The Printer Working Group

4 December 2015
Candidate Standard 5110.4-2015

Hardcopy Device Health Assessment Trusted Network Connect Binding (HCD-TNC)

Status: Approved

Abstract: This document defines a concrete protocol binding over TCG TNC / IETF NEA (technically equivalent) of the abstract PWG Hardcopy Device Health Assessment Attributes (PWG5110.1) for initial network endpoint health assessment (at time of network attachment) and periodic network endpoint health assessment (at runtime) of Imaging Devices.

This document is a PWG Candidate Standard. For a definition of a "PWG Candidate Standard", see:

http://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf

This document is available electronically at:

http://ftp.pwg.org/pub/pwg/candidates/cs-idstnc10-20151204-5110.4.docx
http://ftp.pwg.org/pub/pwg/candidates/cs-idstnc10-20151204-5110.4.pdf

Title: Hardcopy Device Health Assessment Trusted Network Connect Binding (HCD-TNC)

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

About the Imaging Device Security Working Group

The goal of the Imaging Device Security Working Group is to provide the metrics and mechanisms that allow Imaging Devices to fully participate in assessment-protected networks and provide secure, controlled access to Jobs, Documents, and Imaging Services.

For additional information regarding IDS visit:

http://www.pwg.org/ids

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

List of Tables

List of Figures

1. Introduction

This document defines a concrete protocol binding over TCG TNC / IETF NEA (technically equivalent) of the abstract PWG Hardcopy Device Health Assessment Attributes [PWG5110.1] for initial network endpoint health assessment (at time of network attachment) and periodic network endpoint health assessment (at runtime) of Imaging Devices.

1.1 Rationale for HCD-Specific TNC PA Subtypes

TNC Posture Attribute (PA) subtypes are used to distinguish major components of network endpoints to allow dispatch of the appropriate TNC Integrity Measurement Validator (IMV) to process a given TNC posture attribute received from a network endpoint. IETF PA-TNC [RFC5792] assigns standard PA subtypes under the IETF SMI arc to identify generic major components that are common to most network endpoints. To support the dispatch of an appropriate HCD-specific IMV, this document assigns HCD-specific PA subtypes (see sections 9 and 9.1) and mandates their use for standard HCD-specific posture attributes (see sections 5, 5.1, 5.2, and 5.3).

2. Terminology

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 Imaging and Security Terminology

Normative definitions and semantics of printing terms are imported from the Printer MIB v2 [RFC3805], Printer Finishings MIB [RFC3806], and Internet Printing Protocol/1.1: Model and Semantics [RFC2911].

In addition, the following terms are imported or generalized from [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 (e.g., 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.

Correlated Attributes: An ordered set of related attributes that describe an instance of firmware or software. The purpose of these Correlated Attributes is to allow ease-of-access and verification for each code instance.

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

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]

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]

Network Administrator: A user who manages the network configuration of the HCD. [IEEE2600]

Resident Application: Resident applications are those applications that are downloaded via an offline administrative or maintenance update procedure and persist after a power cycle of the HCD. These types of applications augment the normal operation of the HCD and provide additional functions that are available to all users of the HCD.

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

User Application: User applications are applications that are downloaded and executed as part of normal operation of the HCD and may be dynamically installed and executed by users. These applications do not include applications that are added via an offline administrative or maintenance update procedure. Examples of these types of applications include Java or Flash applications. User applications may or may not persist after a power cycle of the HCD.

2.3 TCG TNC Terminology

Normative definitions and semantics of health assessment terms are imported from section 11 “TNC Glossary” of TCG Trusted Network Connect Architecture for Interoperability [TNC-ARCH]:

Access Requestor (AR): An entity that is seeking connectivity to a network or access to a network resource (i.e., service, data, etc.).

Endpoint Integrity Information: The set of information provided by Integrity Measurement Collectors (IMCs) that describes the status and configuration of the Access Requestor (AR).

Integrity Information: The set of platform specific information that makes up a Trusted Platform. This ranges from information about a platform's hardware components, TPM information (e.g. versions), PCRs, peripherals, Trusted Building Blocks, OS/Kernel, drivers, Applications, Anti-Virus information and others. Each specific use-case determines which information set will be of interest. As such, it is expected that for a given situation these will be pre-determined or pre-configured by an authorized entity (e.g. IT administrator).

Integrity Measurement Collector (IMC): The component of an Access Requestor (AR) that measures certain aspects of the AR's integrity, including software versions, patches, Anti-Virus and others.

Integrity Measurement Verifier (IMV): The component of a Policy Decision Point (PDP) that verifies a particular aspect of the AR's integrity, based on measurements received from Integrity Measurement Collectors (IMCs) and/or other data. Note that multiple IMVs may reside on a single PDP.

Isolation: The action of separating an Access Requestor (AR) onto a separate network – virtual or physical – possibly, though not necessarily, for the purposes of performing Remediation on that AR.

Platform Authentication: The action of verifying both the proof-of-identity and integrity-status of a given platform.

Policy Decision Point (PDP): The component in the TCG TNC Architecture that evaluates the status of a TNC Client (seeking network connectivity) and decides upon some network-related action to be enforced by the Policy Enforcement Point (PEP). The PDP embodies the security and integrity related policies governing the network.

Policy Enforcement Point (PEP): The component in the TCG TNC Architecture that controls access to a protected network, whose policies are implemented through a Policy Decision Point (PDP). The PEP enforces the decisions of the PDP.

TNC Client (TNCC): The component of an Access Requestor (AR) that aggregates integrity measurements from Integrity Measurement Collectors (IMCs), assists in the management of the Integrity Check Handshakes, and assists in the measurement and reporting of platform and IMC integrity.

TNC Server (TNCS): The component on a Policy Decision Point (PDP) that manages the flow of messages between Integrity Measurement Collectors (IMCs) and Integrity Measurement Verifiers (IMVs), gathers recommendations from IMVs, and combines those recommendations (based on policy) into an overall TNCS Action Recommendation.

2.4 Acronyms and Organizations

HCD: Hardcopy Device [IEEE2600] and PWG term for Printer or Multifunction Device

IANA: Internet Assigned Numbers Authority, http://www.iana.org/

IEEE: Institute of Electrical and Electronics Engineers, http://www.ieee.org/

IETF: Internet Engineering Task Force, http://www.ietf.org/

IMC: TNC Integrity Measurement Collector (see section 2.3)

IMV: TNC Integrity Measurement Verifier (see section 2.3)

ISO: International Organization for Standardization, http://www.iso.org/

NEA: IETF Network Endpoint Assessment WG, http://datatracker.ietf.org/wg/nea/charter/

PDP: TNC Policy Decision Point (see section 2.3)

PEP: TNC Policy Enforcement Point (see section 2.3)

PWG: IEEE-ISTO Printer Working Group, http://www.pwg.org/

TCG: Trusted Computing Group, http://trustedcomputinggroup.org/

TNC: TCG Trusted Network Communications WG (formerly Trusted Network Connect), http://www.trustedcomputinggroup.org/developers/trusted_network_communications

3. Requirements

3.1 Rationale for HCD-TNC

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

3.2 Use Cases for HCD-TNC

This HCD-TNC specification imports all of the use cases for health assessment that are defined in section 3.2 of [PWG5110.1].

3.3 Out of Scope for HCD-TNC

The following elements of the use cases defined in section 3.2 of [PWG5110.1] and imported above are out of scope for design requirements for this HCD-TNC specification:

1) Specific protocols for accessing network time sources (e.g., NTP).
2) Specific protocols for accessing stored X.509 certificates (e.g., LDAP).
3) Specific protocols for accessing network name services (e.g., DNS).
4) Specific protocols for accessing network security policy services (e.g., RADIUS).
5) Specific protocols for accessing network directory services (e.g., LDAP)
6) Specific protocols for accessing network authentication services (e.g., Kerberos).

