Authentication Step-Up Protocol and Metadata Version 1.0

Candidate OASIS Standard 01

06 March 2017

Specification URIs

This version:

http://docs.oasis-open.org/trust-el/trust-el-protocol/v1.0/cos01/trust-el-protocol-v1.0-cos01.docx (Authoritative)
http://docs.oasis-open.org/trust-el/trust-el-protocol/v1.0/cos01/trust-el-protocol-v1.0-cos01.html
http://docs.oasis-open.org/trust-el/trust-el-protocol/v1.0/cos01/trust-el-protocol-v1.0-cos01.pdf

Previous version:

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

Latest version:

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

Technical Committee:

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

Chairs:

Abbie Barbir (barbira@aetna.com), Aetna
Don Thibeau (don@openidentityexchange.org), Open Identity Exchange

Editors:

Andrew Hughes (AndrewHughes3000@gmail.com), Individual
Peter Alterman (palterman@safe-biopharma.org), SAFE-BioPharma Assn.
Shaheen Abdul Jabbar (shaheen.abduljabbar@jpmchase.com), JPMorgan Chase Bank, N.A.
Abbie Barbir (barbira@aetna.com), Aetna
Mary Ruddy (mary@meristic.com), Identity Commons

Related work:

This specification is related to:

- *Analysis of Methods of Trust Elevation Version 1.0.* Work in progress. https://www.oasis-open.org/committees/download.php/48768.
- *Survey of Methods of Trust Elevation Version 1.0.* Work in progress. https://www.oasis-open.org/committees/download.php/46987/trust-el-survey-v1.0-wd01.doc.
- *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.

Abstract:

Electronic Identity Credential Trust Elevation Methods are used to increase assurance in entity identification using authentication events and related entity information for the purpose of risk mitigation when making access control policy decisions.

The goals of this fourth deliverable are:

- To propose simple Trust Elevation architectural patterns demonstrating the use of Trust Elevation in modern Access Control architectures.
- To describe a common metadata set, mechanisms and protocol elements for Trust Elevation information exchanges.
- To promote the use of Trust Elevation elements to facilitate standardization among the many technologies and approaches currently in use for credential & authentication risk mitigation.

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. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=trust-el#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC'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 TC's web page (https://www.oasis-open.org/committees/trust-el/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Citation format:

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

[Trust-El-Protocol-v1.0]

Authentication Step-Up Protocol and Metadata Version 1.0. Edited by Andrew Hughes, Peter Alterman, Shaheen Abdul Jabbar, Abbie Barbir, and Mary Ruddy. 06 March 2017. Candidate OASIS Standard 01. http://docs.oasis-open.org/trust-el/trust-el-protocol/v1.0/cos01/trust-el-protocol-v1.0-cos01.html. Latest version: http://docs.oasis-open.org/trust-el/trust-el-protocol/v1.0/trust-el-protocol-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

All text is normative except for labeled examples and notes.

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

[trust-el-analysis-v1.0]

Analysis of Methods of Trust Elevation Version 1.0. Edited by Peter Alterman, Shaheen Abdul Jaabar, Jaap Kuipers, Thomas Hardjono, and Mary Ruddy.Work in progress. https://www.oasis-open.org/committees/download.php/48768

[trust-el-survey-v1.0]

Survey of Methods of Trust Elevation Version 1.0. Edited by Peter Alterman, Shaheen Abdul Jabbar, Jaap Kuipers, Thomas Hardjono and Mary Ruddy. Work in progress. https://www.oasis-open.org/committees/download.php/46987

[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

[NIST800-63-2] *NIST Special Publication 800-63-2, Electronic Authentication Guideline*, August 2013. http://dx.doi.org/10.6028/NIST.SP.800-63-2

[NIST800-162] *NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, January 2014. http://dx.doi.org/10.6028/NIST.SP.800-162

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[UMA] Hardjono, T., Maler, E., Machulak, M., Catalano, D. *User-Managed Access (UMA) Profile of OAuth 2.0,* April 2015. https://docs.kantarainitiative.org/uma/rec-uma-core.html

[X.1252] Recommendation ITU-T X.1252 (2010). *Baseline identity management terms and definitions.* http://handle.itu.int/11.1002/1000/10440

[XACML3] OASIS Standard, eXtensible Access Control Markup Language (XACML) Version 3.0, 22 January 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.doc

1.3 Non-Normative References

[ISO ISMS] ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, 2014.

[NIST800-37-1] NIST Special Publication 800-37 r1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, June 2014. http://dx.doi.org/10.6028/NIST.SP.800-37r1

[IDMgmt] Backend Attribute Exchange (BAE) v2.0 Overview

https://gsageo.force.com/IDM/servlet/fileField?entityId=ka0t0000000TNIkAAO&field=File__Body__s

[OAuth2] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <http://www.rfc-editor.org/info/rfc6749>.

[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

[OpenID.Core] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0," August 2015. http://openid.net/specs/openid-connect-core-1_0.html

[SAML2] OASIS Standard, Security Assertion Markup Language (SAML) Version 2.0, 2 December 2009. https://www.oasis-open.org/committees/download.php/35711/sstc-saml-core-errata-2.0-wd-06-diff.pdf

[SAMLAC] OASIS Standard, Authentication Context for the OASIS Security Assertion Markup Language (SAML) Version 2.0, 15 March 2005. https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

[X.1254] Recommendation ITU-T X.1254 (09/2012). *ITU Telecommunication Standardization Sector (ITU-T) Entity authentication assurance framework*. http://handle.itu.int/11.1002/1000/11608

[X.1255] Recommendation ITU-T X.1255 (09/2013). Framework for discovery of identity management information. http://handle.itu.int/11.1002/1000/11951

2 Landscape and Context

This document, the fourth deliverable of the OASIS Trust Elevation Technical Committee, builds on the work of the first three. To recap: the first deliverable, *Survey of Methods of Trust Elevation Version 1.0* **[trust-el-survey-v1.0]**, consists of a broad overview of current and near-future online trust elevation techniques used for (or capable of) elevating 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* **[trust-el-analysis-v1.0]**, 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 identified mechanisms has been included in that deliverable. The third deliverable, *Electronic Identity Credential Trust Elevation Framework Version 1.0* **[trust-el-framework-v1.0]**, is an abstraction intended to help to develop applications conforming to an accepted way of elevating trust of a digital identity.

As has been the pattern for this TC's deliverables, this fourth deliverable builds on the work of the first three and specifies design considerations, implementation considerations and metadata for the elevation of trust through increased identification.

2.1 Goals of the Fourth Deliverable

Trust Elevation Methods are used to increase assurance in entity identification using authentication events and related entity information for the purpose of risk mitigation when making access control policy decisions.

The goals of this Fourth Deliverable are:

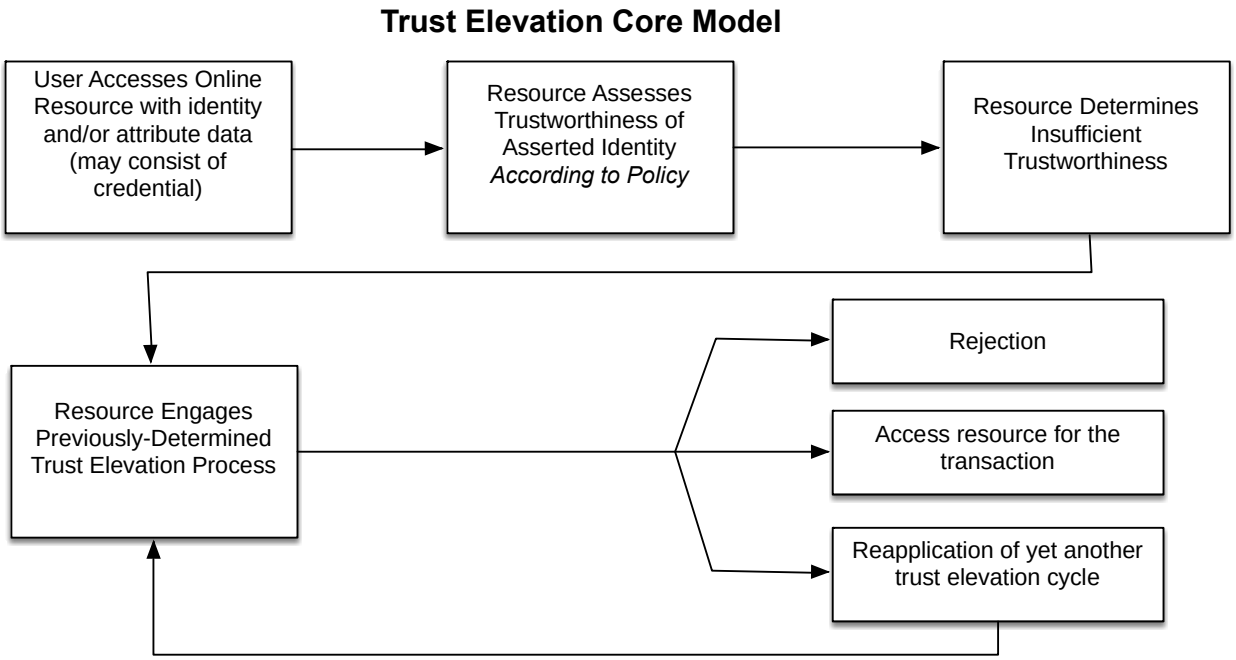
- To propose simple Trust Elevation architectural patterns demonstrating the use of Trust Elevation in modern Access Control architectures.
- To describe a common metadata set, mechanisms and protocol elements for Trust Elevation information exchanges.
- To promote the use of Trust Elevation elements to facilitate standardization among the many technologies and approaches currently in use for credential & authentication risk mitigation.

