BIAS Integration TC

Meeting #14

18 April 2007

San Diego, CA

Agenda

- 1. Administrative Issues
- 1.1 Call to order
- 1.2 Membership, attendance, & introductions
- 1.3 Approval of agenda
- 2. Chair's remarks
- 3. Review of minutes from meetings #13 (posted)
- 3.1 Action item review
- 4. TC business
- 4.1 Recent event debriefs
- 4.2 Security Webinar
- 4.3 Editor role

Agenda (cont'd)

- 5. Results of Editors Meeting (4/5)
- 5.1 Synch/asynch approach (Tilton/editors)
- 6. Results of Security Meeting (4/9)
- 6.1 Section 10 approach (E. Clay)
- 7. INCITS BIAS document update (M. Swayze)
- 7.1 INCITS document status
- 7.2 Changes in current revision
- 7.3 INCITS schedule/OASIS review & comments
- 8. BIAS Messaging Protocol (A. Parikh/M. Gurajara)
- 8.1 Status update & outstanding issues review
- 8.2 Assignments

Agenda (cont'd)

- 9. Technical discussion topics
- 9.1 Data format enumerated types
- 9.2 Degree of statefulness
- 9.3 Compensating processes
- 9.4 Others?
- 10. Reference implementation/prototyping
- 11. Schedule
- 11.1 Meeting schedule
- 11.2 Work schedule
- 12. New business
- 13. Action items
- 14. Adjourn

Working session???

- Originally scheduled 1-3
- Intent – roll up our sleeves and work on:
  - Missing material (e.g., hosting/discovery)
  - Lower level use cases
  - Group walkthrough of doc – develop list of changes/additions needed
- Planned to cancel due to low onsite registration & lack of editors.
- Interest? Participation?

Membership

- Voting members as of today
  - Young Bang — BAH
  - Ed Clay — Sun
  - Murty Gurajada — Raining Data
  - Dale Hapeman — DoD
  - John Mayer-Splain — DHS
  - Ash Parikh — Raining Data
  - Matt Swayze — Daon
  - Guy Swope — Raytheon
  - Cathy Tilton — Daon
  - Alessandro Triglia — OSS Nokalva
  - Gregory Zektser — BAH

Membership (cont'd)

- Membership distribution
  - 35 participants
  - 11 voting members, 6 members, 17 observers, 1 staff
  - 6 sponsor-level members/organizations
    - BAH
    - NIST
    - Raining Data
    - Raytheon
    - Sun
    - DoD

Chair's remarks

- Good news
  - We have WSDL
  - We've made some decisions this month
  - We have a stable INCITS document
- Bad news
  - We've slowed down since 2006
  - We need contributions in gap areas
  - We need more eyes on the document (review/comment)
  - Continue to need more web services expertise
  - No contributions since last meeting
  - No document revision since Feb.

Review of Meeting #13

- Notes posted
  - Corrections?
- Action items – held over from meeting #12:
  - (**Cathy**) Issue call for comments to INCITS on v0.7/0.8.
    - 2nd call sent to INCITS (M1/07-0310). Due date 18 May. CLOSED
  - (**Ed**) Provide a recommendation on how to update Section 14.
    - Offline meeting held 9 April (Mon). See agenda item #6.
  - (**Cathy**) Post the OASIS & i-Pira presentations to the OASIS BIAS website.
    - Posted. CLOSED
  - (**Guy**) Provide an example of low-level use cases (sequence/flow charts) for Annex B. OPEN.
  - (**Cathy**) Post another call for Contributions for Clause 6, Section 7 and the Conformance section.
    - Email call made on 28 March. No responses received.

