April 01, 2013
Candidate Standard 5110.2-2013

The Printer Working Group

PWG Hardcopy Device Health Assessment Network Access Protection Protocol Binding (HCD – NAP)

Status: Accepted

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 health assessment attributes created especially for HCDs, to allow access to such devices based upon the locally defined security policy.

This document is a PWG Candidate Standard. For a definition of a "PWG Candidate Standard", see:
ftp://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf

This document is available electronically at:
ftp://ftp.pwg.org/pub/pwg/candidates/cs-ids-nap10-20130401-5110.2.doc
ftp://ftp.pwg.org/pub/pwg/candidates/cs-ids-nap10-20130401-5110.2.pdf

April 01, 2013
Candidate Standard 5110.2-2013

The Printer Working Group

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 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 terminology used in this document that is not defined in the Terminology section of the PWG Hardcopy Device Health Assessments Attributes specification [HCD-ATR].

2.1 Conformance Terminology

Capitalized terms, such as MUST, MUST NOT, RECOMMENDED, REQUIRED, SHOULD, SHOULD NOT, MAY, and OPTIONAL, have special meaning relating to conformance as defined in Key words for use in RFCs to Indicate Requirement Levels [RFC2119].

The term CONDITIONALLY REQUIRED is additionally defined for a conformance requirement that applies to a particular capability or feature.

2.2 Other Terminology

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

NAP Client – A Hardcopy Device that uses the NAP protocols and process to request system health validation

Health Policy Server – A server or network-accessible service that provides health state validation for NAP

Health Registration Authority – A network-accessible proxy service that obtains health certificate from a certification authority for a NAP Client

Network Access Server – A network gateway device that controls access to network resources.

HRESULT – a signed 32-bit value used as error codes in Microsoft Operating systems. The high-order bit indicates success (0) or failure (1). For additional details, refer to [MS-GLOS] and to [MS-SOH] section heading "Compliance-Result-Codes".

Type-Length-Value (TLV) – a Microsoft data packet format consisting of control flags, a value type specification, a value length specification and a variable length value. Refer to section heading "Type-Length-Value (TLV) Packet" of [MS-SOH] for details.

NAP Agent – an application, service or process that aggregates Statement of Health information from System Health Agents and reports that information to a Health Policy Server.

2.3 Acronyms

CHAP – Challenge-Handshake Authentication Protocol

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

EAP – Extensible Access Protocol

HCD – Hardcopy Device

HCEP – Health Certificate Enrollment Protocol

HRA – Health Registration Authority

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

IANA – Internet Assigned Numbers Authority

IDS – Imaging Device Security

IETF – Internet Engineering Task Force

IP – Internet Protocol

IPSec – Internet Protocol Security

MAC – Media Access Control

NAP – Network Access Protection

NTP – Network Time Protocol

PC – Personal Computer

PEAP – Protected Extensible Access Protocol

PKCS – Public Key Cryptography Standard

PPP – Point-to-Point Protocol

PSTN – Public Switched Telephone Network

PWG – Printer Working Group

RADIUS – Remote Authentication Dial In User Service

RNAP – RADIUS Attributes for Network Access Protection

SCTP – Stream Control Transmission Protocol

SHA – System Health Agent

SHV – System Health Validator

SMI – Structure of Management Information

SoH – Statement of Health

SoHR – Statement of Health Response

SSoH – System Statement of Health

SSL – Secure Sockets Layer

TCP – Transport Control Protocol

TLS – Transport Layer Security

TLV – Type Length Value

UDP – User Datagram Protocol

URI – Universal Resource Indicator

USB – *Universal Serial Bus*

UTF – Unicode Transformation Format

VLAN – Virtual Local Area Network

WCCE – Windows Client Certificate Enrollment protocol

WSHA – Windows Security Health Agent

WSHV – Windows Security Health Validator

3. Requirements (Informative)

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 an HCD that can be defined that can be used to gauge a device'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 Protocol Overview

4.1 NAP Client Architecture

A general NAP Client consists of one or more System Health Agents (SHA), each of which is responsible for monitoring and reporting the status of a particular subsystem, such as firewall or anti-virus status. The SHAs report their respective sub-system status by generating a Statement of Health record containing the new status information.

In addition to the System Health Agents, an additional NAP Agent process or service is responsible for collecting all information from the SHAs and reporting overall system health to the Health Policy Server. The NAP Agent reports this information by collecting the current SoH records and aggregating them into a System Statement of Health (SSoH) record. Note that in a simple NAP Client implementation, a single SHA could function as both a SHA and a NAP Agent.

4.2 NAP Environment

Network Access Protection enabled network can operate in two distinct modes: Monitor Only and Restricted Access. In both modes, a NAP Client generates a System Statement of Health record (4.4.2) which will be validated by a NAP Security Health Validator. For further details, refer to [MS-SOH], [MS-NAPIntro], [MS-NAPArch].

In a Monitor Only mode, the NAP Client will always be allowed full access to the network, however, the client health state, as provided by the NAP Client SSoH information, will be monitored. Remediation information for any security issues may be provided.

In the Restricted Access mode, NAP Clients will always only be allowed access to a restricted portion of the network until their SSoH record has been validated and any security issues have been resolved. In this mode, further access to the secure network is generally allowed through the use of security certificates.

Since the Monitor Only mode does not provide any form of access control, the protocol discussions in the remainder of this section will be primarily concerned with the Restricted Access mode and the behavior of NAP Client requesting access to a restricted network.

4.3 Protocol Transport

The NAP Protocol specification does not define a transport protocol for NAP messages. All NAP messages MUST be carried in a separate transport protocol, such as DHCP or PEAP.

4.4 Message Syntax

4.4.1 Statement of Health (SoH)

The NAP protocol defines two core message types to transmit system health information: the Statement of Health (SoH) message sent by NAP SHAs to indicate the current state of their respective components, and

the Statement of Health Response (SoHR) returned by Health Policy Server to indicate if the NAP Client's current health state is acceptable.

