August 17, 2009
Working Draft

The Printer Working Group

The Printer Working Group (PWG)
Hardcopy Device Health Assessment
Network Endpoint Assessment Protocol Binding
(HCD – NEA)

Status: Interim Draft v3

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 IETF Network Endpoint Assessment (NEA) 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-nea03-20090817.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

Introduction

This document is a guide for implementers of the IETF NEA protocol suite when faced with a requirement for supporting an NEA client embedded within a hardcopy peripheral device. Additionally, this document specifically addresses the scenario where the implementer is required to be compliant with the Printer Working Group (PWG) standard set of health attributes [INCLUDE REFERENCE].

The PWG has authored a set of health attributes, and corresponding data types, that are tailored for assessing "hardcopy-specific" aspects of a device's security posture.

Likewise, the IETF NEA working group has adopted a "standard" set of health attributes and corresponding data types that are appropriate for standard "desktop" computing devices.

This document provides guidance to implementers of the NEA protocol suite when the PWG has defined attributes that are not a part of the standard NEA attribute set. Also, this document clarifies how PWG standard attributes are supported when the PWG attributes intersect with corresponding NEA standard attributes.

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. HCD Statement Of Health for NEA Protocol

This section defines how the specified Hardcopy Device Health Assessment Attributes [HCD-ATR] are to be used with the IETF Network Endpoint Assessment (NEA) attribute protocol [NEA-PA].

4.1 Transport

NEA attributes are carried in messages described in [NEA-PA]. [NEA-PA] messages are subsequently transported in the [NEA-PB] "Posture Broker" protocol, as described in section 3 of [NEA-PA]. For quick reference the protocol layering is illustrated below:

PB-TNC Header
PB-TNC Message of type PB-PA-Message (includes: PA Message Vendor ID, PA subtype, and other fields used by Posture Broker Client and Posture Broker Server for routing)
PA-TNC Message Header
PA-TNC Attribute (e.g., Product Information)
PA-TNC Attribute (e.g., Operational Status)

Figure 1 Overview of a PB-TNC batch that contains a PA-TNC Message

There is another protocol layer (PT) that is referenced by [NEA-PB]; the PT layer is treated as an "abstract" transport layer by the NEA working drafts. The abstract PT layer carries PB messages that subsequently carry PA messages (attributes).

Some concrete implementations of the abstract PT layer include 802.1x/EAP and DHCPv4, and potentially DHCPv6. [NEA-PB] is designed to run over both half-duplex and full-duplex PTs.

4.2 Message Syntax

The "Posture Broker" [NEA-PB] protocol carries Posture Attributes [NEA-PA] between a Posture Broker entity running on a Server and a Posture Broker running on a device under assessment. Another look at the protocol layering is illustrated in Figure 2.

PT Protocol
PB-TNC Header
One or more PA-TNC Messages

Figure 2 Example of PB-TNC message encapsulation

The PT protocol transports PB-TNC Messages, and each PB-TNC Message carries one or more PA-TNC messages. Within the context of this document, the PT protocol is an "abstract" protocol placeholder, while the PB-TNC and PA-TNC messages represent concrete protocol specifications.

The PB-TNC message encapsulates one or more PA-TNC messages, and it's the PA-TNC messages that carry the actual attribute information to which this document pertains. The PB-PA message format is illustrated in the following diagram, followed by the PA-TNC message format.

<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="8">Flags</td><td colspan="24">PA Message Vendor ID = 0x0 (IETF standard PA subtype)</td></tr>
<tr><td colspan="32">PA Subtype = 1 (Operating System)</td></tr>
<tr><td colspan="16">Posture Collector Identifier</td><td colspan="16">Posture Validator Identifier</td></tr>
<tr><td colspan="32">PA Message Body (Variable Length)</td></tr>
</table>

Figure 3 PB-PA message encapsulation

The PB-PA Message format illustrated above is defined in the IETF NEA PB-TNC specification [NEA-PB], section 4.5. All PWG standard attribute messages defined in this document use the same values for "PA Message Vendor ID" and "PA Subtype" fields as assigned above.

