

IDS Working Group

2008-10-23 Face-to-Face Meeting Minutes

1. Attendees

Randy Turner*	Amalfi Systems
Lee Farrell	Canon
Glen Petrie	Epson
Lida Wang	Kyocera
Jerry Thrasher	Lexmark
Dave Whitehead	Lexmark
Ole Skov	MPI Tech
Nancy Chen	Oki Data
Ron Bergman	Ricoh
Brian Smithson	Ricoh
Shah Bhatti	Samsung
Peter Cybuck	Sharp
Craig Whittle	Sharp
Bill Wagner	TIC
Andrey Savov	Toshiba
Pete Zehler	Xerox

* via telephone

On Thursday morning, Ron Bergman opened the IDS session and provided the planned agenda:

- Select Minute Taker
- Approve Minutes from October 2 Conference Call
- Review Action Items
- Randy Turner will compile feedback comments from the NEA, and will forward them to the IDS group
- Joe Murdock will add NAP protocol information to the document and update the conformance section
- Ron will check to see if MS will be at the meeting and will send an email to Mike Fenelon to query the issue
- Attributes Spec: Review of changes in October 13 draft
- HCD-NAP Spec: Review of changes in October 8 draft
- HCD-NAP Issues (from email)
- HCD-NEA Spec plans and schedule
- New Action Items and Open Issues
- Closing Summary

2. Minutes Taker

Lee Farrell

3. Approve Minutes from October 2 Conference Call

There were no objections to the previous Minutes.

IDS Working Group

2008-10-23 Face-to-Face Meeting Minutes

4. Review Action Items

ACTION: Randy Turner will compile feedback comments from the NEA, and will forward them to the IDS group.

→ *The draft has been published and includes the agreed upon items from PWG. **CLOSED***

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

→ **OPEN**

ACTION: Ron Bergman will check to see if MS will be at the meeting and will send an email to Mike Fenelon and Jerry Thrasher to query the issue about how to get NAP attributes registered with Microsoft.

→ *Although originally planning to attend, Mike Fenelon (Microsoft) had a conflict at work and could not be at the meeting. **OPEN***

5. Attributes Spec: Review of changes in October 13 draft

Ron Bergman led a review of the latest modifications to the specification. There were no objections or any significant discussion about the changes.

In Section 5.2.3, Jerry Thrasher noted that he was uncertain about the “condition” under which the attribute HCD_Certification_State would be mandatory. The group agreed to move it to Section 5.3 and list it as optional.

Randy Turner suggested that any conformance items in the SOH mapping document would simply reference the Attributes specification. This would eliminate any problems of maintaining consistency across multiple documents.

Jerry noted that unless anyone had any other comments, he feels that this document is essentially complete. [Later, it was pointed out that the references to the IETF TNC documents will limit the advancement of the Attributes specification. It cannot progress to a Proposed Standard if it references unstable specification documents.]

Randy mentioned that some of the encoding specifics could be included in the Attributes document, or put in a mapping document. Ron said that it would be appropriate to place this detail in each binding document. That would be the place to include any overrides to the statements in the attribute specification document. It was pointed out that the current statement in Section 6 Internationalization Considerations is written as an *intent*, not a mandatory requirement.

Dave Whitehead said he attended a recent OASIS meeting, at which he heard that Microsoft wants to use UTF-8.

The group agreed that a final mark-up draft will be issued and a Working Group Last Call will be initiated.

IDS Working Group
2008-10-23 Face-to-Face Meeting Minutes

6. HCD-NAP Spec: Review of changes in October 8 draft

Ron led a review of the latest modifications to the draft. Again, there were no objections to the changes.

The references in Section 6 must be clarified to indicate that they reference the Attributes specification.

ISSUE: Randy pointed out that although the NAP specification notes UTF-8 in some cases, he sees that a null termination is also suggested. He sees this as potentially confusing, and suggests that we should contact Microsoft for clarification.

ACTION: Ron Bergman will check with Microsoft about the [potentially confusing] requirement for UTF-8 with null termination.