The format of these messages is identical, consisting of a NAP header followed by a series of health attributes (SoHAttribute and SoHRAttribute) specified in a Type-Length-Value (TLV) format.
Message content is further organized into two ReportEntry sets of NAP attribute TLVs: the SoHReportEntry (NAP Client) and the SoHRReportEntry (Health Policy Server).

The SoHReportEntry contains SoHAttribute TLVs indicating the NAP Client's current status. It MAY contain zero or more additional SoHAttributes. A separate SoHReportEntry set will be generated by each System Health Agent resident on a NAP Client. Each ReportEntry set MUST contain a System-Health-ID TLV as the first attribute. The value of the System-Health-ID identifies the SHA that generated the ReportEntry.
The SoHRReportEntry contains SoHRAttribute TLVs that provide current information about the Health Policy Server and the results of processing the SoHAttributes. The SoHRReportEntry MUST contain at least one SoHRAttribute in addition to the required System-Health-ID TLV. The value of the System-Health-ID identifies the SHV that generated the ReportEntry.

4.4.2 System Statement of Health (SSoH)

The System Statement of Health record is an aggregate collection of the SoH records reported from various System Health Agents resident on a NAP Client. The format of the SSoH header consists of a 46 octet NAP header followed by a System Statement of Health (SSoH) header containing a System-Health-Id TLV of 0x00013700. This SSoH header is then followed by the aggregated SoHReportEntries.

4.5 Common NAP Protocols

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

4.5.1 System Statement of Health for NAP Protocol

Microsoft Network Access Protection requires that a NAP Client be able to generate and transmit a System Statement of Health (SSoH) message and receive and process a System Statement of health Response, as specified in [MS-SOH]. The specific transport mechanism used to carry the SSoH message is dependent on which of the multiple network access methods supported by NAP is being used (see section 4.6).

4.5.2 Security Health Agent Protocol

The current Microsoft Statement of Health for NAP Protocol requires that a NAP System Health Agent generate Statement of Health Report Entries (SoHReportEntries) that conform to the format and required value set as specified in [MS-WSH].

The System Health Agent must also 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 Entries are not currently defined.

4.6 Microsoft Supported NAP Access Protocols

The protocol discussion below describes the behavior of various network components and NAP protocols as they would behave in a the NAP Restricted Access operating mode

4.6.1 DHCP

With IPv4 DHCP NAP enforcement, the DHCP server will initially place a NAP Client within a restricted network which provides access to a Health Validator. Support for IPv6 DHCP is not currently provided by NAP.

Network access is controlled through the use of DHCP Subnet mask (255.255.255.255) and gateway (0.0.0.0) settings. A limited set of network routing paths to DNS and remediation servers will be provided to the NAP Client using the Classless Static Routes DHCP option [RFC3442].

Once allowed access to the restricted network, a NAP Client can then generate a SoH and request validation via the DHCP server. If the validation is successful, the NAP Client will be provided with a new DHCP address allowing access to the secure network. If validation fails, the client can be directed to one or more remediation servers where security issues may be resolved, and the validation process is repeated.

The Health Policy validation process is repeated whenever a NAP Client attempts to lease or renew an IP address configuration. If the validation fails, the client will be placed on the restricted network until the remediation process has occurred.

4.6.1.1 Dynamic Host Configuration Protocol Extensions

NAP DHCP clients must provide and recognize the DHCP extensions defined in [MS-DHCPN]. Microsoft DHCP servers support the following DHCP options for NAP clients:

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"
121		Classless Static Routes [RFC 3442]

4.6.2 IEEE 802.1X

NAP clients requesting network access via IEEE 802.1X [IEEE802.1X] port authentication protocols acquire network access by establishing an authenticated connection to the restricted network from an IEEE 802.1X access point. The initial network access is limited by the IEEE 802.1X access point to only allow access to restricted network resources and remediation servers. This limited access will be controlled by the IEEE 802.1X access point using either IP packet filtering or a restricted VLAN ID.

Using the Extensible Authentication Protocol (EAP) pass-through mode of the IEEE 802.1X access point, the NAP client can now establish a Protected Extensible Authentication Protocol (PEAP) connection to the NAP Health Policy Server and requests SoH validation.

4.6.2.1 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 [RADIUS] and IEEE 802.1X [IEEE802.1X] may be used.

4.6.3 Remote Access VPN

NAP clients attempting access via a VPN tunnel can acquire network access by first establishing an authenticated connection to the VPN Server using EAP to provide user authentication information. The VPN server will restrict client access to the network through a set of IP packet filters.

The NAP Client can then establish a PEAP connection to the NAP Health Policy Server, using the Extensible Authentication Protocol (EAP) pass-through mode of VPN Server, allowing the SoH validation process to proceed.

4.6.3.1 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 IEEE 802.1X network is required to be conformant to these extensions.

4.6.4 IPsec

IPSec–based NAP provides 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. Currently available IPsec policy settings can also be applied to individual computers and users to control client access.

To obtain secure IPsec access, the NAP Client uses the Health Certificate Enrollment Protocol (HCEP) to send the SoH to a Health Registration Authority (HRA). The HRA will, on behalf of the NAP client, validate the SoH with the NAP Health Policy Server, returning a valid Health Certificate upon success. In a NAP IPsec environment, a valid Health Certificate can be used for IPsec authentication, providing access to the secure network.

4.6.4.1 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 expected to already be assigned an 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.509 certificates using Public Key Cryptography Standards (PKCS) Message #10 and receive certificate PKCS Message #7 [X509].

4.7 SoH Revalidation

A NAP Client MUST regenerate the SoH and request revalidation of the health certificate if pertinent health attributes change. The behavior and results of SoH revalidation are dependent on the NAP Access protocol used (see section 4.6).

4.7.1 DHCP

If a DHCP SoH revalidation fails, the client will be assigned a new DHCP address, will no longer be granted access to the secure network, and SHOULD enter whatever remediation process is appropriate and available.

4.7.2 IEEE 802.1X

If SoH revalidation fails within an IEEE 802.1X connection, the NAP Client will be limited by the IEEE 802.1X access point to the restricted network profile. The NAP Client SHOULD perform any required remediation actions that are available.