3 Conceptual Models

This section is non-normative.

3.1 Trust Elevation Core Model

As described in *Electronic Identity Credential Trust Elevation Framework Version 1.0,* the following depicts the core model for Trust Elevation.



3.2 Trust Elevation Concepts

While the flow diagram above is easy to understand, implicit in the core model are several key components and processes, as shown in Section 4.2. The first of these is a component which functions as a policy engine capable of consuming the asserted user data and making a determination as to whether that data satisfies the resource's policy for authentication risk mitigation. The resource manager must have previously performed a risk assessment and adopted a risk mitigation strategy (**[NIST RMF]** and **[ISO ISMS]** are examples of methodologies for these antecedent steps).

The second key component is again an antecedent service generated during the risk assessment and mitigation process. It is composed of a capability to recognize which, if any, risks have been adequately mitigated by the initial transaction, which risks remain to be mitigated and preferred methods for satisfying the remaining needs.

The third key component is a component for evaluating the success of the trust elevation transaction. This could be an iteration of the first component, but it has been broken out in the above graphic to clarify the decision flow.

While these components are necessary to implement trust elevation of a presented online identity, they require the resource manager to have engaged in prior planning and assessments in order to generate the information necessary to direct the behavior of the components. In addition to implementing recognized, standards-based risk assessments, the prior work of this Technical Committee provide the

necessary guidance for populating the decision-making components of the core model as well as most comparable models.

Trust Elevation methods are used to increase confidence in entity identification using authentication events and related entity information for the purpose of increased risk mitigation when making access control policy decisions.

Levels of Assurance models are structured such that increased risk mitigation results in increased credential or identity assurance level trust. These models require determination of a given transaction's identity and authentication risk, expressed in terms of level of assurance requirements. Policies are designed such that credential or identity assurance level must meet or exceed the transaction's level of assurance requirement.

As described in *Electronic Identity Credential Trust Elevation Framework Version 1.0*, entity identification confidence may be increased by: mitigating an authentication threat not addressed by the original authentication exchange; improved mitigation of the original authentication threat, or examination of contextual or environmental factors to corroborate the existing identification.

The definition of the composition of a particular assurance level scheme, and related policy evaluation criteria, is the responsibility of the parties involved in the transactions. The scheme should be tailored to the risk tolerance and requirements of the relying party. In other words, it is up to the resource manager to determine when sufficient mitigations of risk have occurred.

3.3 Use of Authorization Architectures and Models

Another way to look at Trust Elevation is as a species of transaction or access control authorization. From this perspective, evaluation of the current state versus policy requirements results in decisions to 'Permit', 'Deny', or 'Require Elevation'.

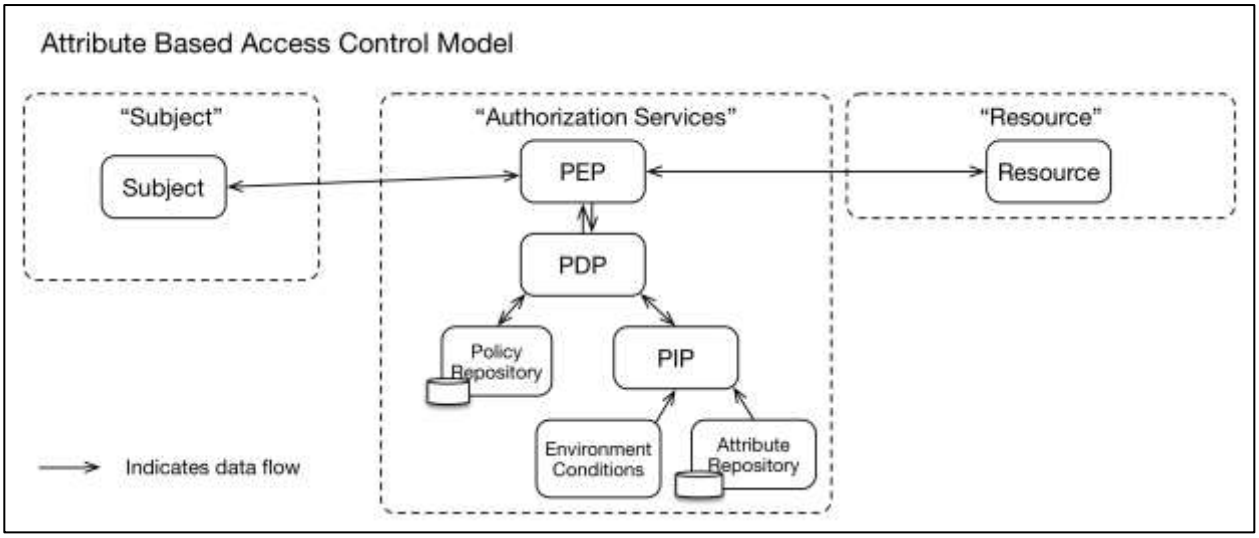
The Trust Elevation core model is compatible with other published authorization models, such as: Attribute Based Access Control (ABAC) **[NIST800-162]**, User Managed Access (**[UMA]**), **[OAuth2]**, **[XACML3]**, and SAML Backend Attribute Exchange.

3.3.1 Attribute Based Access Control Model

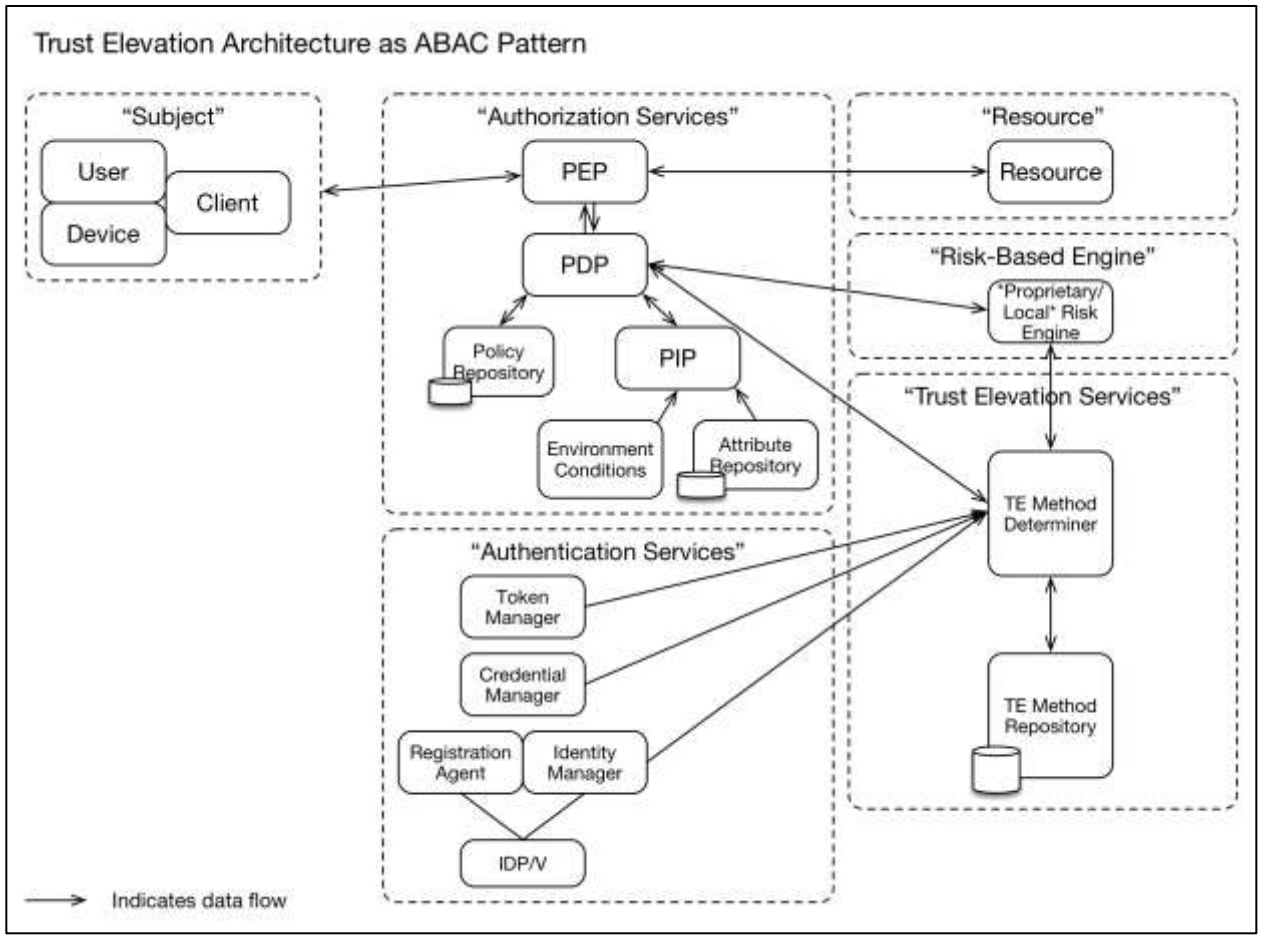
This section illustrates how Trust Elevation would fit into an Attribute Based Access Control model.

