

Charter (IAS)

(1) WG NAME

Identity and Access Services Working Group (IAS-WG)

(2) PURPOSE

Organizations recognize the need for the unambiguous expression of identity. Identity can represent a physical individual, a collection of individuals, a logical entity, a resource or a capability. Identity is a fundamental element for establishing and maintaining business relationships, and for describing the credentials, capabilities, and responsibilities of parties to a relationship.

The principal business problem that drove the formation of the original Identity Services Working Group (under the auspices of Burton Group) is the difficulties companies face when integrating vendor Identity management (IdM) products with their existing infrastructure and, increasingly, in integrating vendor products themselves. As vendors continue to add to their IdM suites, integration between products is a challenge of increasing concern to organizations.

Integration between systems is achieved by:

- **Portability** – Business application components can be decoupled from dependencies on the operating systems and/or underlying hardware on which they run. Application components can access system-level services through programming interfaces. Integration can be achieved because the application relies on the OS or container to perform, for example, authentication or similar Identity-related services on its behalf
- **Interoperability** - Business application components can communicate with identity services (and vice versa) through a set of interfaces that specify a common set of semantics. These interfaces may be implemented by, but not limited to, web services. Interoperability is also important with respect to communication between business application components themselves, but that is not the focus of the charter's interest

The purpose of the IASWG is to establish requirements for the articulation of identity in a services environment. These requirements should correspond to business functions, activities, and expectations, and demonstrate how these will be accomplished in the web services context. The IASWG will identify what identity-related capabilities are required. How these capabilities are accomplished technically is specifically out of scope for this effort. The objective will be to identify and characterize these services in such a way that they may be implemented by another party.

(3) SCOPE:

Scope will be restricted to requirements and use cases, and they will be expressed in business, rather than technology, terms.

We will use a services model as the basis for an Identity and Access Management Architecture (IAM) in order to establish an abstraction layer that masks syntactic differences across vendor IdM products.

The term 'Identity Management' or IdM is in common use today throughout the industry, but we do not wish to limit the services it may so execute strictly to Identity. For purposes of this charter we take 'Identity Services' to include at a minimum the following topics:

- Identity Management: Services related to create, read, update and delete operations on a digital identity
- Authentication: Services related to the matching of credentials supplied by a requestor to those stored in a registry of some type
- Authorization: Services: Services related to managing permissions to resources (Coarse-grained) or to methods within resources (Fine-grained), as they may apply at design time (provisioning) or at run time (access control)
- Policies: Services that establish policy as a way of managing any of the above at run time. We consider the design time aspects of policy (e.g. administration used to create policies) to be out of scope
Where possible, we acknowledge the presence of current technology standards, and assume consumption of them where it makes sense. The group does not want to re-write standards such as XACML, nor does it want to develop identity services at such a low level.

(4) DRAFT TECHNICAL SPECIFICATIONS:

The development of draft technical specifications is not in scope for this Work Group.

(5) OTHER DRAFT RECOMMENDATIONS:

- Identity and Access Management Reference Architecture.
- A set of business-driven scenarios which describe what identity information is needed and how it is used. These scenarios will correspond to the lifecycle of a relationship, including creation, functionality, maintenance, and termination.

The scenarios will be sufficient to describe a broad set of situations as are practical for the composition of IASWG membership. The scenarios should provide sufficient examples of what information is needed and how it is used in order to provide requirements for the technical and vendor community to develop satisfactory and workable solutions.

The IASWG will provide support to the business and vendor community throughout any relevant development of solutions, as well as to standards bodies seeking to formalize its efforts.

- Establish requirements for identity in web services and other environments.

(6) LEADERSHIP:

- Convener: Gavin Illingworth, Bank of Montreal
- WG Chair: TBD
- Editor(s): TBD

(7) AUDIENCE:

Identity Management product vendors and customers who have implemented these product

(8) DURATION:

Estimated to be one year from the date of charter approval

(9) IPR POLICY:

The IASWG will operate under the terms of the Kantara Initiative IPR [Option Patent and Copyright \(RAND\)](#)

(10) RELATED WORK AND LIAISONS:

- Concordia DG
- OASIS
- Use cases / case studies, including AuthN and AuthZ
- Identity and Access Management Reference Architecture.
- Position papers
- Recommendations to vendors

(11) CONTRIBUTIONS:

- None at this time

(12) PROPOSERS:

- Convener: Gavin Illingworth, Bank of Montreal
- John Tolbert, Boeing
- Jeffrey Broberg, Computer Associates, CA