Action items

- New at meeting #13
  - (**Cathy**) Add announcement on INCITS document once posted.
    - Pending (doc just posted 4/16)
  - (**Matt**) Post call for comments on INCITS doc rev 5 once posted.
    - Pending (doc just posted 4/16)
  - (**Editors**) Resolve synch/asynch issue. Incorporate recommended approach next rev of the documents.
    - Meeting held 4/9. See agenda item #5.
  - (**Cathy**) Update calendar for new meeting time. CLOSED.
  - (**All**) Review v0.8 and provide comments by 4/6. OPEN.
  - (**Murty**) Post v0.9 by 4/13. OPEN.
  - (**Cathy**) Look into ID Trust group during symposium.
    - Obtained some information – to be provided.

IDTrust Group

- New group (renamed – former PKI group)
- Website: http://www.oasis-idtrust.org/ (Thanks, Dale.)
- FAQ:
  - What are identification and trusted infrastructure standards?
    - This term applies to standards that provide the basic security required to carry out electronic business so that parties who do not know each other or are widely distributed can communicate securely using a chain of trust. The field encompasses several technology-based identity and trust models and standards, including those that are PKI-based as well as those utilizing other security mechanisms. More information on these standards can found on the IDtrust XML.org community web site.

IDTrust announcement

- The OASIS PKI Member Section has expanded its scope to encompass additional standards-based identity and trusted infrastructure technologies, policies, and practices. Effective immediately, the group will operate under the new name, OASIS Identity and Trusted Infrastructure (IDtrust) Member Section.

- Participants in the PKI Member Section have been automatically subscribed to the new IDtrust mailing lists and rosters in the same role they held in the PKI roster. New participants may join at any time by clicking the "Join this Group" link on http://www.oasis-open.org/apps/org/workgroup/idtrust-ms/index.php

- You may formally affiliate your membership with the IDtrust Member Section by an email request to member-services@oasis-open.org

- IDtrust will oversee the work of the OASIS Enterprise Key Management Infrastructure (EKMI) and PKI Adoption Committees. Other TCs are invited to explore the advantages of working within this Member Section, and the group is also open to ideas for forming new Committees.

- To provide direction for this initiative, OASIS is seeking nominations for the IDtrust Member Section Steering Committee. The nominations period begins now and will extend until 29 March 2007. Elections will be held 2-9 April 2007. This is a great opportunity to help chart a course for growth and innovation and receive recognition as a leader in this important area. See http://lists.oasis-open.org/archives/idtrust-ms/200703/msg00001.html for details.

About IDTrust

- The **OASIS Identity and Trusted Infrastructure (IDtrust) Member Section** promotes greater understanding and adoption of standards-based identity and trusted infrastructure technologies, policies, and practices. The group provides a neutral setting where government agencies, companies, research institutes, and individuals work together to advance the use of trusted infrastructures, including the Public Key Infrastructure (PKI).
- IDtrust was founded in 1999 as PKI Forum. It transitioned its work to the international standards consortium, OASIS, in 2002, where it continued to operate as an independent body focused on broadening adoption for PKI. In 2007, the group expanded its charter and was renamed the OASIS IDtrust Member Section.

TC Business

- Recent event debriefs
  - iPira conference (Ed/Matt)
  - Symposium (Cathy/Matt/others)
- Security Webinar
  - BPEL Webinar in March very successful (350 participants)
  - Planning meeting held 4/9 (coordinator: Dee Shur)
  - Scheduled for week of 5/21 (not Tue/Wed)
  - Each TC/topic – 1-1.5 hours on 1 day, pick time (intl. consid.)
  - 2-4 speakers needed: Volunteers?
  - Offline planning meeting: (date)
  - Guidelines: http://www.oasis-open.org/private/webinar-guidelines.php#overview
- Editor role
  - Suggestion made at annual members meeting
  - Met with positive response

Editors meeting – synch/asynch approach

- The following services need to support asynchronous operations:
  - Identify Subject
  - Enroll
  - Identify
  - Verify
- The same service will be used for synchronous and asynchronous operations.

