Electronic Identity Credential Trust Elevation Framework Version 1.0

Committee Specification 01

22 May 2014

Specification URIs

This version:

http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/cs01/trust-el-framework-v1.0-cs01.doc (Authoritative)
http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/cs01/trust-el-framework-v1.0-cs01.html
http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/cs01/trust-el-framework-v1.0-cs01.pdf

Previous version:

http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/csprd01/trust-el-framework-v1.0-csprd01.doc (Authoritative)
http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/csprd01/trust-el-framework-v1.0-csprd01.html
http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/csprd01/trust-el-framework-v1.0-csprd01.pdf

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 https://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 (https://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. 22 May 2014. OASIS Committee Specification 01. http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/cs01/trust-el-framework-v1.0-cs01.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 https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction

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
(Note that this Publication has been superseded by SP 800-53-3 and -4; see note in text for further comment.)

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

Risk Assessment Methodologies National Strategy for Trusted Identities in Cyberspace (NSTIC), April 25, 2013, http://nstic.blogs.govdelivery.com/2013/04/25/risk-assessment-methodologies-and-authentication-strength/

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) **Risk 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) I**nformation 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

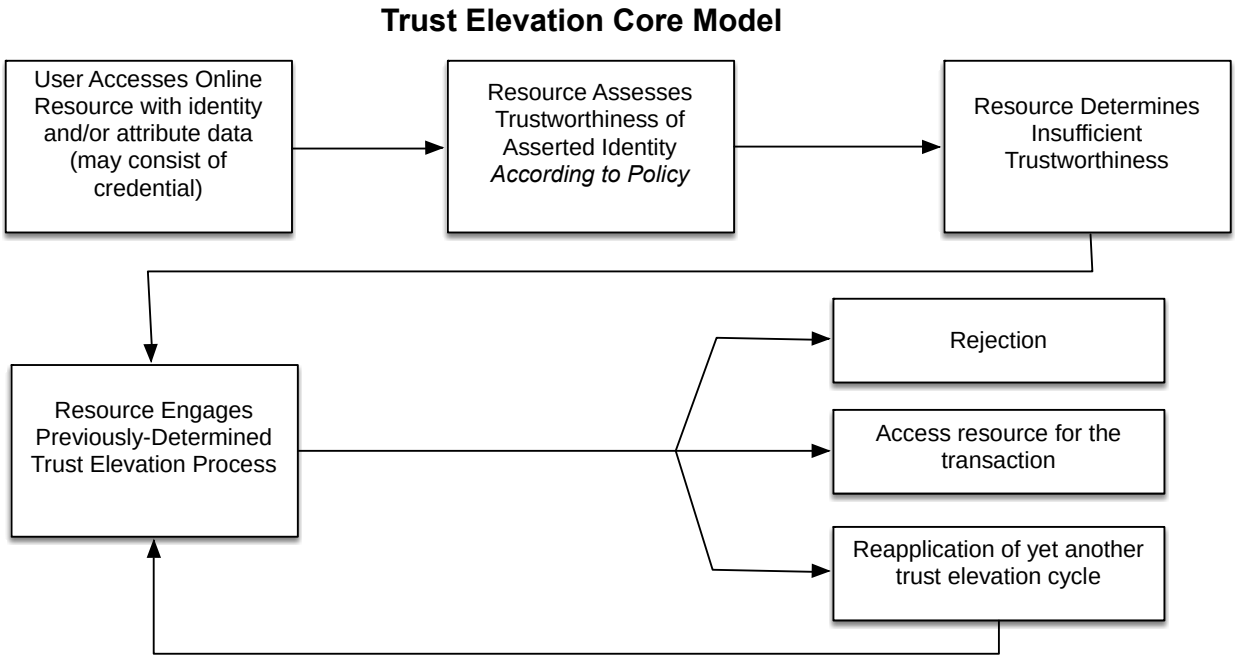
CESG Good Practice Guide 45 CESG (UK National Technical Authority on Information Assurance) and UK Cabinet Office, Government Digital Services, **Identity Proofing and Verification of an Individual**, issue 2.1, September 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204448/GPG_45_Identity_proofing_and_verification_of_an_individual_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 (ITU-T X.1254),
- to array each of the models against those criteria in such a way that they could be compared to each other (the columns), and
- to create viable crosswalks between models by aligning each one's elements with the common threat vectors from X.1254 in rows.

