5 December 2011
Working Draft

The Printer Working Group

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

Status: Interim Draft

Abstract: This document defines a concrete protocol binding over TCG TNC / IETF NEA (technically equivalent) of the abstract PWG Hardcopy Device Health Assessment Attributes for trustworthy network attachment of Imaging Systems.

This document is a PWG Working Draft. For a definition of a "PWG Working Draft", see:

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

This document is available electronically at:

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-tnc10-20111205.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 Figures

No table of figures entries found.

List of Tables

No table of figures entries found.

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 for trustworthy network attachment of Imaging Systems..

2. Terminology

2.1 Conformance Terminology

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

2.2 Printing Terminology

Normative definitions and semantics of printing terms are imported from IETF Printer MIB v2 [RFC3805], IETF Finisher MIB [RFC3806], and IETF IPP/1.1 [RFC2911].

2.3 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): Within the TNC framework for endpoint integrity, the AR is the entity seeking connectivity to network that implements the TNC Architecture. The AR consists of three main components, namely the NAR, TNC Client and the IMC. See glossary for the definition of these components.

Clientless Endpoint (CE): Within the TNC framework, this is a network endpoint without a TNC Client (TNCC).

Endpoint Integrity Information: This is information provided by IMCs describing the status and configuration of the AR.

Flow Controller: The Flow Controller function makes and enforces decisions about network activities utilizing information from the MAP. Flow Controllers take action (e.g. block) on network flows (i.e. network traffic associated with a particular AR, device, user, etc.) based on data obtained via IF-MAP. Examples include: internal firewalls, rate limiters, and proxies.

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): An IMC is a software component that runs on an Access Requestor (AR), measuring certain aspects of the AR's integrity, including software versions, patches, Anti-Virus and others. An IMC may use the TCG Platform Trust Service (PTS) to obtain integrity information regarding every component of the platform on which the IMC sits. Multiple IMCs may reside on a single AR.

Integrity Measurement Verifier (IMV): An IMV is the component of the PDP that verifies a particular aspect of the AR's integrity, based on measurements received from an IMCs and/or other data. Multiple IMVs may reside on a single PDP.

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

Metadata Access Point (MAP): The role in the TNC framework of a broker/server to which metadata may be published and from which metadata may be searched and subscribed to using the IF-MAP protocol.

Metadata Access Point Client (MAPC): The role in the TNC framework of an element which publishes metadata to or searches/subscribes to metadata from a MAP.

Metadata Access Point Server (MAPS): The component of the MAP providing the function that allows other TNC components to publish, subscribe to, and search metadata.

Network Access Authority (NAA): The NAA is the network layer function of the PDP that decides whether an NAR should be granted access to a network.

Network Access Enforcer (NAE): The NAE is the network layer function of the PEP that consumes and enforces access control policies from an NAA.

Network Access Requestor (NAR): The NAR is the component of the Access Requestor (AR) responsible for negotiating and establishing network access onto a given network. The NAR is expected to implement network layer protocols, covering security, message transport and others. In the context of 802.1X, the NAR can be identified as the Supplicant.

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

Platform Trust Services (PTS): The PTS is a system service that exposes trusted platform capabilities to TNC components that reside on a Trusted Platform containing a Trusted Platform Modeul (TPM). PTS services include protected key storage, asymmetric cryptography, random numbers, platform identity, platform configuration reporting and integrity state tracking.

Policy Decision Point (PDP): The PDP is an entity evaluating the status of a TNC Client (seeking network connectivity) and deciding upon some network-related action to be enforced by the PEP. The PDP embodies the security and integrity related policies governing the network.

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

Sensor: The Sensor function monitors network activities and publishes information to the MAP via IF-MAP. Examples include: intrusion detection devices, network virus detection devices, layer 3 traffic monitors, and application traffic scanners.

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

TNC Server (TNCS): The TNCS is the component on the PDP that manages the flow of messages between Integrity Measurement Collectors (IMC) and Integrity Measurement Verifiers (IMV), gathers recommendations from IMVs, and combines those recommendations (based on policy) into an overall TNCS Action Recommendation to the NAA.

3. Requirements

3.1 Rationale for Title of Standard

Provide a rationale for the standard.

3.2 Use Cases

Provide use cases for the standard.