[NIST SP800-162] describes the elements of an Attribute Based Access Control Model.

As shown in the figure below, the primary components of Authorization Services are the Policy Enforcement Point (PEP) which intercepts resource requests; and, the Policy Decision Point (PDP) which checks supplied attributes versus access control policy. The PDP can obtain additional attributes from environmental conditions, Policy Information Point (PIP) and other sources. Based on the policy evaluation, the PDP instructs the PEP to permit or deny access to the resource.



In the diagram below, when the Authorization Services determine that Trust Elevation is required, the Trust Elevation Services take information from “Authentication Services” and “Risk-Based Engine” to evaluate what Trust Elevation Method should be used to achieve the desired result.



3.3.2 User Managed Access Authorization Model

The User-Managed Access protocol (UMA) defines a mechanism for a policy enforcement point – known as the resource server – to delegate authorization of a requesting party to a policy decision point – known as the authorization server – using elements of the OAuth 2.0 authorization framework.

To gain access to a protected resource, an UMA client (web or mobile application operating on behalf of a requesting party) must present a valid access token, called a requesting party token (RPT), to the resource server. The RPT must be valid and associated with sufficient authorization data, issued through a trust elevation process, before the resource server can grant access.

The authorization server, guided by policies set by the owner of the protected resource, elevates trust by testing whether the requesting party meets the policies. As part of this process, it could demand that the requesting party (or the client on their behalf) provide claims, such as identity information or even promises to adhere to constraints set by the resource owner, such as an embargo on information release until a certain date.

One policy the authorization server can consider is what mechanism was used to authenticate the person. UMA doesn’t require use of any particular authentication protocol, but works especially well with OpenID Connect.

The OpenID Connect Core specification defines two claims in the ID Token format called `acr` and `amr`, which provide details about what type of authentication was performed. Their values can be defined by a

domain, a federation, a global registry, or some other trust framework. An UMA authorization server can test a requesting party against policies to evaluate the sufficiency of the authentication mechanism as provided in values of these claims.

In the event that the mechanism was not sufficient, the authorization server can indicate the reason for the authorization failure and what type of credentials would satisfy the policy. At this point, the client can request re-authentication from the OpenID Provider and ultimately re-request the RPT token. This flow would constitute trust elevation by step-up authentication.

3.3.3 XACML Authorization Model

The eXtensible Access Control Markup Language (XACML) standard defines a reference architecture for Attribute-Based Access Control (ABAC), a language for expressing access control rules and policies, and a protocol for generating and processing access control requests and returning responses.

Access to resources is mediated by a Policy Enforcement Point (PEP), which relies on decisions from a Policy Decision Point (PDP). When a user attempts to access a protected resource, the PEP assembles a request, which provides attributes about the user, the resource, the environment, and the action requested. The PEP communicates the request to the PDP, which evaluates it according to pre-defined policies.

To perform Trust Elevation, the access control policy can specify how users must be authenticated, including parameters such as authentication method, credentials accepted, and levels of assurance. Trust elevation in this context means enhancing authentication and/or authorization by means of requiring additional attributes.

Consider the following example: a user requests access to a protected resource. The access control policy governing the resource requires multi-factor authentication using a strongly vetted identity credential by means of setting the MustBePresent attribute to TRUE. The PEP controlling access to the resource has only hitherto validated the user identity by means of a lower assurance username/password combination. When the PEP initially formulates the request, it bases the user identity attribute on the previous username/password authentication event. When the PDP receives the request, it evaluates the request according to the appropriate policy, based on the resource. Since MustBePresent = TRUE, the PDP renders an “Indeterminate” decision, with a status code of “urn:oasis:names:tc:xacml:1.0:status:missing-attribute”. Upon receiving this “Indeterminate” with MissingAttribute status decision from the PDP, the PEP may resubmit a request after acquiring the proper attributes. In this case, the proper attributes could only be gathered through a step-up authentication event. This sequence constitutes a sample Trust Elevation event.

Alternatively, security administrators and resource owners may devise a series of Boolean attributes to test for authentication methods used, i.e.:

subject-id-authenticated-by-password

subject-id-authenticated-by-smart-card

subject-id-authenticated-by-biometric-iris-scan

subject-id-authenticated-by-biometric-fingerprint

subject-id-authenticated-by-two-factors

subject-id-authenticated-by-three-factors

This would allow policy authors to specify which methods are acceptable by testing for a TRUE result among the list they define as meeting security requirements.

Lastly, the Obligation element of XACML could be used to perform Trust Elevation. Any rule that permits access and specifies the authentication level required would add an obligation stating the minimum required authentication level. e.g.,

if “User authorized” then Permit. FulfillOn=Permit -> authenticated-by-two-factors-obligation.

In this case, the PEP does not need any special attributes. It makes a normal authorization request. If the response is Deny or NotApplicable, then the authentication level is irrelevant because the user is not allowed access. If the response is Permit without any authentication level obligations, then access is allowed even at the lowest authentication level. If the response is Permit with specific authentication level

obligations, then the PEP must perform step-up authentication to the authentication level of the highest level of the obligations it received. If the highest level is satisfied, then any lower levels are satisfied. If that step-up fails or cannot be attempted, then access is denied. If step-up succeeds then access is allowed without needing an additional authorization request.

3.3.4 SAML Backend Attribute Exchange (BAE) Model

The Security Assertion Markup Language (SAML) standard defines a means for representing authentication events between different trusting security domains. A SAML assertion may contain a variety of attributes about the requesting subject and the conditions of the authentication event. Subject and Issuer attributes generally relate the name of the subject and the name of the organization with which the subject is associated in the AuthenticationStatement element. The AuthenticationStatement also contains an AuthenticationContext attribute, which details how the subject was authenticated in the context of the current assertion.

SAML-aware relying party applications can request additional attributes via the AttributeQuery element. Moreover, SAML authorities can request full attribute evaluations via the AuthzDecisionQuery element. Relying parties may specify acceptable authentication methods and credentials by using the RequestedAuthnContext element, and can force a fresh authentication event by setting ForceAuthn to true.

Trust Elevation can be exemplified in the following scenario using SAML: a user attempts to access content protected by a SAML-aware relying party (RP) application. The user posts a SAML assertion containing Subject/Issuer attributes and indicates a low level assurance authentication event to the RP. The RP's access control policy requires additional attributes and a higher strength credential and authentication event. The RP initiates a SAML authentication request to the user's home domain. This forces a step-up authentication event and retrieval of additional attributes, as required by the attribute contract. As with the XACML model, trust elevation means enhancing authentication and/or authorization by means of requiring additional attributes.

4 Architecture & Design

4.1 Trust Elevation System Context

This section is normative.

The participants, authentication methods, communication protocols and authorization methods of the Trust Elevation system MUST be agreed upon among the participants.

If new participants and/or methods are introduced to the Trust Elevation system, appropriate onboarding processes MUST be used.

The lack of generally agreed-upon criteria and evaluations of an authentication method's efficacy to counter threats, mitigate impacts or reduce negative occurrence frequency, as well as local extrinsic concerns makes dynamic addition of new authentication methods problematic. One Trust Elevation system may consider a password-based authenticator to be sufficient for identification whereas another Trust Elevation system may require additional fraud detection infrastructure to realize the same degree of sufficiency.

The Trust Elevation system MUST use business rules and technologies related to authentication and authorization for performing trusted transactions that are shared among participants. A Trust Elevation system could refer to: federated systems; systems controlled by a single governing entity; or a single system.

4.2 Assumptions for Trust Elevation Systems

This section is normative.

There are several assumptions that help set the context for this work:

- The resource manager MUST have a defined set of requirements for authentication and/or authorization control. The requirements MAY include combinations of static rules and dynamic risk evaluations.
- In the case of federated services, the federation agreement MUST define the available identification and authentication methods and their relationship to discrete 'levels' of assurance that map to risk mitigation or compensating controls.
- Authentication methods MUST be described sufficiently to allow creation of sets of compatible methods that cover identifiable risks or threats to allow implementers to choose independent authentication factors.

4.3 Architecture & Design Factors

This section is normative.

There are many potential factors that influence the design specific Trust Elevation architectures. The nature and impact of the factors is determined by local requirements.

4.3.1 Definition of 'Elevation' or 'Step-Up'

The semantics of combining authentication methods to increase risk mitigation MUST be dependent on local definition of authentication method characteristics within a Trust Elevation system.

The risk models of the resource manager and/or federation that comprise the Trust Elevation system MUST be considered when defining how combinations of methods modify risk mitigation.

