and Technology
g. NECCC Identity Infrastructure
h. Mortgage Bankers Association/SISAC CPRD Certificate Summary Table
i. ABA PAG v. 0.30
j. NIST SP-800-63 draft
k. AICPA Suitable Trust Services Criteria and Illustrations: Suitable Trust Services Criteria and Illustrations for Security, Availability, Processing Integrity, Online Privacy, and Confidentiality (Including WebTrust and SysTrust)
l. Private correspondence, Microsoft Corp.
m. X.509v3 Certificate Policy for the Federal Bridge Certification Authority
n. X. 509v3 Common PKI Policy for the Federal Government
o. Parker, Robert B., *Back Story*, Berkley Books, 2003

Appendix B-A: Issues in Identity Proofing

Identity Proofing

Identity Proofing is the process of validating critical attributes, as an identity may be thought of as an aggregation of attributes or subset of attributes. Identity proofing is a well-understood activity with a long history that reaches far back before electronic systems were invented.

Most commonly, identity assertions are supported by documents such as a birth certificate, a driver's license, or a passport. In these examples, different governmental entities are responsible for issuing each and there is no central, governmentally-coordinated system to match up these credentials. In fact, the birth certificate is commonly required to receive a driver's license, making the former a "breeder document" for the latter. The driver's license is commonly used as an identity credential for acquiring a passport, making it a "breeder document" for the latter. Some identity credentials are mandatory, like the birth certificate, and some are optional, like the passport and the driver's license.

These credentials are not the only form of identity credential that an individual may use to support his or her assertion of identity. Most individuals living in the more developed nations of the world have records on databases. In addition to governments, many business sectors maintain databases of personal information about individuals: medical records, banking records, credit cards, telephone and ISP accounts, membership databases in hobby groups, political associations, etc.

Some identity credentials are more reliable than others, and correlation of many different credentials and credential types yield greater assurance of identity than reliance on an individual credential. The following list summarizes elements used for supporting identity claims. In general, they are listed by increasing level of reliability. Each of the following elements has an intrinsic weight, that is, they are not equally powerful. (Weights are discussed in Appendix C, the Algorithmic Method.)

- Environmental context - is this a human, a machine/device, a cartoon character? This element suggests that there is no zero level for knowledge about an entity asserting an identity.
- Self-assertion of identity No breeder documents
- Unofficial breeder document such as a business card) – a form of self-assertion of identity
- 3rd Party Assertion of identity, e.g., a parent asserting a child's identity at the Motor Vehicle Administration
- Official 3rd Party Assertion of identity, e.g., Notary
- Credit Reporting Agency or equivalent (external) database lookup - this element incorporates the presence of an individual in one or more on line databases, which may be used to support identity assertions and portable credentials. It differs from database lookups related to issuance of identity documents in that the databases here are not used to issued identity credentials; rather, they record transactions done in the name of the identity asserter;
- Third party database check – differs from a credit database lookup in that it checks a whole different category of data about an individual, e.g., a demographic database which looks at the individual's context, not her specific information;
- Unvalidated Official document – a driver's license presented without being checked by the reviewing entity against the State issuance database
- Unvalidated official document with biometric. Some official documents contain biometrics (photo on a driver's license, for example) and some don't. An official document containing a biometric provides more identity elements than a piece of paper or a card stamped by an official agency of government. Implicit in the trustworthiness of this and all other official documents is the belief that in the process of issuing them, a governmental entity has performed some form of prior identity proofing using some aggregate of these listed

elements. This raises the issues of recursive identity proofing and of second order third party assertions of identity.

- Validated official document – that is, one whose issuance has been verified against an official database of the agency that issued the document.
- Validated official breeder document with biometric – same as above, but with biometric element or elements.
- In-person proofing – while an individual may be physically present and still assert a false identity, the individual is an excellent source of biometric data.

Attributes

Attributes are characteristics of entities, devices or processes. They may be permanent or temporary, contextual or intrinsic. "Vice President, Sales," is both contextual and, given the business world, temporary. They include the usual descriptors: age, height, weight, color of eyes, color of hair (temporary). A credit card account is an attribute for a person. "Dell Latitude D600" is an attribute of a device, its model name.

Attributes are important because they define an entity. In fact, an entity may be defined by the aggregate of its attributes - John Doe, 1234 Mockingbird Lane, Paradise, LA 00000, SSN 123 45 6789 etc. etc. – or by a subset of attributes of interest to a particular business process or service – John Doe, M.D., DEA number 1234567890. As noted in the main text of this document, there are occasions when certain attributes of an entity are more important than the name of the entity, as for example a credit card account number or title on a purchase order.