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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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 (NOTE: THE EXTENT TO WHICH ENABLED CONTROLS SATISFACTORILY MITIGATE THREAT IS DETERMINED BY THE RP)	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 800-63-2	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

- Note: While this version of SP 800-53 has been superseded by -3 and -4, the Technical Committee determined that the requirements had not been affected by the revisions and so the presented version was still valid. That said, the Technical Committee expects the contents of this table to require updating over time.

4 Risk Assessment Methodologies and Authentication Strength

Note: This clause quotes extensively from 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 "(LOA). "[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. "[O]therwise, a fundamental component of interoperability across operators is missing. If relying parties [(RPs)] and Identity Providers [(IdPs)] assess identity risks in different ways: they are unable to articulate their requirements using a common lexicon; deployments end up being done in an ad hoc manner; and relying parties 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. For example, 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.

"[T]he ability for 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.

"The capabilities of identity proofing and authentication have historically 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 will also affect the potential [for] interoperability, or [mutual] recognition, of the credential by other subsequent 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,* especially Section 3.1, 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.

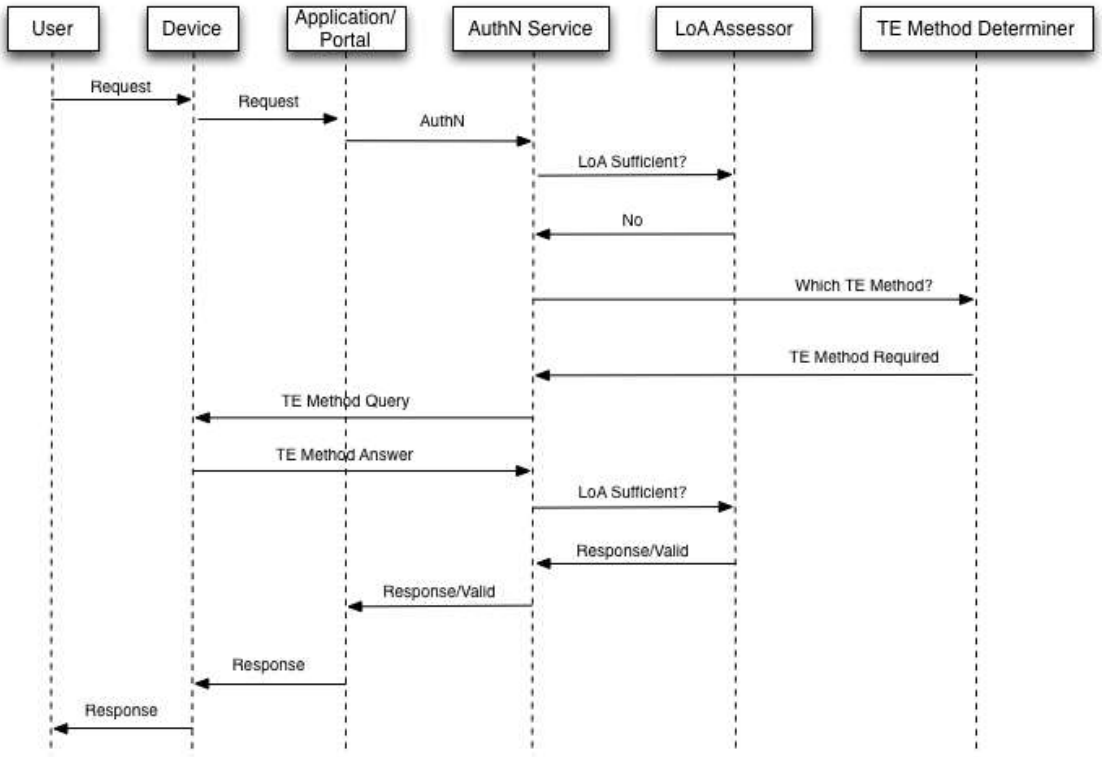


Figure 1. Trust Elevation Use Case Process Flow

Appendix B. Acknowledgements

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

Chairs:

Abbie Barbir, Bank of America
Don Thibeau, OIX

Editors:

Shaheen Abdul Jabbar, JPMorgan Chase Bank, N.A.
Peter Alterman, SAFE-BioPharma Association
Abbie Barbir, 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 Barbir, 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 C. 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.
0.11	12-March-2014	Peter Alterman Steve Olshansky	Minor edits throughout to address comments received.
0.12	31-March-2014	Peter Alterman Steve Olshansky	Minor edits in section 4 to clarify quotations and address comments received; minor edits in table to address comments received, removed appendix white paper: “E-Authentication Partnership Policy…”
0.13	31-March-2014	Steve Olshansky	Cleanup for submission for final TC vote.