PWG -Imaging Device Security (IDS) Working Group

February 3, 2011

Wailea-Makena, HI

PWG F2F Meeting

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

Agenda

11:15 – 11:20 Administrative Tasks
11:20 – 11:30 Review action items
11:30 – 12:00 MPSA Survey and Article
12:00 – 13:00 Lunch
13:00 – 13:15 Document Status
13:15 – 13:45 System Logging
13:45 – 14:30 Common Criteria Evaluation
14:30 – 15:00 Identification, Authentication and Authorization
15:00 – 15:15 Break
15:15 – 15:45 IDS Security Ticket
15:45 – 16:00 Wrap up and adjournment

Administrative Tasks

- Select minute-taker
- Introductions
- IP policy statement:
  "This meeting is conducted under the rules of the PWG IP policy" If you don't agree, Surfs up or snorkels down!
- Approve Minutes from January 27 conference Call

IDS WG Officers

- IDS WG Chairs
  - Joe Murdock (Sharp)
  - Brian Smithson (Ricoh)
- IDS WG Secretary:
  - Brian Smithson (Ricoh)
- IDS WG Document Editors:
  - HCD-ATR: Jerry Thrasher (Lexmark)
  - HCD-NAP: Joe Murdock (Sharp), Brian Smithson (Ricoh)
  - HCD-TNC: Ira McDonald (Samsung), Jerry Thrasher (Lexmark), Brian Smithson (Ricoh)
  - HCD-Remediation: Joe Murdock (Sharp)
  - HCD-NAP-SCCM: Joe Murdock (Sharp)
  - HCD-Log: Mike Sweet (Apple)
  - IDS-IAA: Joe Murdock (Sharp)
  - IDS-CR: Ira McDonald, Joe Murdock, Ron Nevo

Action Items

Action Item #	Entry date	Assignee	Type	Action	Status	Disposition
33	12/10/2009	Randy Turner	SHV	Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV.		Ron Nevo will take this task.
34	12/10/2009	Randy Turner	Remediation	Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints."		Symantec wants an NDA, but PWG cannot do an NDA.. Ron nevo will take over this task. Need to indicate to Symantec that we really wdon;t need too much proprietary information from them, but want to give them our information. Can we get Symantec to attend the April meeting in Cupertino?
44	3/11/2010	Jerry Thrasher Ira McDonald Brian Smithson	NEA Binding	TCG TNC Binding document		Make it a TCG document, not an IETF NEA document
58	6/11/2010	Joe Murdock and Ira McDonald	SCCM	Create a first draft SCCM binding spec based on the NAP binding spec	H	On hold due to priorities.
66	10/20/2010	Brian Smithson Joe Murdock Ira McDonald	admin	Create a project charter for creating IEEE 2600.1 Supporting Documents		With no requirements specification. Wait for NIAP guidance in mid to late January.
67	10/28/2010	Joe Murdock Ira McDonald	auth	Write HCD-Authentication-and-Authorization-Framework specification	P	direction is not "recommendations only", it is "requirements and recommendations" (pointing to existing standards) because there will be a conformance section
69	12/2/2010	Michael Sweet	log format	Write HCD Logging specification	P	New draft Feb 2011
70	12/9/2010	Brian Smithson	admin	Make arrangements for F2F meeting with NIAP/other schemes at Ricoh SF during RSA week		
71	12/9/2010	Joe Murdock	ATR	propose by email a multivalued attribute for log location (a URI) to be added to HCD-ATR		
73	12/9/2010	Joe Murdock Ira McDonald Ron Nevo	reqts spec	start an IDS common requirements spec to include out-of-scope and terminology sections		Base on new PWG template
75	1/13/2011	Joe Murdock Ira McDonald Bill Wagner	MPSA	MPSA Security article	P	Also a WIMS action item

MPSA Articles and Survey

- Continued from WIMS
- Will we have new result data?