4.7.3 VPN

If SoH revalidation fails within a VPN connection, the VPN server will use IP packet filtering to limit network access to the NAP client. The NAP Client SHOULD perform any required remediation actions that are available.

4.7.4 IPsec

If SoH revalidation fails within an IPsec connection, the NAP Client Health Certificate will be revoked and the HCD will have limited access to a restricted network. From within the restricted network, the client SHOULD attempt remediation.

5. Statement Of Health for NAP Protocol

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

5.1 Statement of Health Attribute Encoding for NAP Protocol

5.1.1 Mandatory Attributes

The attributes specified in this section MUST always be included in the SoH attribute set for HCDs.

5.1.1.1 NAP System-Health-ID Packet

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].

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 2 (0x0002)**														**Length = 4 (0x0004)**															
IANA SMI Vendor Code (for PWG) = 2699 (0x0000A8B)																								**Component ID**							

Component ID: This 8 bit field identifies the component type, qualified by the Vendor Code. The following values are defined for HCDs. Values are additive (for example, printer + scanner + copier = 7):

Value	Meaning
1	Printer device
2	Scanner device
4	Copier device
8	Fax device
16, 32, 6, 128	Reserved and MUST be set to 0 on transmission and ignored on receipt

For additional information, refer to [MS-SOH] section heading “System-Health-ID Packet”.

5.1.1.2 NAP Compliance-Results-Codes TLV

This variable length attribute contains an array of SoH Result Codes indicating the compliance of the Hard Copy Device.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 4 (0x0004)**														**Length**															
Value (variable)																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **Value** field.

Value (variable): an array of HRESULT values that indicate the results of evaluation by the server.

For additional information, refer to [MS-GLOS] and to [MS-SOH] section heading “Compliance-Result-Codes”.

5.1.1.3 NAP Failure Category TLV

This fixed length attribute classifies the type of failure that has occurred. A SoHR message MUST contain this TLV, a Compliance-Result-Codes TLV, or both. This attribute MAY be present in a SoH message. This attribute does not have an equivalent definition in the current HCD Attribute Specification [HCD-ATR].

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 14 (0x0E)**														**Length=1**															
Value																															

Value (1 byte): An 8 bit field that MUST contain one of the following values:

Value	Meaning
0	No failure occurred
1	Failure that is not due to components or communications of the client or server
2	Failure due to client component
3	Failure due to client communication
4	Failure due to server component
5	Failure due to server communication

For additional information, refer to [MS-SOH] section heading “Failure Category”.

5.1.1.4 Forwarding Enabled TLV

This Boolean attribute indicates whether the device is configured to forward data between interfaces.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length**															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 22 (0x0016)																**Inner Length = 1**															
ForwardingEnabled																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **MachineTypeModel** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **MachineTypeModel** field.

ForwardingEnabled (2 bytes): a Boolean value represented in two bytes as follows:

00	Not enabled
01	Enabled

For additional information, refer to **ForwardingEnabled** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.5 Default Password Enabled TLV

This Boolean attribute indicates whether any password or security credentials on the device are set to the factory default value.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length**															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 20 (0x0014)																**Inner Length = 1**															
DefaultPasswordEnabled																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **MachineTypeModel** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **MachineTypeModel** field.

DefaultPasswordEnabled (2 bytes): a Boolean value represented in two bytes as follows:

00	Not enabled
01	Enabled

For additional information, refer to **DefaultPasswordEnabled** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.6 PSTN Fax Enabled TLV

This Boolean attribute indicates whether the FAX interface is enabled.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length**															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 40 (0x0028)																**Inner Length = 1**															
PSTNFaxEnabled																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **MachineTypeModel** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **MachineTypeModel** field.

PSTNFaxEnabled (2 bytes): a Boolean value represented in two bytes as follows:

00	Not enabled

01	Enabled

For additional information, refer to **PSTNFaxEnabled** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.7 Firewall Setting TLV

A variable length field indicating the state (open/closed) of each IP protocol port on the device. To reduce the amount of data that must be transmitted, only information on open ports should be transmitted. If a port is not listed in the Firewall Setting TLV, it is assumed to be blocked.

<table>
<tr><th>00</th><th>01</th><th>02</th><th>03</th><th>04</th><th>05</th><th>06</th><th>07</th><th>08</th><th>09</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="2">0 0</td><td colspan="14">TLV Type = 7 (0x0007)</td><td colspan="16">Length</td></tr>
<tr><td colspan="32">IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)</td></tr>
<tr><td colspan="16">TLV Subtype = 21 (0x0015)</td><td colspan="16">Inner Length</td></tr>
<tr><td colspan="8">Reserved</td><td>B</td><td colspan="7">Protocol</td><td colspan="16">Port Number</td></tr>
<tr><td colspan="32">…</td></tr>
</table>

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **FirewallSetting** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **FirewallSetting** field.

FirewallSetting (variable):

Reserved: reserved for future use, MUST be on transmission and ignored on receipt.

B: a single bit field indicates if this port is blocked or allowed; it MUST be set to 1 if the protocol and port combination is blocked; otherwise it MUST be set to 0.Since the IDS NAP binding only lists open ports, this value will always be 0.

Protocol: an 8-bit unsigned integer that MUST specify the protocol number being blocked or allowed. The values used in this field are the same ones used in the IPv4 Protocol and IPv6 Next Header fields. Protocol identifier values must be defined in the [IANA] protocol registry.

Port Number: a 16-bit unsigned integer that MUST specify the port number being blocked or allowed. The values used in this field are specific to the protocol identified by the Protocol field. [IANA] maintains registries for TCP, UDP and SCTP port numbers.

For additional information, refer to **FirewallSetting** in [HCD-ATR], clause 4.2.6 in [RFC5792], and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.8 Machine Type Model TLV

This variable length attribute indicates the particular machine type and model of the device.

