

IDS Working Group

2009-01-22 Conference Call Minutes

1. Attendees

Randy Turner	Amalfi Systems
Lee Farrell	Canon
Glen Petrie	Epson
Ira McDonald	High North
Dave Whitehead	Lexmark
Nancy Chen	Oki Data
Brian Smithson	Ricoh
Peter Cybuck	Sharp
Ron Nevo	Sharp
Bill Wagner	TIC

Dave Whitehead 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-20080108.pdf>
- Review Action Items
- Other/New Items
 - * TNC IF-TNCCS
 - * Microsoft NAP and the Class Plug-in
 - * Remediation
 - * Document Review Comments
 - * Other?
- 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 January 8 Conference Call

It was noted that Dave Whitehead opened the January 8 teleconference, not Ron Nevo. There were no other objections to the previous Minutes. The Minutes will be updated, and were approved pending the noted correction.

IDS Working Group
2009-01-22 Conference Call 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”?

→ *Still needs to pursue this further. No new information to report.*

→ **ONGOING**

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

→ *Randy has a name (Justin Hitchins) for the logo requirements. No contact information yet, though.*

→ **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.

→ **OPEN**

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

→ *Ron is asking for feedback on what was generated.*

→ **OPEN**

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.

→ **CLOSED**

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

→ **CLOSED**

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

→ *Done with Microsoft Printing Group, but still needs to occur with NAP Group.*

→ **CLOSED**

IDS Working Group

2009-01-22 Conference Call Minutes

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. Need to identify the appropriate point of contact within Microsoft.

→ **OPEN**

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

→ *No one has prepared any comments, but Nancy had a question.*

→ **OPEN**

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

→ **OPEN**

6. Secure/Authenticated Time

Ira pointed out that the NIST-supported time offered over the internet has a 50msec skew. Peter suggested that this should be sufficient for any kind of audit trail purposes. For anything better, he thinks a network appliance would need to implement it, not the MFD.

Ira noted that the IDS requirement for “secure time” (to be changed to “authenticated time”) would not be fulfilled with this approach.

As Ira suggested at the previous teleconference, it was repeated that we should not require the MFD to independently be responsible for obtaining authenticated time, but should rely on the network (i.e., some network appliance) to provide this capability.

Randy said that the time should be required from a trusted source, and the time should be obtained via a secure protocol.

Randy mentioned the IETF TICTOC activity as interesting reference material.

It was suggested that a survey of alternatives of supplying secure time should be done, resulting in a recommendation for possible solutions.

ACTION: Ron Nevo will examine which time protocols could be used for providing authenticated time with high integrity, and make appropriate recommendations.

→ **NEW**

7. Microsoft NAP and the Class Plug-in

Randy has had some e-mail discussions with the Microsoft Printing team about a class plug-in. He summarized two main points:

- They understand the value of a class plug-in as it pertains to NAP.
- Anything regarding NAP and hardcopy devices is out of scope for the Microsoft Printing team, and it is suggested that the PWG should be talking to the NAP team. No NAP team point of contact was provided.

Randy said he will follow up to find a point of contact within the Microsoft NAP group.

8. Quarantine State

Nancy raised the question about whether the mapping of a [required] Quarantine State attribute described in the TNC SOH document should be in the Attributes document or the Binding document.

She also wonders whether the NEA has a similar attribute.

ACTION: Nancy Chen will identify a specific issue that she has found with regard to the Quarantine State attribute in the TNC SOH document, and will post it (and any recommendations) to the e-mail list.

→ **NEW**

ACTION: Everyone will consider the Quarantine State attribute issue that Nancy Chen has raised and will provide recommendations for resolving.

→ **NEW**

9. Remediation

Before the meeting time elapsed, Dave requested the group to consider the following question:

Are there any common remediation steps that we can document?

Document Review Comments

There was no time for this topic.

10. Next Teleconference

February 5, 1:00pm EST.

11. Summary of New Action Items

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

ACTION: Ron Nevo will examine which time protocols could be used for providing authenticated time (with high integrity), and make appropriate recommendations.

IDS Working Group

2009-01-22 Conference Call Minutes

ACTION: Nancy Chen will identify a specific issue that she has found with regard to the Quarantine State attribute in the TNC SOH document, and will post it (and any recommendations) to the e-mail list.

ACTION: Everyone will consider the Quarantine State attribute issue that Nancy Chen has raised and will provide recommendations for resolving.

IDS meeting adjourned.