It was noted that HCD Name and HCD Model should be merged to be consistent with the Attributes specification document.

“HCD NAME” was changed to “HCD MACHINE TYPE MODEL.”

The question was raised about whether the Sub-Type values should be renumbered to eliminate any “holes” in the numbering sequence. It was suggested that this would be a good time to do it, given that there probably has not been any prototyping done yet.

It was agreed that the definitions of each attribute mentioned in the binding specification(s) could be modified to reference the attribute definition in the Attributes specification. It was also suggested that the content in the binding document could then be presented in a table format for easier reading.

Randy pointed out that extensible protocols are typically adopted with most of the core features, and a smaller set of feature extensions. In the IDS usage of NAP, virtually all of the features are non-standard extensions.

7. HCD-NAP Issues (from e-mail)

Ron addressed the following questions:

Dear PWG-IDS Members,

We have read through "wd-ids-naps0h10-20081008.pdf" and would like to confirm the items listed below.
Could you kindly let us know answers or comments on our questions ?

Q1. Section 4.4 HCD Attribute Encoding
C. VALUE FIELD is fixed size (4octet) or variable size ?
2. SUB-TLV FIELD is fixed size (8bit) or variable size ?

Q2. Section 4.6.4 HCD DOWNLOADABLE AP NAME SUB-TLV (Sub-Type = 7, Sub-Length =variable)
2.Downloadable Application Name (4 octets)
We suppose the length of Downloadable Application Name should be variable.

IDS Working Group

2008-10-23 Face-to-Face Meeting Minutes

Q3. Section 4.6.12 HCD CERTIFICATION STATE SUB-TLV (Sub-Type = 14, Sub-Length = 4octets)

In wd-idsattributes10-20081013, Section 4.1 General Attribute Definitions HCD_Certification_State "Since it is being deferred to Phase 2 of the IDS definition process."

This attribute is not yet defined clearly and being deferred to Phase2. Could you let us know when this attribute will be defined ?

Q4. 4.7.1 HCD CONFIGURATION STATE SUB-TLV (Sub-Type = 15, Sub-Length = 4octets)

This attribute is not yet defined clearly. Could you let us know when this attribute will be defined ?

Q5. 4.6.1 HCD FIRMWARE VERSION SUB-TLV (Sub-Type = 5, Sub-Length = 16 octets)
4.6.5 HCD DOWNLOADABLE AP VERSION SUB-TLV (Sub-Type = 8, Sub-Length = 20 octets)

4.6.9 HCD RESIDENT AP VERSION SUB-TLV (Sub-Type = 11, Sub-Length = 16 octets)

The format of VERSION is defined as fixed format.

1. Major Version Number (4 octets)
2. Minor Version Number (4 octets)
3. Build Number (4 octets)
4. Service Pack, Major Number (2 octets)
5. Service Pack, Minor Number (2 octets)

However, some firmware or applications version numbers may not fit to the specified format.

In such case, is it possible to apply the following rules ?

If the version number is longer than 16 octets, use only the first 16 octets.

If the version number is shorter than 16 octets, the rest of data are filled with 0x00.

Thanks in Advance.

Q1→ The specification will be modified to clarify.

Q2→ The length should be fixed-length.

Q3→ It will not be defined.

Q4→ It is vendor-specific, and will not be defined.

Q5→ The definition should be clarified further. We need to add a string version to the Attribute document. It was suggested that both the numeric and string versions should be conditionally mandatory—with either one or the other (or both) supported.

There was some doubt about whether a string version would actually be useful for remediation, but the group agreed to the approach.

IDS Working Group

2008-10-23 Face-to-Face Meeting Minutes

ISSUE: Do we want to use the SOH Microsoft Product-Name TLV 10 or define something else in the PWG namespace?

ACTION: Ron Bergman or Dave Whitehead will contact Mike Fenelon to determine whether the SOH Microsoft Product-Name TLV 10 is appropriate for PWG use, or whether we should define something else in the PWG namespace?