For example, in one federation repetition of a password authentication to re-confirm the authenticator may change the risk mitigation from ‘Low’ to ‘Medium’. In a different federation, the same risk mitigation change might require a second authentication method which is different from the first one used.

The full range of permitted combinations and their effect on risk mitigation SHOULD be defined for the local entities.

4.3.2 Use of Shared Definitions

As with authentication method combinations, the specification of each permitted authentication method MUST be shared within a Trust Elevation system.

Note: if a fingerprint template biometric is to be used, common specification of sampling mechanics, template calculation and comparison algorithms is essential. Variance in specification within a Trust Elevation system will result in different semantic meaning when combining authentication methods.

4.3.3 Authentication State Tracking

Authentication state per Subject MAY need to be kept.

The Trust Elevation system MAY need to know which authentication methods have been attempted in prior transaction attempts in order to select the a different authentication method or factor to be attempted next.

Tracking state per Subject and transaction attempt may prove to be a complex undertaking unless care is taken when designing elevation policy.

4.3.4 Location of Policy Decisions

The architecture and design SHOULD be able to accommodate local, remote and distributed policy evaluation. Policy evaluation for trust elevation purposes may occur within a single system, or may occur in several different systems then combined.

A mechanism for calculating the combined result of the policy evaluation MUST be designed.

4.3.5 Consideration of Time or Quality Degradation

When designing the state model for the authorization system, time-related degradation of information quality or authenticator validity SHOULD be considered. The degradation COULD be defined as nil, or according to a specified time function.

4.3.6 Responsiveness to Threat Environment

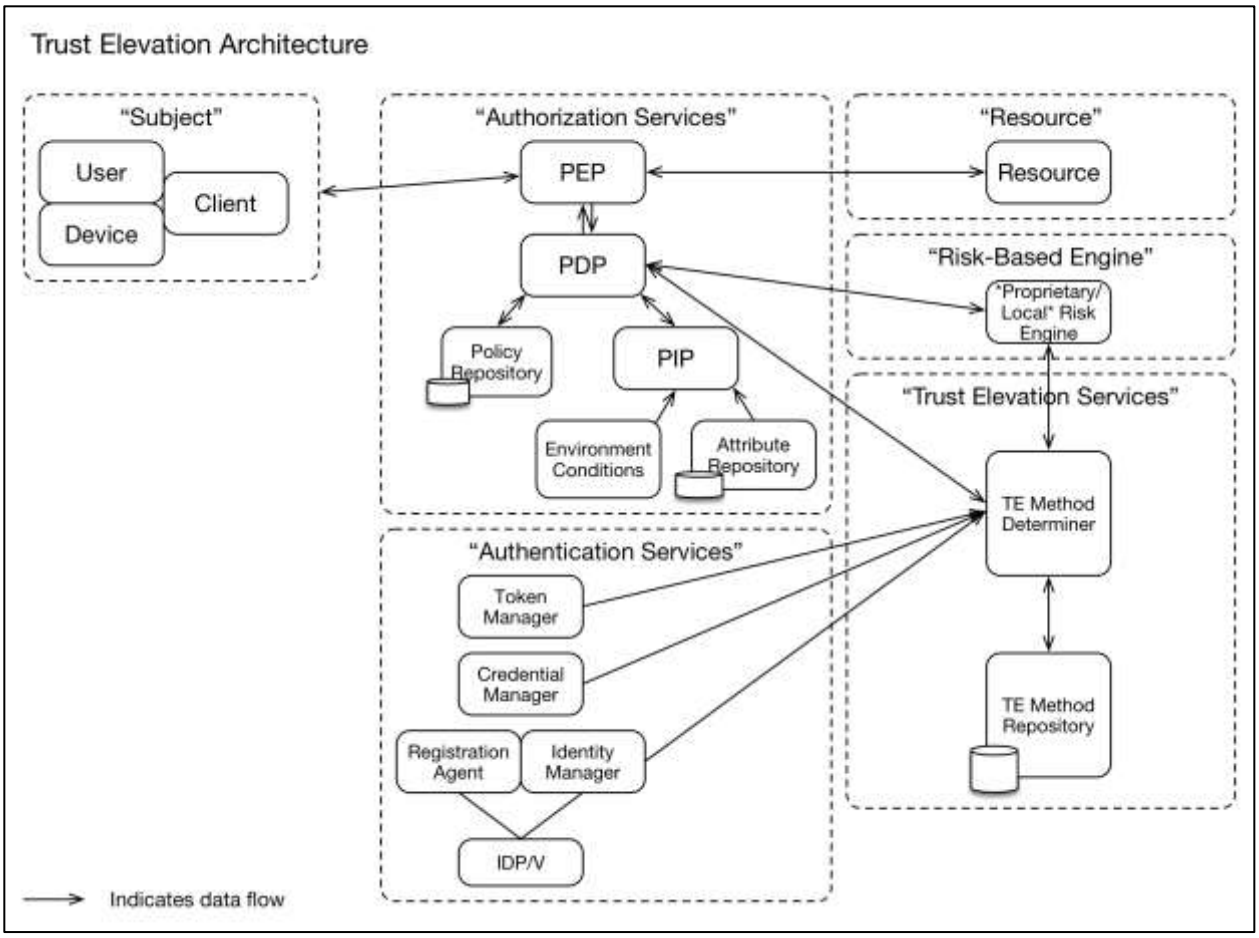
The effect of changes in the threat environment might cause changes of calculated assurance levels. Designers SHOULD determine if and how to respond to changes to the threat environment.

If a system component is observed to be under active attack, the authorization system SHOULD require increased assurance levels through use of additional authentication methods.

4.4 Trust Elevation Architecture Components

This section is normative.

The following architecture diagram shows Trust Elevation system components and other components related to Trust Elevation systems and their core functions. The dashed line boxes represent the boundary for each major component. The solid line boxes represent the functions within the major components. In other authorization model representations, the functions may have different names and may possibly appear within different major component boundaries.



4.4.1 Trust Elevation Services Component

The Trust Elevation Services component is comprised of the Trust Elevation Method Determiner and the Trust Elevation Method Repository.

When the Authorization Services component determines that the Subject is not permitted to access the resources due to insufficient identification and authentication assurance, the Trust Elevation Services component is used to select an additional authentication method or methods which would allow the Subject to access the resources.

The Trust Elevation Services Component enables the Authorization Services to ask the Subject to retry access using different or additional authenticators.

The Trust Elevation Services are aware of the methods and authenticators previously used by the Subject to attempt access. This enables mitigation of identification threats different from the initial authentication methods and authenticators, without having to hard code all combinations of authenticators that could be used.

For example, if the initial authenticator used username/password (a ‘know’ factor), the Trust Elevation Services would not recommend that authenticator if asked for another single factor authenticator: it might return a ‘have’ or ‘are’ factor authentication method, or a ‘know’ factor authentication method that is not username/password.

4.4.1.1 Trust Elevation Method Determiner

The Trust Elevation Method Determiner makes Trust Elevation policy decisions.

It receives requests from the Authorization Services component that MUST include current authentication state information of the Subject and the desired Level of Assurance.

The Trust Elevation Method Determiner uses policies stored in the Trust Elevation Method Repository to determine which, if any, authentication methods could be used to achieve the desired Level of Assurance.

The Trust Elevation Policy MUST map the combinations of authenticators to the desired assurance levels.

Given the desired assurance level, the Trust Elevation Method Determiner MUST be able to evaluate Trust Elevation Policy to identify the list of authentication methods that could be used to achieve the desired assurance level.

The current authentication state information MAY include data about: authenticators presented to the Authorization Services component; authentication methods that were used by the Subject to achieve the current authentication state; and, the current Level of Assurance of the Subject.

If the authentication capabilities of Subjects (user, device or client) are dynamic or dependent on device, user or software abilities and features, the Method Determiner MAY need information about the specific capabilities of the specific Subject in order to avoid unnecessary round trips to the Subject.

4.4.1.2 Trust Elevation Method Repository

The Trust Elevation Method Repository contains information necessary to the functions of the Trust Elevation Method Determiner.

The Trust Elevation Method Repository MUST contain information about the implemented authentication methods and their characteristics. These characteristics are used in the Trust Elevation Policy when the concepts of ‘stronger’ authenticators or ‘more’ assurance are represented.

If the Trust Elevation system uses authentication factors to determine authenticator strength, it COULD treat a single factor authenticator as weaker than a two-factor authenticator. In this case the characteristics SHOULD include details of which authentication factors are used.

4.5 Other Architecture Components

This section is non-normative.

These components interact with Trust Elevation systems but are not part of the Trust elevation systems.

4.5.1 Authorization Services Component

The Authorization Services component must be capable of requesting and processing Trust Elevation information. Trust Elevation Services may be treated as an information source or a remote policy engine.

The Authorization Services component may need additional functionality to handle and track multiple access attempts by the Subject as the Subject responds to elevation requests.

4.5.2 Risk-Based Engine Component

If a Risk-Based Engine Component exists, it represents systems that may be used by the resource manager to detect, measure and respond to threats in the operational environment. Detection of increased online attacks could cause the resource manager to require a greater degree of identification or authentication for access to resources.