Document Status

- HCD-Assessment-Attributes

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20110127.pdf
  - Stable (needs a binding prototype)
  - Latest version fixed a simple typo
- HCD-NAP Binding

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100930.pdf
  - Stable
- HCD-TNC Binding
  - Initial Draft still under development
- HCD-NAC Business Case White Paper

  ftp://ftp.pwg.org/pub/pwg/ids/white/tb-ids-hcd-nac-business-case-20100422.pdf
  - Final

Document Status

- HCD-Remediation

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf
  - Initial Draft
- HCD-NAP-SCCM Binding
  - Specification on hold
- HCD-CLF

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110126.pdf
  - Draft
- IDS-Identification-Authentication-Authorization

  Mind Map:

  ftp://ftp.pwg.org/pub/pwg/ids/white/ids-iaa-framework-20110202.xmind

  Specification:

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.pdf

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.docx
- IDS-CR

HCD Common Log

- System Log IDS Attribute

HCD Health Assessment Attribute Name	(DataType)
	Description
HCD_SysLog_URI	(string)
	The HCD_SysLog_URI attribute is a variable length string that specifies the location(s) where the HCD's system log is to be stored. Locations are provided as a URI and MUST conform to RFC 2396. When multiple locations are provided, the log is to be written to locations in the order indicated by the list, starting with the first provided location. If no explicate HCD_SysLog_URI locations have been defined by a system administrator, the system default internal log location MUST be returned.

- Document Review

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110126-rev.pdf

Common Criteria

- NIAP CC Status
- Common Criteria Support Documents Project Charter
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids2600sd-charter-20110202.pdf

