January 30, 2009
Working Draft

The Printer Working Group

The Printer Working Group (PWG)
Hardcopy Device Health Assessment
Network Access Protection Protocol Binding
(HCD – NAP)

Status: Initial Draft

Abstract: This standard is one part of a set of documentation that defines the application of security policy enforcement mechanisms to imaging devices. This document specifies how the Microsoft Network Access Protection (NAP) protocol is to be used, along with the set of heath assessment attributes created especially for hard copy devices, to allow access to hard copy devices based upon the locally defined security policy.

This document is available electronically at:

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-nap10-20090130.pdf

About the IEEE-ISTO

The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and flexible operational forum and support services. The IEEE-ISTO provides a forum not only to develop standards, but also to facilitate activities that support the implementation and acceptance of standards in the marketplace. The organization is affiliated with the IEEE (http://www.ieee.org/) and the IEEE Standards Association (http://standards.ieee.org/).

For additional information regarding the IEEE-ISTO and its industry programs visit http://www.ieee-isto.org.

About the IEEE-ISTO PWG

The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and Technology Organization (ISTO) with member organizations including printer manufacturers, print server developers, operating system providers, network operating systems providers, network connectivity vendors, and print management application developers. The group is chartered to make printers and the applications and operating systems supporting them work together better. All references to the PWG in this document implicitly mean "The Printer Working Group, a Program of the IEEE ISTO." In order to meet this objective, the PWG will document the results of their work as open standards that define print related protocols, interfaces, procedures and conventions. Printer manufacturers and vendors of printer related software will benefit from the interoperability provided by voluntary conformance to these standards.

In general, a PWG standard is a specification that is stable, well understood, and is technically competent, has multiple, independent and interoperable implementations with substantial operational experience, and enjoys significant public support.

For additional information regarding the Printer Working Group visit: http://www.pwg.org

Contact information:

The Printer Working Group
c/o The IEEE Industry Standards and Technology Organization
445 Hoes Lane
Piscataway, NJ 08854
USA

Imaging Device Security Web Page:

http://www.pwg.org/ids/

IDS Mailing List:

ids@pwg.org

Instructions for subscribing to the IDS mailing list can be found at the following link:
http://www.pwg.org/mailhelp.html

Implementers of this specification are encouraged to join the IDS Mailing List in order to participate in any discussions of the specification. Suggested additions, changes, or clarification to this specification, should be sent to the IDS Mailing list for consideration.

Table of Contents

1. Introduction

Many corporate network and security administrators are beginning to deploy various security policy enforcement mechanisms that measure the "health" of networked device being attached to the network infrastructure, in addition to merely authenticating the user or device. The goal of these health assessment mechanisms is to provide a level of assurance that the device being granted access to network resources will do no harm to the network or other networked devices. For PCs, servers, etc.; these health assessment schemes allow the administrator to access the condition of the device's operating system, anti-virus program, personal firewall, and other attributes of the device to ensure that they are in compliance with the security policy for the network.

Currently, Hardcopy Devices and other imbedded devices such as IP phones do not participate in any of these protocols and are allowed to bypass health assessment when attaching to the network. In many health assessment schemes, this is merely the entry of the device's MAC or IP address into an exception table. This, however, creates a vulnerability in the network assessment scheme, as it is fairly simple for the MAC or IP address of the excepted HCD to be spoofed by another device that would normally be subject to the health assessment.

2. Terminology

This section defines the following terms that are used throughout this document:

2.1 Conformance Terminology

Capitalized terms, such as MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, MAY, NEED NOT, and OPTIONAL, have special meaning relating to conformance as defined in RFC 2119 [RFC2119].

2.2 Other Terminology

In addition, the following terms are imported or generalized from other source documents:

Hardcopy Device (HCD) – A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, multifunction peripherals (MFPs), multifunction devices (MFDs), all-in-ones, and other similar products. [IEEE2600]

Administrator – A user who has been specifically granted the authority to manage some portion or all of the HCD and whose actions may affect the security policy. Administrators may possess special privileges that provide capabilities to override portions of the security policy. [IEEE2600]

Application – Persistent computer instructions and data placed on the HCD, via download or additional hardware (daughter card), that are separate from, and not a part of, the base Firmware. Applications are an addition to the base Firmware that provide additional function beyond that provided by the base Firmware.