<table>
<tr><th>00</th><th>01</th><th>02</th><th>03</th><th>04</th><th>05</th><th>06</th><th>07</th><th>08</th><th>09</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="2">0 0</td><td colspan="14">TLV Type = 7 (0x0007)</td><td colspan="16">Length</td></tr>
<tr><td colspan="32">IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)</td></tr>
<tr><td colspan="16">TLV Subtype = 2 (0x0002)</td><td colspan="16">Inner Length</td></tr>
</table>

MachineTypeModel
…

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **MachineTypeModel** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **MachineTypeModel** field.

MachineTypeModel (variable): a null terminated UTF-8 string providing the machine type and model of the Hard Copy Device

For additional information, refer to **MachineTypeModel** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.9 Vendor Name TLV

This variable length attribute indicates the name of the manufacturer of the imaging device.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 3 (0x0003)																Inner Length															
VendorName																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **VendorName** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **VendorName** field.

VendorName (variable): a null terminated UTF-8 string providing the name of the manufacturer of the HCD

For additional information, refer to **VendorName** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.10 Vendor SMI Code TLV

This fixed length attribute indicates the name of the manufacturer of the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length = 11 (0x000B)															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 4 (0x0004)																Inner Length = 3 (0x0003)															
VendorSMICode																															

VendorSMICode (3 bytes): a 24 bit unsigned integer that contains a globally unique SMI Network Management Private Enterprise Code of the vendor, as defined by IANA. Note that NAP packet format specifications required limiting the Vendor SMI code to three octets.

For additional information, refer to **VendorSMICode** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.11 Firmware Name TLV

This variable length attribute identifies the firmware loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length**															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 60 (0x003C)																**Inner Length**															
FirmwareName																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **FirmwareName** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **FirmwareName** field.

FirmwareName (variable): a null terminated UTF-8 string that uniquely identifies the firmware loaded in the HCD

For additional information, refer to **FirmwareName** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.12 Firmware Version TLV

This fixed length attribute identifies the current version of firmware loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length=24 (0x0018)**															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 63 (0x003F)																**Inner Length=16 (0x0010)**															
Major Version Number																															
Minor Version Number																															
Build Number																															
Major Service Pack Number																**Minor Service Pack Number**															

FirmwareVersion (16 bytes): a vendor-specific 128-bit field that uniquely identifies the firmware version. This attribute follows the format for the Numeric Version specified in clause 4.2.3 of [RFC5792]. It is composed of a Major Version Number, Minor Version Number, Build Number, Major Service Pack Number, and Minor Service Pack Number. For the NAP protocol binding, all FirmwareVersions will specify a Major and Minor Service Pack version of zero.

For additional information, refer to **FirmwareVersion** in [HCD-ATR], clause 4.2.3 in [RFC5792], and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.13 Firmware String Version TLV

This variable length attribute identifies the current version of firmware loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 62 (0x003E)																Inner Length															
FirmwareStringVersion																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **FirmwareStringVersion** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **FirmwareStringVersion** field.

FirmwareStringVersion (variable): a null terminated UTF-8 string that uniquely identifies the current version of firmware loaded in the HCD

For additional information, refer to **FirmwareStringVersion** in [HCD-ATR] and section heading “Vendor-Specific Packet” in [MS-SOH].

5.1.1.14 Firmware Patches TLV

This variable length attribute identifies the patch(es) that have been applied to the firmware loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 61 (0x003D)																Inner Length															
FirmwarePatches																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **FirmwarePatches** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **FirmwarePatches** field.

FirmwarePatches (variable): a null terminated UTF-8 string that uniquely identifies the patch(es) that have been applied to the firmware loaded in the HCD. All patches must be listed in the order in which they were applied, beginning with the first patch applied and ending with the last patch applied.

For additional information, refer to **FirmwarePatches** in [HCD-ATR] and section heading “Vendor-Specific Packet” in [MS-SOH].

5.1.1.15 Attributes Natural Language TLV

This variable length attribute specifies the local language used by all localized string attributes in this SoH.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length=24 (0x0018)															
IANA SMI Vendor Code (for PWG) = 2699 (0xA8B)																															
TLV Subtype = 1 (0x0001)																Inner Length=16 (0x0010)															
Language_ID																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **Language_ID** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the Languaged_ID field.

Language_ID: a variable length string containing the language code that indicates the local language used for the localized HCD string attributes within this SOH. The values are specified as defined in [RFC5646].

5.1.1.16 Time Source TLV

This variable length attribute identifies the source of time settings that is being used by the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 23 (0x0017)																Inner Length															
TimeSource																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **TimeSource** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **TimeSource** field.

TimeSource (variable): a null terminated UTF-8 string that uniquely identifies the source of time settings that is being used by the HCD. Note: a value of “onboard” MAY be used for a resident real-time clock; a URI MAY be used for network time servers [RFC868][RFC1305].

For additional information, refer to **TimeSource** in [HCD-ATR] and section heading “Vendor-Specific Packet” in [MS-SOH].

5.1.1.17 User Application Enabled TLV

This Boolean attribute indicates whether the device is configured to allow the execution of User Applications.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 104 (0x0068)																Inner Length = 1															
UserApplicationEnabled																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **MachineTypeModel** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **MachineTypeModel** field.

UserApplicationEnabled (2 bytes): a Boolean value represented in two bytes as follows:

00	Not enabled
01	Enabled

For additional information, refer to **UserApplicationEnabled** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.1.18 User Application Persistence Enabled TLV

This Boolean attribute indicates whether the device is configured to allow User Applications to remain available in the system after use.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length**															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 105 (0x0069)																**Inner Length = 1**															
UserApplicationPersistenceEnabled																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **MachineTypeModel** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **MachineTypeModel** field.

UserApplicationPersistenceEnabled (2 bytes): a Boolean value represented in two bytes as follows:

00	Not enabled
01	Enabled

For additional information, refer to **UserApplicationPersistenceEnabled** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.2 Conditionally Mandatory Attributes

The attributes specified in this section MUST be included in the SoH attribute set for an HCD if the particular capability, as described before each attribute, is implemented on the HCD.