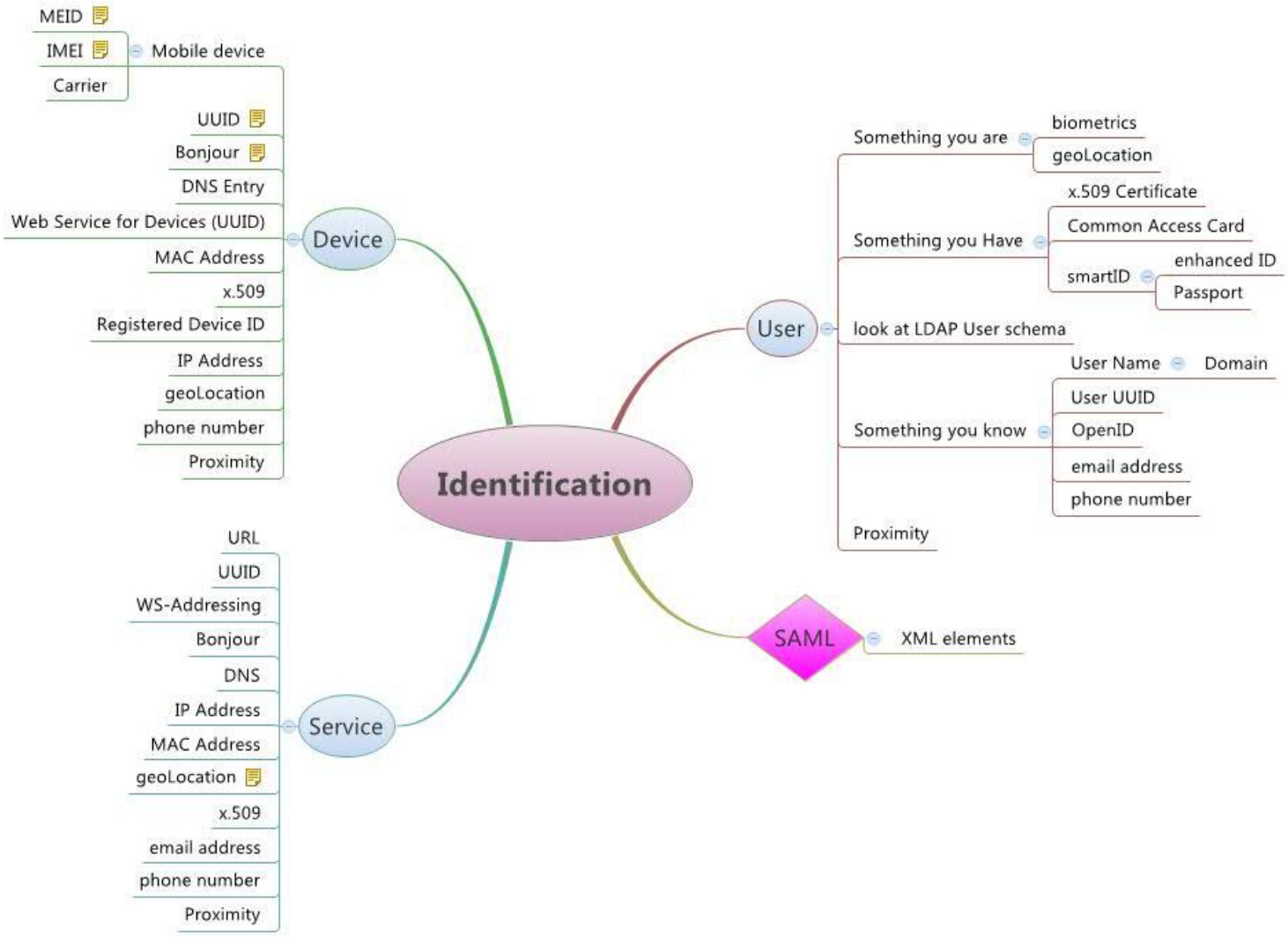
IDS IAA

- Mindmap file:
  - ftp://ftp.pwg.org/pub/pwg/ids/white/ids-iaa-framework-20110202.xmind