Firmware – Persistent computer instructions and data embedded in the HCD that provides the basic functions of that device. Firmware is only replaced during a specialized update process. [IEEE2600]

Device administrator – A user who controls administrative operations of the HCD other that its network configuration (e.g., management of users and resources of the HCD). [IEEE2600]

Network administrator – A user who manages the network configuration of the HCD. [IEEE2600]

User – An entity (human user or IT entity) outside the HCD that interacts with the HCD. [IEEE2600]

3. Requirements

3.1 Rationale for HCD Health Assessment Attributes

Hardcopy Devices generally do not include the same software infrastructure and patch management mechanisms as a PC or server, and don't currently include anti-virus programs or personal firewalls. However there are attributes of a HCD that can be defined that can be used to gauge an HCD's compliance with a security policy.

3.2 Use Models

Several use cases are presented in the PWG Hardcopy Device Health Assessment Attributes specification [HCD-ATR]. Since this specification represents a binding of the protocol defined in the referenced specification, the use cases presented in the referenced specification are applicable to this specification.

4. NAP Statement Of Health Protocol

This section defines how the specified Hardcopy Device Health Assessment Attributes [HCD-ATR] are to be used with the Microsoft NAP Statement Of Health (SOH) protocol [MS-SOH].

4.1 NAP/SOH Attribute Encoding

All Statement Of Health attributes are presented using the Type/Length/Value (TLV) Structure defined in [MS-SOH] clause 2.2.1.

4.2 NAP/SOH Required Attributes

The attributes specified in this section must always be included in the SOH attribute set.

4.2.1 SYSTEM HEALTH ID TLV

This attribute provides the identifier of the System Health Agent (SHA) or the System Health Validator (SHV) generating the SOH or SOHR report entry. This must be the first entry in the SOH or the SOHR. This attribute does not have an equivalent definition in the HCD Attribute Specification [HCD-ATR]. The *Value* field contains two parts.

1. **VENDOR SMI CODE FIELD** For Hard Copy Devices this 24 bit field will contain the value of the PWG SMI, which is 2699 (0xA8B).
2. **COMPONENT ID FIELD** This 8 bit field defines the component type, qualified by the *Vendor SMI Code*. The following values are defined for hard copy devices. Values are additive (e.g. printer + scanner + copier = 7).
   1 = Printer Device
   2 = Scanner Device
   4 = Copier Device
   8 = Fax Device

For additional information, refer to [MS-SOH] clause 2.2.3.1.

4.2.2 COMPLIANCE RESULT CODES TLV

This variable length attribute contains an array of SOH Result Codes indicating the compliance of the Hard Copy Device. For additional information, refer to [MS-SOH] clause 2.2.3.2.

4.2.3 FAILURE CATEGORY TLV

This variable length attribute contains an array of SOH Result Codes indicating the compliance of the Hard Copy Device. This attribute does not have an equivalent definition in the current HCD Attribute Specification [HCD-ATR]. Its format and values are defined in [MS-SOH] clause 2.2.3.4.

4.3 NAP/SOH Optional Attributes

The attributes specified in this section are optionally included in the implemented SOH attribute set.

4.3.1 PRODUCT NAME TLV

(Type = 0x0A or 0x8A, Length = variable) USE HCD Name

This attribute contains a null terminated UTF-8 string providing the name of the firmware product installed on the Hard Copy Device. This attribute provides the capability specified by HCD_Firmware_Name. Reference: HCD_Firmware_Name in the PWG Hardcopy Device Health Assessment Attributes specification [HCD-ATR].

4.4 HCD Attribute Encoding

All Hardcopy Device Statement Of Health attributes are presented using the following NAP specified Type/Length/Value (TLV) Structure. For additional information, refer to [MS-SOH] clause 2.2.3.2.

A) **TYPE FIELD** This 16 bit field MUST contain the code 0x07 to indicate one or more attributes, that are not defined by Microsoft, will follow.

B) **LENGTH FIELD** This 16 bit field defines the length, in octets, of the *Value* field.

C) **VALUE FIELD** This field contains the set of HCD asses**sment attributes i**ncluded. The Value field for HCD attributes SHALL be st*ructur*ed as follows:

1) **SMI VALUE FIELD** This 24 bit field contains the value 2699 (0xA8B) which represents the IANA SMI Private Enterprise code assigned to the PWG. The value is used by the NAP Health Registration Authority to select the appropriate validator module to process the attributes in the Sub-TLV field.

2) **SUB-TLV FIELD** This field contains one or more HCD Attribute Sub-TLVs. Each HCD Attribute Sub-TLV will have the same format as defined for the NAP/SOH Attribute TLVs, with the M bit always reset to zero. A summary of this format is shown below:

a) **SUB-TYPE FIELD** This is a 16 bit value containing a PWG assigned Sub-Type Code.

(1) **SUB-LENGTH FIELD** This is a 16 bit value that defined the length, in octets, of the following Sub-Type Value field.

(2) **SUB-TYPE VALUE FIELD** This field contains the value of the attribute. The length of this field is as specified by the Sub-Length field.

