

Call for Participation: OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC

Submitted by cesign on Thu, 2011-08-04 13:21

Type:

Call for Participation

OASIS members & interested parties,

A new OASIS technical committee is being formed. The OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) Technical Committee has been proposed by the members of OASIS listed in the charter below. The TC name, statement of purpose, scope, list of deliverables, audience, IPR mode and language specified in the proposal will constitute the TC's official charter. Submissions of technology for consideration by the TC, and the beginning of technical discussions, may occur no sooner than the TC's first meeting.

The eligibility requirements for becoming a participant in the TC at the first meeting are:

- (a) you must be an employee of an OASIS member organization or an individual member of OASIS, and
- (b) you must join the Technical Committee, which members may do by using the "Join this TC" button on the TC's home page at [a].

To be considered a voting member at the first meeting, you must:

- (a) join the Technical Committee at least 7 days prior to the first meeting (on or before 29 August 2011); and
- (b) you must attend the first meeting of the TC, at the time and date fixed below (5 September 2011).

Participants also may join the TC at a later time. OASIS and the TC welcomes all interested parties.

Non-OASIS members who wish to participate may contact us about joining OASIS [b]. In addition, the public may access the information resources maintained for each TC: a mail list archive, document repository and public comments facility, which will be linked from the TC's public home page at [c].

Please feel free to forward this announcement to any other appropriate lists. OASIS is an open standards organization; we encourage your participation.

[a] <http://www.oasis-open.org/committees/trust-el> [1]

[b] See <http://www.oasis-open.org/join/> [2]

[c] <http://www.oasis-open.org/committees/trust-el> [1]

Additional info:

CALL FOR PARTICIPATION

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

The charter for this TC is as follows.

1.a The name of the TC:

OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) Technical Committee

1.b Statement of Purpose:

The Trust Elevation Technical Committee will identify methods being used currently to authenticate electronic identities by online relying parties and service providers, and similar methods in development or identified in theoretical models. By comparison and factoring of those methods, the TC will propose and describe a set of standardized protocols that service providers may use to elevate the trust in an electronic identity credential presented to them for authentication, at levels of identity assurance or risk mitigation, representing increasing degrees of authentication certainty.

The Trust Elevation TC will collect information on trust elevation techniques, or risk mitigation techniques, being standardized, marketed and implemented in the public or private sector and will perform analyses of them and their approaches, assessing their effectiveness at assuring the identity of the electronic claimant, and working towards creating a general model of how effective the trust elevation / risk mitigation efforts are in creating trusted online transactions. Once the initial collection and analyses have been completed, the TC will correlate the results with various other trusted credential and trusted transaction models. The more widely-recognized and adopted these standardized protocols are, the more useful they will be to governments, businesses and individuals engaged in eGovernment and eCommerce.

The Trust Elevation TC is intended to respond to the suggestions of several governments, including the US government's NSTIC strategy document [3] that national and global identity infrastructures can be developed and supported by private sector cooperation among providers, users and subjects of trusted identity systems. The EIC-TEM documentation from this TC should promote interoperability among multiple identity providers, and among multiple identity federations & frameworks, by facilitating clear communication about common and comparable operations to present, evaluate and apply identity [data/assertions] to sets of declared authorization levels.

[1] Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, Dec. 2003.

[2] NIST Special Publication (SP) 800-63, Rev. 1, Electronic Authentication Guidelines, Dec. 2008.

[3] Office of the President, National Strategy for Trusted Identities in Cyberspace (NSTIC), April 2011: <http://www.nist.gov/nstic/> [3]

1.c Scope:

Work within the TC's scope includes descriptions of the process steps and component services necessary to confirm a conclusion of trust elevation between each pair of levels. Those descriptions and analysis may include catalogs of data services (or types of service), taxonomies or functional definitions of the types of identity and assertion data on which those services operate, substantive data exchanges or models, and model message exchange patterns.

The TC may include functional data security/integrity requirements in its process descriptions, e.g., certain trust

elevation methods may only be recommended if conducted within certain minimum levels of data integrity protection.