ISSUE: Currently, the PWG IDS group has chosen NOT to create PWG-specific PA subtypes for hardcopy devices. Therefore, there is only one posture collector on an HCD that responds to attribute requests. Which leads to a decision about WHICH NEA standard PA-subtype to use to represent this single PA-subtype. Two PA-subtypes were considered, “NEA Client” and “Operating System”. The “NEA Client” PA subtype seemed a little too narrowly focused as a target for all PWG attribute requests. Instead, I chose to temporarily “overload” the “Operating System” PA subtype, choosing to re-define this PA subtype to “System” in the case of hardcopy devices. My overall opinion is that we SHOULD define PWG-specific PA subtypes and target attribute requests to the appropriate collector within an HCD. There are a number of hardcopy device architecures currently shipping in the marketplace that are multifunction devices, with each “function” implemented on a different CPU and memory space in the device (separate computing device). With a single PA-subtype, there is no way to “address” these other functional computing devices within the multifunction product, yet these devices also have “product names”, “operating system versions”, etc. At the most recent face-to-face IDS meeting (8/18/2009), the consensus was still to NOT create PWG-specific PA subtypes. I think we should reconsider this decision as there are too many scenarios in hardcopy device architectures that would not be addressed by our current direction.

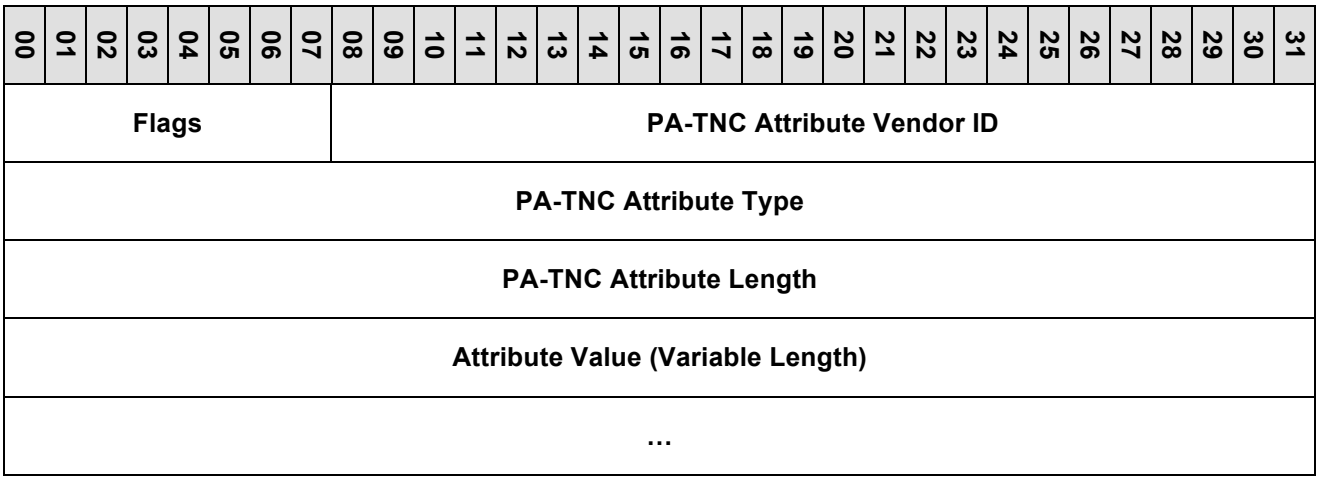


Figure 4 PA-TNC Attribute Descriptor

Implementations of this specification must set the “PA-TNC Attribute Vendor ID” field to the IANA SMI Private Enterprise value associated with the PWG (0xA8B). In the following sections describing attributes, the PA-TNC Attribute Descriptor illustrated in Figure 4 will be used to specify the encoding of each PWG attribute type.

4.3 PWG Attribute Type Definitions – IANA Considerations

This document defines new PWG-specific PA-TNC Attribute Types to be used by PWG-compliant Posture Collectors and Posture Validators in the presence of HCD assessment. These Attribute Types and their corresponding values will be registered with IANA on final publication of this document.

Code	Attribute Type
1	HCD_Machine_Type_Model
2	HCD_Firmware_Name
3	HCD_Vendor_Name
4	HCD_Vendor_SMI_Code

5	HCD_Firmware_Version
6	HCD_Firmware_Patches
7	HCD_User_Application_Name
8	HCD_User_Application_Version
9	HCD_User_Application_Patches
10	HCD_Resident_Application_Name
11	HCD_Resident_Application_Version
12	HCD_Resident_Application_Patches
13	HCD_Firewall_Setting
14	HCD_Certification_State
15	HCD_Configuration_State
16	HCD_Forwarding_Enabled
17	HCD_PSTN_Fax_Enabled
18	HCD_Default_Password_Enabled
19	HCD_Time_Source
20	HCD_Firmware_String_Version
21	HCD_User_Application_String_Version
22	HCD_Resident_Application_String_Version
23	HCD_Configuration_Flags

4.4 HCD Statement of Health Attribute Encoding for NEA PA-TNC Protocol

In the following sub-sections, an example PA-TNC message encoding will be illustrated for both mandatory and optional PWG attribute types. In each case where the specific PWG attribute intersects with an existing NEA attribute definition, a reference to the appropriate NEA specification will be included.