5.1.2.1 User Application Name TLV

This variable length attribute uniquely identifies the name of a User Application that has been loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 100 (0x0064)																Inner Length															
Correlation_ID																															
UserApplicationName																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, **Correlation_ID,** and **UserApplicationName** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **Correlation_ID** and **UserApplicationName** fields.

Correlation_ID: a unique identifying ID for this User Application. This value is used to link related application attributes.

UserApplicationName (variable): a null terminated UTF-8 string that uniquely identifies a User Application that has been loaded in the HCD

For additional information, refer to **UserApplicationName** in [HCD-ATR] and section heading “Vendor-Specific Packet” in [MS-SOH].

5.1.2.2 User Application Version TLV

This fixed length attribute identifies the current version of a User Application that has been loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length=28 (0x001C)															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 103 (0x0067)																Inner Length=20 (0x0014)															
Correlation_ID																															
Major Version Number																															
Minor Version Number																															
Build Number																															
Major Service Pack Number																Minor Service Pack Number															

Correlation_ID: the correlation identification value from the UserApplicationName attribute for this application.

UserApplicationVersion (16 bytes): a vendor-specific 128-bit field that uniquely identifies the User Application version. This attribute follows the format for the Numeric Version specified in clause 4.2.3 of [RFC5792]. It is composed of a Major Version Number, Minor Version Number, Build Number, Major Service Pack Number, and Minor Service Pack Number. For the NAP protocol binding, all **UserApplicationVersions** will specify a Major and Minor Service Pack version of zero.

For additional information, refer to **UserApplicationVersion** in [HCD-ATR], clause 4.2.3 in [RFC5792], and section heading “Vendor-Specific Packet” in [MS-SOH].

5.1.2.3 User Application String Version TLV

This variable length attribute identifies the current version of a User Application that has been loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 102 (0x0066)																Inner Length															
Correlation_ID																															
UserApplicationStringVersion																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, **Correlation_ID,** and **UserApplicationStringVersion** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **Correlation_ID** and **UserApplicationStringVersion** fields.

Correlation_ID: the correlation identification value from the UserApplicationName attribute for this application.

UserApplicationStringVersion (variable): a null terminated UTF-8 string that uniquely identifies the current version of the User Application.

For additional information, refer to **UserApplicationStringVersion** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.2.4 User Application Patches TLV

This variable length attribute identifies the patch(es) that have been applied to a User Application that has been loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 101 (0x0065)																Inner Length															
Correlation_ID																															
UserApplicationPatches																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, **Correlation_ID,** and **UserApplicationPatches** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **Correlation_ID** and **UserApplicationPatches** fields.

Correlation_ID: the correlation identification value from the UserApplicationName attribute for this application.

UserApplicationPatches (variable): a null terminated UTF-8 string that uniquely identifies the patch(es) that have been applied to the User Application. All patches must be listed in the order in which they were applied, beginning with the first patch applied and ending with the last patch applied.

For additional information, refer to **UserApplicationPatches** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.2.5 Resident Application Name TLV

This variable length attribute uniquely identifies the name of a Resident Application that has been loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length**															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 80 (0x0050)																**Inner Length**															
Correlation_ID																															
ResidentApplicationName																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, **Correlation_ID,** and **ResidentApplicationName** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **Correlation_ID** and **ResidentApplicationName** fields.

Correlation_ID: a unique identifying ID for this Resident Application. This value is used to link related application attributes.

ResidentApplicationName (variable): a null terminated UTF-8 string that uniquely identifies the Resident Application that has been loaded in the HCD

For additional information, refer to **ResidentApplicationName** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.2.6 Resident Application Version TLV

This fixed length attribute uniquely identifies the current Resident Application version that has been loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length=24 (0x0018)**															
IANA SMI Vendor Code (for PWG) = 2699 (0xA8B)																															
TLV Subtype = 83 (0x0053)																**Inner Length=16 (0x0010)**															
Correlation_ID																															
Major Version Number																															
Minor Version Number																															
Build Number																															
Major Service Pack Number																**Minor Service Pack Number**															

Correlation_ID: the correlation identification value from the ResidentApplicationName attribute for this application.

ResidentApplicationVersion (16 bytes): a vendor-specific 128-bit field that uniquely identifies the Resident Application version. This attribute follows the format for the Numeric Version specified in clause 4.2.3 of [RFC5792]. It is composed of a Major Version Number, Minor Version Number, Build Number, Major Service Pack Number, and Minor Service Pack Number. For the NAP protocol binding, all ResidentApplicationVersions will specify a Major and Minor Service Pack version of zero.

For additional information, refer to **ResidentApplicationVersion** in [HCD-ATR], clause 4.2.3 in [RFC5792], and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.2.7 Resident Application String Version TLV

This variable length attribute identifies the current version of Resident Application that has been loaded in the HCD.

<table>
<tr><th>00</th><th>01</th><th>02</th><th>03</th><th>04</th><th>05</th><th>06</th><th>07</th><th>08</th><th>09</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td>0</td><td colspan="14">TLV Type = 7 (0x0007)</td><td colspan="16">Length</td></tr>
<tr><td colspan="32">IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)</td></tr>
<tr><td colspan="16">TLV Subtype = 82 (0x0052)</td><td colspan="16">Inner Length</td></tr>
<tr><td colspan="32">Correlation_ID</td></tr>
<tr><td colspan="32">ResidentApplicationStringVersion</td></tr>
<tr><td colspan="32">…</td></tr>
</table>

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, **Correlation_ID,** and **ResidentApplicationStringVersion** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **Correlation_ID** and **ResidentApplicationStringVersion** fields.

Correlation_ID: the correlation identification value from the ResidentApplicationName attribute for this application.

ResidentApplicationStringVersion (variable): a null terminated UTF-8 string that uniquely identifies the current version of Resident Application that has been loaded in the HCD

For additional information, refer to **ResidentApplicationStringVersion** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.2.8 Resident Application Patches TLV

This variable length attribute identifies the patch(es) that have been applied to a User Application that has been loaded in the HCD.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 81 (0x0051)																Inner Length															
Correlation_ID																															
ResidentApplicationPatches																															
…																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, **Correlation_ID,** and **UserApplicationPatches** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **Correlation_ID** and **ResidentApplicationPatches** fields.