- Identification, Authentication, Authorization
  - Specification outline

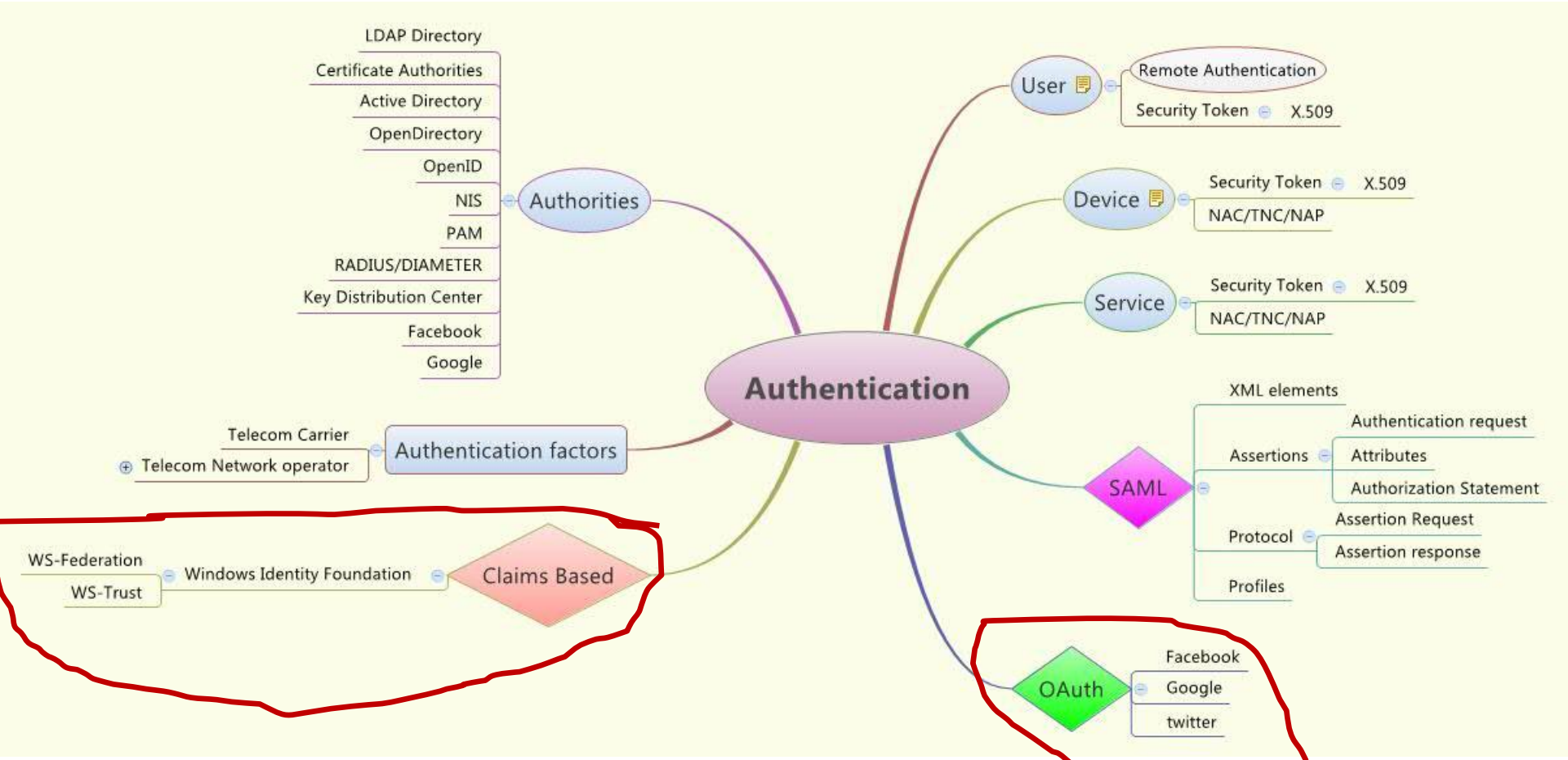
ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110202.pdf