3.3 Out of Scope

Provide a list of use cases that are out-of-scope and the reasons.

3.4 Design Requirements

Provide a list of requirements based on the rationale and use cases.

4. TNC Protocol Overview

4.1 TNC Architecture

The 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. A detailed discussion of the TNC Architecture is in Appendix A – TNC Architecture.

4.2 TNC Transport Protocol

Put brief summary here of:
(a) IETF PT-EAP [PT-EAP] for assessment *before* an IP address is assigned (the endpoint is joining the network);
(b) IETF PT-TLS [PT-TLS] for assessment *after* an IP address is assigned (the endpoint is already on the network).

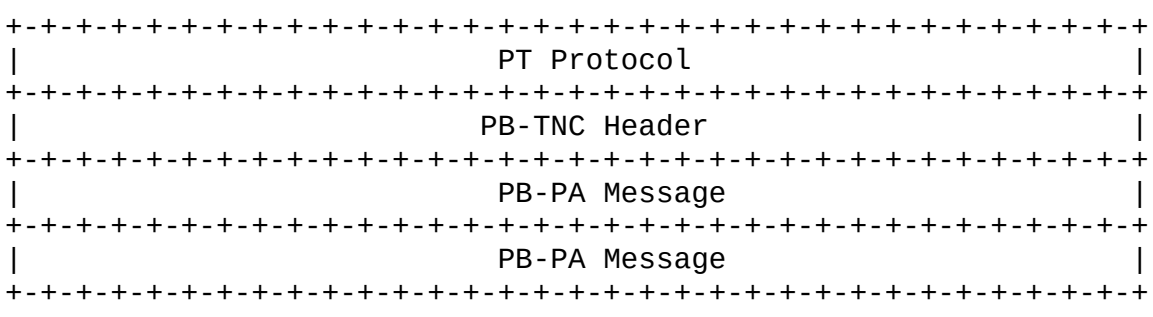
Also put a brief summary here of the relevant TCG TNC transport specs.

4.3 PB-TNC Message Syntax

Put a brief summary here of:
(a) IETF PA-TNC [RFC5792] which is identical to TCG TNC IF-M: TLV Binding [TNC-IFM-TLV];
(b) IETF PB-TNC [RFC5793] which is identical to TCG TNC IF-TNCCS: TLV Binding [TNC-TNCCS-TLV].

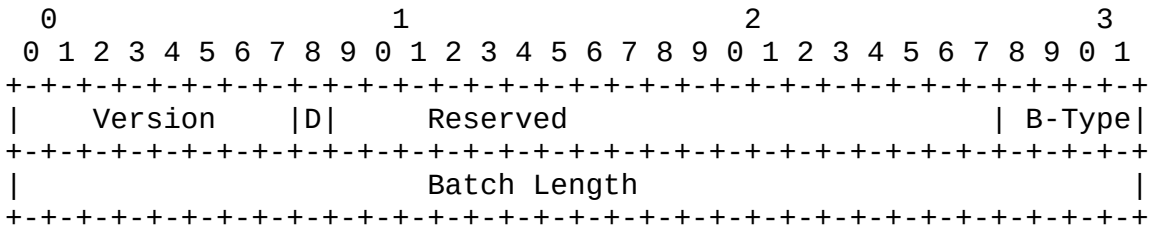
4.3.1 PB-TNC Message Encapsulation

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



4.3.2 PB-TNC Message Header Format

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



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

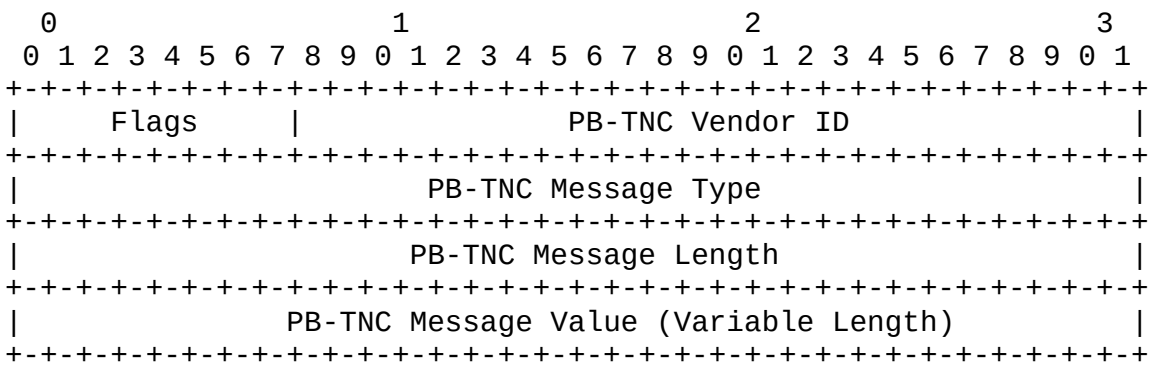
Directionality (1 bit): Value MUST be 0 for a TNC Client request for [RFC5793] conformance.