Correlation_ID: the correlation identification value from the ResidentApplicationName attribute for this application.

ResidentApplicationPatches (variable): a null terminated UTF-8 string that uniquely identifies the patch(es) that have been applied to the Resident Application. All patches must be listed in the order in which they were applied, beginning with the first patch applied and ending with the last patch applied.

For additional information, refer to **ResidentApplicationPatches** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.3 Optional Attributes

The attributes specified in this section MAY be included in the SoH attribute set for HCDs.

5.1.3.1 Configuration State TLV

This variable length attribute is a vendor-specific field that uniquely identifies the state of any configuration settings that are included in the creation of the attribute.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	TLV Type = 7 (0x0007)														Length															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 200 (0x00C8)																Inner Length															
ConfigurationState…																															
ConfigurationState																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **ConfigurationState** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **ConfigurationState** field.

ConfigurationState (variable): a null terminated UTF-8 string that uniquely identifies the state of any configuration settings in the HCD that are included in the creation of the attribute.

For additional information, refer to **ConfigurationState** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

5.1.3.2 Certification State TLV

This variable length attribute is a vendor-specific field that uniquely identifies the state of a particular set of configuration settings that are included as part of a certification process.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	**TLV Type = 7 (0x0007)**														**Length**															
IANA SMI Vendor Code (for PWG) = 2699 (0x00000A8B)																															
TLV Subtype = 201 (0x000C9)																**Inner Length**															
CertificationState…																															
CertificationState																															

Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **IANA SMI Vendor Code, TLV Subtype**, **Inner Length**, and **CertificationState** fields.

Inner Length (2 bytes): a 16-bit unsigned integer that MUST specify the length, in bytes, of the **CertificationState** field.

CertificationState (variable): a null terminated UTF-8 string that uniquely identifies the state of a particular set of configuration settings in the HCD that are included as part of a certification process.

For additional information, refer to **CertificationState** in [HCD-ATR] and section heading "Vendor-Specific Packet" in [MS-SOH].

6. Conformance

This section describes the conformance requirements for an implementation of a NAP client. If covers conformance requirements for Statement of Health Attributes, Statement of Health processing and NAP protocol requirements.

6.1 SoH Attribute Conformance

A conforming implementation MUST support all mandatory PWG HCD Statement of Health attributes as defined in Section 5.1.1 of this document. A conforming implementation MUST also support all applicable conditionally mandatory attributes as defined in Section 5.1.2 of this document.

6.2 Microsoft SoH Attribute Conformance

The Microsoft NAP specification requires that a conforming implementation must provide the following required Microsoft NAP attributes in an SSoH packet (refer to [MS-SOH] for attributes details):

MS-Machine-Inventory	
MS-Quarantine-State	
MS-Packet-Info	
MS-MachineName	The value of this should be mapped to the hostname or NetBIOS name. If defined, the NetBIOS name SHOULD be used.
MS-CorrelationId	
MS-Machine-Inventory-Ex	For the NAP binding, the value of this should be set to 0x03 (server).
NAPSystemHealthID	*For a Statement of Health containing the PWG NAP SoH attributes, this must be set to the value 0x0000A8B*

6.3 Microsoft SSoH Conformance

A conforming implementation MUST conform to the System Statement of Health requirements as defined in [MS-SOH]. NAP implementations MUST support version 2 SSoH headers as defined in [MS-SOH] section heading “SoH Mode Subheader”.

6.4 NAP Protocol Conformance

A conforming implementation MUST meet the NAP protocol requirements defined in [MS-SOH] section heading “Protocol Details”.

A conforming imaging device must support at least one of the NAP Access protocols described in 4.6.

6.5 SoH Revalidation

When critical NAP attribute values have changed, a conforming NAP Client MUST consider itself as no longer being compliant with SoH. The conforming NAP Client MUST generate an updated Statement of Health and repeat the validation process.

PWG HCD NAP attributes that require immediate revalidation are:

Configuration Flags
Configuration State
Certification State
Default Password Enabled
Firewall Setting
Firmware Name
Firmware Version
Firmware String Version
Firmware Patches
Forwarding Enabled
PSTN Fax Enabled
Resident Application Name
Resident Application Version
Resident Application String Version
Resident Application Patches
Time Source
User Application Enabled
User Application Persistence Enabled

PWG HCD NAP attributes that require revalidation at the earliest opportunity are:

User Application Name
User Application Version
User Application String Version
User Application Patches

7. 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 defined in “PWG Hardcopy Device Health Assessment Attributes” [HCD-ATR]. No IANA registrations are required for this document.

8. Internationalization Considerations

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

9. Security Considerations

The Statement of Health for NAP protocol [MS-SOH] specification, section heading “Security”, 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 heading “Security” 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.

10. References

Note about references to Microsoft documents [MS-*]: The references provided below identify the version or date of the document that was used, but the URI to obtain the document will likely refer to an updated version. Microsoft does not provide durable URIs for referring to specific versions or dates of these documents.

10.1 Normative References

[HCD-ATR] Thrasher, J., Murdock, J. “PWG Hardcopy Device Health Assessment Attributes”, Stable Draft. Current document available at ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-current.pdf

[IEEE802.1X] “IEEE Std. 802.1X-2010, IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control”, IEEE, 2010, available at http://standards.ieee.org/getieee802/

[ISO10646] ISO, "Information technology -- Universal Coded Character Set (UCS)", ISO/IEC 10646:2012, 2012, http://www.iso.org/iso/home/store/catalogue_ics.htm.

[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.