4.5 HCD Attributes

The attributes specified in this table are for hardcopy devices and do not have an equivalent function in the [MS-SOH] attribute set. To be conformant with this specification, attributes in this table are to be implemented by hardcopy devices according to the Conformance column.

SUB-TLV	Sub-Type	Sub-Length	Definition	Conformance
HCD MACHINE TYPE MODEL	1	variable	Refer to [HCD-ATR]	Mandatory
HCD VENDOR NAME	3	variable	Refer to [HCD-ATR]	Mandatory
HCD VENDOR SMI CODE	4	3 octets	Refer to [HCD-ATR]	Mandatory
HCD FIREWALL SETTING	13	Variable	Refer to [HCD-ATR]	Mandatory
HCD CONFIGURATION FLAGS	26	4 octets	Refer to section 4.5.1	Mandatory
HCD FIRMWARE VERSION	5	16 octets	Refer to section 4.5.2	Conditionally Mandatory
HCD FIRMWARE VERSION STRING	23	variable	Refer to section 4.5.3	Conditionally Mandatory
HCD FIRMWARE PATCHES	6	Variable	Refer to section 4.5.4	Conditionally Mandatory
HCD DOWNLOADABLE AP NAME	7	Variable	Refer to section 4.5.5	Conditionally Mandatory
HCD DOWNLOADABLE AP VERSION	8	20 octets	Refer to section 4.5.6	Conditionally Mandatory
HCD DOWNLOADABLE AP VERSION STRING	24	Variable	Refer to section 4.5.7	Conditionally Mandatory
HCD DOWNLOADABLE AP PATCHES	9	Variable	Refer to section 4.5.8	Conditionally Mandatory
HCD RESIDENT AP NAME	10	Variable	Refer to section 4.5.9	Conditionally Mandatory
HCD RESIDENT AP VERSION	11	16 octets	Refer to section 4.5.10	Conditionally Mandatory
HCD RESIDENT AP VERSION STRING	25	Variable	Refer to section 4.5.11	Conditionally Mandatory
HCD TIME SOURCE	20	Variable	Refer to [HCD-ATR]	Conditionally Mandatory
HCD MIN CIPHER SUITE	21	Variable	Refer to [HCD-ATR]	Conditionally Mandatory
HCD MIN CIPHER KEY LENGTH	22	4 octets	Refer to [HCD-ATR]	Conditionally Mandatory
HCD CONFIGURATION STATE	15	4 octets	Refer to [HCD-ATR]	Optional
HCD CERTIFICATION STATE	14	4 octets	Refer to [HCD-ATR]	Optional

4.5.1 HCD CONFIGURATION FLAGS SUB-TLV

This attribute provides the current state of the Boolean configuration parameters. Each Boolean is actually represented using two bits, where one bit is used to indicate of the parameter is supported and the second provides the Boolean value. The bits definitions are defined as follows:

Bit 0 (LSB) **Forwarding Enabled:** When true, indicates the interface on which health assessment is being performed is also being used as a bridge, route, or proxy from any other interface, including itself.

Bit 1 **Forwarding Supported:** When true, indicates the hard copy device supports the forwarding function between interfaces and the Forwarding Enabled bit is valid. When false, the Forwarding Enabled bit is to be ignored and treated as if a false value was present.

Bit 2 **Administrative Password Configured:** When true, indicates the Administrator Passwords or other credentials on the device have been changed from the out of box configuration.

Bit 3 **Administrative Password Configuration Supported:** When true, indicates the hard copy device supports modification of the out of box credentials. When false, the Administrative Password Configured bit is to be ignored and treated as if a false value was present.

Bit 4 **PSTN FAX Enabled:** When true, indicates the PSTN FAX interface or another modem interface on the hard copy device is enabled.

Bit 5 **PSTN FAX Supported:** When true, indicates the hard copy device supports a PSTN FAX interface or another modem interface. When false, the Administrative PSTN FAX Enabled bit is to be ignored and treated as if a false value was present.

Bit 6 **Secure Time Enabled:** When true, indicates the hard copy device is configured to acquire the current time from a known secure source in a secure manner.

Bit 7 **Secure Time Supported:** When true, indicates the hard copy device can be configured to acquire the current time from a known secure source in a secure manner.. When false, the Secure Time Enabled bit is to be ignored and treated as if a false value was present.

Bits 8 through 32 are reserved and MUST be zero on transmission and ignored upon receipt.

4.5.2 HCD FIRMWARE VERSION SUB-TLV

(Sub-Type = 5, Sub-Length = 16 octets)

This attribute contains 5 parts to define the version of the firmware installed on the Hard Copy Device. All value are to be the binary representation of the defined parameter. This attribute MUST be included only if the HCD Firmware Version String SUB-TLV is not present.

