

IDS Working Group

2009-01-08 Conference Call Minutes

1. Attendees

Lee Farrell	Canon
Glen Petrie	Epson
Dave Whitehead	Lexmark
Ira McDonald	High North
Nancy Chen	Oki Data
Brian Smithson	Ricoh
Shah Bhatti	Samsung
Peter Cybuck	Sharp
Ron Nevo	Sharp

Ron Nevo opened the IDS session and provided the planned agenda topics:

- Identify Minute Taker
- PWG IP Policy
- Approval of previous minutes:
<ftp://ftp.pwg.org/pub/pwg/ids/minutes/IDS-call-minutes-20081215.pdf>
- Review Action Items
- How to proceed with MS profile of NAP
- Secure Device Identifier
- Document Review Comments
- Next Steps / Next Meetings

2. Minutes Taker

Lee Farrell

3. PWG Operational Policy

It was noted that all attendees should be aware that the meeting is conducted under the PWG Membership and Intellectual Property rules. There were no objections.

4. Approve Minutes from December 15 Conference Call

There were no objections to the previous Minutes.

5. Review Action Items

ACTION: Randy Turner will try to find other contacts that would be willing to work with the PWG to help deploy NEA health assessment. (Juniper, Symantec, Cisco are suggested candidates.) Is someone willing to sit down with the PWG and “have discussions”?

→ **ONGOING**

IDS Working Group

2009-01-08 Conference Call Minutes

ACTION: Randy Turner will post the Microsoft name(s) for the PWG to make contact with regard to logo requirements.

→ **OPEN**

ACTION: Joe Murdock will add NAP protocol information to document and update the conformance section.

→ **OPEN**

ACTION: Brian Smithson will update and re-write the Network Access Protection Protocol Binding document, taking into account the comments from the October meeting and the comments that Dave Whitehead has posted.

→ *Brian said that he does not think he will be able to start on this task for another two weeks. He will try to have it done in time for review prior to the face-to-face meeting.*

→ **OPEN**

ACTION: Ron Nevo and Dave Whitehead will update the IDS Wiki pages to reflect current status.

→ **OPEN**

ACTION: Jerry Thrasher will attempt to re-write the definitions of “resident” and “downloadable”.

→ *The definitions have been added to the current draft.* **CLOSED**

ACTION: Joe Murdock will include sequence diagrams as illustrative examples for the NAP binding document.

→ **OPEN**

ACTION: Peter Cybuck will examine the NIST standards for insight or material on secure time.

→ **OPEN**

ACTION: Dave Whitehead will examine the NTP standard (RFC 4330) for insight or material on secure time. (There is a reference to MIL-03 which should be followed.)

→ **OPEN**

ACTION: Randy Turner will follow up with Microsoft to ask if they will recognize a class plug-in for NAP.

→ **OPEN**

6. Secure Time/Authenticated Time

Peter said that he has done some research on this topic, and has determined that NIST has a standard (or multiple standards?) on time servers, but he needs more time to investigate. Ira indicated that the authenticated NTP server provided by NIST only operates with NIST-distributed symmetric keys that are tied to individual machines. Unfortunately, this approach does not scale well for our purposes. Pete acknowledged this problem, and repeated his desire for more investigation time.

IDS Working Group

2009-01-08 Conference Call Minutes

Ira suggested that we should change our use of the term “secure time” to “authenticated time.” The group agreed, resulting in the following Action Item:

ACTION: Jerry Thrasher will change the term “secure time” to “authenticated time” throughout the Attributes document.

Ira also suggested that we should not require the MFD to independently be responsible for obtaining authenticated time, but should rely on the network to provide this capability.

7. How to proceed with MS profile of NAP

Although it was previously suggested to invite someone at Microsoft to attend a PWG face-to-face meeting, the group now thinks it might be more practical to hold a teleconference instead.

ACTION: Dave Whitehead will coordinate with Randy Turner to generate a proposal to Microsoft on proceeding with obtaining NAP information on what they envision would be the content of a profile—including remediation.

8. Secure Device Identifier

Dave referenced the following specification from IEEE, which has been brought to the attention of the Trusted Computing Group (TCG):

Secure Device Identifier (IEEE P802.1AR/D1.9)

Abstract: A secure device identifier (DevID) is cryptographically bound to a device, and supports authentication of the device’s identity. Locally significant identities can be securely associated with an initial manufacturer provisioned DevID, and used in provisioning and authentication protocols to allow a network administrator to establish the trustworthiness of a device and select appropriate policies for transmission and reception of data and control protocols to and from the device.

The specification apparently looks promising, but might need some additional consideration or progress before being useable within IDS.

Ron said that the referenced specification seems to allow anyone to create an ID—and then claim it is correct.

Ira believes that NAP or NAC will [eventually] need to include some kind of attribute that contains an ID of some sort.

The group agreed to follow the progress of the IEEE effort to evaluate future applicability.

IDS Working Group
2009-01-08 Conference Call Minutes

9. Document Review Comments

Downloadable and Resident definitions have been included in the last draft. No one had any objections to the new text, but most of the attendees indicated that they had not yet read the new material.

ACTION: Everyone will review the latest Attributes document draft prior to the next teleconference, and prepare comments for discussion.

10. Next Teleconference

Subsequent teleconferences are scheduled for January 22 and February 5

11. Summary of New Action Items and Open Issues

In addition to the existing OPEN Actions Items, the following new items were generated:

ACTION: Jerry Thrasher will change the term “secure time” to “authenticated time” throughout the Attributes document.

ACTION: Dave will coordinate with Randy to generate a proposal to Microsoft on proceeding with obtaining NAP information on what they envision would be the content of a profile—including remediation.

ACTION: Everyone will review the latest Attributes document draft prior to the next teleconference, and prepare comments for discussion.

IDS meeting adjourned.