Where possible, the TC generally will rely on existing widely-used definitions and data categories. The TC may also make functional comparisons of alternative assurance level schemes, so as to map its trust elevation processes to a variety of regulatory frameworks.

The following work will be out of scope for the TC:

- Mandates of specific message formats or schema. The TC will provide process and data requirements that can be equally applied regardless of transport method or data schema encoding. No one data format or schema will be mandated. The TC may provide detailed instances of assurance & elevation message exchanges, as examples, but its output should be generally applicable regardless of schema encoding.

1.d List of deliverables:

The Trust Elevation TC will create the following deliverables:

1. The initial deliverable is a comprehensive list of methods being used currently to authenticate identities online to the degree necessary to transact business where material amounts of economic value or personally identifiable data are involved. First Public Review Draft to be completed by six months after the first meeting.
2. The second deliverable is an analysis of the identified methods to determine each one's ability to provide a service provider with assurance of the submitter's identity sufficient for elevation between each pair of assurance levels, to transact business where material amounts of economic value or personally identifiable data are involved. First Public Review Draft to be completed by [nine] months after the first meeting.
3. The third deliverable will be an "Electronic Identity Credential Trust Elevation Methods Protocol" specification that recommends particular methods as satisfying defined levels 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. The first Public Review Draft will be completed by [fifteen] months after the first meeting.
4. Other deliverables may be identified over time as the TC engages in its work.

The TC may re-factor the deliverables above as it sees fit into fewer, more, or differently combined documents. In any case, the deliverables shall:

- Be vendor-neutral and product-agnostic. (The TC may also elect to provide proof-of-concept instances, but will strive to facilitate ease of implementation regardless of data schema choices.)
- To the extent feasible, re-use rather than re-invent suitable existing definitions of policy concepts such as identity tokens and personally-identifiable data.
- To the extent feasible, be consistent with generally accepted definitions of service-oriented architectural principles.
- Describe with specificity their application to established US NIST levels of assurance.
- Include a catalog or list of common types of services and functions.
- Include a set of definitions or sources of definitions for common functional types of data elements.

1.e IPR Mode under which the TC will operate:

The Trust Elevation TC will operate under the RF on Limited Terms mode of the OASIS IPR Policy.

1.f Anticipated audience or users:

The Trust Elevation TC is intended for the following audiences: Architects, designers and implementers of providers and consumers of enterprise identity management services.

1.g Language:

Work group business and proceedings will be conducted in English.

2. Additional Non-normative Information

2.a Similar or applicable work

The proposers are unaware of any currently published work that covers the scope described here. Some elements of the project may be informed by or related to the following:

- Rec. ITU-T X.1250, Baseline capabilities for enhanced global identity management and interoperability (09/2009)
- CA/Browser Forum, Extended Validation Certificate Guidelines, Baseline Requirements, July 2011. Also included in ETSI TS 102042, ?Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates? and draft ITU-T Rec. 1261, Extended Validation Certificate Framework.
- 3GPP, TS 33.220, Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)
- Common Access Card, Hspd-12
- GSA, ICAM Trust Framework
- Trusted Computing Group, Trusted Platform Modules (2007) ? re-published by the Common Criteria Control Board and ISO SC27 as 11889.
- Trusted Computing Group, Trusted Network Connect modules (2007).

- ISO/IEC JTC 1/SC 27/WG 3, Evaluation criteria for IT security -- Part 3: Security assurance components (ISO/IEC 15408-3:2008).
- ENISA, Mapping ENISA Authentication Levels (Nov. 2008).
- NIST Special Publication (SP) 800-63, Rev. 1, Electronic Authentication Guidelines, Dec. 2008.
- Oxford Internet Institute, M. Rundle, ed, Towards a Policy and Legal Framework for Identity Management: A Workshop Report, Oct. 2009.
- IDABC: Study on eID Interoperability for PEGS (Dec. 2009).
- Kantara Initiative, Identity Assurance Framework: Glossary, Levels of Assurance & Service Assessment Criteria, Feb. 2010.
- Open Identity Exchange, The Open Identity Trust Framework (OITF) Model, Mar. 2010.
- ITU-T Rec. ITU-T X.1500: Overview of Cybersecurity information exchange techniques (Apr 2011).