3.4 Design Requirements for HCD-TNC

This HCD-TNC specification should:

1) Define conformance profiles that are consistent with [PWG5110.1].
2) Follow the naming conventions used in [PWG5110.1].
3) Define conformance requirements for both PT-EAP [RFC7171] (layer 2) and PT-TLS [RFC6876] (layer 4) transport protocol bindings.
4) Define well-known delimiters for multi-valued attributes such as FirmwarePatches, specifically CR/LF pairs.
5) Define conformance requirements for both initial network endpoint health assessments via [RFC7171] and subsequent, potentially more extensive, network endpoint health assessments via [RFC6876].
6) Support the use of vendor extension attributes.

4. TNC Protocol Overview

4.1 TCG TNC Architecture

The TCG TNC Architecture [TNC-ARCH] is intentionally general, in order to accommodate a wide variety of network devices, topologies and implementation configurations – it includes multiple roles, functions, and interfaces.

Note: The TCG TNC Architecture is a strict superset of the technically equivalent IETF TNC Architecture – which itself encompasses all the interfaces and protocols that are relevant to this PWG specification. Throughout this PWG specification, the shorter and more meaningful IETF NEA acronyms (e.g., PA-TNC) are used for specific TNC protocol layers for readability.

4.2 IETF PT-EAP – TNC Layer 2 Transport Protocol

IETF PT-EAP [RFC7171] defines a Posture Transport protocol that is identical on-the-wire to TCG TNC IF-T: Protocol Bindings for Tunneled EAP Methods [TNC-IFT-EAP]. PT-EAP is especially useful for initial attachement endpoint assessment *before* an IP address is assigned (i.e., the endpoint is joining the network).

4.2.1 IETF PT-EAP Message Format

The following PT-EAP message format diagram is excerpted from section 3.3 of IETF PT-EAP [RFC7171]. Since PT-EAP is an EAP method, the first four fields (e.g. Code, Identifier, Length and Type as shown in Figure 1) in each message are mandated by and defined in EAP. The other fields, e.g. Flags, Version and Data are specific to PT-EAP.

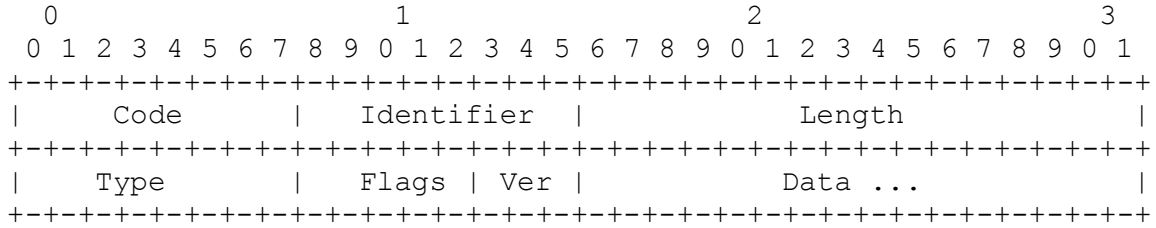

Figure 1 – IETF PT-EAP Message Format

Code (8 bits): Value of this field specifies the type of the PT-EAP message. Value MUST be Request(1) or Response(2).

Identifier (8 bits): Value of this field aids in matching Request(1) messages with corresponding Response(2) messages.

Length (16 bits): Value of this field specifies the length of the PT-EAP message, starting from the Code field.

Type (8 bits): Value of this field specifies the EAP Method Type [RFC3748] assignment for PT-EAP (to be assigned by IANA).

Flags (5 bits): Value this field specifies the PT-EAP flags. Bit 0 is the Start flag and MUST be set to 1 for the first message from the PT-EAP Server. If the Start flag is set, then the PT-EAP message MUST NOT contain Data. All other bits are reserved and MUST be set to 0 for [RFC7171] conformance.

Version (3 bits): Value of this field is used for version negotiation. Value MUST be set to 1 for [RFC7171] conformance. Version 0 is reserved and MUST never be sent. New versions of PT-EAP (values 2-7) may be defined by Standards Action, as defined in [RFC5226].

Data (variable length): Value of this field specifies the data to be processed by the PB-TNC layer [RFC5793].

4.3 IETF PT-TLS – TNC Layer 4 Transport Protocol

IETF PT-TLS [RFC6876] defines a Posture Transport protocol that is identical on-the-wire to TCG TNC IF-T: Binding to TLS [TNC-IFT-TLS]. PT-TLS is especially useful for periodic monitoring endpoint assessment *after* an IP address is assigned (i.e., the endpoint is already attached to the network.

4.3.1 IETF PT-TLS Message Format

The following PT-TLS message format diagram is excerpted from section 3.5 of IETF PT-TLS [RFC6876]:

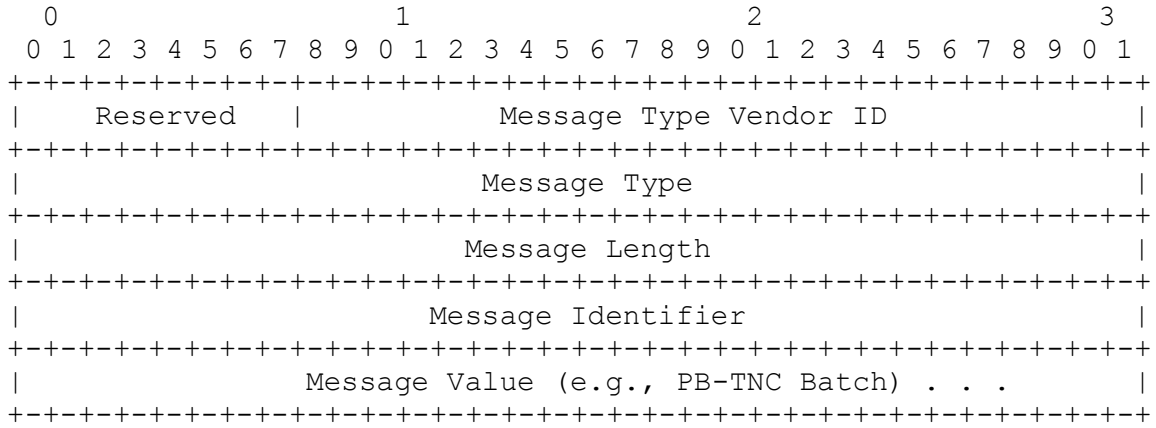

Figure 2 – IETF PT-TLS Message Format

Reserved (8 bits): Value MUST be 0 for IETF PT-TLS [RFC6876] conformance.

Message Type Vendor ID (24 bits): Value MUST be 24-bit SMI Private Enterprise Number of the party who owns this Attribute Type namespace. Value MUST be 0 for IETF

namespace, 0x5597 (21911) for TCG namespace, or 0x0A8B (2699) for PWG namespace. Value of 0xffffff is reserved and MUST not be used.

Message Type (32 bits): Value MUST be an IETF, TCG, or PWG standard message type. Value of 0xffffffff is reserved and MUST not be used. IETF standard PT-TLS message types are defined in section 3.6 of [RFC6876] and registered with IANA.

Message Length (32 bits): Value is the length of the PT-TLS Message contained in the Message Value field.

Message Identifier (32 bits): Value of this field contains a value that uniquely identifies the PT-TLS message on a per message sender (Posture Transport Client or Server) basis. Value MUST be a monotonically increasing counter starting at zero indicating the number of the messages the sender has transmitted over the TLS session.

Message Value (variable length): Value specifies the contents of the PT-TLS Message, e.g., PB-TNC Batch (7).