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).

4.3.3 PB-TNC Message Format

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



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.

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

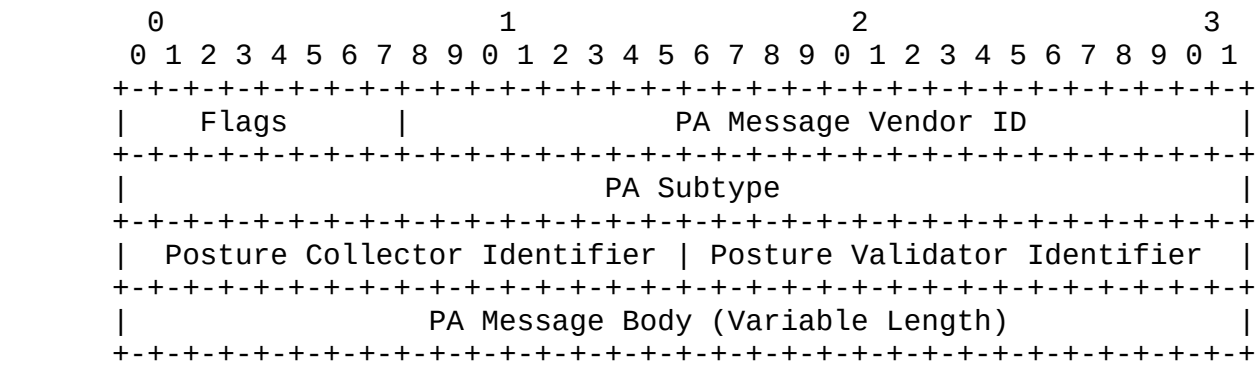
Message Type (32 bits): Value MUST be an IETF, TCG, or PWG standard message type. Value of 0xffffffff is reserved and MUST not be used. IETF standard PB-TNC message types are defined in section 4.3 of [RFC5793] and registered with IANA. A TNC Client will send a PB-PA (1) message type.

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

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

4.3.4 PB-PA Message Type Format

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



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.

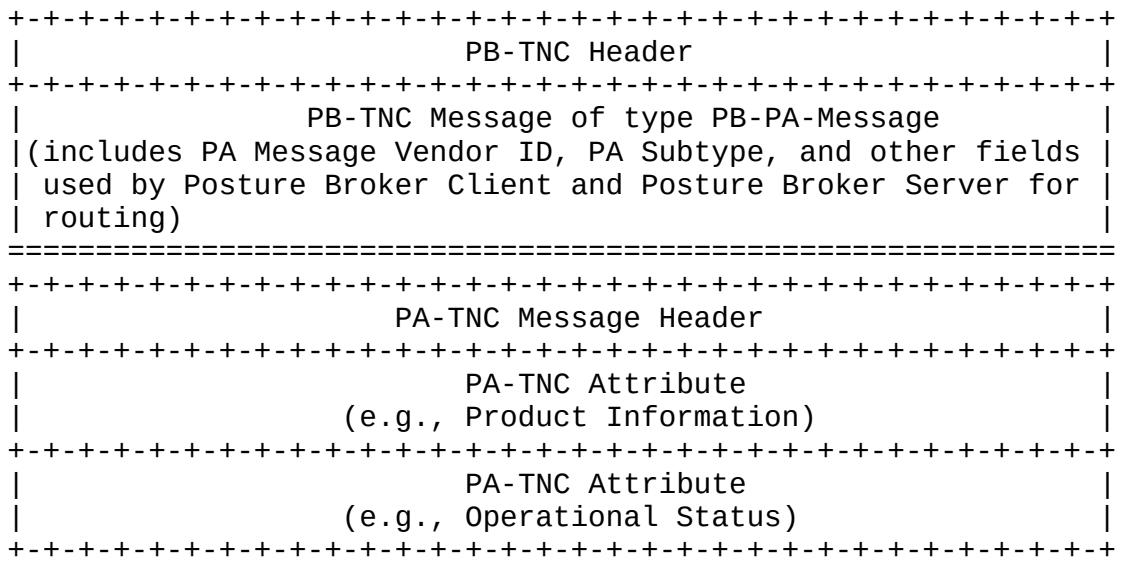
Posture Validator Identifier (16 bits): Value of this field contains the identifier of the Posture Validator associated with this PA message. The Posture Broker Server MUST assign a unique Posture Validator Identifier value (but not 0xffff) to each Posture Validator involved in a message exchange.