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)

4.5.3 HCD FIRMWARE VERSION STRING SUB-TLV

This attribute contains vendor specific null terminated UTF-8 string that describes the version of the firmware installed on the Hard Copy Device. This attribute MUST be included only if the HCD Firmware Version SUB-TLV is not present.

4.5.4 HCD FIRMWARE PATCHES SUB-TLV

This variable length attribute contains a null terminated UTF-8 string defining the firmware patches that have been installed on the Hard Copy Device. This attribute MUST be included only if the Firmware Patches have been installed on the HCD Firmware.

4.5.5 HCD DOWNLOADABLE AP NAME SUB-TLV

This variable length attribute provides the name of an application that has been downloaded into the Hard Copy Device. This attribute MUST be included for each Downloadable Application currently installed on the HCD. The attribute contains two parts.

1. Correlation ID (4 octets) This part is used to group the Downloadable Application Name with the corresponding HCD Downloadable Ap Version, the HCD Downloadable Ap Version String, and the HCD Downloadable Ap Patches attributes.
2. Downloadable Application Name (variable) This part contains a null terminated UTF-8 string providing the name of the downloadable application,

4.5.6 HCD DOWNLOADABLE AP VERSION SUB-TLV

This attribute contains 6 parts to define the version of a downloaded application on the Hard Copy Device. This attribute MUST be included the Downloadable Application, if the HCD Downloadable Ap Version String SUB-TLV is not present, for each Downloadable Application currently installed on the HCD.

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)
6. Correlation ID (4 octets) This part is used to group the Downloadable Application Version with the corresponding HCD Downloadable Ap Name, the HCD Downloadable Ap Version String, and the HCD Downloadable Ap Patches attributes.

4.5.7 HCD DOWNLOADABLE AP VERSION STRING SUB-TLV

This attribute contains vendor specific null terminated UTF-8 string that describes the version of a downloaded application on the Hard Copy Device. This attribute MUST be included for the Downloadable Application, if the HCD Downloadable Ap Version SUB-TLV is not present, for each Downloadable Application currently installed on the HCD. The attribute contains two parts.

1. Correlation ID (4 octets) This part is used to group the Downloadable Application Version String with the corresponding HCD Downloadable Ap Name, HCD Downloadable Ap Version, and the HCD Downloadable Ap Patches attributes.
2. Downloadable Application Name (variable) This part contains a null terminated UTF-8 string defining the version of the downloadable application.

4.5.8 HCD DOWNLOADABLE AP PATCHES SUB-TLV

This variable length attribute defines the firmware patches that have been installed for a downloaded application on the Hard Copy Device. This attribute MUST be included for each Downloadable Application currently installed on the HCD containing one or more firmware patches. The attribute contains two parts.

1. Correlation ID (4 octets) This part is used to group the Downloadable Application Patches with the corresponding HCD Downloadable Ap Name, HCD Downloadable Ap Version, and the HCD Downloadable Ap Version String attributes.
2. Downloadable Application Patches (variable) This part contains a null terminated UTF-8 string defining the version of the downloadable application,

4.5.9 HCD RESIDENT AP NAME SUB-TLV

This variable length attribute contains a null terminated UTF-8 string providing the name of a resident application currently enabled on the Hard Copy Device. This attribute MUST be included for each Resident Application currently installed on the HCD.

4.5.10 HCD RESIDENT AP VERSION SUB-TLV

This attribute contains 6 parts to define the version of a resident application currently enabled on the Hard Copy Device. This attribute MUST be included for the Resident Application, if the HCD Resident Ap Version String SUB-TLV is not present, for each Resident Application currently installed on the HCD.

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)
6. Correlation ID (4 octets) This part is used to group the Resident Application Version with the corresponding HCD Resident Ap Name, the HCD Resident Ap Version String, and the HCD Resident Ap Patches attributes.

4.5.11 HCD RESIDENT AP VERSION STRING SUB-TLV

This attribute contains vendor specific null terminated UTF-8 string that describes the version of a resident application currently enabled on the Hard Copy Device. This attribute MUST be included for the Resident Application, if the HCD Resident Ap Version SUB-TLV is not present, for each Resident Application currently installed on the HCD. The attribute contains two parts.

1. Correlation ID (4 octets) This part is used to group the Resident Application Version String with the corresponding HCD Resident Ap Name, HCD Resident Ap Version, and the HCD Resident Ap Patches attributes.
2. Resident Application Name (variable) This part contains a null terminated UTF-8 string defining the version of the resident application,

4.5.12 HCD RESIDENT AP PATCHES SUB-TLV

This variable length attribute contains a null terminated UTF-8 string defining the firmware patches that have been installed for a resident application currently enabled on the Hard Copy Device. This attribute MUST be included for each Resident Application currently installed on the HCD containing one or more firmware patches. The attribute contains two parts.