4.3.2 IETF PT-TLS Message Types

The standard IETF message types defined in section 3.6 of IETF PT-TLS [RFC6876] include: Experimental(0), Version Request(1), Version Response(2), SASL Mechanisms(3), SASL Mechanism Selection(4), SASL Authentication Data(5), SASL Result(6), PB-TNC Batch(7), and PT-TLS Error(8).

4.4 IETF PB-TNC – TNC Posture Broker Protocol

IETF PB-TNC [RFC5793] defines a Posture Broker protocol that is identical on-the-wire to TCG TNC IF-TNCCS: TLV Binding [TNC-TNCCS-TLV].

4.4.1 IETF PB-TNC Message Encapsulation

The following PB-TNC message encapsulation diagram is excerpted from section 3.4 of IETF PB-TNC [RFC5793]:

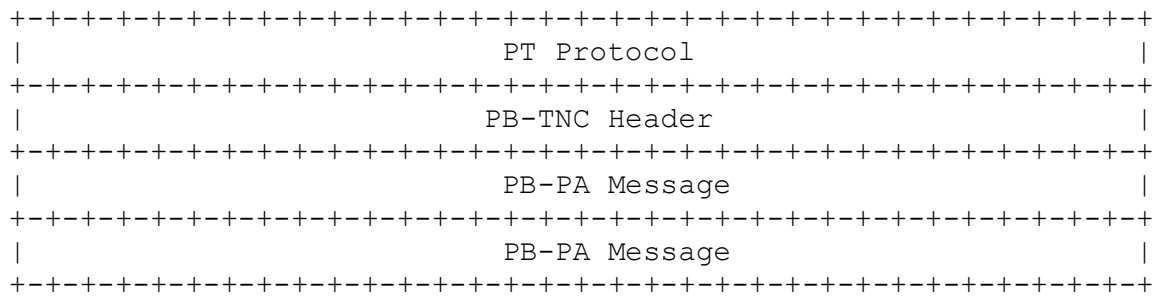

Figure 3 – IETF PB-TNC Message Format

4.4.2 IETF PB-TNC Message Header Format

The following PB-TNC message header format diagram is excerpted from section 4.1 of IETF PB-TNC [RFC5793]:

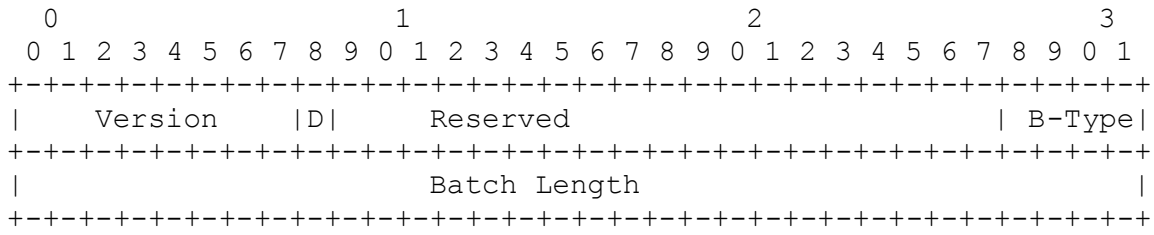

Figure 4 – IETF PB-TNC Message Header Format

Version (8 bits): Value MUST be 2 for [RFC5793] conformance.

Directionality (1 bit): Value MUST be 0 for a TNC Client request for [RFC5793] conformance.

Reserved (19 bits): Value MUST be 0 for [RFC5793] conformance.

Batch Type (4 bits): Value of this field drives the state machine for PB-TNC defined in section 3.2 of [RFC5793]. Value MUST be CDATA(1) or CRETRY(4) or CLOSE(6) for a TNC Client request for [RFC5793] conformance. Defined values in section 4.1 of [RFC5793] are: CDATA(1), SDATA(2), RESULT(3), CRETRY(4), SRETRY(5), and CLOSE(6).

Batch Length (32 bits): Value of this field contains the size of the full PB-TNC batch in octets. This length includes the PB-TNC header and all the PB-TNC messages in the batch. Value MUST be at least 8 (for the fixed-length fields in this header).

4.4.3 IETF PB-TNC Message Body Format

The following PB-TNC message body format diagram is excerpted from section 4.2 of IETF PB-TNC [RFC5793]:

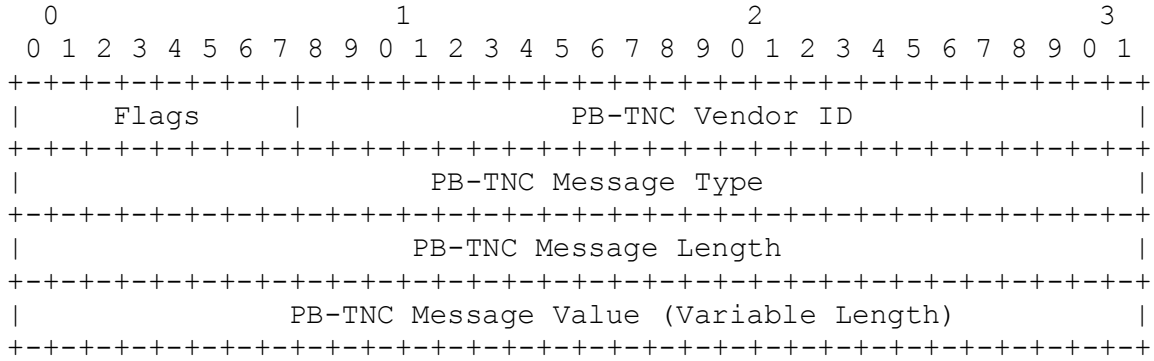

Figure 5 – IETF PB-TNC Message Body Format

Flags (8 bits): Value of this field affects processing of the associated message. Bit 0 (0x80) is the NOSKIP flag – if set to 1, then TNC Servers (Validators) MUST not process this message if this Message Type is NOT supported. All other bits are reserved and MUST be set to 0 for [RFC5793] conformance.

PB-TNC Vendor ID (24 bits): Value MUST be 24-bit SMI Private Enterprise Number of the party who owns this Attribute Type namespace. Value MUST be 0 for IETF namespace, 0x5597 (21911) for TCG namespace, or 0x0A8B (2699) for PWG namespace. Value of 0xffffff is reserved and MUST not be used.

PB-TNC Message Type (32 bits): Value MUST be an IETF, TCG, or PWG standard message type. Value of 0xffffffff is reserved and MUST not be used. IETF standard PB-TNC message types are defined in section 4.3 of [RFC5793] and registered with IANA. A TNC Client will send a PB-PA (1) message type.

PB-TNC Message Length (32 bits): Value is the length of the PB-TNC Message contained in the Message Value field.

PB-TNC Message Value (variable length): Value specifies the contents of the PB-TNC Message.