4.4.1 Mandatory Attributes

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

4.4.1.1 HCD_Default_Password_Enabled

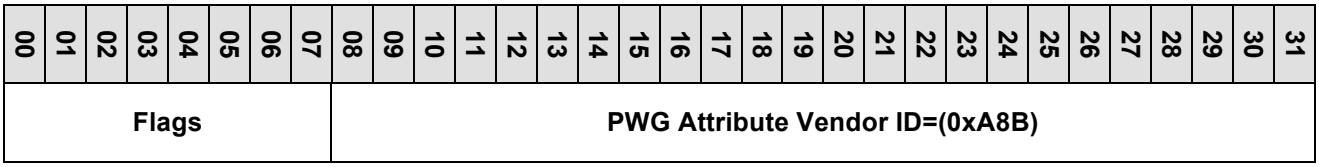
This document contains no PWG-specific encoding of this attribute. Instead, see section 4.2.12 of the IETF NEA PA-TNC [NEA-PA] specification describing the NEA attribute “Factory Default Password”.

4.4.1.2 HCD_Firewall_Setting

This document contains no PWG-specific encoding of this attribute. Instead, see section 4.2.6 of the IETF NEA PA-TNC [NEA-PA] specification describing the NEA attribute “Port Filter”.

4.4.1.3 HCD_Firmware_Name

The HCD_Firmware_Name attribute is a variable length string that specifies the name attributed to the firmware that is contained in the HCD.



PWG Attribute Type = (0x2)
PWG Attribute Length=(12 + Length of HCD Firmware Name String)
HCD Firmware Name String (UTF-8 encoded)
…

4.4.1.4 HCD_Firmware_Patches

TBD

4.4.1.5 HCD_Firmware_String_Version

TBD

4.4.1.6 HCD_Firmware_Version

TBD

4.4.1.7 HCD_Forwarding_Enabled

This document specifies no PWG-specific encoding of this attribute. Instead, see section 4.2.11 of [NEA-PA] describing the NEA attribute “Forwarding Enabled”.

4.4.1.8 HCD_Machine_Type_Model

The HCD_Machine_Type_Model attribute is a variable length string that indicates the particular machine type and model of the 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
Flags								PWG Attribute Vendor ID=(0xA8B)																							
PWG Attribute Type = (0x1)																															
PWG Attribute Length=(12 + Length of Machine_Type_Model String)																															

HCD_Machine_Type_Model String (UTF-8 encoded)
…

4.4.1.9 HCD_User_Application_Enabled

See section 4.4.1.13

4.4.1.10 HCD_User_Application_Persistence_Enabled

See section 4.4.1.13

4.4.1.11 HCD_Vendor_Name

The manufacturer or vendor name of the HCD being assessed. The attribute value is a variable length string encoded in UTF-8.

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
Flags								PWG Attribute Vendor ID=(0xA8B)																							
PWG Attribute Type = (0x3)																															
PWG Attribute Length=(12 + Length of HCD_Vendor_Name String)																															
HCD_Vendor_Name String (UTF-8 encoded)																															
…																															

4.4.1.12 HCD_Vendor_SMI_Code

This attribute value represents the device manufacturer's private IANA enterprise number.

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
Flags								PWG Attribute Vendor ID=(0xA8B)																							
PWG Attribute Type = (0x04)																															

PWG Attribute Length= (0x10)	
0	HCD Vendor SMI Value

The HCD Vendor SMI Value is a 24-bit number, assigned by IANA, to an individual organization. If a particular device vendor does not have an assigned SMI Value, then this field will be set to 0.