The linkage between identity and attributes is complex, and it should be evident that attributes may be used for both authentication and authorization. The authorization function of a system determines what subset of attributes are important to that system, which ones it wants to see. Attributes, then, are independent parts of the authentication to authorization coupling model for each system.

Some X.509v3 certificates are used as "attribute certificates" whose identity fields are not populated with either distinguished or common name, but with a position title, or a status, i.e., "matriculating student" in which the certificate is not used as an identity token at all, but rather, directly as an authorization token. In this case, the coupling between attribute certificate and authorization decision is very tightly coupled, indeed.

In this model, as in others, there is not necessarily a two-way relationship between the identity and the "role" attribute. That is, John Doe may be a matriculating student, but not all matriculating students are John Doe, or even many John Does. Any student presenting a "matriculating student" attribute certificate with no identity attached to his or her university library may be authorized for full access, in which case the coupling between authentication of attribute is very tight but there is no coupling at all between identity and authorization. This last is a common use case for the Shibboleth identity management scheme found in the higher education community.

Clearly, then, attributes may or may not be equal to identities, and they may or may not lead directly to authorization to a resource. Furthermore, attribute checking may be part of identity proofing or not. The function of attributes in identity management, authentication and authorization is defined by each automated system that uses them as part of its authorization scheme. This is another reminder that each system is responsible for the degree of coupling between authentication of identity and authorization to access to that system.

Appendix B-B: Issues in Credential Management

Credential Management

Credential management is the process of issuing, maintaining, and disposing of credentials. The issuance of credentials includes processes for authorizing their issuance, authenticating the entities receiving the credentials, generating the credentials, and distributing the newly issued credentials to their owners and to the relevant system components (e.g., Directories). The maintenance of credentials includes handling of modifications or updates, renewing, recovering, revoking or disabling, backups, archiving, and providing status change notifications. The disposing of the credential includes destroying, archiving, and providing status change notifications.

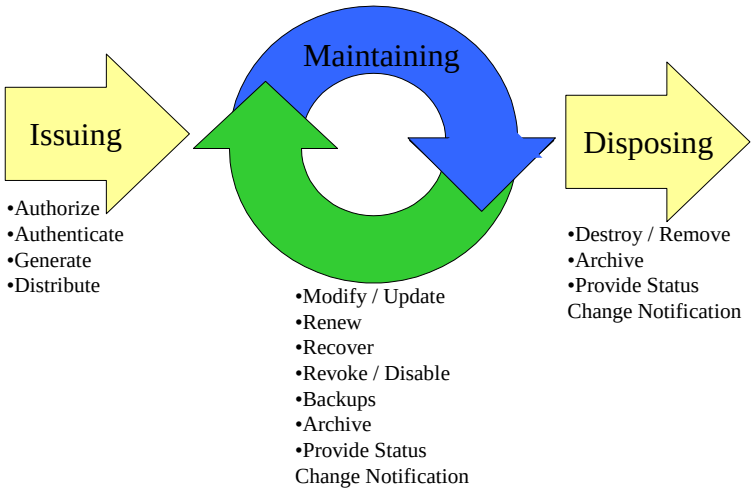


Figure 1 – Credential Management Process

The extent to which these processes are relevant to a particular credential management life cycle depends on the characteristics of the particular credential, the media on which it exists, and the environment in which it is intended for use. For this reason, the management of the system or physical token on which credentials exist should be considered an integral part of the credential management life cycle.

Reliability of the Credential

Credentials are issued with the purpose of establishing an identity with a certain degree of confidence. The reliability of the credential is not only dependent on the observable characteristics of that credential, but on the underlying process used to authenticate the identity of its owner, the binding between that authenticated identity and the credential, and the integrity of the system maintaining and supporting the credential.

Passwords or pass-phrases, Kerberos tickets and digital certificates are examples of electronic credentials. Some observable characteristics of such types of credentials include password length, key-size, and choice of cryptographic algorithm. The use of a digital certificate containing a large factor public key signed using a highly secure cryptographic system does say something about the reliability of a

certificate as a credential, but it is in itself meaningless. Cryptographic strength is meaningless unless great care is used to authenticate the owner of the public key and the disclosures made by the credential issuer provides sufficient reassurance of the integrity of its operations and certificate management practices, thus generating confidence in the binding between the certificate and the identity of its subject.