- Upon receipt, the server will either:
  - Immediately process the request and return the results, or
  - Return a token & expiration date, indicating that the service is being handled asynchronously

- If a token is returned, the client/requester will be responsible for polling for the results using the following service calls, using the token as the only parameter:
  - Get Identify Subject Results
  - Get Enroll Results
  - Get Identify Results
  - Get Verify Results
- The requester can use the Query Capabilities call to determine if the server supports synchronous, asynchronous, or both for each of the 4 operations.

Security meeting

- We will break the security section into 3 main topics –
  - Integrity & Authenticity
    - Signing
  - Confidentiality/Privacy
    - Encryption
  - Access control
    - To services
- For each, we will identify potential mechanisms and considerations for using them (e.g., when to use)
  - Integrity
    - CBEFF security block (app level)
    - Signed XML (signed SAML assertions)
    - TSIK
  - Encryption
    - Comms/channel/connection level – https (ssl, tls)
    - App level
  - Access control
    - WSS (?)

Security meeting (cont'd)

- We will identify MINIMUM requirements as:
  - Signed XML for integrity
  - https for confidentiality
- Other, higher levels will be optional
- Could do –
  - Required – signing
  - Strongly recommended – encryption
  - As needed – access control
- [Decided on minimums stated above.]

- Could also have different security conformance levels or types.
- Recommendations based on environments?
- Will address security of operations across wire, not data at rest.
- Will mention key management (perhaps referencing existing standards) but note that this is NOT specifically addressed by BIAS.

INCITS BIAS document update

- **INCITS project 1823-D, BIAS**
  - Essentially complete
  - Latest draft (Rev 5): http://www.incits.org/tc_home/m1htm/2007docs/m1070198.pdf
  - Will be posted on TC documents page & call for comments made (probably due ~11 May)
  - Expected to go to ballot for public review in April timeframe & public review in June
- Description of changes

BIAS Messaging Protocol

- **OASIS document: BIAS Messaging Protocol**
  - Working draft – WSDL complete, gaps in other areas
  - Latest draft (Ed draft 0.8): http://www.oasis-open.org/committees/download.php/22543/bias-1%200-biasmp-ed-08.pdf
  - WSDL: http://www.oasis-open.org/committees/download.php/22544/bias.wsdl
  - Goal: Ready for review by Fall 2007
- Status

Gaps/call

- We are in great need of contributions to the BIAS Messaging Protocol document in the following areas:
  - **Section 6**
    - Title – BIAS endpoints & applications
    - Planned Content - describes and identifies of BIAS endpoints, applications, and an overview of BIAS message exchanges. Expand to contain information related to ***how to host, publish, and discover BIAS services***.
  - **Section 7**
    - Title – General provisions
    - Planned Content - contains general provisions which are invoked by other clauses
  - Contributions are requested by ***6 April 2007***, but will be accepted after that date as well.
- Review and comment on the current draft & WSDL is also needed.
- In addition, we are looking for inputs in the area of asynchronous services.

Technical discussion topics

- Data format enumerated types (biometric/biographic)
- Alignment of XML header with ISO CBEFF Pt3?
- Degree of statefulness
- Compensating processes
- Hosting/discovery (sample UDDI? Other registries?)
- How do we look WRT WS-I?
- Do we need to add XACML to security area?
- What do we need to specify that is not in the WSDL? Are all schemas complete between the 2 docs? Do we need a data dictionary?
- Dependencies/assumptions/prerequisites?
- Query capability info requirement for registry entry?
- How manage aggregate services? SP assign UUID to their implementation?
- Sample message exchanges?
- Others?

Implementation

- Reference implementation
- Prototyping
- Samples
- Interop demos? (when)

Schedule

- Meeting schedule
  - Meeting #15 16 May
  - Meeting #16 13 June
  - Meeting #17 ?
- Work schedule
  - Comments & contributions 27 Apr
  - Rev 0.9 & WSDL 4 May
  - Comments on 0.9 14 May
  - TC review 16 May

Wrap up

- New business
- Action items

- Adjourn