4.4.1.13 HCD_Configuration_Flags

This attribute is a composite (or compound) attribute that is a bitmask containing the value of 2 other mandatory attributes and 1 conditionally mandatory attribute

- HCD_User_Application_Enabled
- HCD_User_Application_Persistence_Enabled
- HCD_PSTN_Fax_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
Flags								PWG Attribute Vendor ID=(0xA8B)																							
PWG Attribute Type = (0x17)																															
PWG Attribute Length= (0x10)																															
0																													X	X	X

Bit 31 = 1 = HCD_User_Application_Enabled
Bit 30 = 1 = HCD_User_Application_Persistence_Enabled
Bit 29 = 1 = HCD_PSTN_Fax_Enabled

Since HCD_PSTN_Fax_Enabled is a conditionally mandatory attribute, products that do not have this capability will always set this bit to 0.

4.4.2 Conditionally Mandatory Attributes

HCDs MUST support the attributes in this section if the particular capability, as described before each attribute, is implemented on the HCD.

4.4.2.1 Downloadable Application Attributes

The following attributes MUST be supported if the HCD supports user-downloadable applications.

4.4.2.1.1 HCD_User_Application_Name

Sdfsdfjf

4.4.2.1.2 HCD_User_Application_Patches

Sldkfjsdf

4.4.2.1.3 HCD_User_Application_String_Version

Sdlkfjsdf

4.4.2.1.4 HCD_User_Application_Version

Sldkjsdf

4.4.2.2 Resident Application Attributes

The following attributes MUST be supported if the HCD supports the addition of resident applications to the HCD's operating software.

4.4.2.2.1 HCD_Resident_Application_Name

TBD

4.4.2.2.2 HCD_Resident_Application_Patches

TBD

4.4.2.2.3 HCD_Resident_Application_String_Version

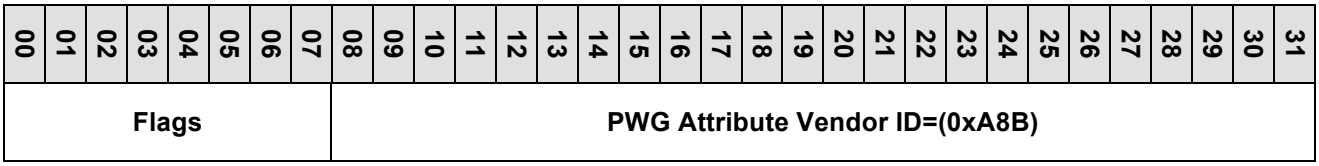
TBD

4.4.2.2.4 HCD_Resident_Application_Version

TBD

4.4.2.3 HCD_Time_Source

The HCD_Time_Source attribute is a variable length string that indicates where the device acquires its time setting. Regardless of the time source, the HCD shall provide administrative protection for its internal time. Examples of this attribute include: ("onboard" for a resident RTC or a Hostname or URL string for a network time source)



PWG Attribute Type = (0x13)
PWG Attribute Length = (12 + length of HCD_Time_Source string)
HCD Time Source String
…

ISSUE: The HCD Time Source String can be a string "onboard", a hostname, or URL string. There is an overall requirement that "string data type" attributes be encoded in UTF-8. When the HCD Time Source String is encoded as an ASCII "onboard" value, then this value is UTF-8. However, to generally REQUIRE that hostnames and URL strings be encoded in UTF-8, we may be causing temporary interoperability problems. Support for internationalized URLs and DNS Hostnames is nascent in the internet community, and requires upgrading the DNS infrastructure, as well as browsers and other internet client software that translates domain names to IP addresses. Some of this transition has already begun but the vast majority of software (including the latest browsers) still do not support internationalized domain names and/or URLs. I have inquiries into the IETF IDNABIS working group regarding how we might approach this issue. For now, I have chosen to NOT require that the HCD Time Source String be UTF-8 encoded, even though the ASCII encoding fits nicely into UTF-8.

4.4.3 Optional Attributes

Support for the following attributes is OPTIONAL for an HCD.