[RFC2616] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.”, IETF, June 1999, available at http://www.ietf.org/rfc/rfc2616.txt

[RFC2818] E. Rescorla, “HTTP Over TLS”, IEF, May 2000, available at http://www.ietf.org/rfc/rfc2818.txt

[RFC3442] T. Lemion, S. Cheshire, B. Volz, "The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4" (RFC 3442), IETF, November 2003, available at http://www.ietf.org/rfc/rfc3442.txt

[STD63] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 3629/STD 63, November 2003, http://www.ietf.org/rfc/rfc3629.txt

[RFC5792] P. Sangster, K. Narayan “PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)” (RFC 5792), IETF, March 2010, available at http://www.ietf.org/rfc/rfc5792.txt.

[RFC5646] A.Philips, M. Davis “Tags for Identifying Language” (RFC 5646), IETF, September 2009, available at http://w ww.ietf.org/rfc/rfc5646.txt.

[UNICODE] Unicode Consortium, "Unicode Standard", Version 6.2.0, 2012, http://www.unicode.org/versions/Unicode6.2.0/

[MS-GLOS] Windows Protocols Master Glossary, v20090630, June 2009, Microsoft Corporation, available at http://msdn.microsoft.com/en-us/library/cc232129.aspx

[MS-SOH] Statement of Health Protocol for Network Access Protection (NAP) Protocol Specification, v20090116, January 2009, Microsoft Corporation, available at http://msdn.microsoft.com/en-us/library/cc246924.aspx

[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-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

[X509] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280 May 2008

[IANA] The Internet Assigned Numbers Authority. http://www.iana.org

[RADIUS] Remote Authentication Dial In User Service, RFC 2865 June 2000, RFC 3580 September 2003

10.2 Informative References

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

[MS-NAPArch] Network Access Protection Platform Architecture, Microsoft Corporation, February 2008, available at http://download.microsoft.com/download/3/9/f/39ff0ca3-56d1-4d93-af46-98f92134d040/NAPArch.doc

[MS-NAPIntro] Introduction to Network Access Protection, Microsoft Corporation, February 2008, available at http://technet.microsoft.com/en-us/network/cc984252.aspx

11. Authors Addresses

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

Joe Murdock
Sharp Labs of America
5750 NW Pacific Rim Blvd.
Camas, WA 98607
Phone:
FAX:
e-mail: jmurdock@sharplabs.com

Ron Bergman
e-mail: RGBergman@hotmail.com

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

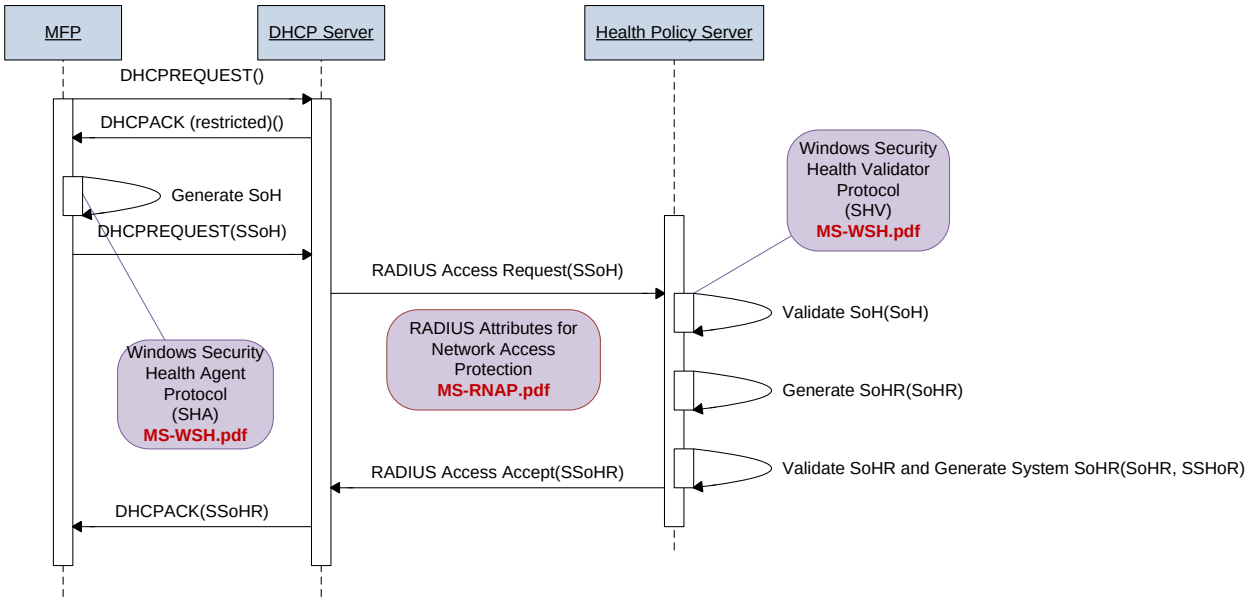
The authors would like to especially thank the following individuals who also contributed significantly to the development of this document:

