

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>

1 Copyright © 2011 The Printer Working Group. All rights reserved.

2  
3 This document may be copied and furnished to others, and derivative works that comment  
4 on, or otherwise explain it or assist in its implementation may be prepared, copied,  
5 published and distributed, in whole or in part, without restriction of any kind, provided that  
6 the above copyright notice, this paragraph and the title of the Document as referenced  
7 below are included on all such copies and derivative works. However, this document itself  
8 may not be modified in any way, such as by removing the copyright notice or references  
9 to the IEEE-ISTO and the Printer Working Group, a program of the IEEE-ISTO.

10  
11 Title: *Hardcopy Device Health Assessment Trusted Network Connect Binding (HCD-TNC)*

12  
13 The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES,  
14 WHETHER EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY  
15 IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR  
16 PURPOSE.

17  
18 The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make  
19 changes to the document without further notice. The document may be updated, replaced  
20 or made obsolete by other documents at any time.

21  
22 The IEEE-ISTO takes no position regarding the validity or scope of any intellectual  
23 property or other rights that might be claimed to pertain to the implementation or use of  
24 the technology described in this document or the extent to which any license under such  
25 rights might or might not be available; neither does it represent that it has made any effort  
26 to identify any such rights.

27  
28 The IEEE-ISTO invites any interested party to bring to its attention any copyrights,  
29 patents, or patent applications, or other proprietary rights which may cover technology that  
30 may be required to implement the contents of this document. The IEEE-ISTO and its  
31 programs shall not be responsible for identifying patents for which a license may be  
32 required by a document and/or IEEE-ISTO Industry Group Standard or for conducting  
33 inquiries into the legal validity or scope of those patents that are brought to its attention.  
34 Inquiries may be submitted to the IEEE-ISTO by e-mail at: [ieee-isto@ieee.org](mailto:ieee-isto@ieee.org).

35  
36 The Printer Working Group acknowledges that the IEEE-ISTO (acting itself or through its  
37 designees) is, and shall at all times, be the sole entity that may authorize the use of  
38 certification marks, trademarks, or other special designations to indicate compliance with  
39 these materials.

40  
41 Use of this document is wholly voluntary. The existence of this document does not imply  
42 that there are no other ways to produce, test, measure, purchase, market, or provide other  
43 goods and services related to its scope.

44

## 45 **About the IEEE-ISTO**

46  
47 The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and  
48 flexible operational forum and support services. The IEEE-ISTO provides a forum not  
49 only to develop standards, but also to facilitate activities that support the implementation  
50 and acceptance of standards in the marketplace. The organization is affiliated with the  
51 IEEE (<http://www.ieee.org/>) and the IEEE Standards Association  
52 (<http://standards.ieee.org/>).  
53

54 For additional information regarding the IEEE-ISTO and its industry programs visit:

55  
56 <http://www.ieee-isto.org>.

57  
58

## 59 **About the IEEE-ISTO PWG**

60  
61 The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and  
62 Technology Organization (ISTO) with member organizations including printer  
63 manufacturers, print server developers, operating system providers, network operating  
64 systems providers, network connectivity vendors, and print management application  
65 developers. The group is chartered to make printers and the applications and operating  
66 systems supporting them work together better. All references to the PWG in this  
67 document implicitly mean “The Printer Working Group, a Program of the IEEE ISTO.” In  
68 order to meet this objective, the PWG will document the results of their work as open  
69 standards that define print related protocols, interfaces, procedures and conventions.  
70 Printer manufacturers and vendors of printer related software will benefit from the  
71 interoperability provided by voluntary conformance to these standards.  
72

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

76

77 For additional information regarding the Printer Working Group visit:

78  
79 <http://www.pwg.org>

80

81 Contact information:

82

83 The Printer Working Group  
84 c/o The IEEE Industry Standards and Technology Organization  
85 445 Hoes Lane  
86 Piscataway, NJ 08854  
87 USA  
88