1. Correlation ID (4 octets) This part is used to group the Resident Application Patches with the corresponding HCD Resident Ap Name, HCD Resident Ap Version, and the HCD Resident Ap Version String attributes.
2. Resident Application Patches (variable) This part contains a null terminated UTF-8 string defining the version of the resident application.

5. Conformance

5.1 Common Conformance Requirements

The Microsoft Network Access Protection protocol supports multiple network access methods. All access methods share a minimum set of common protocol conformance requirements.

5.1.1 Statement of Health for NAP Protocol

Microsoft Network Access Protection requires that a NAP client be able to generate and transmit a Statement of Health (SoH) message and receive and process a Statement of health Response, as specified in MS-SOH . The specific transport mechanism used to carry the SoH message is dependent on which of the multiple network access methods supported by NAP is being utilized (see sections 5.2 to 5.5 below).

5.1.2 Security Health Agent Protocol

The current Microsoft Statement of Health for NAP Protocol requires that a NAP Health Agent delivering SoH data to current existing Windows NAP health validators generate Statement of Health Report Entries (SoHReportEntries) that conform to the format and required value set as specified in MS-WSH. It also requires that the HealthAgent process SoH Response values and condition codes as described in [MS-WSH]. Definition and processing of PWG and other vendor supplied extensions to the current SoH Report Entrires are not currently defined.

5.2 DHCP Conformance Requirements

5.2.1 Dynamic Host Configuration Protocol Extensions

Microsoft conformance requires that NAP DHCP clients provide and recognize the DHCP extensions defined in [MS-DHCPN]. Specifically, the following DHCP options and responses must be properly processed:

DHCP Option Code	Vendor-specific Option Code	Description
43	0xDC	Statement of Health
43	0xDD	NAP subnet mask
43	0xDE	NAP Correlation Id
43	0xDF	IPv6 Remediation server list
77		DHCP User Class "Default Network Access Protection"

5.3 802.1x Conformance Requirements

NAP clients requesting network access via 802.1x port authentication protocols must establish a separate protected connection within the Extensible Authentication Protocol (EAP) used for 802.1x. This connection must be established using the Protected Authentication Protocol (PEAP).

5.3.1 Protected Extensible Authentication Protocol

A conforming NAP client must be able to establish a PEAP connection to a Network Access Server as required by MS-PEAP. This connection would typically be established with the NAS using EAP messages over PPP, but other transport protocols, such as RADIUS and 802.1x may be used.

5.4 VPN Conformance Requirements

NAP clients requesting network access a VPN network connection must establish a separate protected connection within the Extensible Authentication Protocol (EAP) using RADIUS attributes. This connection must be further secured using the Protected Authentication Protocol (PEAP).

5.4.1 RADIUS Attributes for NAP

MS-RNAP describes a set of RADIUS vendor extensions defined by Microsoft for NAP network authentication and validation using RADIUS messages. A NAP client using RADIUS for access to a VPN or 802.1x network is required to be conformant to these extensions.

5.5 IPSec Conformance requirements

IPSec–based NAP provide a NAP client secure and safe access to an established network through the use of Health Certificates. This NAP access method is useful for NAP clients that are already established on the physical network, but are required to be validated for secure network access.

5.5.1 Health Certificate Enrollment Protocol

MS-HCEP defines a protocol for authenticating a client and validating a Statement of Health using HTTP protocols. A HCEP NAP client is required to already be assigned a IP address, and be capable of establishing a HTTP 1.1 (RFC 2616) or HTTPS (RFC 2818) connection. Additionally the NAP client must be able to request x.508 certificates using Public Key Cryptography Standards (PKCS) Message #10 and PKCS Message #7.TBD (Joe Murdock): **T**his section is to include a link to the discussion of the required NAP protocols.

6. IANA and PWG Considerations

This section provides the registration information to be used by the Printer Working Group for the registration of the Hardcopy Device (HCD) Health Assessment Attribute Sub-Type codes. The values defined in this specification are contained in the following table. No IANA registrations are required for this document.