ISSUE: Because of Ron Bergman's departure from the PWG, the NAP Binding document is in need of a new Editor.

Shah Bhatti had issued an e-mail with two questions from Samsung:

The first is:

In the NAP protocol, what if a NAP client, which was already checked as a compliant device via NAP 802.1x protocol by the NAP server and are using 802.1x protocol, wants to use dynamic IP by DHCP?

Then, should the NAP client send a SoH message "again" to the NAP server via NAP DHCP protocol?

The main point is whether the information of each client status is shared in the server-side or not.

if shared in the server-side, each client does not have to send its message again and just requests the sever to use another protocol.

if not, each client sends its status whenever he want to use or change into another protocol.

The second is:

When binding HCD with NAP protocol, is there another (or something special only to HCDs) system health agent(SHV) and system health validator?

Referring MS NAP protocol, a 3rd party is able to create his/her own SHA and SHV.

SHAs and SHVs for firewall, Windows update patch, and virus vaccine is already applied in the current Windows OS.

Is there another health information for HCD?

The answer to the first question is beyond the scope of IDS, and should be asked of Microsoft.

The answer to the second question is that each vendor—or the PWG—will need to define a plug-in to do the health assessment. Bill Wagner pointed out that without such a plug-in, our work would not be very useful.

IDS Working Group

2008-10-23 Face-to-Face Meeting Minutes

What are Microsoft's plans for this kind of development? Is Microsoft planning to write it, or will they help the PWG to create it? Without support from Microsoft, the PWG activity will be severely limited.

ACTION: Dave Whitehead will contact Microsoft with regard to defining a plug-in to do the [NAP-based] health assessment. Perhaps a general explanation about deployment plans would be useful?

Other questions for Dave to ask Microsoft:

- Because there are multiple assessment protocols, is it conceivable that multiple assessment protocols run simultaneously—with each requiring independent (i.e., redundant) assessment?
- How does Microsoft envision the process for remediation?
- Does Microsoft have any plans for a gateway between NAP and NEA?

Bill pointed out that until we have a better sense of Microsoft's plans with regard to NAP and hardcopy devices, it might not be wise to continue with the NAP Binding specification.

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”?

Ron mentioned that it might be possible that the NAP protocol could be implemented as a gateway to/through the NEA protocol.

8. HCD-NEA Binding Specification plans and schedule

ISSUE: The NAP Binding document is in need of an Editor.

Although the attendees acknowledged the need, there were no volunteers at the meeting.

9. Summary of New Action Items and Open Issues

ACTION: Ron Bergman will check with Microsoft about the [potentially confusing] requirement for UTF-8 with null termination.

ACTION: Ron Bergman or Dave Whitehead will contact Mike Fenelon to determine whether the SOH Microsoft Product-Name TLV 10 is appropriate for PWG use, or whether we should define something else in the PWG namespace?
[It was suggested that any contact with Mike Fenelon should be cc:'d to Erhan Soyer-Osman.]

ACTION: Dave Whitehead will contact Microsoft with regard to defining a plug-in to do the health assessment. Perhaps a general explanation about deployment plans would be useful?

IDS Working Group

2008-10-23 Face-to-Face Meeting Minutes

ACTION: Dave Whitehead will attempt to obtain answers from Microsoft to the following questions:

- Because there are multiple assessment protocols, is it conceivable that multiple assessment protocols run simultaneously—with each requiring independent (i.e., redundant) assessment?
- How does Microsoft envision the process for remediation?
- Does Microsoft have any plans for a gateway between NAP and NEA?

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”?

ISSUE: Because of Ron Bergman’s departure from the PWG, the NAP Binding document is in need of a new Editor.

ISSUE: The NAP Binding document is in need of an Editor.

10. Closing Summary

The attendees extended a hearty thanks to Ron Bergman for his diligent efforts as the IDS Working Group Chair, as well as his many years of contributions in other PWG activities.

Dave Whitehead and Ron Nevo will be assuming the roles of co-Chairs for the IDS WG in the future.

IDS meeting adjourned.