Reliability of the Token

Tokens conveying electronic credentials must do so reliably. The reliability of the tokens depends on their physical characteristics and the quality of the underlying token management system and processes. The physical characteristics of the token include form factors, appearance, types of information displayed externally, internal storage capacity, interfaces, sturdiness, et cetera. To be considered reliable, tokens need to be able to withstand normal wear, be compatible with the systems with which they are intended to interface, and be able to convey accurately the credentials they carry.

The token management process must be an integral part of the credential management life cycle. It needs to be well defined and tailored to support the particular type of credential. The nature of the credential and the sensitivity (intrinsic value) of the resources it provides access to will dictate how strict the inventory controls on blank and active tokens must be. Also, the token delivery mechanism (e.g., in-person, by mail, by courier) and whether tokens are delivered active and ready to use will impact inventory-control requirements and other token management details. In general good token inventory controls should be implemented that include maintaining accurate custody records at all times. Coordination with the credential management is necessary to ensure that tokens are available on which to load newly issued credentials.

In addition to token inventory and delivery controls, contingencies should be in place to address lost or damaged tokens. These functions are critical to ensuring timely authorized access to IT resources and data. These functions should be integrated with help desk and credential management functions.

Strength of Binding

There should be a strong bond between credentials and their owners. The ways in which such bonds are established vary according to the type of credential. The binding between the credential and its owner's identity starts by establishing the owner's identity and obtaining authorization to issue the credential. Typically, after the credential is issued (sometimes on a token, i.e., "something you have"), usually a secret ("something you know") and / or a biometric ("something you are") are used to maintain such binding. For example, an employee may be issued a badge upon employment, that badge would be the token on which a digital certificate (a credential) is loaded to computing resources and data. Also, there is a separate credential on the token that gives her access to the building and her work area within that building. The issuance of these credentials and the assignment of privileges are authorized by management. To use the certificate credential, she needs to enter a password that activates the associated private key on the token. For physical access, guards may inspect the picture on the card (a type of biometric) and look her name up on an access list. The strength of the binding between a token and a credential and the identity of the credential owner ultimately is evaluated according to the nature of the access provided. The measures that can be considered strong binding in one environment may not be sufficient in others. Having a picture on a badge may be considered a strong binding at a guard's checkpoint, but would do little at a door activated by a proximity reader. Sometimes, multiple mechanisms are needed to provide the necessary binding under different situations even when the same token and the same credential are used.

Reliability of Credential Management System

Ultimately, the reliability of an electronic credential relies on the reliability of the system that manages it. A system that does not prevent insiders from subverting control mechanisms, or outsiders from spoofing, will expose to misuse the resources it is intended to safeguard. Even systems based on the same type of credential and token will differ. Most commonly, differences in the operating environment translate into variations of manual processes. All systems must therefore be evaluated individually. The Federal

Government has standards, guidelines, and regulations intended to address the need to evaluate the controls and security of IT systems. The banking industry, among others, also has a body of standards and practices on which to base the evaluation of the controls and security of their computer-based systems. Although a sufficient body of standards and practices exist, there is little uniformity. The use of these standards and practices can be costly and resource intensive, and consensus is needed on their selection and application among parties relying on electronic authentication as a technical enabler for electronic services.

The following list of elements for assessing the security of credentials stored on tokens was extracted from the American Bar Association (ABA) PKI Assessment Guidelines (PAG). The first column identifies types of controls that should be assessed in evaluating the security and reliability of electronic authentication systems. The second column is a placeholder for pointers to further information and guidelines for the implementation and evaluation of the respective controls. While originally PKI-specific, the list of system controls serves to cover all elements of credential management system controls and works equally well for UserID/password type credentials. Also, while the following list comes from the American Bar Association, it is largely compatible with other lists of auditable credential management elements found in other assessment schemas, i.e., ANSI X9.79 and the AICPA WebTrust model.