4.4.4 IETF PB-PA Message Type Format

The following PB-PA message type format diagram is excerpted from section 4.5 of IETF PB-TNC [RFC5793]:

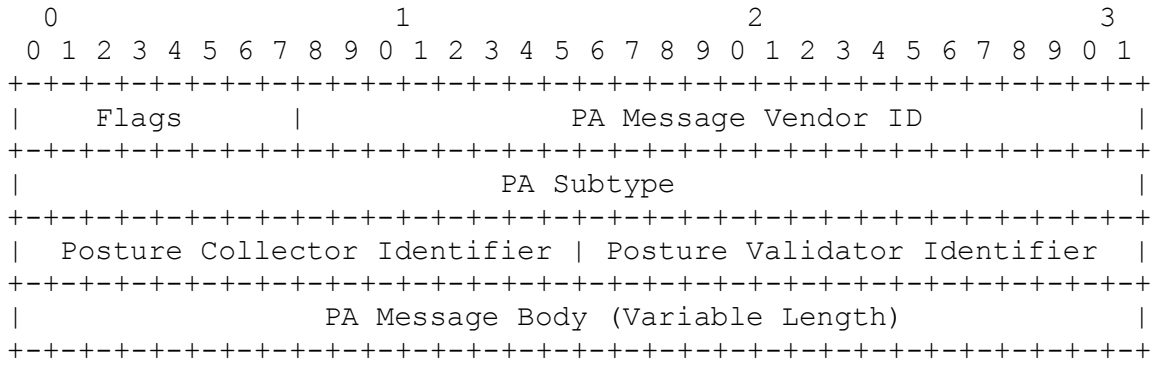

Figure 6 – IETF PB-PA Message Type Format

Flags (8 bits): Value of this field affects the delivery of this message to the Posture Collectors. Bit 0 (0x80) is the EXCL (exclusive) flag – if set to 1, then the receiving Posture Broker Client SHOULD deliver this message only to the Posture Collector specified by the Posture Collector Identifier field – however if that Posture Collector has not expressed an interest in PA messages with this Vendor ID and PA Subtype, then the message SHOULD be silently discarded. All other bits are reserved and MUST be set to 0 for [RFC5793] conformance.

PA Message Vendor ID (24 bits): Value MUST be 24-bit SMI Private Enterprise Number of the party who owns this Attribute Type namespace. Value MUST be 0 for IETF namespace, 0x5597 (21911) for TCG namespace, or 0x0A8B (2699) for PWG namespace. Value of 0xffffff is reserved and MUST not be used.

PA Subtype (32 bits): Value identifies the type of PA message contained in the PA Message Body field. IANA maintains a registry of PA subtypes. New vendor-specific PA subtypes (those used with a non-zero PA Message Vendor ID) may be defined and employed by vendors without IETF or IANA involvement. Value of 0xffffff is reserved and MUST not be used.

Posture Collector Identifier (16 bits): Value of this field contains the identifier of the Posture Collector associated with this PA message. The Posture Broker Client MUST assign one or more Posture Collector Identifier values (but not 0xffff) to each Posture Collector involved in a message exchange.

Posture Validator Identifier (16 bits): Value of this field contains the identifier of the Posture Validator associated with this PA message. The Posture Broker Server MUST assign a unique Posture Validator Identifier value (but not 0xffff) to each Posture Validator involved in a message exchange.

PA Message Body (variable length): Value specifies the contents of the PB-PA Message.

4.5 IETF PA-TNC – TNC Posture Attribute Protocol

IETF PA-TNC [RFC5792] defines a Posture Attribute protocol that is identical on-the-wire to TCG TNC IF-M: TLV Binding [TNC-IFM-TLV].

4.5.1 Overview of IETF PA-TNC Message within IETF PB-TNC Message

The following PA-TNC message within a PB-TNC message format diagram is excerpted from section 3.2 IETF PA-TNC [RFC5792]:

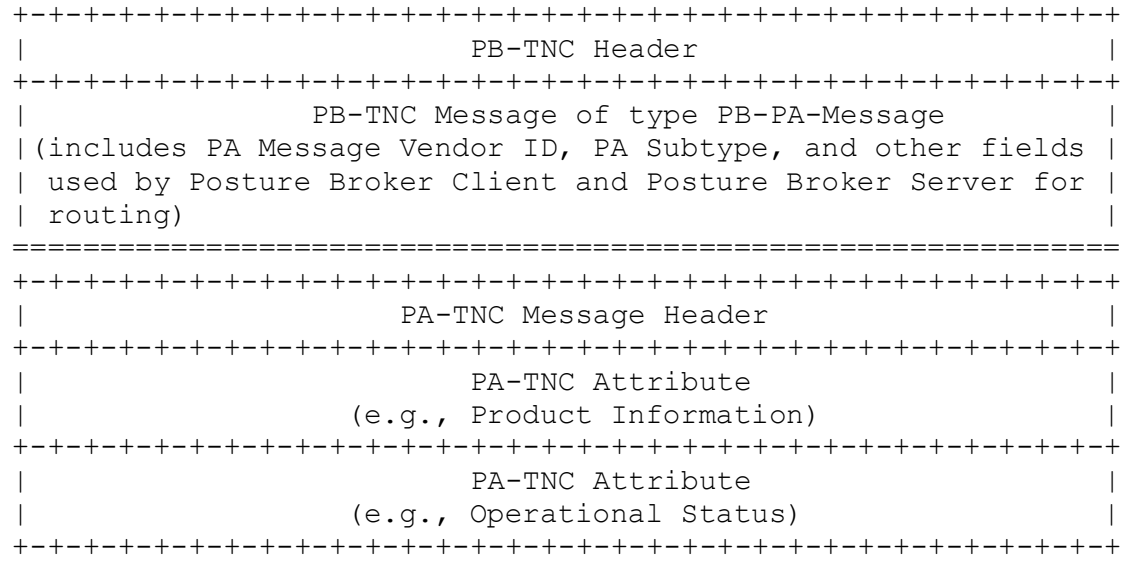

Figure 7 – IETF PA-TNC Message within IETF PB-TNC Message Format

4.5.2 IETF PA-TNC Message Header Format

The following PA-TNC message header format diagram is excerpted from section 3.6 of IETF PA-TNC [RFC5792]:

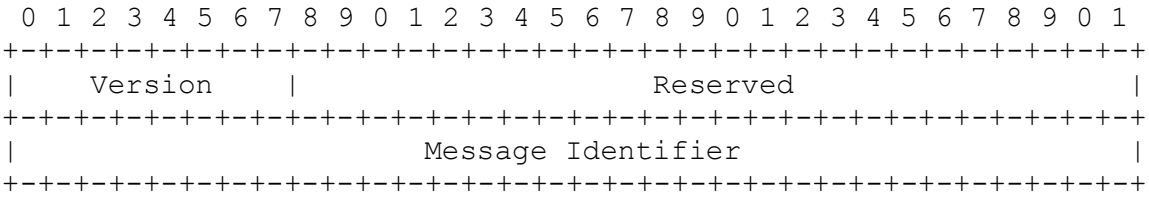

Figure 8 – IETF PA-TNC Message Header Format

Version (8 bits): Value MUST be 1 for [RFC5792] conformance.

Reserved (24 bits): Value MUST be 0 for [RFC5792] conformance.

Message Identifier (32 bits): Value uniquely identifies this message within this assessment.

4.5.3 IETF PA-TNC Attribute Format

The following PA-TNC attribute format diagram is excerpted from section 4.1 of IETF PA-TNC [RFC5792]:

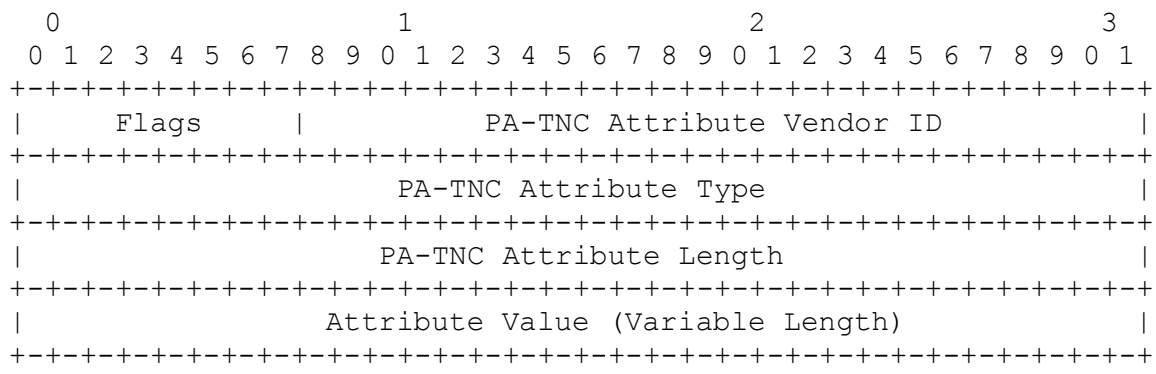

Figure 9 – IETF PA-TNC Attribute Format

Flags (8 bits): Value of this field affects processing of the associated attribute. Bit 0 (0x80) is the NOSKIP flag – if set to 1, then TNC Servers (Validators) MUST not process any attribute in the PA-TNC message if this attribute is NOT supported. All other bits are reserved and MUST be set to 0 for [RFC5792] conformance.