2.b Date & time of first meeting

The first meeting will be held Monday, September 5, 2011, at 11:00 US Eastern time, by teleconference. The National Institute of Standards and Technology (NIST), the Open Identity Exchange and the eCitizen Foundation will co-sponsor the first meeting.

2.c Ongoing meeting schedule

To be decided by the committee. Bi-weekly teleconferences and the occasional (semi-annual) face to face work session may be appropriate. Meeting leadership will be shared among the three co-sponsors mentioned above on a rotating basis until the TC membership decides on another approach.

2.d Participants

The names, electronic mail addresses, and membership affiliations of at least Minimum Membership who support this proposal:

Peter Alterman; NIST, peter.alterman@nih.gov [4]

Don Thibeau; OIX, don@openidentityexchange.org [5]

Abbie Barbir; Bank of America, abbie.barbir@bankofamerica.com [6]

Dazza Greenwood; eCitizen, civicsdotcom-econtracts@yahoo.com [7]

Anil Saldhana; RedHat, Anil.Saldhana@redhat.com [8]

Brendan Peter; CA Technologies, Brendan.Peter@ca.com [9]

Mary Ruddy; Identity Commons, mary@meristic.com [10]

John "Mike" Davis; Veterans Health Administration, Mike.Davis@va.gov [11]

Tony Rutkowski, Yaana Technology, tony@yaanatech.com [12]

Debbie Bucci, National Institutes of Health, Bucci@exchange.nih.gov [13]

Shahrokh Shahidzadeh, Intel Corporation, Shahrokh.shahidzadeh@intel.com [14]

2.e Primary Representative Statements of Support

Paul Lipton, primary representative CA Technologies ? I approve the Trust Elevation TC charter.

Mark Little, primary representative RedHat ? I approve the Trust Elevation TC charter.

Abbie Barbir, primary representative of Bank of America - I approve the Trust Elevation TC charter.

Peter Alterman, primary representative of the National Institute for Standards and Technology - I approve the Trust Elevation TC charter.

Don Thibeau, primary representative of the Open Identity Exchange - I approve the Trust Elevation TC charter.

John "Mike" Davis, primary representative of the Veterans Health Administration - I approve the Trust Elevation TC charter.

Dazza Greenwood, primary representative of the eCitizen Foundation - I approve the Trust Elevation TC charter.

Debbie Bucci, primary representative of the National Institutes of Health - I approve the Trust Elevation TC charter.

Mary Ruddy, primary representative of the Identity Commons - I approve the Trust Elevation TC charter.

Blake Dournaee, primary representative of Intel Corporation - I approve the Trust Elevation TC charter.

Tony Rutkowski, primary representative of Yaana Technology - I approve the Trust Elevation TC charter.

2.f Convener

The convener will be Peter Alterman, National Institute of Standards and Technology.

2.g Member Section

OASIS IDtrust Member Section

Associated TC:

Electronic Identity Credential Trust Elevation Methods (Trust Elevation)

Associated MS:

IDtrust

Deadline:

Wed, 2011-08-03 - Mon, 2011-09-05

Links:

[1] <http://www.oasis-open.org/committees/trust-el>

[2] <http://www.oasis-open.org/join/>

[3] <http://www.nist.gov/nstic/>

[4] <mailto:peter.alterman@nih.gov>

[5] <mailto:don@openidentityexchange.org>

[6] <mailto:abbie.barbir@bankofamerica.com>

[7] <mailto:civicsdotcom-econtracts@yahoo.com>

[8] <mailto:Anil.Saldhana@redhat.com>

[9] <mailto:Brendan.Peter@ca.com>

- [10] <mailto:mary@meristic.com>
- [11] <mailto:Mike.Davis@va.gov>
- [12] <mailto:tony@yaanatech.com>
- [13] <mailto:Bucci@exchange.nih.gov>
- [14] <mailto:Shahrokh.shahidzadeh@intel.com>