E-Authentication System Controls	Reference
Self-assessment and third party oversight	
Management, change control, backup of mission-critical systems	
Means by which a given user is identified and user identity is authenticated (identity proofing)	
Policies have titles that accurately match the LOA desired	
Validation procedures	
Validation procedures for identity credentialing authority	
Sufficient information presented to validate identity and that critical information is not placed in non-validated category	
Acceptance procedures for presented credentials	
Whether automatic renewal is permitted	
Credential reissuing procedures	
Credential revocation procedures	
Auditing and logging	
Frequency of review of audit logs	
Crypto algorithms and key lengths for credential and issuer credential	
Control over credential generation	
Credential distribution process and controls	
Credential activation process	
Trustworthiness of personnel operating systems for activation, deactivation and destruction of credentials	

Length of archiving	
Completeness of documentation of computer security controls	
Hardware and software security ratings	
Network security controls	
Formal approval procedures for policies and procedures documents	
Subscriber agreements	

Conclusion

Credential management is the process of issuing, maintaining, and disposing of credentials. The trustworthiness of electronic credentials is entwined with the environment in which they are used, the processes used to manage the credentials, the tokens or media on which the credentials reside, and the processes used to manage such tokens. The management processes for credentials and tokens need to be integrated and matched to the intended level of assurance. The implementation of credential and token management processes should be assessed on a periodic basis to ensure they continue to match the necessary assurance levels.

Appendix B-C: An Approach to Calculating Identity Assurance

If it were possible to come up with an algorithm for calculating the degree of confidence a transaction partner could have in a proffered electronic credential, and if it were possible to have this approach widely accepted, it would go a long way towards solving the thorny problems of trust associated with agreeing on the meaning of levels of assurance of identity among e-business and e-government service providers.

In the absence of a single reference standard for LOA such as the Federal Government has (and it is not inconceivable that such a reference standard may be implemented), it may be possible to create an algorithm that yields a reliable calculation of LOA for Authorization purposes. In fact, it is possible that a reliable algorithm running a comprehensive set of implementations may in fact discover a standard set of LOA that may be generally adopted. Certainly, the Government's guideline document, while being a great advance in this area, may not present a model that satisfies the needs of the private sector.

This Appendix presents an approach for calculating LOA.

As discussed above, two general categories of consideration comprise the elements involved in determining LOA: the "absolute" degree to which a person or device is known to the credential issuer based exclusively on identity proofing activities and the trustworthiness of the credential on token.

Graphing Confidence in Identity

As we have discussed, there are elements associated with each of these two categories. For Identity Proofing, see Appendix A, above. Since each element identified in Identity Proofing has a weight, that is, each element is not equally valuable, it is at least theoretically possible to assign a numeric value to each. Weight increases with value, broadly defined, so that self-assertion carries a weight of 2 (context carries a weight of 1), while in-person proofing with an official biometric credential that is validated against the issuing database carries a weight of, say, 30 (arbitrary).

There are "geometric" considerations. The credential issuer will always know if it is dealing with a human, or a device, or lines of code, or a fictional character such as Don Quixote de la Mancha. Therefore, the credentialing authority will never have zero identity information about a credential candidate. On the other end of the spectrum, there comes a point at which the credential issuer is 100% sure of the identity of a candidate and further documentation of whatever kind, does not result in increased confidence in the candidate's identity. In general, then, the more and better information an issuer has about a candidate's identity, the more confidence it has in the identity proofed, up to absolute or 100% certainty.

Consider an ID Proofing session that includes an in-person proofing supported by a biometrically-enabled identity token that is validated against the database that issued the credential on the token plus a credit reporting agency query that matches information given by the candidate or printed on the token is a top. Additional identity validation does not yield more assurance of identity.

Whether or not absolute certainty is an attainable condition or not is an open question; it is possible, however, to demonstrate that it can be approached, as though it were the integral of the function. In practical, real-world terms, it is possible to attain the equivalent of 100% certainty of identity. We refrain from invoking the philosophical concerns of late nineteenth and twentieth century existentialists, psychologists and epistemologists.

We can present this as a graph, with the X axis being numbers from one through 100 (for example), representing the sum of the values of the identity proofing elements that a candidate successfully

satisfies, and the Y axis being the percentage of certainty the credential provider has in the identity proofed.

The trick is in knowing how to array the sum of an identity proofing event (X axis) against the confidence in that proofing (the Y axis). In order to approach a solution for this problem, we can begin with the methodology the Federal Government has laid out in its documentation. Using those as broad guidelines, we shall plot them. Since OMB guidance gives us four LOA, we shall use those to represent:

under 25% confidence at Level 1;

25% - 50% confidence at Level 2;

50% - 75% confidence at Level 3;

75% - 100% confidence at Level 4,

Using four bands of the same size is a generalization for purposes of modeling and may not turn out to be a valid assumption. Nevertheless, with this initial estimate we can begin construction of an actual graph

Assigning a numeric value to each proofing element, then summing, gives a number. The Federal Bridge CA Certificate Policy categorizes satisfactory identity proofing for four levels of assurance of identity. While the government has been very careful not to equate the two scales, it is possible to use both for purposes of arraying proofing sums against broad percentages of confidence. Discrepancies should be of interest to the government, assuming they do not demonstrate methodological incompetence!

