Kantara Initiative
Work Groups & Programs

March 2010

J. Trent Adams
adams@isoc.org

Outreach Specialist / Trust & Identity
Internet Society

Leadership Council Chair
Kantara Initiative
**Work Groups & Programs**

**Work Groups:**
Produce work according to their charter as approved by the Leadership Council
Any Participant can be a full voting member of a Work Group
May create formal output: specifications, white papers, code, etc.
Can submit output for Member vote as a Kantara Initiative Recommendation
Has a voting representative sit on the Leadership Council
Work Groups & Programs

Programs:

- Produce work according to their charter as approved by the Board of Trustees
- Generally tasked with work that requires signed agreements and has fiduciary responsibilities
- Program contributors are nominated by an independent committee and approved by the BoT
- Often work closely with one or more Work Groups engaged in related work
Work Groups & Programs

Work Groups:
- Clients WG
- Consumer Identity WG
- eGovernment WG
- Health Identity Assurance WG
- Identity and Access Services WG
- Identity Assurance WG
- IdP Selection WG
- ID-WSF Evolution WG
- Information Sharing WG
- Japan WG
- Privacy and Public Policy WG
- Telecommunications Identity WG
- Universal Login Experience WG
- User-Managed Access WG

Programs:
- Identity Assurance Review Board
- Interoperability Review Board
Work Groups & Programs

Work Groups:
- Clients WG
- Consumer Identity WG
- eGovernment WG
- Health Identity Assurance WG
- Identity and Access Services WG
- Identity Assurance WG
- IdP Selection WG
- ID-WSF Evolution WG
- Information Sharing WG
- Japan WG
- Privacy and Public Policy WG
- Telecommunications Identity WG
- Universal Login Experience WG
- User-Managed Access WG
- Interoperability Review Board
- Identity Assurance Review Board

Programs:
- Identity Assurance Review Board
Select Work Groups & Programs

- Identity and Access Services WG
- Information Sharing WG
- Universal Login Experience WG
- User-Managed Access WG
- Identity Assurance Review Board
- Interoperability Review Board
Select Work Groups & Programs

- Identity and Access Services WG
- Information Sharing WG
- Universal Login Experience WG
- User-Managed Access WG
- Identity Assurance Review Board
- Interoperability Review Board
Identity and Access Services Working Group – IAS-WG

- Began life in late 2007 as a Burton Group-sponsored initiative – the Identity Services Working Group (ISWG)
- Met via conference call and several F2F meetings held in Toronto
- Status of work presented at Burton Catalyst 2008
- Developed an Identity Services Framework (see Burton references)
- Burton published two papers based on the ISWG work:
  - The Challenge of Identity Services (September 2008)
  - Identity Services Architecture: Working Toward Consensus (February 2009)
- ISWG approached Kantara in late 2009 and requested that it become a chartered group
IAS-WG: Drivers

• The business problem:
  - Organizations face many difficulties when integrating vendor Identity Management (IdM) products into their existing infrastructure.
  - As vendors continue to add to their IdM suites, integration between products is a challenge of increasing concern.

• Our purpose and objectives:
  - Establish requirements for the articulation of identity in a services environment.
  - Ensure that requirements correspond to business functions, activities, and expectations.
  - Demonstrate how these will be accomplished in the web services context. The IASWG will identify what identity-related capabilities are required.
  - Identify and characterize these services in such a way that they may be implemented by another party e.g. vendors.
IAS-WG: Scope

- Restricted to requirements and use cases
- Expressed in business, rather than technology, terms
- Based on a services model as the basis for an Identity and Access Management Architecture (IAM)
- Establish an abstraction layer that masks syntactic differences across vendor IdM products
- Topics include:
  - **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 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.
IAS-WG : Current Status

- Charter approved by Kantara LC in December 2009
- Nine voting participants to date
- Six non-voting participants to date
- Election of chair person and editor/s pending
- Next conference call – week of March 15, 2010
- If you are interested in participating and would like more information:
  - [http://kantarainitiative.org/confluence/display/ias/Home](http://kantarainitiative.org/confluence/display/ias/Home)
  - **Gavin Illingworth**, Bank of Montreal Financial Group
    416 513- 5652
    gavin.illingworth@bmo.com
  - **John Tolbert**, The Boeing Company
    john.w.tolbert@boeing.com
Select Work Groups & Programs

- Identity and Access Services WG
- Information Sharing WG
- Universal Login Experience WG
- User-Managed Access WG
- Identity Assurance Review Board
- Interoperability Review Board
Information Sharing WG

The Customer - Supplier Engagement Framework
InfoSharing : Use Cases

Sally’s Car Buying Scenario

Our framework helps eliminate guesswork and waste on both customer and supplier sides.
InfoSharing : *In Progress* ...