5 Implementation Considerations

This section is normative.

5.1 Orchestration

Orchestration of Trust Elevation systems interaction with access control system components is required.

The access control components MUST be capable of requesting additional authentication or information from the Subject.

Since the Trust Elevation services component determines which authentication methods are required after the first round of policy evaluation, all components in the access control service MUST be able to handle the extra requests.

5.2 Enumeration of Authentication Methods

The implemented authentication methods MUST be enumerated and details stored in the Trust Elevation Repository.

The details that SHOULD be captured are identified in Deliverable 2, comprised of threats eliminated and risks mitigated. The detailed information will enable analysts to design Trust Elevation sequences that use complementary authentication methods to strengthen risk mitigation.

5.2.1 Subject Component

Authentication methods recorded in the Trust Elevation Method Repository MAY involve any combination of User, Device and Client.

Because the Subject might interact with the Authorization Services at different points in time with different User, Device or Client elements, authentication methods MUST NOT make assumptions about the relationships between the Subject, User, Device or Client.

Note: the same User attempting access from a different device that has an identical device model has lower assurance than use of the originally registered device. Authentication methods involving the device need to be able to differentiate between those devices.

5.2.2 Effect of Device Capability Changes

Devices may have different authentication method capabilities at enrolment versus at the time of the transaction. Device hardware used for authentication SHOULD NOT be assumed to be available or functioning.

5.3 User Enrolment

Enrolment is a key phase to support execution of Trust Elevation. At enrollment time, the Trust Elevation system MUST identify, record and possibly provision authentication methods. These authentication methods COULD include user, device, geo-location, network location and environmental elements.

6 Trust Elevation Sequence (Example)

This section is non-normative.

The specific structure and content of the Policy Table and Methods Table are defined within the Trust Elevation system, driven by the Relying Party's authentication policies.

In this simple example, a static mapping of Relying Party defined Transaction Risk Levels to pre-defined authentication strengths encoded as "Authentication Levels" (AL) is shown. The Relying Party defines which Authentication Level transitions are required for each Transaction Risk Level.

The policies are based on the 'authentication factors' approach to risk mitigation. The Relying Party policy sets out the permitted combinations of authentication factors required to move from one Authentication Level to another Authentication Level.

Note that all transitions for all risk levels are not necessarily defined. The Policy Table only shows valid policies for this Relying Party within this trust system. If a particular transition is not defined, it is deemed to be invalid.

6.1 Use Case: Online banking transactions

6.1.1 Description

A bank customer (Subject) initially logs on to the bank site (through a browser or mobile app) to view their account balance. Then, they decide to perform a higher risk transaction that requires a higher level of authentication: a funds transfer of $X.

6.1.2 Pre-conditions

- Subject has an existing relationship with the bank (i.e., is an account holder)
- Subject has previously registered their authentication methods (e.g., password, device, biometric)
- There are three Authentication Levels defined by the bank (the Relying Party)

6.1.2.1 Transaction Risk Levels

Transaction Designation	Transaction Name	Transaction Risk Level
T1	Check Account Balance	Low
T2	Transfer Funds Out	Med

6.1.2.2 Policy Table*

The Policy Table is defined during system design by the Relying Party.

Transaction Risk Level	Initial Strength	Desired Strength	Authentication needed*	Policy designation
Low	AL0	AL1	One factor, either what you know or have	P1
Med	AL0	AL2	Two factors, any class	P2
	AL1	AL2	One factor, different than used for AL1 authentication	P3
High	AL0	AL3	Three factors	P4
	AL1	AL3	Two factors, any class, different than used for AL1 authentication	P5
	AL2	AL3	One factor, different than used for AL1 OR AL2 authentication	P6

Where AL0 represents a "user not logged in" state.

*Authentication policies are set by the relying party.

6.1.2.3 Methods Table

The Methods Table enumerates the authentication methods available in the trust system.

Method designation	Method description	Class(es)	SF strength	Threats addressed*
M1	PIN (>=4 char)	Know	1	
M2	Password (>=8char)	Know	1	
M3	Device ID	Have	1	
M4	Crypto key (TLS protocol)	Have	2	
M5	Biometric – face	Are	NA	
M6	Biometric – fingerprint	Are	NA	
M7	PIN + Device ID	K+H	2	
M8	Crypto key + face	H+A	3	

*For the benefit of relying party operators setting up policies.

6.1.3 Process Flows

6.1.3.1 Transaction 1: Check Account Balance

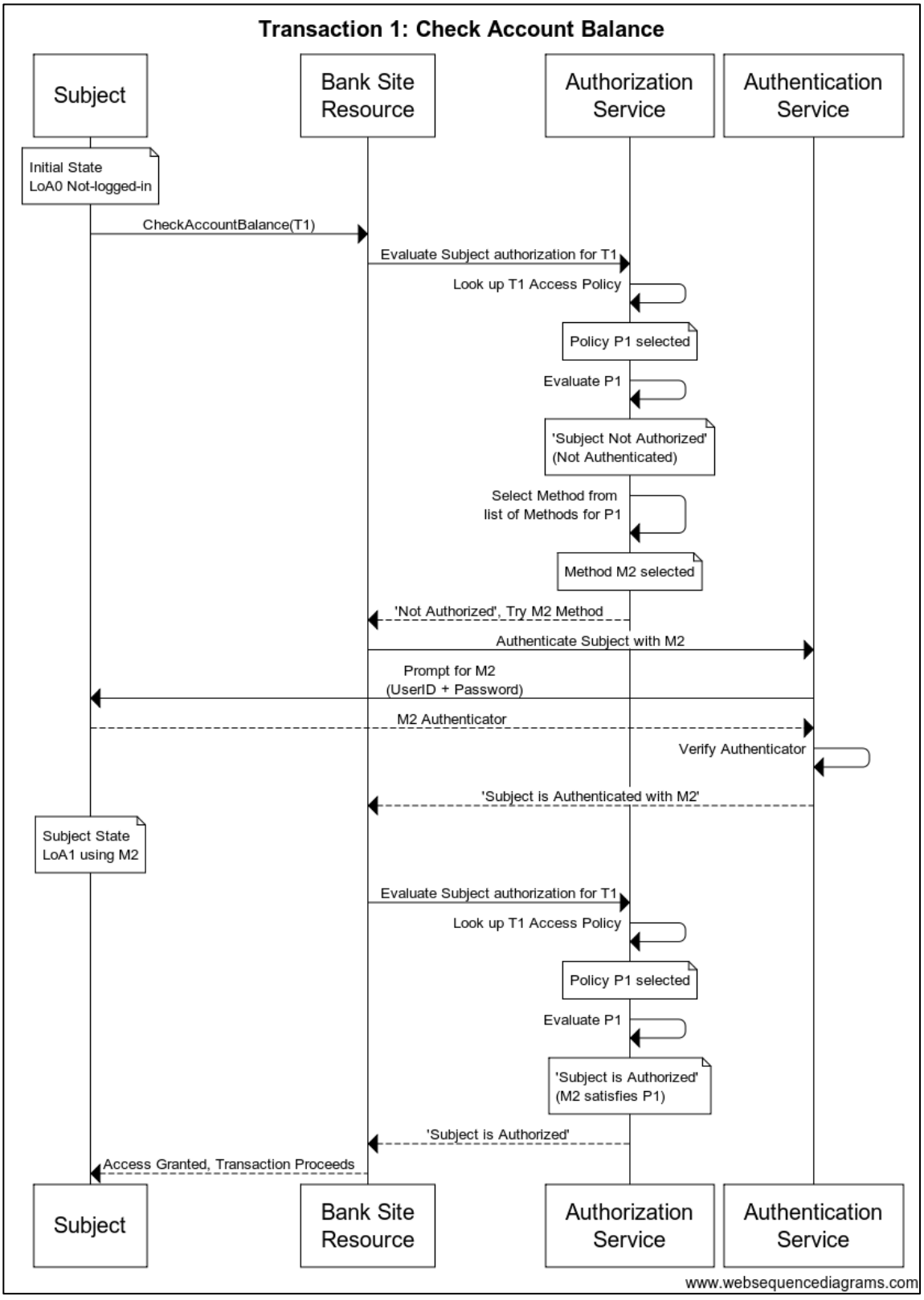
Note: In the process flow the PEP is not shown and is assumed to be part of the Resource.

```
Title Transaction 1: Check Account Balance
Note over Subject: Initial State \nLoA0 Not-logged-in
Subject->Bank Site\nResource: CheckAccountBalance(T1)
Bank Site\nResource->Authorization\nService: Evaluate Subject authorization
for T1
Authorization\nService-> Authorization\nService: Look up T1 Access Policy
Note over Authorization\nService: Policy P1 selected
```

```
Authorization\nService-> Authorization\nService: Evaluate P1
Note over Authorization\nService: 'Subject Not Authorized'\n(Not
Authenticated)
Authorization\nService-> Authorization\nService: Select Method from \nlist of
Methods for P1
note over Authorization\nService: Method M2 selected
Authorization\nService-->Bank Site\nResource: 'Not Authorized', Try M2 Method
Bank Site\nResource-> Authentication\nService: Authenticate Subject with M2
Authentication\nService->Subject: Prompt for M2 \n (UserID + Password)
Subject--> Authentication\nService: M2 Authenticator
Authentication\nService-> Authentication\nService: Verify Authenticator
Authentication\nService--> Bank Site\nResource: 'Subject is Authenticated with
M2'
Note over Subject: Subject State \nLoA1 using M2
Bank Site\nResource-> Authorization\nService: Evaluate Subject authorization
for T1
Authorization\nService-> Authorization\nService: Look up T1 Access Policy
note over Authorization\nService: Policy P1 selected
Authorization\nService-> Authorization\nService: Evaluate P1
note over Authorization\nService: 'Subject is Authorized' \n(M2 satisfies P1)
Authorization\nService-->Bank Site\nResource: 'Subject is Authorized'
Bank Site\nResource-->Subject: Access Granted, Transaction Proceeds
```


6.1.3.2 Transaction 1: Sequence

Note: In the process flow the PEP is not shown and is assumed to be part of the Resource.



