## Section 1: TC Charter

### (1)(a) TC Name

OASIS Identity and Access Management (IAM) Technical Committee

### (1)(b) Statement of Purpose

It is frequently observed by practitioners new to identity and access management (IAM) that while there are many standards, statements of principles, and technologies in this area, there is no authoritative reference that defines a complete IAM system including authentication and attribute-based-access-control (ABAC) style authorization functionality. There is also a dearth of documented successful ABAC implementations that might serve as guidance for prospective implementers. The net effect is confusion in the market so that a decision to invest in IAM capability is perceived as high-risk by enterprise decision makers. This perception impedes investment in IAM systems, to the detriment of business effectiveness, security, and IAM solution providers.

The FICAM Roadmap--while it is well known, widely cited, and in principle mandatory for all US Federal agencies--is not specified in sufficient detail to reduce this risk for Federal implementers.  The FICAM Roadmap v2 (2011) is also out of date and incomplete, in that it is almost entirely devoid of guidance on ABAC, much less data tagging to enable object-level access control. Meanwhile, the need for better capability to enforce all applicable access control policies across and between enterprises in order to protect sensitive data has been recognized, both as a result of high-profile events like WikiLeaks, Sony, Anthem, etc., and because of the continuing movement toward maintaining sensitive information like health records on-line. While evolution of the FICAM Roadmap to include ABAC is planned, progress is very slow because of institutional factors.

Another FICAM-scale effort is under way to develop an Identity Ecosystem pursuant to the US National Strategy for Trusted Identities in Cyberspace, NSTIC. While not incompatible with FICAM, this effort started three years ago with a "clean sheet" approach for developing an architectural framework and is also progressing slowly due to institutional factors as well as the very large scope of the project. Like FICAM, the emerging ID Ecosystem is mostly focused on strong authentication, with ABAC as a distant second priority and data tagging and support for explicit digital policy management barely on the radar.

A mature SDO with extensive experience and interest in all the relevant IAM technologies can move more quickly and develop a complete IAM architecture that is compatible with high-level guidance from FICAM and NSTIC but which fully integrates advanced authorization functionality (e.g., supports ABAC and digital-policy management), and is implementable and testable. Such a product would promote the convergence of emerging public- and private-sector IAM frameworks as well as accelerating investment in more-capable systems for secure information sharing among government and private-sector entities.

https://ssl.gstatic.com/ui/v1/icons/mail/images/cleardot.gifThe goal of the IAM TC is to develop a testable reference architecture for a complete identity and access management system that implements the requirements of the US Federal Identity Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance, v2, as well as adhering to the Guiding Principles of NSTIC. The reference architecture will also implement ABAC authorization as envisioned in the work of the OASIS SAML and XACML TCs. The product of the proposed TC's work will be a reference architecture that is specified at the level of testable interfaces and component functions, but that does not specify products or proprietary standards. However, the architecture should be implementable with existing (or reasonably expected to be existing before completion of the TCs work) commercial or open-source IAM products. The target for TC-level approval of the initial deliverables is one year from establishment of the TC.

### 

### (1)(c) Scope

The scope of the IAM TC is development of system design artifacts for a system of interest that includes all functions necessary to provide access-control capability across a multi-organizational environment of arbitrary size. Anticipated normative products are a set of logical system- and subsystem-level specifications of functions and interfaces, and corresponding conceptual-level conformance and interoperability test specifications.

Although the system of interest is defined as providing “access-control capability”, this does not exclude “identity” (authentication) functionality. Authentication is considered a pre-requisite to implementing effective access control, but by itself is generally insufficient for authorization of access to any protected resource.

The TC will also develop supporting systems-engineering artifacts as non-normative products. These will include documentation of the requirements accepted for the IAM system design. Sources for these requirements will include but not be limited to the FICAM Roadmap (v2 or as updated) and the NSTIC Guiding Principles and IDESG Baseline Requirements for the ID Ecosystem. The TC may also develop non-normative operational concept (CONOPS) documents as needed to describe how the specified technology system fits within a business, financial and legal context.

The TC may produce a non-normative compilation of such missing functional standards that might serve as the basis for future work in the IAM TC or elsewhere.