PA-TNC Attribute Vendor ID (24 bits): Value MUST be 24-bit SMI Private Enterprise Number of the party who owns this Attribute Type namespace. Value MUST be 0 for IETF namespace, 0x5597 (21911) for TCG namespace, or 0x0A8B (2699) for PWG namespace. Value of 0xffffff is reserved and MUST not be used.

PA-TNC Attribute Type (32 bits): Value is the type of the attribute in the Attribute Value field. Value of 0xffffffff is reserved and MUST not be used.

PA-TNC Attribute Length (32 bits): Value is the length in octets of the entire PA-TNC attribute, including the PA-TNC Attribute Header – therefore, the value MUST always be at least 12.

Attribute Value (variable length): Value specifies the contents of the PA-TNC attribute.

5. HCD Statement of Health for TNC Protocol

This section defines how the specified Hardcopy Device Health Assessment Attributes [PWG5110.1] MUST be used in the TNC Protocol, i.e., IETF PB-TNC [RFC5793] carrying IETF PA-TNC [RFC5792] messages.

Conforming HCDs MUST supply health assessment attributes in the following order:

1) All included REQUIRED or OPTIONAL IETF PA-TNC [RFC5793] attributes;

2) All unique REQUIRED PWG HCD attributes;

3) All unique CONDITIONALLY REQUIRED PWG HCD attributes;

4) All unique OPTIONAL PWG HCD attributes;

5) Any included PWG HCD attributes that are duplicates (in the PWG namespace) of corresponding IETF PA-TNC [RFC5793] attributes.

Conforming HCDs MUST supply all PWG-defined health assessment attributes using the PWG standard PA subtypes specified in PWG health assessment attributes definitions in sections 5.1, 5.2, and 5.3 and defined in section 9.1 (see section 1.1 for the rationale). Conforming HCDs SHOULD supply all applicable PWG-defined health assessment attributes for all supported major components defined as RECOMMENDED in section 9.1 (e.g., Console, Finisher, Interface, Marker, Scanner).

Note 1: The following encoding choices are for consistency w/ IETF PA-TNC [RFC5792]: (a) fixed length attribute values MUST always be *unpadded* (e.g., VendorSMICode); (b) boolean attribute values MUST always be 32-bits (e.g., DefaultPasswordEnabled); and (c) variable length string attribute values MUST always be *unpadded* and MUST NOT be null-terminated (e.g., AttributesNaturalLanguage).

Note 2: All HCD health assessment attributes MUST be supplied in their complete form (i.e., they MUST NOT be truncated to fit transport protocol binding packet sizes or other constraints).

Note 3: The health assessment attributes FirmwarePatches, UserApplicationPatches, and ResidentApplicationPatches each contain a list of patch values, which MUST be separated by trailing CR/LF pairs. Therefore any patch value member MUST NOT contain either CR (0x0D) or LF (0x0A).

Note 4: All correlated health assessment attributes (FirmwareXxx, UserApplicationXxx, and ResidentApplicationXxx) MUST conform to the special ordering rules for sets of firmware, user application, and resident application attributes defined in section 5.4.

5.1 Mandatory Attributes

Conforming HCDs MUST support all of the REQUIRED attributes defined in this section.

Note: The IETF PT-TLS [RFC6876] posture transport protocol binding supports large packet sizes (65,536 octets or greater), while the IETF PT-EAP [RFC7171] posture transport protocol binding supports only small packet sizes (typically less than 1,536 octets).

Due to large packet sizes, conforming HCDs supplying health assessment attributes via the IETF PT-TLS [RFC6876] posture transport protocol binding MUST include all of the REQUIRED attributes defined in this section.

In the case of small packet sizes, conforming HCDs supplying health assessment attributes via the IETF PT-EAP [RFC7171] posture transport protocol binding MAY omit any of the following otherwise REQUIRED attributes defined in this section:

- VendorName – values can be large strings
- DefaultPasswordEnabled – see FactoryDefaultPasswordEnabled in [RFC5792]
- FirewallSetting – see PortFilter in [RFC5792]
- ForwardingEnabled – see ForwardingEnabled in [RFC5792]
- FirmwareName – values can be large strings
- FirmwarePatches – values can be large strings
- FirmwareStringVersion – values can be large strings

5.1.1 AttributesNaturalLanguage

This variable length string attribute specifies the natural language tag [RFC5646] for all HCD string attributes in this health assessment message. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x01 (1)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length natural language tag that conforms to [RFC5646]

5.1.2 MachineTypeModel

This variable length string attribute specifies the machine type and model of this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x02 (2)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the machine type and model of this device, which SHOULD be consistent with the values of:
(a) sysDescr in IETF MIB-II [STD17]; and
(b) hrDeviceDescr in IETF Host Resources MIB v2 [RFC2790] for the row with hrDeviceType equal to hrDevicePrinter.

5.1.3 VendorName

This variable length string attribute specifies the name of the manufacturer of this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x03 (3)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the manufacturer name of this device, which SHOULD be consistent with the values of:
(a) sysDescr in IETF MIB-II [STD17]; and
(b) hrDeviceDescr in IETF Host Resources MIB v2 [RFC2790] for the row with hrDeviceType equal to hrDevicePrinter.

5.1.4 VendorSMICode

This integer attribute specifies the globally unique 24-bit SMI code assigned by IANA of the manufacturer this device, which SHOULD be consistent with the value of sysObjectID in IETF MIB-II [STD17]. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x04 (4)
Attribute Length: 0x0F (decimal 12 plus 3 for length of attribute value)
Attribute Value (24-bits): fixed length 8-bit reserved flags followed by *unpadded* 24-bit IANA registered SMI code of the manufacturer of this device.

5.1.5 DefaultPasswordEnabled

Note: This PWG HCD attribute is equivalent to the FactoryDefaultPasswordEnabled attribute defined in section 4.2.12 of IETF PA-TNC [RFC5792]. It is included here for completeness in the PWG namespace.

This boolean attribute specifies whether or not any factory default administrator passwords or other credentials are currently set on this device. If set to to ‘0’ (false), then no administrator passwords or other credentials are set to factory defaults. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x14 (20)
Attribute Length: 0x10 (decimal 12 plus 4 for length of attribute value)
Attribute Value (32-bits): fixed length integer field contains either ‘0’ or ‘1’.

5.1.6 FirewallSetting

Note: This PWG HCD attribute is equivalent to the PortFilter attribute defined in section 4.2.6 of IETF PA-TNC [RFC5792]. It is included here for completeness in the PWG namespace.

Note: Protocol mappings of this attribute to other representations (e.g., the PWG Semantic Model XML schema) need to consider the compact binary encoding (e.g., the B flag) of this PWG HCD Attribute.

This variable length string specifies the current firewall settings of this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x15 (21)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length firewall setting array that conforms to the following encoding.