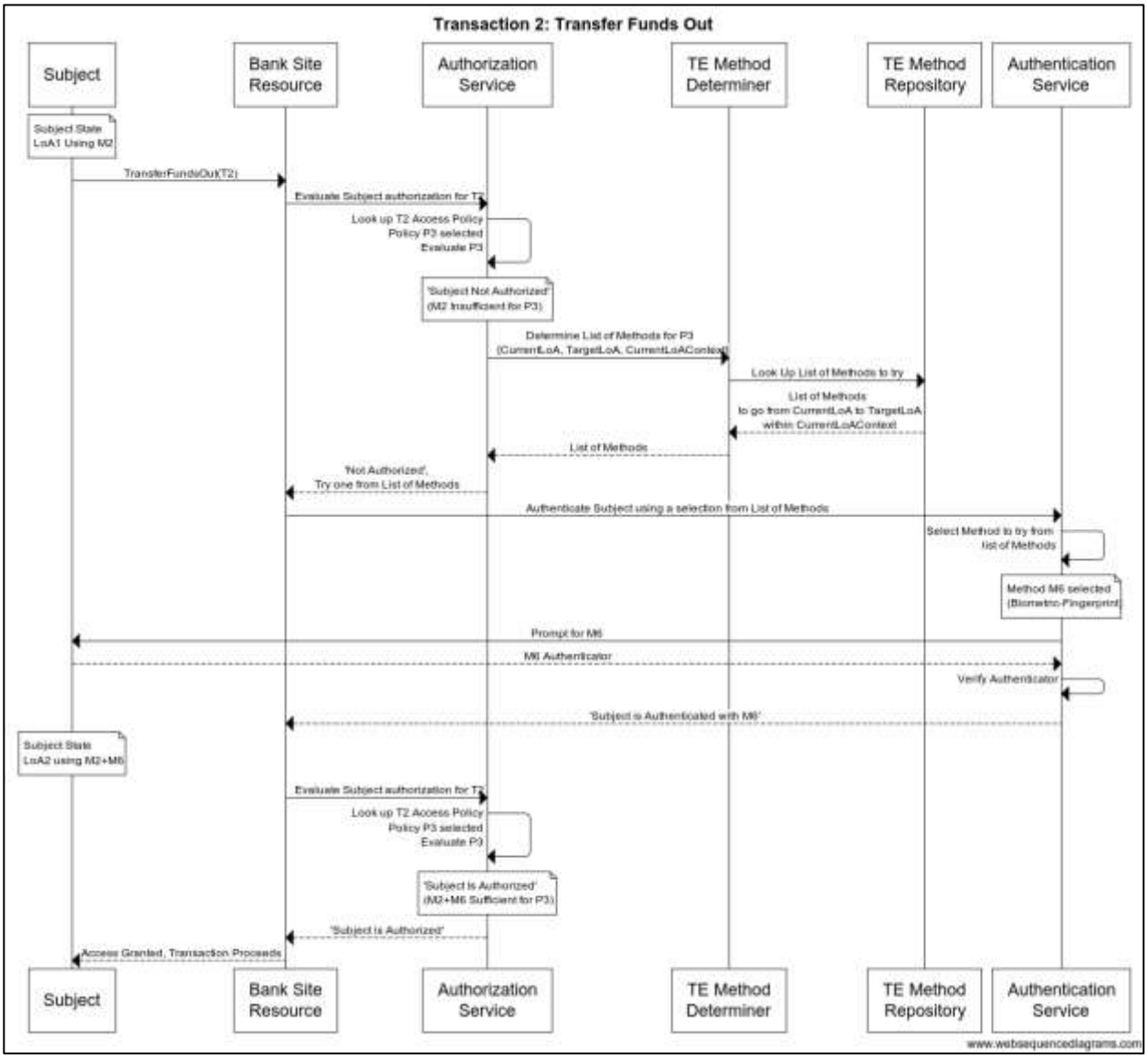
6.1.3.3 Transaction 2: Transfer Funds Out

Note: In the process flow the PEP is not shown and is assumed to be part of the Resource.

```
Title Transaction 2: Transfer Funds Out
Note over Subject: Subject State \nLoA1 Using M2
Subject->Bank Site\nResource: TransferFundsOut(T2)
Bank Site\nResource->Authorization\nService: Evaluate Subject authorization
for T2
Authorization\nService-> Authorization\nService: Look up T2 Access
Policy\nPolicy P3 selected\nEvaluate P3
Note over Authorization\nService: 'Subject Not Authorized'\n(M2 Insufficient
for P3)
Authorization\nService->TE Method\nDeterminer: Determine List of Methods for
P3\n{CurrentLoA, TargetLoA, CurrentLoAContext}
TE Method\nDeterminer->TE Method\nRepository: Look Up List of Methods to try
TE Method\nRepository-->TE Method\nDeterminer: List of Methods\nto go from
CurrentLoA to TargetLoA\nwithin CurrentLoAContext
TE Method\nDeterminer-->Authorization\nService: List of Methods
Authorization\nService-->Bank Site\nResource: 'Not Authorized',\nTry one from
List of Methods
Bank Site\nResource-> Authentication\nService: Authenticate Subject using a
selection from List of Methods
Authentication\nService-> Authentication\nService: Select Method to try from
\nlist of Methods
note over Authentication\nService: Method M6 selected\n(Biometric-Fingerprint)
Authentication\nService->Subject: Prompt for M6
Subject--> Authentication\nService: M6 Authenticator
Authentication\nService-> Authentication\nService: Verify Authenticator
Authentication\nService--> Bank Site\nResource: 'Subject is Authenticated with
M6'
Note over Subject: Subject State \nLoA2 using M2+M6
Bank Site\nResource->Authorization\nService: Evaluate Subject authorization
for T2
Authorization\nService-> Authorization\nService: Look up T2 Access
Policy\nPolicy P3 selected\nEvaluate P3
Note over Authorization\nService: 'Subject Is Authorized'\n(M2+M6 Sufficient
for P3)
Authorization\nService-->Bank Site\nResource: 'Subject is Authorized'
Bank Site\nResource-->Subject: Access Granted, Transaction Proceeds
```

6.1.3.4 Transaction 2: Sequence

Note: In the process flow the PEP is not shown and is assumed to be part of the Resource.



7 Metadata and Assertions

This section is non-normative.

7.1 Component-Component Communications

Content of Authorization Service (PDP) to Trust Elevation Method Determiner request:

- Current Authentication Level
- Method(s) that were used to achieve current Authentication Level
- Target Authentication Level

Content of Trust Elevation Method Determiner to Authorization Service (PDP) response:

- List of methods that could be used to achieve target Authentication Level

Content of Authorization Service (PDP)-Authentication Service request:

- Subject ID
- List of methods to choose from

7.2 PDP to TE Method Determiner Request

The fragments below are examples showing the kinds of information to exchange between components.

```
<trustel:MethodTypeRequest>
   <trustel:CurrentLoA>....</trustel:CurrentLoA>      //current Authentication Level in numerical
value
   <trustel:TargetLoA>...</trustel:TargetLoA> //Target Authentication Level in numerical value
   <trustel:CurrentLoAContext>
            <trustel:Method>...</trustel:Method> //could be "|" delimited array of methods
            <trustel:AuthnDeviceSig>..</trustel:AuthnDeviceSig> //Device Fingerprint
            <trustel:AuthnLocation>...</trustel:AuthnLocation>  //Device location
            <trustel:AuthnIP>...</trustel:AuthnIP>     //IP of the device
            <trustel:AuthnTime>...</trustel:AuthnTime> //time of request
   </trustel:CurrentLoAContext>
</trustel:MethodTypeRequest>
```

7.3 TE Method Determiner to PDP Response

```
<trustel:MethodTypeResponse>
   <trustel:Method>...</trustel:Method>       //could be "|" delimited array of methods
</trustel:MethodTypeResponse>
```

8 Conformance

In order to conform with this specification, the Trust Elevation system under consideration:

[1] MUST be designed and use an architecture that conforms to the normative statements in section 4

[2] MUST be implemented in conformance with the normative statements in section 5

Appendix A. Acknowledgments

This section is non-normative.