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

4.4 PA-TNC Message Syntax

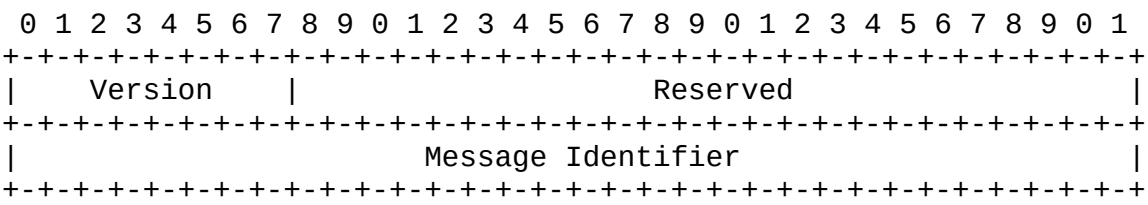
4.4.1 Overview of PB-TNC Message with PA-TNC Message

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



4.4.2 PA-TNC Message Header Format

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



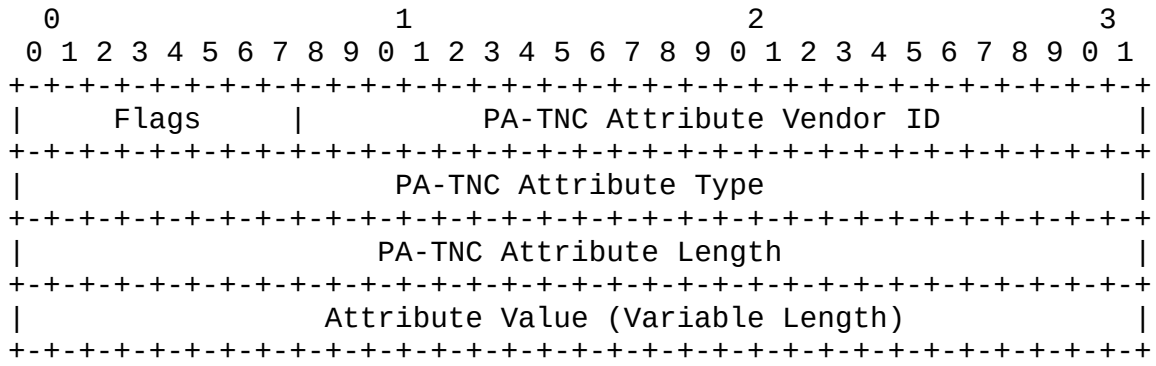
Version (8 bits): Value MUST be 1 for [RFC5792] conformance.

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

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

4.4.3 PA-TNC Attribute Format

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



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.

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.

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.

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 [HCD-ATR] are to be used with the TNC Protocol, in particular with IETF PB-TNC [RFC5793] carrying IETF PA-TNC [RFC5792] messages.

5.1 Mandatory Attributes

[[[ISSUE: Need to resolve encoding and ordering of HCD attributes with respect to TNC components.]]]

5.1.1 AttributesNaturalLanguage

This variable length string attribute specifies the local language used by all localized string attributes in this SoH. The PA-TNC Attribute fields (see section 4.4.3) are set to:

Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x01 (1)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attibute 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:

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 [RFC1213]; 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 this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

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 [RFC1213]; 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 [RFC1213]. The PA-TNC Attribute fields (see section 4.4.3) are set to:

Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x04 (4)
Attribute Length: 0x0F (decimal 12 plus length of attribute value)
Attribute Value (32-bits): fixed length 8-bit reserved flags followed by 24-bit SMI code of the manufacturer of this device (unpadded).