The following FirewallSetting (PortFilter) format diagram is excerpted from section 4.2.6 of IETF PA-TNC [RFC5792]:

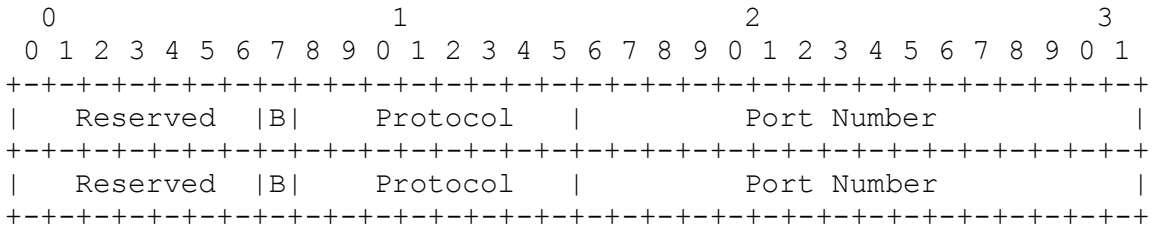

Figure 10 – IETF PA-TNC FirewallSetting Format

Reserved (7 bits): This field is reserved for future use. It MUST be set to 0 on transmission and ignored upon reception.

B Flag (Blocked or Allowed Port): The setting of Blocked (1) or Allowed (0) applies to traffic in both directions (incoming and outgoing) without any consideration of directionality of connections or associations. Posture Collectors SHOULD clear this bit to Allowed (0) to specify compact port filters. Posture Collectors MUST NOT specify a mixed list of Blocked and Allowed ports in a port filter.

Protocol (8 bits): This field specifies the IANA-registered transport protocol number (e.g., TCP is 6) being blocked or allowed.

Port Number (16 bits): This field specifies the transport protocol port number being blocked or allowed. Port numbers MAY be well-known and registered with IANA or they MAY be private or ephemeral port numbers according to the rules of the particular transport protocol.

5.1.7 ForwardingEnabled

Note: This PWG HCD attribute is equivalent to the ForwardingEnabled attribute defined in section 4.2.11 of IETF PA-TNC [RFC5792]. It is included here for completeness in the PWG namespace.

This boolean attribute specifies whether this device is forwarding traffic between *any* network interfaces. If set to to '0' (false), then this device MUST NOT forward any traffic between any network interfaces (including so-called loopback in and out of the same network interface). Note that these are the rigorous semantics specified for Forwarding Enabled in section 4.2.11 of [RFC5792]. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x16 (22)
Attribute Length: 0x10 (decimal 12 plus 4 for length of attribute value)
Attribute Value (32-bits): fixed length integer field contains either '0' or '1'.

5.1.8 FirmwareName

This variable length string attribute specifies the name of the firmware currently installed on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x3C (60)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the firmware name for this device.

5.1.9 FirmwarePatches

This variable length string attribute describes all of the firmware patches (from the oldest to the newest) currently installed on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x3D (61)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the list of all firmware patches (from the oldest to the newest) currently installed on this device. Each patch value MUST be delimited by a trailing CR/LF pair (0x0D/0x0A).

5.1.10 FirmwareStringVersion

This variable length string attribute specifies the string version of the firmware currently installed on this device, which SHOULD conform to section 4.2.4 “String Version” of IETF PA-TNC [RFC5792] which defines the internal string fields Product Version Number, Internal Build Number, and Configuration Version Number. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x3E (62)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the firmware string version for this device, which SHOULD conform to section 4.2.4 “String Version” of IETF PA-TNC [RFC5792] which defines the internal string fields Product Version Number, Internal Build Number, and Configuration Version Number.

5.1.11 FirmwareVersion

This fixed length string attribute specifies the build version of the firmware currently installed on this device, which SHOULD conform to section 4.2.3 “Numeric Version” of IETF PA-TNC [RFC5792] which defines the internal integer fields Major Version Number, Minor Version Number, Build Number, Service Pack Major, and Service Pack Minor. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x3F (63)
Attribute Length: 0x1C (decimal 12 plus 16 for length of attribute value)

Attribute Value (128-bits): A fixed length octet string containing the firmware build version for this device, which SHOULD conform to section 4.2.3 “Numeric Version” of IETF PA-TNC [RFC5792] which defines the internal integer fields Major Version Number, Minor Version Number, Build Number, Service Pack Major, and Service Pack Minor.

5.1.12 UserApplicationEnabled

This boolean attribute specifies whether or not the ability is supported and currently enabled for users to dynamically download and execute free-standing applications (not part of any Document data) on this device. If set to to ‘0’ (false), then users MUST NOT be allowed to dynamically download or execute such applications on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x68 (104)
Attribute Length: 0x10 (decimal 12 plus 4 for length of attribute value)
Attribute Value (32-bits): fixed length integer field contains either ‘0’ or ‘1’.

5.1.13 UserApplicationPersistenceEnabled

This boolean attribute specifies whether or not the ability is supported and currently enabled for user dynamically downloaded applications to persist outside the boundaries of a single Job on this device. If set to to ‘0’ (false), then user dynamically downloaded applications MUST be deleted when their associated original Job reaches completion. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x69 (105)
Attribute Length: 0x10 (decimal 12 plus 4 for length of attribute value)
Attribute Value (32-bits): fixed length integer field contains either ‘0’ or ‘1’.

5.1.14 PSTNFaxEnabled

This boolean attribute specifies whether or not any PSTN facsimile interfaces are currently installed and enabled on this device. If set to to ‘0’ (false), then no PSTN facsimile interfaces are currently installed and enabled on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x28 (40)
Attribute Length: 0x10 (decimal 12 plus 4 for length of attribute value)
Attribute Value (32-bits): fixed length integer field contains either ‘0’ or ‘1’.

5.1.15 TimeSource

This variable length string attribute specifies where the device acquires its time setting or the empty string if no time source is configured. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x17 (23)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string specifying the time source for this device or the empty string if no time source is configured.

5.2 Conditionally Mandatory Attributes

Conforming HCDs MUST support each of the CONDITIONALLY REQUIRED attributes defined in this section, if the particular capability associated with each attribute is implemented on the HCD. Conforming HCDs MUST return all of these CONDITIONALLY REQUIRED attributes in PT-TLS reports and MAY return any of these attributes in PT-EAP reports (due to packet size restrictions).

Note: The IETF PT-TLS [RFC6876] posture transport protocol binding supports large packet sizes (65,536 octets or greater). The IETF PT-EAP [RFC7171] posture transport protocol binding supports only small packet sizes (typically less than 1,536 octets).

In the case of large packet sizes, conforming HCDs supplying health assessment attributes via the IETF PT-TLS [RFC6876] posture transport protocol binding MUST include all of the following applicable CONDITIONALLY REQUIRED attributes defined in this section.

In the case of small packet sizes, conforming HCDs supplying health assessment attributes via the IETF PT-EAP [RFC7171] posture transport protocol binding MAY omit any of the following applicable otherwise CONDITIONALLY REQUIRED attributes defined in this section:

- UserApplicationPatches – values can be large strings
- UserApplicationStringVersion – values can be large strings
- ResidentApplicationPatches – values can be large strings
- ResidentApplicationStringVersion – values can be large strings

5.2.1 UserApplicationName

CONDITIONALLY REQUIRED: This attribute MUST be supported if the HCD supports user-downloadable applications.

This variable length string attribute specifies the name of a user application currently installed on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x64 (100)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the user application name on this device.

5.2.2 UserApplicationPatches

CONDITIONALLY REQUIRED: This attribute MUST be supported if the HCD supports user-downloadable applications.

This variable length string attribute describes all of the patches (from the oldest to the newest) for this user application currently installed on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x65 (101)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the list of all user application patches (from the oldest to the newest) for this user application currently installed on this device. Each patch value MUST be delimited by a trailing CR/LF pair (0x0D/0x0A).

5.2.3 UserApplicationStringVersion

CONDITIONALLY REQUIRED: This attribute MUST be supported if the HCD supports user-downloadable applications.