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

Chairs:

Abbie Barbir, Aetna
Don Thibeau, OIX

Editors:

Andrew Hughes, Individual
Shaheen Abdul Jabbar, JPMorgan Chase Bank, N.A.
Peter Alterman, SAFE-BioPharma Association
Abbie Barbir, Aetna
Mary Ruddy, Identity Commons

Document Contributors:

Peter Alterman, SAFE-BioPharma Association
Abbie Barbir, Aetna
Andrew Hughes, Individual
Shaheen Abdul Jabbar, JPMorgan Chase Bank, N.A.
Eve Maler, Forgerock
Steven Legg, Individual
Diana Proud-Madruga, Individual
Mary Ruddy, Identity Commons
Michael Schwartz, Gluu
Martin Smith, Individual
Don Thibeau, OIX
Cathy Tilton, Daon
John Tolbert, Queralt, Inc
David Turner, Voltage Gate
Colin Wallis, New Zealand Government

Technical Committee Member Participants:

Shaheen Abdul Jabbar, JPMorgan Chase Bank, N.A.
Orlando Adams, U.S. Bank
Peter Alterman, SAFE-BioPharma Assn
Abbie Barbir, Aetna
John Bradley, Open Identity Exchange
David Brossard, Axiomatics
Doron Cohen, SafeNet, Inc.
Ed Coyne, Veterans Health Administration
John Davis, Veterans Health Administration
Suzanne Gonzales-Webb, Veterans Health Administration
Dazza Greenwood, M.I.T.
Richard Grow, Veterans Health Administration
Thomas Hardjono, M.I.T.
Rainer Hoerbe, Individual
Andrew Hughes, Individual
Mohammad Jafari, Veterans Health Administration
Gershon Janssen, Individual
Kevin Mangold, NIST
Carl Mattocks, Individual
Steve Olshansky, Internet Society (ISOC)

Brendan Peter, CA Technologies
Diana Proud-Madruga, Veterans Health Administration
Mary Ruddy, Identity Commons
Anthony Rutkowski, Yaana Technologies, LLC
Marty Schleiff, The Boeing Company
Michael Schwartz, Individual
Shahrokh Shahidzadeh, Intel Corporation
Jeffrey Shultz, NIST
Don Thibeau, Open Identity Exchange
Cathy Tilton, Daon
John Tolbert, Queralt, Inc.
David Turner, Voltage Gate
Colin Wallis, New Zealand Government

Appendix B. State Models for Assurance Level Evaluation

This section is non-normative.

8.1 Evaluation of Assurance Requirements at Transaction Time

One of the core assumptions of Trust Elevation is that a subject attempting a transaction is unable to meet the policy requirements for identification certainty unless an Elevation event occurs.

An important concept is that measured assurance levels change over time due to many factors. At the instant of authorization policy evaluation, the current state of identity attribute assurance level and authenticator assurance level are compared to the Transaction's Assurance Level Requirement. If the measured assurance levels are greater or equal to the requirement, the transaction proceeds.

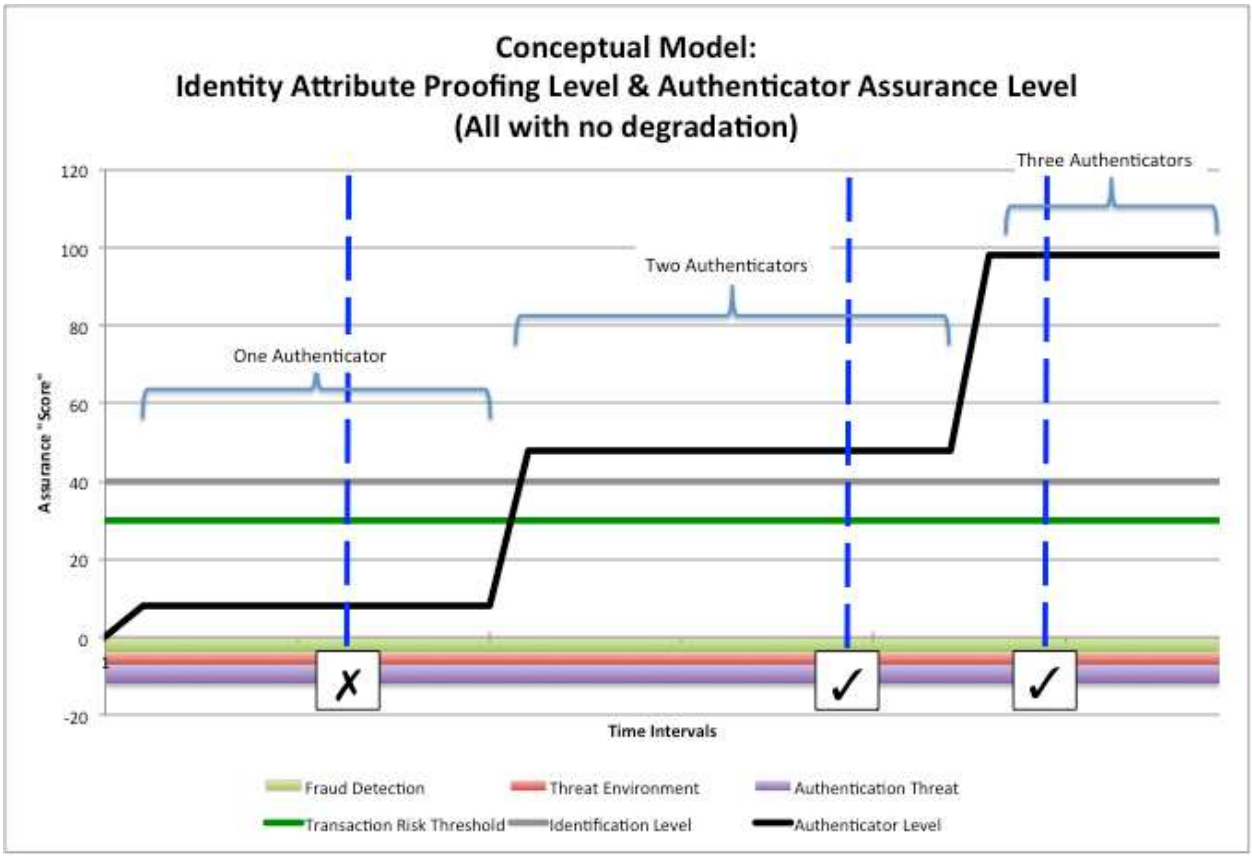
The graphics show that the assurance level of the Identity Information Attributes established via the Identity Proofing and Verification processes are separate and unlinked to the assurance level of the Authentication Event (which includes Credential and Authenticator details). This approach is consistent with the NIST SP800-63 LOA calculation method.

8.1.1 Up-Front Policy Evaluation of Proofing and Authenticator Levels

This graphic illustrates a scenario where the levels of identity attribute assurance and authenticator assurance are determined in advance and do not degrade over time.

The vertical dashed lines represent the potential points in time of the transaction event. The identity attribute assurance and authenticator assurance levels are compared to the transaction assurance level requirement. If both values are greater than the requirement, the transaction can proceed (check mark). If one or both are lower, the transaction cannot proceed (X mark) and is either rejected or directed to a trust elevation event.

Trust Elevation in this scenario combines authentication factors to step up combined authenticator assurance to meet or exceed the transaction requirement.



Notes:

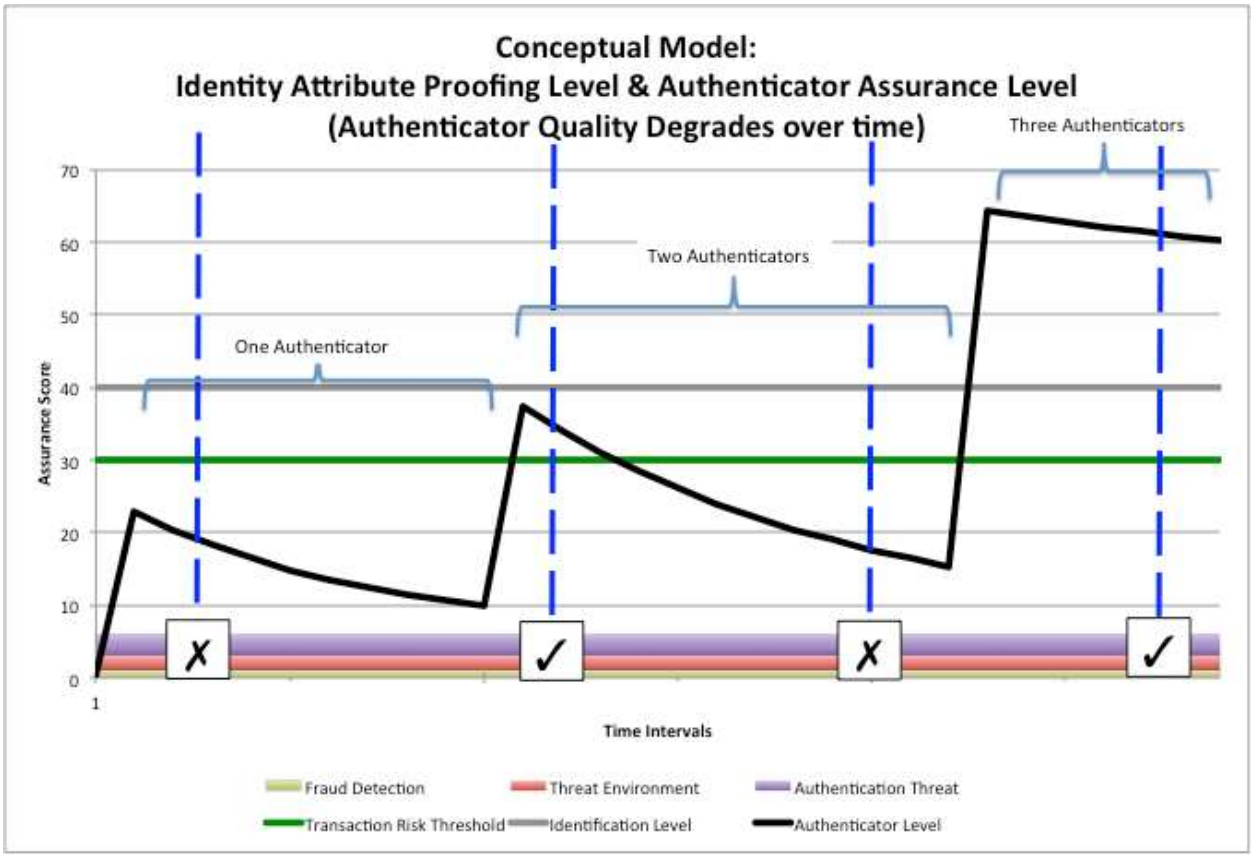
- The 'Assurance Score' is a simple numerical representation of the degree of certainty for illustrative purposes. 'Assurance Level 3' has been arbitrarily defined as '30' on the scale
- The Grey line represents the assurance level resulting from the Identity Proofing and Verification process; established at Subject Registration time by the Registration Agent.
- The Black line represents the authenticator assurance level resulting from the Authentication event. It takes credential, authentication secrets and authenticator generation factors into account.
- The Green line represents the Resource Owner defined assurance score/level required for the transaction. It is based on the Resource Owner's risk determination methods. In this example, the Transaction Requirement is '30' or 'LOA3'
- The Black line initially shows the effect of a single authenticator, then two authenticators, then three authenticators.

8.1.2 Time-Based Degradation of Authenticator Assurance Levels

The assurance level of the Authenticator is important. This graphic illustrates a scenario where the authenticator assurance level changes over time due to time-based degradation of the credential, secrets and authenticator generation processes.

The vertical dashed lines represent the potential points in time of the transaction event. The identity attribute assurance and authenticator assurance levels are compared to the transaction assurance level requirement. If both values are greater than the requirement, the transaction can proceed (check mark). If one or both are lower, the transaction cannot proceed (X mark) and is either rejected or directed to a trust elevation event.

This scenario shows that due to rapid degradation of authenticator assurance for most time periods, Trust Elevation to three authenticators is needed for the transaction policy.



Notes:

- The 'Assurance Score' is a simple numerical representation of the degree of certainty for illustrative purposes. 'Assurance Level 3' has been arbitrarily defined as '30' on the scale
- The Grey line represents the assurance level resulting from the Identity Proofing and Verification process; established at Subject Registration time by the Registration Agent.
- The Black line represents the authenticator assurance level resulting from the Authentication event. It takes credential, authentication secrets and authenticator generation factors into account.
- The Green line represents the Resource Owner defined assurance score/level required for the transaction. It is based on the Resource Owner's risk determination methods. In this example, the Transaction Requirement is '30' or 'LOA3'
- The Black line initially shows the effect of a single authenticator, then two authenticators, then three authenticators.
- The downward slopes represent the time-based degradation of certainty of the authenticator
- Although not shown explicitly, refresh to original values could be achieved by re-issuance of credentials, or generation of new keys.

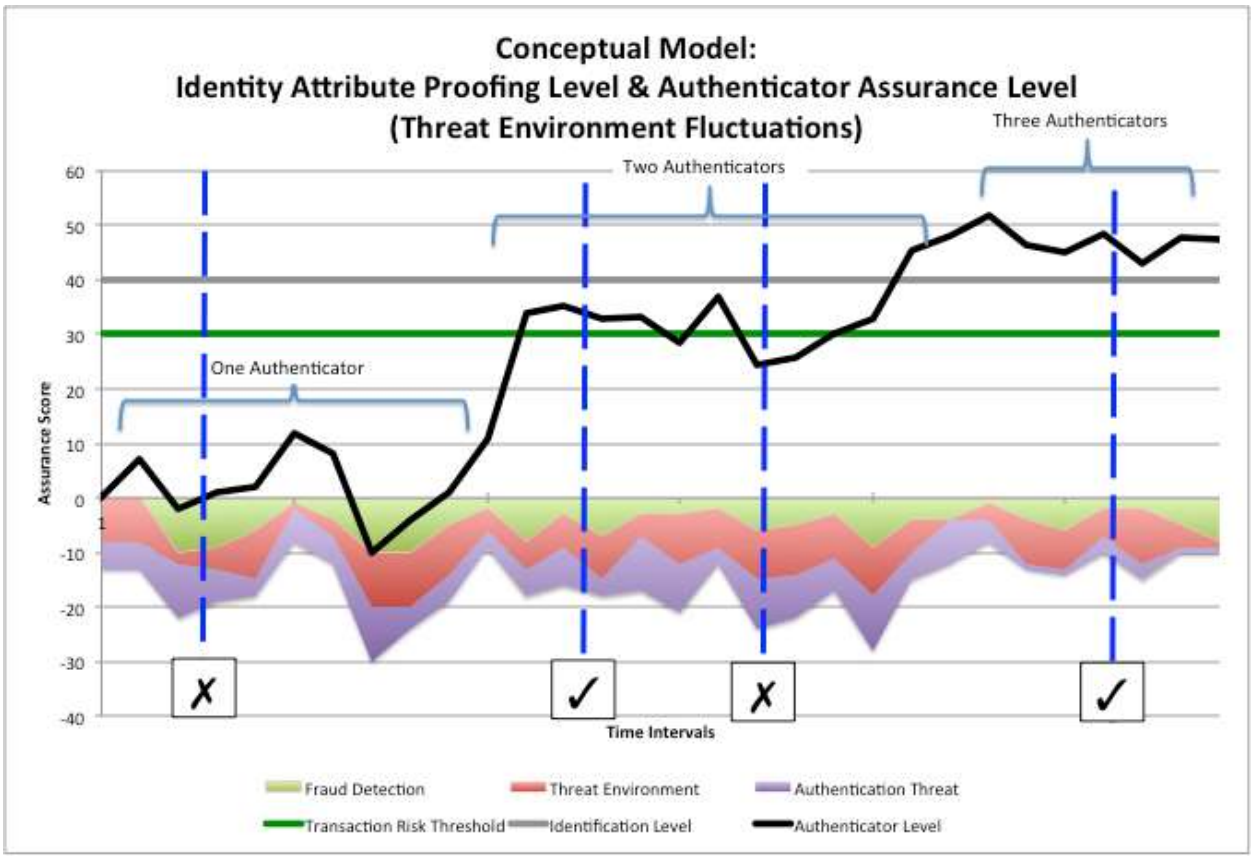
8.1.3 Threat Environment Effects on Effective Authenticator Level

The last graphic illustrates a more complex example in which the overall threat level affects the Authenticator assurance level. A simplistic calculation is used where increasing threat environment, increasing detected fraud and decreased system security subtract directly from the authenticator assurance score.

This mimics the effect that a risk-based authentication system or risk engine might have on transaction assurance requirement evaluation.

As in the previous illustrations, the vertical dashed lines represent the potential points in time of the transaction event.

Where the increased threat level causes the effective authenticator assurance level to dip below the green transaction requirement line, Trust Elevation could be used to achieve the minimums necessary. Note that in the 'Two Authenticators' region, the transaction could proceed or fail depending on the magnitude of the threat levels. If the transaction fails, the Relying Party could choose to retry at a later time, or request additional Authenticators.



Appendix C. Revision History

This section is non-normative.

Revision	Date	Editor	Changes Made
Draft 04b	2015-09-04	A. Hughes	Minor updates to base draft.
Draft 04c	2015-09-26	A. Hughes	Added contributions to draft.
Draft 05	2015-10-15	A. Hughes	Final draft version for TC review and approval.
Draft 06	2015-11-07	A. Hughes	Minor updates for Final draft version
Draft 07	2015-11-07	A. Hughes	Minor updates for Final draft version
Draft 08	2016-03-15	A. Hughes	Disposition of comments received
Draft 09	2016-08-18	A. Hughes	Updates to Conformance Clause and related items.
Draft 091	2016-09-12	A. Hughes	Finalization of Conformance Clause
Darft 092	2016-09-14	A. Hughes	Corrected acknowledgements items