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110202.docx

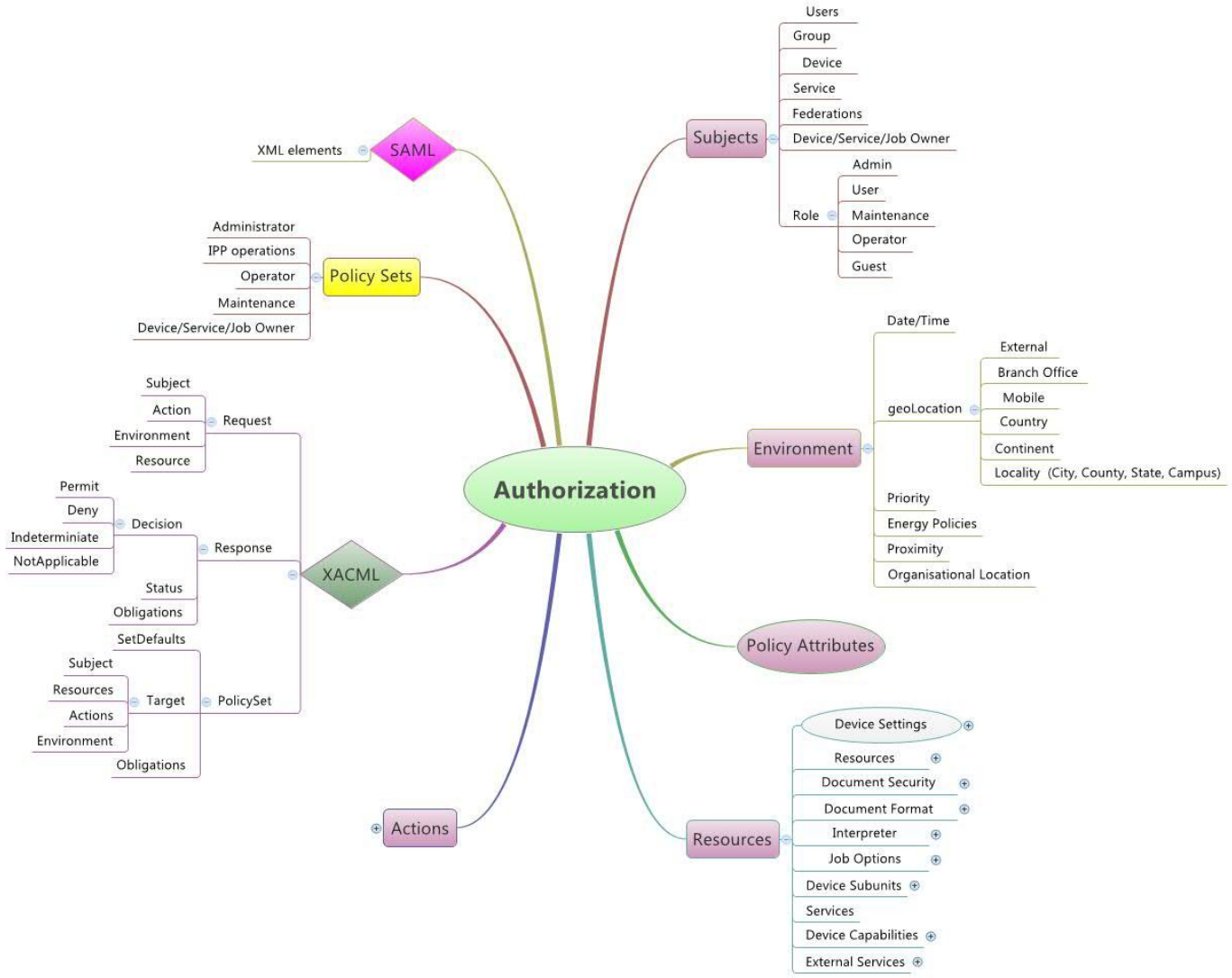
Identification Framework



Authentication Framework



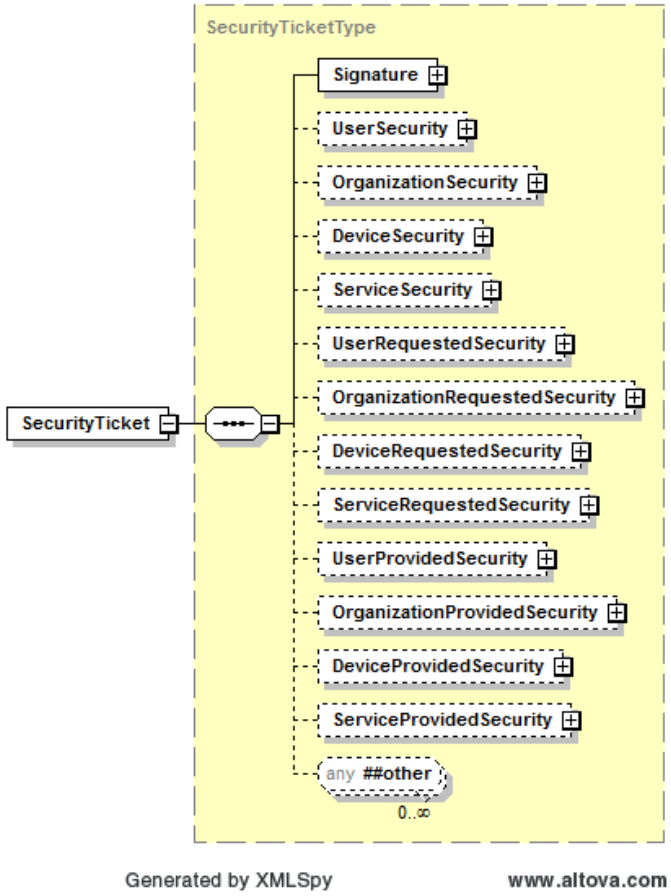
Authorization Framework



Security Ticket

- Review XML Schema Element

  ftp://ftp.pwg.org/pub/pwg/ids/white/ids-security-20110202.xsd



Security Ticket

- How does a device or service advertise it's supported security capabilities?
  - Add a supported security element to the security ticket?
  - Overload of xxxSecurity or a
  - A separate element in the system or service capabilities?
  - In the semantic model, the system object would provide all supported methods, while each service (system, print, etc.) would list only those used by the service.
- Add required physical hardware security requirements (e.g. don't save data to disk, encrypted disk, etc.) to security information?

Cloud Consideration in the Security Ticket

- How does the printer advertise it's public key? Do we add public key to the identity element?
  - How best to pass the public key through a cloud manage/provider directly to the user?
- Need to consider what to encrypt
  - In a cloud environment, want to provide end-to-end encryption of job data, but the job ticket (or at least the security ticket) need to be readable by the cloud print provider and manager so they can match security requirements between the user, devices and services.
- Cloud Job privacy
  - How to avoid tracking of a job or partial interception.
  - Provide a way to explicitly hide job origination information? (wikileaks type of use case)
    - Runs contrary to the IDS logging assumptions, but is this appropriate for the cloud use model?

Wrap up

- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference call February 24, 2011
- Adjournment