This variable length string attribute specifies the string version of this user application currently installed on this device, which SHOULD conform to section 4.2.4 “String Version” of IETF PA-TNC [RFC5792] which defines the internal string fields Product Version Number, Internal Build Number, and Configuration Version Number. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)

Attribute Type: 0x66 (102)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the string version of this user application currently installed on this device, which SHOULD conform to section 4.2.4 "String Version" of IETF PA-TNC [RFC5792] which defines the internal string fields Product Version Number, Internal Build Number, and Configuration Version Number.

5.2.4 UserApplicationVersion

CONDITIONALLY REQUIRED: This attribute MUST be supported if the HCD supports user-downloadable applications.

This fixed length string attribute specifies the build version of this user application currently installed on this device, which SHOULD conform to section 4.2.3 "Numeric Version" of IETF PA-TNC [RFC5792] which defines the internal integer fields Major Version Number, Minor Version Number, Build Number, Service Pack Major, and Service Pack Minor. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x67 (103)
Attribute Length: 0x1C+length (decimal 12 plus 16 for length of attribute value)
Attribute Value (128-bits): A fixed length octet string containing the build version of this user application currently installed on this device, which SHOULD conform to section 4.2.3 "Numeric Version" of IETF PA-TNC [RFC5792] which defines the internal integer fields Major Version Number, Minor Version Number, Build Number, Service Pack Major, and Service Pack Minor.

5.2.5 ResidentApplicationName

CONDITIONALLY REQUIRED: This attribute MUST be supported if the HCD supports the addition of resident applications.

This variable length string attribute specifies the name of a resident application currently installed on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x50 (80)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the resident application name on this device.

5.2.6 ResidentApplicationPatches

CONDITIONALLY REQUIRED: This attribute MUST be supported if the HCD supports the addition of resident applications.

This variable length string attribute describes all of the patches (from the oldest to the newest) for this resident application currently installed on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x51 (81)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the list of all resident application patches (from the oldest to the newest) for this resident application currently installed on this device. Each patch value MUST be delimited by a trailing CR/LF pair (0x0D/0x0A).

5.2.7 ResidentApplicationStringVersion

CONDITIONALLY REQUIRED: This attribute MUST be supported if the HCD supports the addition of resident applications.

This variable length string attribute specifies the string version of this resident application currently installed on this device, which SHOULD conform to section 4.2.4 “String Version” of IETF PA-TNC [RFC5792] which defines the internal string fields Product Version Number, Internal Build Number, and Configuration Version Number. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x52 (82)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string containing the string version of this resident application currently installed on this device, which SHOULD conform to section 4.2.4 “String Version” of IETF PA-TNC [RFC5792] which defines the internal string fields Product Version Number, Internal Build Number, and Configuration Version Number.

5.2.8 ResidentApplicationVersion

CONDITIONALLY REQUIRED: This attribute MUST be supported if the HCD supports the addition of resident applications.

This fixed length string attribute specifies the build version of this resident application currently installed on this device, which SHOULD conform to section 4.2.3 “Numeric Version” of IETF PA-TNC [RFC5792] which defines the internal integer fields Major

Version Number, Minor Version Number, Build Number, Service Pack Major, and Service Pack Minor. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: Any PWG-registered value (see section 9.1)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x53 (83)
Attribute Length: 0x1C+length (decimal 12 plus 16 for length of attribute value)
Attribute Value (128-bits): A fixed length octet string containing the build version of this resident application currently installed on this device, which SHOULD conform to section 4.2.3 “Numeric Version” of IETF PA-TNC [RFC5792] which defines the internal integer fields Major Version Number, Minor Version Number, Build Number, Service Pack Major, and Service Pack Minor.

5.3 OptionalAttributes

Conforming HCDs MAY support any of the OPTIONAL attributes defined in this section.

5.3.1 CertificationState

Note: An example implementation of this attribute could be a cryptographically secure hash of the HCD configuration (e.g., firmware version, port filter settings, protocols enabled/disabled, etc.) that is set to a specific state as part of the certification process.

This variable length string attribute 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). A change to any configuration setting that is required for the device to maintain its certification status MUST cause a change, within the limits of information theory, in the value of this attribute. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0xC8 (200)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string specifying the certification state for this device.

5.3.2 ConfigurationState

Note: An example implementation of this attribute could be a cryptographically secure hash of the HCD configuration settings.

This variable length string attribute uniquely identifies the state of any configuration settings in the HCD that are included in creation of the attribute. A change to any configuration setting that is included in the creation of the attribute MUST cause a change, within the limits of information theory, in the value of this attribute. The configuration

settings included as part of this attribute SHOULD be administratively configurable. The PA-TNC Attribute fields (see section 4.4.3) are set to:

PWG PA Subtype: 0x00000005 (5 – System)
Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0xC9 (201)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attribute Value: A variable length string specifying the configuration state for this device.

5.4 Correlated Attributes

Each **ordered** set of **Correlated Attributes** (firmware, user application, or resident application) MUST:

1) Represent exactly one instance of firmware or an application;

2) Be a complete set (4-tuple) for IETF PT-TLS [RFC6876] or a minimal set (2-tuple) for IETF PT-EAP [RFC7171], when Patches and String Version SHOULD NOT be included for small packet sizes;

3) Occur in exactly the following order: Name, [Patches, StringVersion,] Version.

Note: Each **ordered** set of **Correlated Attributes** MUST include an empty string or all zeros integer if there is no known value for one of the **Correlated Attributes** (except for Name which MUST NOT be empty).

6. Conformance Requirements

6.1 HCD TNC Binding Conformance

1) Conforming HCDs that support any TNC transport protocol binding defined in this specification MUST:

2) Conform to section 7 Internationalization Considerations;

3) Conform to section 8 Security Considerations;

4) Support multiple instances of the **Correlated Attributes** (Name, Patches, StringVersion, and Version) for firmware, user applications (if implemented), and resident applications (if implemented) defined in section 5.4; and

5) Conform to the requirements for ordered sets of **Correlated Attributes** (Name, Patches, StringVersion, and Version) for firmware, user applications (if implemented), and resident applications (if implemented) defined in section 5.4;

6) Conform to section 9.1 PWG Standard PA Subtypes and the component conformance requirements defined in Table 1.

6.2 HCD TNC Attribute Conformance

This section contains the implementation requirements for HCDs that support any TNC transport protocol binding.

6.2.1 Mandatory Attributes

Conforming HCDs MUST support all of following attributes defined in section 5.1:

- AttributesNaturalLanguage
- DefaultPasswordEnabled
- FirewallSetting
- FirmwareName
- FirmwarePatches
- FirmwareStringVersion
- FirmwareVersion
- ForwardingEnabled

- MachineTypeModel
- PSTNFaxEnabled
- TimeSource
- UserApplicationEnabled
- UserApplicationPersistenceEnabled
- VendorName
- VendorSMICode

6.2.2 Conditionally Mandatory Attributes

Conforming HCDs MUST support the following attributes defined in section 5.2 if the particular capability (UserApplication or ResidentApplication) is implemented on the HCD:

- UserApplicationName
- UserApplicationPatches
- UserApplicationStringVersion
- UserApplicationVersion
- ResidentApplicationName
- ResidentApplicationPatches
- ResidentApplicationStringVersion
- ResidentApplicationVersion

Note: In the case of small packet sizes in the IETF PT-EAP [RFC7171] transport binding the XxxPatches and XxxStringVersion attributes MAY be omitted – see section 5 and section 5.4 for rules on omission of these string attributes.

6.2.3 Optional Attributes

Conforming HCDs MAY support any of the following attributes defined in section 5.3:

- CertificationState
- ConfigurationState

7. Internationalization Considerations

For interoperability and basic support for multiple languages, conforming implementations MUST support the Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [RFC3629] encoding of Unicode [UNICODE] [ISO10646] and the Unicode Format for Network Interchange [RFC5198].