Code	Description
1	HCD Machine Type Model
3	HCD Vendor Name
4	HCD Vendor SMI Code
5	HCD Firmware Version
6	HCD Firmware Patches
7	HCD Downloadable AP Name
8	HCD Downloadable AP Version
9	HCD Downloadable AP Patches
10	HCD Resident AP Name
11	HCD Resident AP Version
12	HCD Resident AP Patches
13	HCD Firewall Setting
14	HCD Certification State
15	HCD Configuration State
16	Reserved (HCD Forwarding Enabled)
17	Reserved (HCD PSTN FAX Enabled)
18	Reserved (HCD Admin Password Configured)
19	Reserved (HCD Secure Time Enabled)
20	HCD Time Source
21	HCD MIN Cipher Suite
22	HCD MIN Cipher Key Length
23	HCD Firmware Version String
24	HCD Downloadable AP Version String
25	HCD Resident AP Version String
26	HCD Configuration Flags

7. Internationalization Considerations

For interoperability and basic support for multiple languages, conforming Printer implementations MUST support the UTF-8 [RFC3629] encoding of Unicode [UNICODE] [ISO10646].

8. Security Considerations

The NAP Statement Of Health protocol [MS-SOH] specification, section 5, provides a detailed discussion of security issues relative to the Network Access Protection (NAP) protocol. Since this specification defines a set of attributes to be used by NAP in a manner as defined in the MS-SOH specification, MS-SOH section 5 is also applicable to this specification.

Microsoft has patents that may cover protocols and procedures presented within this document. Microsoft has not granted to the Printer Working Group any licenses under these or any other Microsoft patents. It is strongly recommended that any entity implementing this specification, contact Microsoft at protocol@microsoft.com, regarding a patent license.

9. References

9.1 Normative References

[ISO10646] "Information Technology - Universal Multiple-octet Coded Character Set (UCS)" (ISO/IEC Standard 10646), ISO, 2006.

[HCD-ATR] Thrasher, J., “PWG Hardcopy Device Health Assessment Attributes”, Work in process. Current document available at ftp://ftp.pwg.org/pub/pwg/ids/wd/

[IEEE2600] “IEEE Std. 2600™-2008, Information Technology: Hardcopy Device and System Security”, IEEE, 2008

[RFC868] Postel, J., and K Harrenstien, “Time Protocol” (RFC 868), IETF, May 1983, available at http://www.ietf.org/rfc/rfc0868.txt

[RFC1305] D. Mills.”Network Time Protocol (NTP), version 3” (RFC 1305), IETF, March 1992, available at http://www.ietf.org/rfc/rfc1305.txt

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels” (RFC 2119),. IETF, March 1997, available at http://www.ietf.org/rfc/rfc2119.txt.

[RFC3629] Yergeau, F., "UTF-8 Transformation of ISO 10646" (RFC 3629), IETF, November 2003, available at http://www.ietf.org/rfc/rfc3629.txt

[RFC4330] Mills, D., “Simple Network Time Protocol (SNTP), version 4“ (RFC 4330), IETF, January 2006., available at http://www.ietf.org/rfc/rfc4330.txt.

[TLS-CIPHER] “Transport Layer Security (TLS) Parameters”, IANA, January 2009, available at http://www.iana.org/assignments/tls-parameters

[UNICODE] Davis, M., et al, "Unicode Standard v5.1.0", Unicode Standard, April 2008, available at http://www.unicode.org/versions/Unicode5.1.0/

[MS-SOH] Statement of Health Protocol for Network Access Protection (NAP) Protocol Specification, v20090106, January 2009, Microsoft Corporation, available at http://download.microsoft.com/download/9/5/e/95ef66af-9026-4bb0-a41d-a4f81802d92c/%5BMS-SOH%5D.pdf

[MS-WSH] Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol Specification, v20090106, Microsoft Corporation, January 2009, available at http://download.microsoft.com/download/a/e/6/ae6e4142-aa58-45c6-8dcf-a657e5900cd3/%5BMS-WSH%5D.pdf

[MS-DHCPN] Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP), v20090106, Microsoft Corporation, January 2009, available at,http://download.microsoft.com/download/a/e/6/ae6e4142-aa58-45c6-8dcf-a657e5900cd3/%5BMS-DHCPN%5D.pdf

[MS-EAP] Microsoft Extensible Authentication Protocol (need correct URL if this document is needed)

[MS-PEAP] Protected Extensible Authentication Protocol (PEAP) Specification, v20090106, Microsoft Corporation, January 2009, available at http://download.microsoft.com/download/a/e/6/ae6e4142-aa58-45c6-8dcf-a657e5900cd3/%5BMS-PEAP%5D.pdf

[MS-RNAP] Vendor-Specific RADIUS Attributes for Network Access Protection (NAP) Data Structure, v20090106, Microsoft Corporation, January 2009, available at http://download.microsoft.com/download/a/e/6/ae6e4142-aa58-45c6-8dcf-a657e5900cd3/%5BMS-RNAP%5D.pdf

[MS-HCEP] Health Certificate Enrollment Protocol, v20090106, Microsoft Corporation, January 2009, available at http://download.microsoft.com/download/9/5/e/95ef66af-9026-4bb0-a41d-a4f81802d92c/%5BMS-HCEP%5D.pdf