An Arbitrary Table of Identity Proofing Elements and Weights

Mechanism	**Weight**
Environmental context	1
Self-assertion of identity	2
Unofficial breeder document	2
3rd Party Assertion of identity, e.g., Notary	5
Unvalidated Official breeder document	2 each to 3x
Unvalidated official breeder document with biometric	2 each to 3x
validated official breeder document	10 each to 3x
validated official breeder document with biometric	15 each to 3x
Credit Reporting Agency or equivalent (external) database lookup	3 each to 2
In-person proofing	20

The Federal Bridge CA considers presentation of two antecedent tokens with biometrics (driver's license, government ID card, passport, etc.) presented in person, where at least one of the tokens is validated

against the issuer database, to satisfy the *identity proofing* requirements for High Level of Assurance. (Other credential, token and process requirements, not germane to this graph, also must be met.)

Candidates for national security clearances must go through much more rigorous identity proofing than the Federal Bridge requires for High Assurance. Nevertheless, this gives us a data point in the top quartile. Since the FBCA Certificate Policy requires this degree of identity proofing in order to issue a High assurance credential, we should probably consider this the lower limit of High. Also, this exercise demonstrates that no single identity proofing element by itself is sufficient to satisfy the requirement for high LOA.

The total weight using this completely arbitrary model works out to be:

In-Person Proofing	20
One biometric validated official breeder document	15
One unvalidated biometric official breeder document	2
Total 37	

Q.E.D. the government minimum for the 75th percentile of confidence in identity is 37.

We now have two data points: the minimum, which as noted previously is not zero but one (context).

For medium assurance, the Federal Common Policy for PKI requires:

In-person proofing	20
One biometric validated official breeder document	15
Total	35

Or

In-person proofing	20
One Credit Reporting Agency or equivalent (external) database lookup	3
Total	23

A fudge factor is included in the Common Policy Medium level to accommodate remote employees who cannot easily or inexpensively satisfy the in-person proofing requirements, but the language describing this loophole is sufficiently vague to make actual mapping impossible. How does one put a metric on "RAs may accept notarized authentication of an applicant's identity to support identity proofing of remote applicants, assuming agency identity badging requirements are otherwise satisfied," for example?

So, the Federal Common Policy for PKI gives two data points for Medium, the lower of which we can suggest should be the minimum or 50th percentile, while the more rigorous one, weighing nearly as much as the High Assurance Level, should be near the high end of the quartile, near 75%.

In another example, a teenager applies for her first learner's permit. In order to satisfy the identity proofing requirement in Maryland, the child must perform the following *identity proofing* activities:

In-person proofing	20
3rd Party Assertion of Identity	3
One unvalidated, non-biometric breeder document	2

Total	25

So, in order to acquire an official Authorization token (learner's permit), the child must present 25 points' worth of identity proofing credentials. One then concludes that to be authorized to drive in Maryland, a Medium LOA Authentication is required for Authorization. This seems a reasonable conclusion.

It might be beneficial to spread the numbers out some more (that is, raise the weight on in-person proofing and validated biometric breeder document, in order to get a bigger spread.

Graphing Confidence in Credential Management

In the same way that an algorithm can be found that models the identity proofing process and returns a specific number for a specific implementation, an algorithm may be generated that models the reliability, or trustworthiness of a particular credential management scheme. This is especially true as identity credential management systems already are subjected to independent assessment by trained auditors during structured reviews. Adding a metric element to the assessment process would seem to be a minor extension of current practice.

What is needed is a model for assigning numeric values to the reliability of elements. The process described for identity proofing, above, may be replicated for credential management. This could leave us with two graphs, one for each of the two key elements of determining LOA.

Preferably, a single graph may be constructed, with the identity proofing metric for an electronic identity process on one axis and the credential management metric on the other. The results of many model runs would likely yield a scattergram that may be mathematically described and from which "objective" levels of assurance or trust would become visible. The mathematical models for this process have yet to be defined, but they clearly call for longitudinal inputs.

A third dimension, representing the reliability of the credential processing model, might be added to yield a view of the reliability of the overall process of using electronic identity credentials in a business process. Further discussion of this point is presented in a companion document to this one, still in preparation.

The reason a single graph is preferable to two related graphs is that the two factors are mutually dependent: very reliable identity proofing is debased by unreliable credential management, and vice versa. Assurance of identity is based on both identity proofing and credential management, so both metrics are needed to yield a single compound number on a curve or associated with a cluster.