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

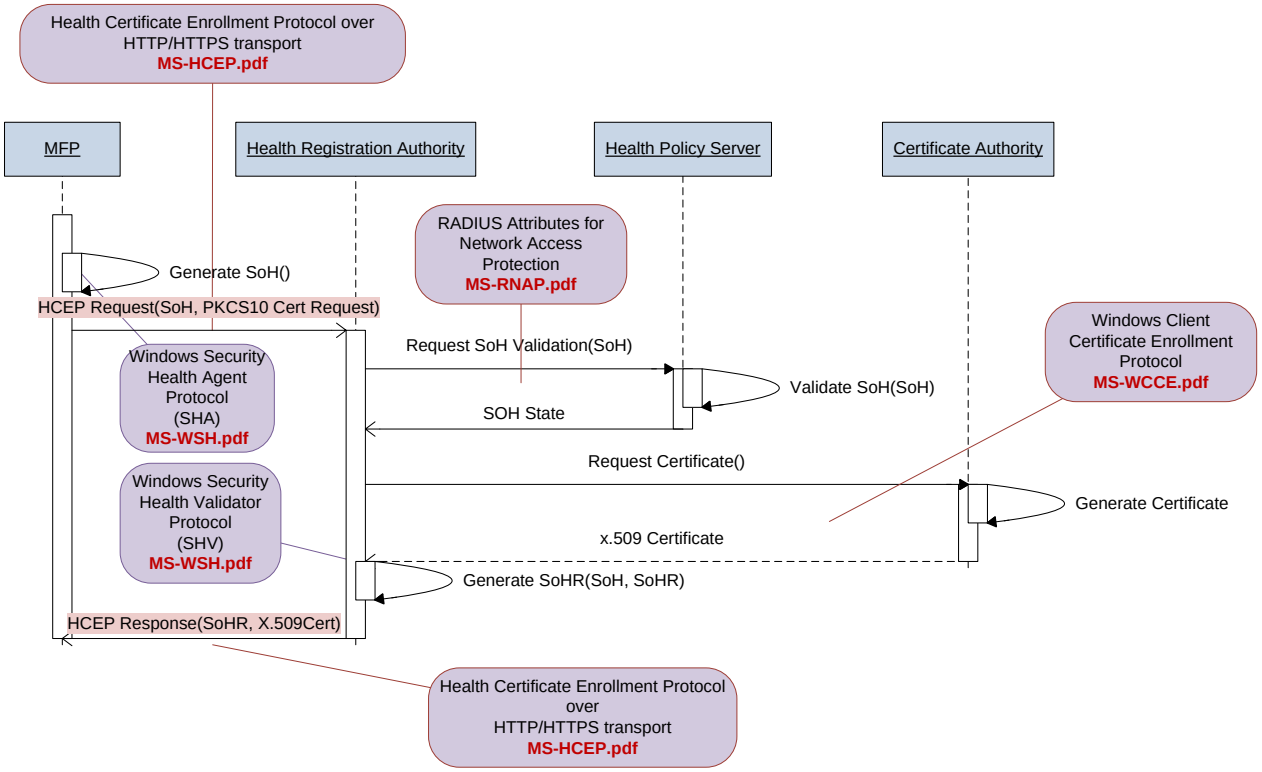
Nancy Chen	
Peter Cybuck	
Lee Farrell	
Ira McDonald	High North
Ron Nevo	Samsung
Glen Petrie	Epson
Kevin Sigl	Hewlett Packard
Bill Wagner	TIC
Dave Whitehead	Independent consultant
Craig Whittle	Sharp
Peter Zehler	Xerox
Alan Sukert	Xerox

12. Appendix A NAP Sequence Diagrams

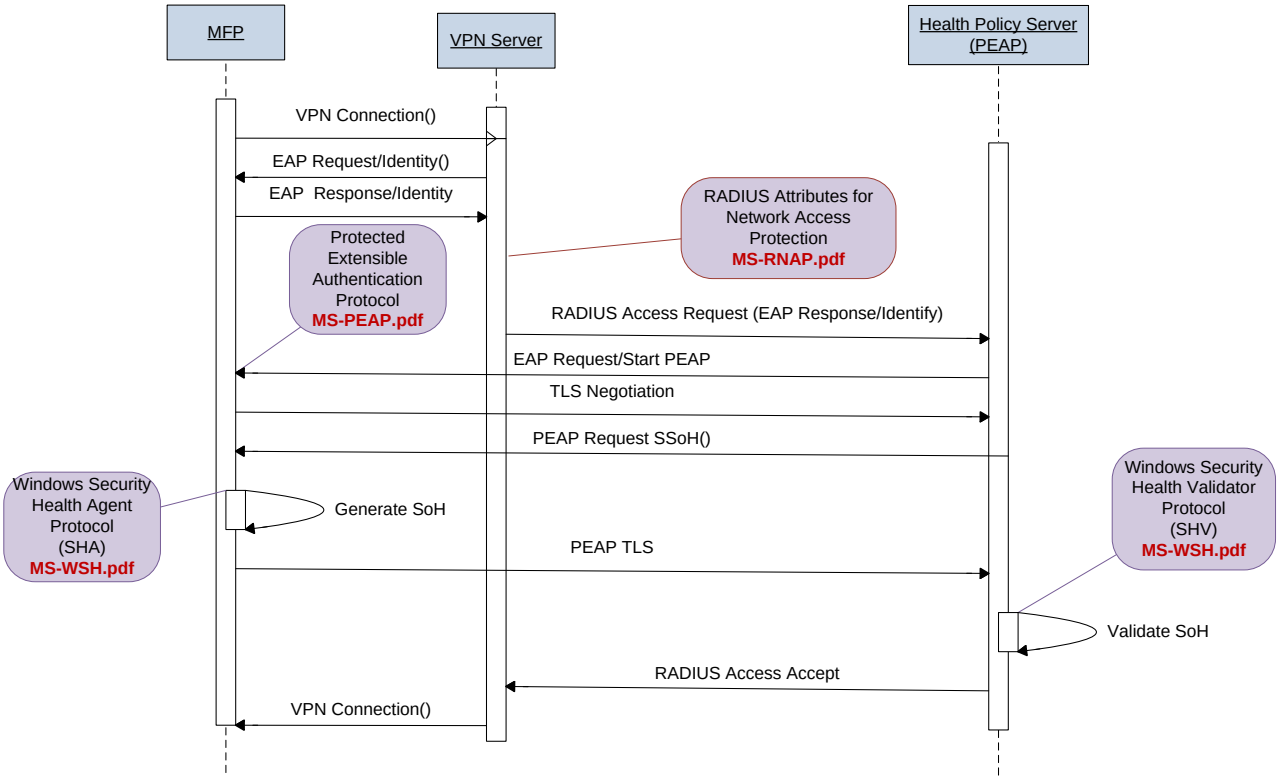
12.1 DHCP Access Sequence (DHCP Extensions)



12.2 IPsec Security Certificate Acquisition Access Sequence (HCEP)



12.3 VPN Security Certificate Acquisition Sequence (HCEP)



12.4 IEEE 802.1X Access Sequence (EAP)

To support IEEE 802.1X network access, the client is expected to negotiate an authenticated IEEE 802.1X connection with the authenticating switch or Access Point. For NAP validations, the switch or Access Point operates in a pass through mode for EAP.