9.2 Informative References

[MS-NAP] Background information on Microsoft Network Access Protection is available at: http://technet.microsoft.com/en-us/network/bb545879.aspx

10. Author's Addresses

Brian Smithson
Ricoh Americas Corporation
10460 Bubb Road
Cupertino, CA 95014
Phone: 408-346-4435
FAX:
e-mail: brian.smithson@ricoh-usa.com

Ron Bergman
Ricoh Americas Corporation
2635 Park Center Drive
Simi Valley, CA 93065
Phone: 805-426-6542
FAX:
e-mail: Ron.Bergman@ricoh-usa.com

Jerry Thrasher
Lexmark International
740 New Circle Road
Lexington, KY 40550
Phone:
FAX:
e-mail: thrasher@lexmark.com

The authors would like to especially thank the following individuals who also contributed significantly to the development of this document:

The following individuals also contributed to the development of this document:

Nancy Chen	Okidata
Peter Cybuck	Sharp
Lee Farrell	Canon
Ira McDonald	High North
Joe Murdock	Sharp
Ron Nevo	Sharp
Glen Petrie	Epson
Kevin Sigl	Hewlett Packard
Bill Wagner	TIC
Dave Whitehead	Lexmark
Craig Whittle	Sharp
Peter Zehler	Xerox

11. Appendix X Document Revisions

This section is to be removed when this document is approved!

A. Changes to create the January 30, 2009 version

- Many formatting things to make sections autonumber, cross-references work, tables and lists be consistent, etc.
- Removed details that were already specified in [MS-SOH] and [HCD-ATR] and replaced with pointers to those documents.
- Changed three sections of HCD Attributes into a single table with some additional subsections where details were required.
- Made some language changes to distinguish between what this specification requires from what NAP protocol requires.
- Fixed up the References section for consistent presentation and added/corrected hyperlinks as needed.

B. Changes to create the December 3, 2008 version

- Some miscellaneous changes in the front matter to remove remnants of documents past (from WIMS, IPP, PMP, …)
- Broke "(Type = …)" off of the section headers and change format to normal.
- Incorporated changes from Joe Murdock in clauses 5 and 9.

C. Changes to create the October 23, 2008 version

Section 4.4, item C, entry 2: Added "A summary of this format is shown below:

- **SUB-TYPE FIELD** This is a 16 bit value containing a PWG assigned Sub-Type Code.
- **SUB-LENGTH FIELD** This is a 16 bit value that defined the length, in octets, of the following Sub-Type Value field.
- **SUB-TYPE VALUE FIELD** This field contains the value of the attribute. The length of this field is as specified by the Sub-Length field."

Section 4.5.1: Changed "NAME" to "MACHINE TYPE MODEL"

Changed "…defining the name of the hard copy device." To …"as defined by the HCD_Machine_Type_Model attribute. Reference: HCD_Machine_Type_Model in the PWG Hardcopy Device Health Assessment Attributes specification [HCD-ATR]."

Section 4.5.2: Removed, was "HCD MODEL SUB-TLV". Renumbered following sections.

Section 4.6.1: Added "All value are to be the binary representation of the defined parameter."

Section 4.6.4, item 2: Changed "4 octets" to "variable".

Section 4.6.12: Added "See the HCD_Certification_State attribute description in the PWG Hardcopy Device Health Assessment Attributes [HCD-ATR] for further information.

Section 6: Changed "NAME" to "MACHINE TYPE MODEL" Removed HCD Model entry.

D. Changes to create the October 8, 2008 version

Section 5 Changed: "Should this section include a discussion of the NAP protocols required or add a new section?."
To: "This section is to include a link to the discussion of the required NAP protocols."

Section 6 Changed "…to be used by IANA…" To: "…to be used by the Printer Working Group…"
Added: "contained in the following table. No IANA registrations are required for this document."

Section 7 Removed: " This document presents no internationalization considerations for HCD-NAP implementations. The NAP Statement Of Health protocol [MS-SOH] specification does not include a user interface and does not include any

provisions for internationalization.

Added: " For interoperability and basic support for multiple languages, conforming Printer implementations MUST support the UTF-8 [RFC3629] encoding of Unicode [UNICODE] [ISO10646]."

Section 8 Removed: " Add a section regarding Microsoft patents"

Added " Microsoft has patents that may cover protocols and procedures presented within this document. Microsoft has not granted to the Printer Working Group any licenses under these or any other Microsoft patents. It is strongly recommended that any entity implementing this specification, contact Microsoft at protocol@microsoft.com, regarding a patent license."