8. Security Considerations

Implementations of this specification MUST provide integrity protection and confidentiality protection of the transmitted health assessment attributes. Integrity protection is typically accomplished via secure hashes of health assessment attributes and confidentiality protection is typically accomplished via encryption of health assessment attributes – both features are implemented directly in the standard IETF PT-TLS [RFC6876] and IETF PT-EAP [RFC7171] transport bindings. Implementations of this specification MUST conform to all of the security requirements stated in section 5 Security Considerations of IETF PA-TNC [RFC5792], section 4 Security Considerations of IETF PT-EAP [RFC7171], section 5 Security Considerations of IETF PB-TNC [RFC5793], and section 4 Security Considerations of IETF PT-TLS [RFC6876]

9. IANA and PWG Considerations

There are no IANA or PWG registration considerations for this document, except for the new PWG Standard PA Subtype values defined below. See the standard imaging device health attributes defined in [PWG5110.1].

9.1 PWG Standard PA Subtypes

This section defines PWG Standard PA Subtypes. Each PA subtype defined here identifies a specific component relevant to the hardcopy device's endpoint posture. This allows a small set of generic PWG PA-TNC attributes (e.g., FirmwareVersion) to be used to describe a large number of different components (e.g., system, interface, console, etc.). It also allows Posture Collectors and Posture Validators to specialize in a particular component and only receive PWG PA-TNC messages relevant to that component. For comparison, see section 3.5 "IETF Standard PA Subtypes" of IETF PA-TNC [RFC5792].

The following PWG Standard PA Subtypes are technically and numerically aligned with the PWG Imaging System State and Counter MIB [PWG5106.3].

Notes:

1) Conforming HCDs SHOULD report firmware correlated attributes for all implemented major HCD components that typically run independent firmware (marked as RECOMMENDED below).

2) A Media Path often can include a "feeder" element that allows high-speed input of media to a Scanner, Marker, or Finisher.

Table 1 – PWG Standard PA Subtypes for HCD Components

Decimal Value	Component Name	Component Definition	Conformance
0	Testing	Reserved for use in spec examples, experimentation, and testing	**OPTIONAL**
1	Other	Other component	**OPTIONAL**
2	Unknown	Unknown component	**OPTIONAL**
4	Console	Console (note 1)	**RECOMMENDED**
5	System	Imaging System (overall)	**REQUIRED**
6	Cover	Cover, door, or interlock	**OPTIONAL**
8	Input Tray	Media input tray	**OPTIONAL**
9	Output Tray	Media output tray	**OPTIONAL**
10	Marker	Marker (note 1)	**RECOMMENDED**
13	Media Path	Media path (note 2)	**OPTIONAL**
14	Channel	Input job channel (e.g., IPP)	**OPTIONAL**
15	Interpreter	Interpreter (PDL or PCL)	**OPTIONAL**
30	Finisher	Finisher (stapler, folder, etc.) (note 1)	**RECOMMENDED**
40	Interface	Interface (local or network) (note 1)	**RECOMMENDED**
50	Scanner	Scanner (note 1)	**RECOMMENDED**

10. References

10.1 Normative References

[IEEE2600] IEEE, “Standard for Information Technology: Hardcopy Device and System Security”, IEEE 2600-2008, 2008

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

[PWG5106.3] I. McDonald, “PWG Imaging System State and Counter MIB v2.0”, March 2008, http://ftp.pwg.org/pub/pwg/candidates/cs-wimscountmib20-20080318-5106.3.pdf

[PWG5110.1] J. Murdock, J. Thrasher, "PWG Hardcopy Device Health Assessment Attributes", PWG 5110.1, May 2014, http://ftp.pwg.org/pub/pwg/candidates/cs-idsattributes11-20140529-5110.1.pdf

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119/BCP 14, March 1997, http://www.ietf.org/rfc/rfc2119.txt

[RFC2790] S. Waldbusser, P. Grillo, "Host Resources MIB", RFC 2790, March 2000, http://www.ietf.org/rfc/rfc2790.txt

[RFC2911] T. Hastings, R. Herriot, R. deBry, S. Isaacson, P. Powell, "Internet Printing Protocol/1.1: Model and Semantics", RFC 2911, September 2000, http://www.ietf.org/rfc/rfc2911.txt

[RFC3805] R. Bergman, H. Lewis, I. McDonald, "Printer MIB v2", RFC 3805, June 2004, http://www.ietf.org/rfc/rfc3805.txt

[RFC3806] R. Bergman, H. Lewis, I. McDonald, "Printer Finishing MIB", RFC 3806, June 2004, http://www.ietf.org/rfc/rfc3806.txt

[RFC5646] A. Phillips, M. Davis, “Tags for Identifying Languages”, RFC 5646 / BCP 47, September 2009, http://www.ietf.org/rfc/rfc5646.txt

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

[RFC5793] R. Sahita, S. Hanna, R. Hurst, K. Narayan, "PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5793, March 2010, http://www.ietf.org/rfc/rfc5793.txt

[RFC6876] P. Sangster, N. Cam-Winget, J. Salowey, " PT-TLS: A TLS-based Posture Transport (PT) Protocol", RFC 6876, February 2013, http://www.ietf.org/rfc/rfc6876.txt

[RFC7171] N. Cam-Winget, P. Sangster, "PT-EAP: Posture Transport (PT) Protocol For EAP Tunnel Methods", RFC 7171, May 2014, http://www.ietf.org/rfc/rfc7171.txt

[STD17] K. McCloghrie, M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", RFC 1213/STD 17, March 1991, http://www.ietf.org/rfc/rfc1213.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

[TNC-ARCH] S. Hanna, L. Lorenzin, "TCG Trusted Network Connect – TNC Architecture for Interoperability", Version 1.4, Revision 4, May 2009, http://www.trustedcomputinggroup.org/developers/

[TNC-IFM-TLV] R. Sahita, S. Hanna, R. Hurst, "TCG Trusted Network Connect – TNC IF-M: TLV Binding", Version 1.0, Revision 40, May 2014, http://www.trustedcomputinggroup.org/developers/

[TNC-IFT-EAP] P. Sangster, “TCG TNC IF-T: Protocol Bindings for Tunneled EAP Methods”, Version 2.0, Revision 4, May 2014, http://www.trustedcomputinggroup.org/developers/

[TNC-IFT-TLS] S. Hanna, P. Sangster, “TCG TNC IF-T: Binding to TLS”, Version 2.0, Revision 7, February 2013, http://www.trustedcomputinggroup.org/developers/

[TNC-TNCCS-TLV] R. Sahita, S. Hanna, R. Hurst, "TCG Trusted Network Connect – TNC IF-TNCCS: TLV Binding", Version 2.0, Revision 20, May 2014, http://www.trustedcomputinggroup.org/developers/

[UNICODE] Unicode Consortium, "Unicode Standard", Version 8.0.0, June 2015, http://unicode.org/versions/Unicode8.0.0/

10.2 Informative References

[RFC3552] E. Rescorla, B. Corver, “Guidelines for Writing RFC Text on Security Considerations”, RFC 3552 / BCP 72, July 2003, http://www.ietf.org/rfc/rfc3552.txt

[RFC5226] T. Narten, H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226 / BCP 26, May 2008, http://www.ietf.org/rfc/rfc5226.txt

11. Editor's Address

Ira McDonald
High North Inc
PO Box 221
Grand Marais, MI 49839
Email: blueroofmusic@gmail.com
Phone: +1-906-494-2434

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

Joe Murdock	Sharp
Brian Smithson	Ricoh
Dr. Andreas Steffen	HSR (Hochschule für Technik Rapperswil, Switzerland)
Alan Sukert	Xerox
Jerry Thrasher	Lexmark