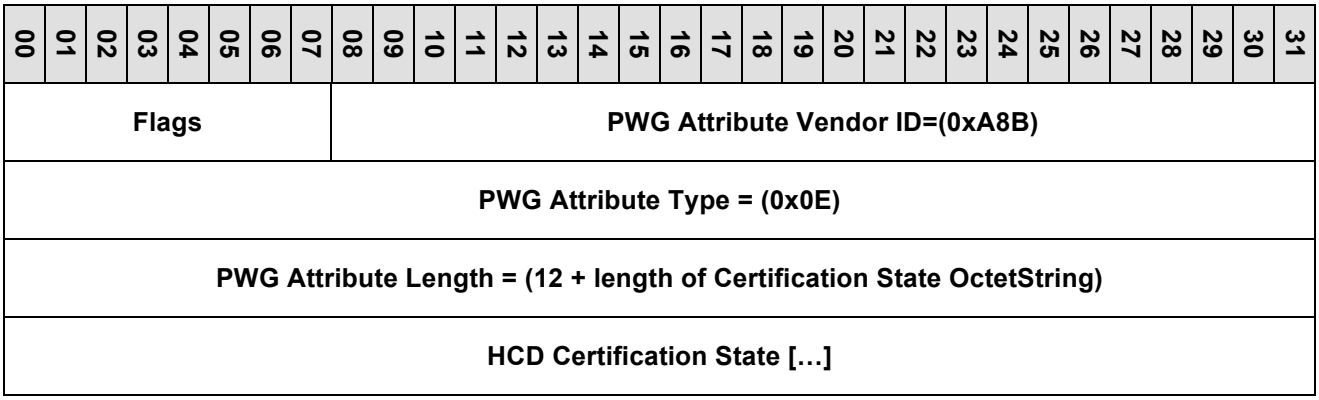
4.4.3.1 HCD_Configuration_State

The HCD_Configuration_State attribute is an administratively configured, vendor-specific variable length field that uniquely identifies the state of any configuration settings in the HCD that are included in 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
Flags								PWG Attribute Vendor ID=(0xA8B)																							
PWG Attribute Type = (0x0F)																															
PWG Attribute Length = (12 + length of Configuration State OctetString)																															
HCD Configuration State […]																															

4.4.3.2 HCD_Certification_State

The HCD_Certification_State attribute is a vendor-specific variable length field that uniquely identifies the state of a particular set of configuration settings in the HCD that are included as part of a certification process (e.g., Common Criteria certification).



5. Conformance

[HCD-ATR] defines a subset of attributes as “mandatory to implement” for implementations that are required to be conforming with [HCD-ATR]. Additionally, this specification requires that IETF NEA implementations conforming to the [HCD-ATR] as well as this specification are required to set the “NOSKIP” flag (bit 0) [NEA-PA]in all attribute messages that contain “mandatory to implement” attributes.

The NOSKIP flag in attribute messages indicates that if an implementation does not understand the attribute being requested, that the entire request be aborted, and an error code returned to a posture collector. Conforming implementations must implement the mandatory attributes and therefore “understand” these attributes and know how to handle them correctly.

TBD – To include initial consensus on PT protocol recommendations from the IETF NEA Working Group

6. Internationalization Considerations

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

7. Security Considerations

[NEA-PA] section 5, provides a detailed discussion of security issues relative to the NEA attribute protocol referenced herein. Since this specification defines a set of attributes to be used by [NEA-PA], readers of this document are encouraged to read [NEA-PA] section 5 for an understanding of security issues related to the transport of the attributes discussed in this specification.

Additional security considerations can be found within the NEA “Posture Broker” protocol [NEA-PB].

8. References

8.1 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/

[NEA-PA] IETF Network Endpoint Assessment Attribute Protocol draft is available at: http://www.ietf.org/html.charters/nea-charter.html

[NEA-PB] IETF Network Endpoint Assessment Posture Broker Protocol draft is available at: http://www.ietf.org/html.charters/nea-charter.html

8.2 Informative References

TBD

9. Author's Addresses

Randy Turner
Amalfi Systems, LLC
10001 Venice Blvd. Suite 204
Los Angeles, CA 90034

Phone: 323-828-9207

e-mail: rturner@amalfisystems.com

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

Dave Whitehead - Lexmark

10. Appendix X Document Revisions

10.1 Version 1

Created basic IEEE/PWG Document template and proposed outline, including basic NEA PA and PB protocol headers.

10.2 Version 2

Replaced IETF-style ASCII protocol header specifications with IEEE/PWG-style MS-Word document formats.

10.3 Version 3

10.3.1 Rewritten Introductory Section

Rewrote introductory section to include specific goals of this mapping document

10.3.2 IANA Considerations

Included IANA registrations for PWG-specific attribute types

10.3.3 Protocol Mappings

Introduced initial set of protocol mappings to the document, including all PWG-specific attributes EXCEPT any resident or user application mappings.

10.3.4 Conformance

Added initial conformance section noting requirements for “NOSKIP” flags when PWG-mandatory attributes are specified.