Section 9 Added Normative References [ISO10646], [RFC3629] and [UNICODE].

E. Changes to create the September 10, 2008 version.

Section 4.5.5 moved to 4.6.3 & renumbered both sections.

Section 4.5.5 (was 4.5.6) Removed "Update to new NEA format" Added " It is recommended that the HCD present only the port numbers, with their assigned protocol, that are currently allowed." Added "1. Reserved (7 bits) These bits MUST be zero on transmission and ignored upon receipt." Changed "Blocked Flag (1 byte)" to " Blocked Flag (1 bit)" Changed "byte" to "octet" in two places.

Section 4.5.6 (was 4.5.7) Changed "byte" to "bit" in two places. Added " Bits 8 through 32 are reserved and MUST be zero on transmission and ignored upon receipt."

Section 4.6.2 Changed SubType value to 23, was 6. Changed "HCD Firmware" to "HCD Firmware Version"

Section 4.6.3 (was 4.5.5) Added " This attribute MUST be included only if the Firmware Patches have been installed on the HCD Firmware."

Section 4.6.4 (was 4.6.3) Added " This attribute MUST be included for each Downloadable Application currently installed on the HCD."

Sections 4.6.5 (was 4.6.4) and 4.6.6 (was 4.6.5) Added ", for each Downloadable Application currently installed on the HCD"

Section 4.6.7 (was 4.6.6) Added " This attribute MUST be included for each Downloadable Application currently installed on the HCD containing one or more firmware patches."

Section 4.6.8 (was 4.6.7) Added " This attribute MUST be included for each Resident Application currently installed on the HCD."

Section 4.6.9 (was 4.6.8) Added " This attribute MUST be included for the Resident Application, if the HCD Resident Ap Version String SUB-TLV is not present, for each Resident Application currently installed on the HCD."

Section 4.6.10 (was 4.6.9) Added ", for each Resident Application currently installed on the HCD."

Section 4.6.11 (was 4.6.10) Added "This attribute MUST be included for each Resident Application currently installed on the HCD containing one or more firmware patches."

Section 4.6.13 (was 4.6.12) Added "[RFC868]", "[RFC4330]", and "[RFC1305]".

Section 4.6.14 (was 4.6.13) Added "[TLS-CIPHER]".

New "Section 6 IANA and PWG Considerations" Subsequent sections have been renumbered.

Section 9.1 Added references "[RFC868]", "[RFC1305]", "[RFC4330]", and

F. Changes to create the September 3, 2008 version.

Section 2.2 Other Terminology: Removed Applet definition.

Section 4.5: Added "All attributes in this section MUST be implemented by all hardcopy devices conformant to this specification.

Section 4.5: Moved the following paragraphs to section 4.6 (HCD Conditionally Mandatory Attributes)

HCD FIRMWARE VERSION SUB-TLV (now 4.6.1)
HCD DOWNLOADABLE AP NAME SUB-TLV (now 4.6.3)
HCD DOWNLOADABLE AP VERSION SUB-TLV (now 4.6.4)
HCD DOWNLOADABLE AP PATCHES SUB-TLV (now 4.6.6)
HCD RESIDENT AP NAME SUB-TLV (now 4.6.7)
HCD RESIDENT AP VERSION SUB-TLV (now 4.6.8)
HCD RESIDENT AP PATCHES SUB-TLV (now 4.6.10)
HCD CERTIFICATION STATE SUB-TLV (now 4.6.11)
HCD TIME SOURCE SUB-TLV (now 4.6.12)
HCD MIN CIPHER SUITE SUB-TLV (now 4.6.13)
HCD MIN CIPHER KEY LENGTH SUB-TLV (now 4.6.14)

Section 4.5: Moved paragraph 4.5.15 (HCD CONFIGURATION STATE SUB=TLV) to section 4.7 paragraph 4.7.1 (HCD Optional Attributes)

Added Paragraph 4.5.7 HCD CONFIGURATION FLAGS SUB-TLV

Section 4.6: Added the following new paragraphs:

4.6.2 HCD FIRMWARE VERSION STRING SUB-TLV
4.6.5 HCD DOWNLOADABLE AP VERSION STRING SUB-TLV
4.6.9 HCD RESIDENT AP VERSION STRING SUB-TLV

Section 4.6: Added to paragraphs 4.6.1, 4.6.2, 4.6.4, 4.6.5, 4.6.8, and 4.6.9 a sentence indicating this attribute MUST be included only if the corresponding version type was not present.

Section 4.6, paragraphs 4.6.3, 4.6.4, 4.6.5, 4.6.6, and 4.6.7, 4.6.8. 4.6.9, 4.6.10; added a correlation identifier field to each attribute to allow multiple entries.