The E-Authentication Partnership recommends that the Algorithmic method be subjected to further study to clarify outstanding issues and to determine whether or not it can usefully return data that can determine LOA for an instance of credential service provision.

Appendix C. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Chairs:

Abbie Barber, Bank of America
Don Thibeau, OIX

Editors:

Shaheen Abdul Jabbar, JPMorgan Chase Bank, N.A.
Peter Alterman, SAFE-BioPharma Association
Abbie Barber, Bank of America
Steve Olshansky, Individual Member
Mary Ruddy, Identity Commons

Document Contributors:

Shaheen Abdul Jabbar, JPMorgan Chase Bank, N.A.
Peter Alterman, SAFE-BioPharma Association
Abbie Barber, Bank of America
Leif Johansson, SUNET/NORDUnet
Rebecca Nielsen, Booz Allen Hamilton
Steve Olshansky, Individual Member
Mary Ruddy, Identity Commons
Shahrokh Shahidzadeh, Intel
Cathy Tilton, Daon
Colin Wallis, New Zealand Government
Thomas Hardjono, M.I.T.

Technical Committee Member Participants:

David Brossard, Axiomatics
Abbie Barbir, Bank of America, Chair
Antonio Campanile, Bank of America
William Barnhill, Booz Allen Hamilton
Rebecca Nielsen, Booz Allen Hamilton
Brendan Peter, CA Technologies
Brian Spector, CertiVox Ltd.
Cathy Tilton, Daon
Mary Ruddy, Identity Commons
Rainer Hoerbe, Individual
Gershon Janssen, Individual
Jaap Kuipers, Individual
Carl Mattocks, Individual
Steve Olshansky, Individual
Shahrokh Shahidzadeh, Intel Corporation
Lucy Lynch, Internet Society (ISOC)
Shaheen Abdul Jabbar, JPMorgan Chase Bank, N.A.
Anthony Bass, Lockheed Martin
Scott Fitch, Lockheed Martin
Daniel Greenwood, M.I.T.
Thomas Hardjono, M.I.T.
Colin Wallis, New Zealand Government

Kevin Mangold, NIST
John Bradley, Open Identity Exchange
Don Thibeau, Open Identity Exchange, Chair
Anil Saldhana, Red Hat
Peter Alterman, SAFE-BioPharma Assn
Doron Cohen, SafeNet, Inc.
John Walsh, Sypris Electronics
Marty Schleiff, The Boeing Company
Dale Rickards, Verizon Business
Ed Coyne, Veterans Health Administration
John Davis, Veterans Health Administration
Suzanne Gonzales-Webb, Veterans Health Administration
Mohammad Jafari, Veterans Health Administration
Anthony Rutkowski, Yaana Technologies, LLC

Appendix D. Revision History

Revision	Date	Editor	Changes Made
0.1	7-Jun, 2013	Steve Olshansky	Initial Draft
0.2	24-June, 2013	Steve Olshansky	Per "track changes" from v0.1; deleted "Philosophical Approach" section carried over from 2nd deliverable, added venn diagram and related text, added text about reaching LoA4, other minor edits.
0.3	11-July, 2013	Steve Olshansky	Per "track changes" from v0.2; deleted N/A rows from table, added 800-63 legend and ITU-T X.1254 Authentication phase threat definitions to table, added placeholder Appendix D (Glossary), other minor edits.
0.4	22-August, 2013	Peter Alterman Steve Olshansky	Per "track changes" from v0.3; bash exercise, major cleanup and reorganization, moved table to Appendix A, added Appendix B "Use Case Examples"
0.5	5-September, 2013	Peter Alterman Steve Olshansky	Cleanup and reorganization, changed use case, added Conformance statement, moved table to back into document body.
0.6	10-September, 2013	Peter Alterman Abbie Barbir Steve Olshansky Colin Wallis	Minor updates and cleanup to prepare for wider distribution for community review and feedback.
0.7	17-October-2013	Peter Alterman Leif Johansson Steve Olshansky	Added minor clarifications throughout, added ISO/IEC 27001 references column to table, added Appendix B white paper.
0.8	30-October-2013	Steve Olshansky	Added non-normative references to CESG Good Practice Guides.
0.9	1-November-2013	Peter Alterman Steve Olshansky Shahrokh Shahidzadeh	Minor edits throughout.
0.10	6-December-2013	Steve Olshansky	Minor edits throughout.