The TC may develop digital access policies (XACML policy sets) or user or resource attribute profiles (e.g., DLP or privacy-protection attribute profiles) but only for the purpose of constructing interoperability or conformance test plans for IAM components

Out of scope--

The TC will not undertake to develop specifications for functions for which where there are no existing public standards or de facto standards implemented in multiple IAM products (e.g., for the functions of federating digital policy sets, or binding access-relevant metadata to protected resources in a way that is accessible to a policy-decision-point component.),

Except as described above, the TC will not develop specific digital access policies (XACML policy sets) or user or resource attribute profiles (e.g., DLP or privacy-protection attribute profiles).

The TC will not develop a reference implementation of the IAM Framework, but may conduct limited testing of IAM component software that implements in-scope standards, for example, to verify interoperability or asserted or presumed functionality. Any facilities required for such limited tests will be provided by TC Members.

### (1)(d) Deliverables

The principal TC final deliverables, with a target of one year from establishment of the TC, include—

1. Logical design artifacts specifying all technology subsystems of a multi-organizational IAM system (or environment) at the level of functional performance and interfaces;
2. Conceptual-level test plans that can be used to demonstrate conformance of the overall system and each sub-system, and interoperability among the sub-systems (i.e., conforming IAM components.)

The exact specification of these artifacts will be determined as one of the initial tasks of the TC.

Other TC deliverables (non-normative) will include—

1. Guidance documents aimed at helping potential implementers evaluate the IAM Framework in relation to their needs, and plan for implementing non-technology systems that will interact with a technology system implementing the IAM Framework. The documents will likely include:
   1. the functional requirements and constraints satisfied by the IAM Framework (e.g., requirements derived from the FICAM Roadmap and the NSTIC Guiding Principles);
   2. one or more CONOPS documents illustrating how an IAM-Framework implementation would satisfy key business transaction use cases, cross-organizational governance and coordination processes, potential service-provider and service consumer financial arrangements to support operation of the IAM capability.
2. Intermediate artifacts supporting the TC’s work processes. One of the first of these will likely include a systems engineering management plan (SEMP) that will define the nature of the other intermediate and final deliverable artifacts more specifically and establish the baseline schedule and key milestones or gate reviews for the work. Another will likely be a requirements traceability matrix that will provide a link between initial stakeholder requirements and system and subsystem functions. Because of the TC’s constraint that *“ . . . the architecture should be implementable with existing (or reasonably expected to be existing before completion of the TC’s work) commercial or open-source IAM products,”* the TC will also likely develop a list of initial requirements that were dropped from the final accepted requirements because they could not be satisfied with existing products implementing existing standards. This could provide the basis for future standards-development work in OASIS or elsewhere.

### (1)(e) IPR Mode

This TC will operate under the “Non-Assertion" IPR mode as defined in the OASIS Intellectual Property Rights (IPR) Policy.

### (1)(f) Audience

The anticipated audience for this work includes:

1. Vendors and service providers developing and offering identity and access-management (IAM) related software products or SaaS, including, for example: user credentialing systems; user attribute repositories and attribute aggregation products; authentication services; policy-decision-point (PDP) software; and digital policy development and management software (PAP and similar); and policy-enforcement point (PEP) products for adapting protected information resources to externalized authentication and authorization.
2. Integrators and consultants who will assist enterprise implementers of IAM capability in specifying and deploying a complete IAM physical (product-specific) technology solution that implements the IAM Framework, and in developing the related non-technology processes (e.g., access-policy governance and creation and approval of appropriate digital policy sets.)
3. “Ecosystem” service providers, including for example: trust-framework provider (COI federation) managers; consumer identity providers; and independent authoritative attribute providers (e.g., authorities for licensing or certifying professionals like physicians, law-enforcement officers, or emergency medical technicians.)
4. Independent testers and certifiers of interoperability and conformance with the IAM Framework specs.
5. Business or government enterprises, typically having:
   1. multiple information services subject to internal policies and external regulations on access to protected information resources (that is, relying-party systems), and
   2. employees and customers requiring interoperable credentials for access to internal (own-enterprise) and external (in the relevant trust ecosystem) information resources.
6. Oversight, policy, and compliance authorities, and public-interest advocates for privacy, etc., who may require or recommend conformance with the IAM Framework as a way of clearly and economically expressing their requirements to regulated entities.