5.1.5 DefaultPasswordEnabled

[[[ISSUE: This PWG HCD attribute is now redundant with the IETF/TCG standard PA-TNC attribute FactoryDefaultPasswordEnabled defined in section 4.2.12 of IETF PA-TNC [RFC5792]. Should it be represented under both IETF and PWG SMI posture subtrees?]]]

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:

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

5.1.6 FirewallSetting

[[[ISSUE: This PWG HCD attribute is now redundant with the IETF/TCG standard PA-TNC attribute PortFilter defined in section 4.2.6 of IETF PA-TNC [RFC5792]. Should it be represented under both IETF and PWG SMI posture subtrees?]]]

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

Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x15 (21)
Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)
Attibute 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]:

```
  0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved  |B|    Protocol   |         Port Number           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved  |B|    Protocol   |         Port Number           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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): This single-bit field specifies whether the following port is blocked or allowed. This bit MUST be set to 1 if the protocol and port combination is blocked. Otherwise, this field MUST be set to 0. Posture Collectors MUST NOT provide a mixed list of blocked and non-blocked ports for a particular protocol.

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

[[[ISSUE: This PWG HCD attribute is now redundant with the IETF/TCG standard PA-TNC attribute ForwardingEnabled defined in section 4.2.11 of IETF PA-TNC [RFC5792]. Should it be represented under both IETF and PWG SMI posture subtrees?]]]

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:

Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x16 (22)
Attribute Length: 0x10 (decimal 12 plus 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:

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 currently installed on this device. The PA-TNC Attribute fields (see section 4.4.3) are set to:

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) for this device.

5.1.10 FirmwareStringVersion

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

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.

5.1.11 FirmwareVersion

This fixed length string attribute specifies the build version of the firmware currently installed on this device, which MAY conform to section 4.2.4 “String Version of IETF PA-TNC [RFC5792]. The PA-TNC Attribute fields (see section 4.4.3) are set

Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x3F (63)
Attribute Length: 0x1C+length (decimal 12 plus length of attribute value)
Attribute Value (16 bits): A fixed length octet string containing the firmware build version for this device, which MAY conform to section 4.2.3 “Numeric Version” of IETF PA-TNC [RFC5292].

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 applications 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:

Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x64 (100)
Attribute Length: 0x10 (decimal 12 plus 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 deleted when their associated original Job reaches completion. The PA-TNC Attribute fields (see section 4.4.3) are set to:

Flags: 0x00 (SKIP)
Vendor ID: 0x0A8B (2699 – PWG)
Attribute Type: 0x65 (101)
Attribute Length: 0x10 (decimal 12 plus length of attribute value)
Attribute Value (32-bits): fixed length integer field contains either '0' or '1'.

5.2 Conditionally Mandatory Attributes

[to be supplied]

5.3 Optional Attributes

[to be supplied]

6. Conformance Requirements

Provide a list of conformance requirements for the standard.

7. Internationalization Considerations

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

8. Security Considerations

Provide security considerations for this specification.

9. IANA Considerations

Provide IANA registration information for this specification.

10. References

10.1 Normative References

[REFERENCE] F. Last author list or standards body, "Title of referenced document", Document Number, Month YYYY, URL (if any)

10.2 Informative References

[REFERENCE] F. Last author list or standards body, "Title of referenced document", Document Number, Month YYYY, URL (if any)

11. Editor's Address

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

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

Joe Murdock	Sharp
Brian Smithson	Ricoh
Jerry Thrasher	Lexmark

12. Appendix A – TNC Architecture

12.1.1 TNC Roles

The TNC Architecture defines the following two required roles:

Access Requestor (AR): The role that access to a protected network in order to conduct activities on the network.

Policy Decision Point (PDP): The role that performs the decision-making regarding the AR's network access request, in light of the access policies.

The TNC Architecture defines the following three optional roles:

Policy Enforcement Point (PEP): The role that enforces the decisions of the PDP regarding network access – The PEP is the element which is connected to the AR.

Metadata Access Point (MAP): The role that stores and provides state information about ARs which may be useful to policy decision making and enforcement.

MAP Client (MAPC): The role that publishes or consumes state information about ARs to/from the MAP.

12.1.2 TNC Layers

The TNC Architecture defines the following three abstract layers:

Network Access Layer: Components whose main function pertains to traditional network connectivity and security. The TNC functions included in this layer are the Network Access Requestor (NAR), the Network Access Enforcer (NAE) and the Network Access Authority (NAA).

Integrity Evaluation Layer: Components whose function is to evaluate the overall integrity of the Access Requestor with respect to certain access policies, with input from the functions at the Integrity Measurement Layer. The TNC functions included in this layer are the TNC Client (TNCC) and the TNC Server (TNCS).

Integrity Measurement Layer: Components whose function is to collect and verify integrity-related information for a variety of security applications on the Access Requestor. The TNC functions included in this layer are the Integrity Measurement Collectors (IMCs) and the Integrity Measurement Verifiers (IMVs).

12.1.3 TNC Functions

The TNC Architecture defines a number of functions – see their definitions in section 2.3 of this document.

The required Access Requestor (AR) consists of the following functions: Network Access Requestor (NAR), TNC Client (TNCC), and Integrity Measurement Collector (IMC).

The required Policy Decision Point (PDP) consists of the following functions: Network Access Authority (NAA), TNC Server (TNCS), and Integrity Measurement Verifier (IMV).

The optional Policy Enforcement Point (PEP) consists of the following function: Network Access Enforcer (NAE).

The optional Metadata Access Point (MAP) consists of the following function: Metadata Access Point Server (MAPS).

The optional MAP Client consists of the following functions: Flow Controller and Sensor.

12.1.4 TNC Interfaces

The TNC Architecture defines the following interfaces:

Integrity Measurement Collector Interface (IF-IMC): The interface between Integrity Measurement Collectors (IMCs) and a TNC Client (TNCC).

Integrity Measurement Verifier Interface (IF-IMV): The interface between Integrity Measurement Verifier (IMVs) and a TNC Server (TNCS).

TNC Client-Server Interface (IF-TNCCS): The interface between the TNC Client (TNCC) and the TNC Server (TNCS) as it pertains to the exchange of integrity measurement data.

Vendor-Specific IMC-IMV Messages (IF-M): The interface that pertains to vendor-specific information exchange that may occur between IMCs and IMVs.

Network Authorization Transport Protocol (IF-T): The interface that pertains to the transportation of messages between the AR element and the PDP element.

Platform Trust Services Interface (IF-PTS): The interface that provides platform trust services to ensure that TNC components are trustworthy.

Policy Enforcement Point Interface (IF-PEP): The interface that allows the PDP to communicate with the PEP, especially allowing the PDP to instruct the PEP to isolate the AR during remediation and later grant it full network access once remediation is complete.

Metadata Access Point Interface (IF-MAP): The interface that allows elements in the TNC architecture to share and correlate stateful runtime metadata such as relationships of TNC components to endpoints, users, capabilities, roles, and attributes. IF-MAP provides publish, subscribe, and search interfaces between MAP Clients and the MAP. The data published and available via IF-MAP augments other sources of data for security related decision making.

12.1.5 TNC Support Profiles

The TNC family of specifications includes support profiles for aspects of network access control which are related to, but do not fall directly under, the TNC Architecture. In particular is the following:

Clientless Endpoint Support Profile (CESP) [TNC-CESP]: Outlines an approach and enforcement mechanisms to ensure interoperability and enforce compliance in environments where some endpoints lack a TNC Client. Many existing endpoints do not – or cannot – run a TNC Client to provide integrity information, yet still require access to a protected network.

13. Appendix X – Change History

13.1 5 December 2011

Editorial – Changed status to Interim Draft.
Editorial – Added one-line Abstract and Introduction as placeholders.
Editorial – Moved TNC Architecture details (not necessary to understanding this document) from mainline section 4.1 to new Appendix A – TNC Architecture, per IDS WG review.
Editorial – Revised section 4.3.4 to add field definitions for PB-PA message type format, per IDS WG review.
Editorial – Revised section 5.1 to add all HCD mandatory attributes, per IDS WG review and updated HCD spec.

13.2 4 August 2011

Initial version.