- Lexicon
- Sally & Customer – Supplier Engagement Framework
- Information Sharing Literature Review
- Draft Standard for Personal Request for Proposals (PRFP)
- Draft Individual Information Sharing Agreement
Select Work Groups & Programs

- Identity and Access Services WG
- Information Sharing WG
- Universal Login Experience WG
- User-Managed Access WG
- Identity Assurance Review Board
- Interoperability Review Board
Universal Login Experience (ULX) WG

- Co-chairs:
  - Mike Graves (Janrain)
  - Bob Morgan (U of Washington)
  - Paul Trevithick (Azigo)

- *We know how to sign in using userid + password but…*
  - What if the site also wants to offer SAML, OpenID, or Infocard? Or all three?
  - How can we make this usable by mere mortals?
  - What’s the UX with and without an active client?
  - What’s the word? “log in”, “sign in” or “connect”?
ULX: *Universal Connect*

My NCBI | Connect

Limits  Advanced search  Help

Search  Clear

[PubMed]

...prises more than 19 million citations for articles from MEDLINE and life science publications may include links to full-text in PubMed Central or publisher web sites.
ULX : Connect 1st Time

Cross Protocol
- OpenID
- SAML
- Infocard

Other Features
- Horz scrolling
- Search for IdP by name
- Plan to add support for local userid + password, Facebook Connect, others…

Connect using:

- Google
- Yahoo!
- OhioState
- Equifax
- AOL
- ACXIOM
- Citigroup
- Wave

Search: i.e. type Boston University
ULX : Connect Again
Select Work Groups & Programs

- Identity and Access Services WG
- Information Sharing WG
- Universal Login Experience WG
- User-Managed Access WG
- Identity Assurance Review Board
- Interoperability Review Board
User-Managed Access (UMA)

- Chair: Eve Maler
- Vice-Chair & Spec Editor: Paul Bryan
- Use Cases Editor: Hasan ibne Akram
- Graphics/UX Editor: Domenico Catalano
- Implementation Coordinator: Maciej Machulak
UMA: Technical Proposition

- “...let an individual control the authorization of data sharing and service access made between online services on the individual's behalf”

- Enable an Internet-scale digital footprint dashboard model for user control and empowerment over data sharing
  - “Privacy is not secrecy!” – Bob Blakley
UMA : Facts & Stats

- WG launched on 6 August 2010 under the Reciprocal Royalty-Free IPR option
- Well-attended weekly telecons, occasional F2Fs, several public meetings, and a webinar
- Major draft deliverables to date:
  - Core Protocol spec (destination: IETF)
  - Scenarios and Use Cases document
  - A raft of explanatory material
- Implementor mailing list started recently
  - Two funded commitments to implement and deploy experimentally
Select Work Groups & Programs

- Identity and Access Services WG
- Information Sharing WG
- Universal Login Experience WG
- User-Managed Access WG
- Identity Assurance Review Board
- Interoperability Review Board
Identity Assurance Review Board (ARB)

- Sub-committee of the Board of Trustees
- Oversight of the Assurance and Accreditation Certification Program
- 2 Flavours of certification:
  - Assessor Accreditation
    - for auditors to become accredited
  - Certified Credential Service Providers (CSPs)
    - for CSPs to earn certification through a Kantara Accredited Assessor
ARB: Lines of Responsibility

Kantara Board of Trustees

Identity Assurance Working Group

Assurance Review Board

Reports to

Liaison

Owns & Publishes

Observes & Applies

IAF Reccs.

SAC

AAS AQR
ARB: Current Status

- Assurance and Accreditation Program Pilot in progress
- Now receiving applications from potential Auditors and Credential Service Providers seeking Accreditation and Certification
- To learn more visit:
Select
Work Groups & Programs

- Identity and Access Services WG
- Information Sharing WG
- Universal Login Experience WG
- User-Managed Access WG
- Identity Assurance Review Board
- Interoperability Review Board
Interoperability Review Board

- Kantara Board of Trustees sub-committee
- IRB Goal - cultivate and manage new certification programs covering a spectrum of developing protocols.
- Responsible for monitoring the conduct of the Kantara Initiative Interoperable Testing Program.
- To learn more: http://bit.ly/9HKwXP
IRB : Membership Coverage

• The Kantara Initiative Board of Trustees appoints the voting members of the IRB

• IRB should consist of implementer and deployer members representing a cross-section of the identity and access management community.

• Where two members are referenced, ideally one should be an implementer and one a deployer.
  • 2 SAML / ID-WSF
  • 2 SOAP Based Web Services
  • 2 Oauth / XRD
  • 2 Government Policy Makers
  • 1 Standards Development Organization
The Kantara Initiative Interoperable program will initially test implementations (executable computer code built in accordance to a specification) where there is significant interest in the technical specifications being tested in the program.

Standards initially targeted for the testing program:

- SAML
- Web Services: ID-WSF, WS-Security & WS-Trust
- OAuth
- OpenID
- XRD
IRB: Potential Testing Modalities

- **Full Matrix**
  - Requires each vendor to test with every other participant to ensure testing mirrors real world identity federation interoperability requirements.
  - The IRB may grant full certification based on the outcome of these events.

- **In the Queue**
  - Testing is performed one-to-one (versus Full Matrix where all potential matches are required).
  - Testing occurs on line remotely 3 to 4 months prior to a Full Matrix test.
  - In Queue candidates must to commit to participation in the next Full Matrix testing.
  - IRB may grant pre-certification based on the outcome of these events.
  - Implementations could advertise successful pre-certification in advance of the subsequent full certification test.

- **Face-to-Face**
  - Testing is performed in the same physical location at Face-to-Face Interoperability events.
  - The IRB may grant full or partial certification based on the outcome of these events.
Kantara Initiative
Work Groups & Programs

Thank you!

http://kantarainitiative.org

NOTE: Any mistakes in this presentation were probably my own, and not those of the hard-working participants.

J. Trent Adams
adams@isoc.org