### 

### (1)(g) Language

TC business will be conducted in English. The output documents will be written in (US) English.

### (References for Section 1)

FICAM Roadmap and Implementation Guidance, v2

http://www.idmanagement.gov/sites/default/files/documents/FICAM\_Roadmap\_and\_Implementation\_Guidance\_v2%25200\_20111202\_0.pdf

NSTIC Guiding Principles

http://www.nist.gov/nstic/guiding-principles.html

NIST Guide to ABAC Definition and Considerations

http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

NSTIC Pilots

http://www.ise.gov/blog/jeremy-grant/progress-identity-management-highlighting-government-and-industry-pilot-projects

OASIS XACML Technical Committee

https://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=xacml

OASIS SAML Technical Committee

https://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=security

[OASIS Identity in the Cloud Technical Committee, Committee Note 01 (Use Cases)](http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html)

http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html

International Council on Systems Engineering (NCOSE)

https://www.incose.org/

## Section 2: Additional Information

### (2)(a) Identification of Similar Work

There is extensive work within OASIS and elsewhere that is relevant to the work of the IAM Framework TC. A principal goal of the TC is to synthesize these existing standards, principles, requirements, and recommendations into a framework that is complete, consistent, implementable and testable.

The US Federal Identity, Credentialing and Access Management (FICAM) Roadmap provides high-level, mostly authentication-focused guidance for US Federal agencies that will be used by the TC as a source of requirements for the IAM Framework. Likewise the Identity Ecosystem Executive Steering Group (IDESG), initiated by the US National Strategy for Trusted Identities in Cyber-space (NSTIC) Program Management Office at the US National Institute of Standards and Technology (NIST) is developing baseline requirements for an Identity Ecosystem that implements the NSTIC Guiding Principles. These will also be used by the TC as requirements sources.

The NSTIC PMO has funded a number of pilot projects to develop or demonstrate new approaches to various aspects of the future ID Ecosystem. Of particular relevance to the TC’s work is the “Trustmark” pilot being conducted by Georgia Tech Research Institute (GTRI.) The Trustmark pilot is developing a set of “trustmark definitions” that comprise a building-block approach to defining the technology and other features implemented by an IAM service provider. The conceptual assessment (test) criteria that have been developed for the pilot’s trustmarks may be helpful to the TC in generating conceptual test criteria for IAM Framework components.

The OASIS SAML and XACML standards will be incorporated into the IAM Framework; other OASIS work, for example, the Identity in the Cloud TC’s Use Cases Committee Note, is relevant. The TC expects to have liaison with other OASIS activities via cross-membership on related TCs.

In OASIS and elsewhere there has been considerable work in specifying principles and related IAM techniques and technology to support particular areas of information-access policy. Implementing privacy controls is perhaps the most active area, but the OASIS XACML TC’s work on profiles for export control, intellectual property and data-loss prevention are other examples. The IAM Framework TC’s scope excludes work of this kind, but the TC should address how diverse attribute profiles or digital policy sets can be combined and managed efficiently.

### (2)(b) First TC Meeting

[TBD – likely about 60 days after submission of the TC proposal to the OASIS process, ideally coincident with an IAM-related event of some sort. Exact date must be established before submission.]

### (2)(c) Ongoing Meeting Schedule

The TC will meet weekly or as otherwise agreed upon by the members of the technical committee.

### (2)(d) TC Proposers

Martin Smith, [BFC.McLean@gmail.com](mailto:BFC.McLean@gmail.com) , Individual

John Tolbert, [john.tlbert@queraltinc.com](mailto:john.tlbert@queraltinc.com) , Queralt, Inc.

[Others TBD]

### (2)(e) Primary Representatives' Support

[to be provided before submission for final list of TC Proposers in (2)(d) who are organizational Oasis Members.]

### (2)(f) TC Convener

Martin Smith, BFC Consulting, LLC – Individual Member

### (2)(g) OASIS Member Section

None initially.

### (2)(h) Anticipated Contributions

[TBD]

### (2)(i) FAQ Document

None. (FAQs – and answers – to be developed from Charter submission review comments.)

### (2)(j) Work Product Titles and Acronyms

Work product titles and acronyms will be decided by the TC.

## Extra Stuff: Notes and cribbings of co-proposers, reviewers… content to be deleted