89

90 **About the Imaging Device Security Working Group**

91

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

96

97 For additional information regarding IDS visit:

98

99 <http://www.pwg.org/ids>

100

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

104

## Table of Contents

105		
106	1. Introduction .....	7
107	2. Terminology .....	8
108	2.1 Conformance Terminology .....	8
109	2.2 Printing Terminology .....	8
110	2.3 TNC Terminology .....	8
111	3. Requirements .....	11
112	3.1 Rationale for Title of Standard .....	11
113	3.2 Use Cases .....	11
114	3.3 Out of Scope .....	11
115	3.4 Design Requirements .....	11
116	4. TNC Protocol Overview .....	12
117	4.1 TNC Architecture .....	12
118	4.2 TNC Transport Protocol .....	12
119	4.3 PB-TNC Message Syntax .....	13
120	4.3.1 PB-TNC Message Encapsulation .....	13
121	4.3.2 PB-TNC Message Header Format .....	13
122	4.3.3 PB-TNC Message Format .....	14
123	4.3.4 PB-PA Message Type Format .....	15
124	4.4 PA-TNC Message Syntax .....	16
125	4.4.1 Overview of PB-TNC Message with PA-TNC Message .....	16
126	4.4.2 PA-TNC Message Header Format .....	16
127	4.4.3 PA-TNC Attribute Format .....	17
128	5. HCD Statement of Health for TNC Protocol .....	18
129	5.1 Mandatory Attributes .....	18
130	5.1.1 AttributesNaturalLanguage .....	18
131	5.1.2 MachineTypeModel .....	18
132	5.1.3 VendorName .....	18
133	5.1.4 VendorSMICode .....	19
134	5.1.5 DefaultPasswordEnabled .....	19
135	5.1.6 FirewallSetting .....	20
136	5.1.7 ForwardingEnabled .....	21
137	5.1.8 FirmwareName .....	21
138	5.1.9 FirmwarePatches .....	21
139	5.1.10 FirmwareStringVersion .....	22
140	5.1.11 FirmwareVersion .....	22
141	5.1.12 UserApplicationEnabled .....	22
142	5.1.13 UserApplicationPersistenceEnabled .....	22
143	5.2 Conditionally Mandatory Attributes .....	23
144	5.3 Optional Attributes .....	23
145	6. Conformance Requirements .....	24
146	7. Internationalization Considerations .....	24
147	8. Security Considerations .....	24
148	9. IANA Considerations .....	24

149 10. References.....25  
150 10.1 Normative References.....25  
151 10.2 Informative References .....25  
152 11. Editor’s Address.....25  
153 12. Appendix A – TNC Architecture .....26  
154 12.1.1 TNC Roles .....26  
155 12.1.2 TNC Layers.....26  
156 12.1.3 TNC Functions .....27  
157 12.1.4 TNC Interfaces.....27  
158 12.1.5 TNC Support Profiles .....28  
159 13. Appendix X – Change History .....28  
160 13.1 5 December 2011 .....28  
161 13.2 4 August 2011 .....28

**List of Figures**

**No table of figures entries found.**

**List of Tables**

**No table of figures entries found.**

170 **1. Introduction**

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

174  
175  
176

177

## 178 2. Terminology

### 179 2.1 Conformance Terminology

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

### 183 2.2 Printing Terminology

184 Normative definitions and semantics of printing terms are imported from IETF Printer MIB  
185 v2 [RFC3805], IETF Finisher MIB [RFC3806], and IETF IPP/1.1 [RFC2911].  
186

### 187 2.3 TNC Terminology

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

191  
192 **Access Requestor (AR):** Within the TNC framework for endpoint integrity, the AR is the  
193 entity seeking connectivity to network that implements the TNC Architecture. The AR  
194 consists of three main components, namely the NAR, TNC Client and the IMC. See  
195 glossary for the definition of these components.

196  
197 **Clientless Endpoint (CE):** Within the TNC framework, this is a network endpoint without  
198 a TNC Client (TNCC).

199  
200 **Endpoint Integrity Information:** This is information provided by IMCs describing the  
201 status and configuration of the AR.

202  
203 **Flow Controller:** The Flow Controller function makes and enforces decisions about  
204 network activities utilizing information from the MAP. Flow Controllers take action (e.g.  
205 block) on network flows (i.e. network traffic associated with a particular AR, device, user,  
206 etc.) based on data obtained via IF-MAP. Examples include: internal firewalls, rate  
207 limiters, and proxies.

208  
209 **Integrity Information:** The set of platform specific information that makes up a Trusted  
210 Platform. This ranges from information about a platform's hardware components, TPM  
211 information (e.g. versions), PCRs, peripherals, Trusted Building Blocks, OS/Kernel,  
212 drivers, Applications, Anti-Virus information and others. Each specific use-case



213 determines which information set will be of interest. As such, it is expected that for a given  
214 situation these will be pre-determined or pre-configured by an authorized entity (e.g. IT  
215 administrator).  
216

217 **Integrity Measurement Collector (IMC):** An IMC is a software component that runs on  
218 an Access Requestor (AR), measuring certain aspects of the AR's integrity, including  
219 software versions, patches, Anti-Virus and others. An IMC may use the TCG Platform  
220 Trust Service (PTS) to obtain integrity information regarding every component of the  
221 platform on which the IMC sits. Multiple IMCs may reside on a single AR.  
222

223 **Integrity Measurement Verifier (IMV):** An IMV is the component of the PDP that verifies  
224 a particular aspect of the AR's integrity, based on measurements received from an IMCs  
225 and/or other data. Multiple IMVs may reside on a single PDP.  
226

227 **Isolation:** The action of separating an Access Requestor onto a separate network –  
228 virtual or physical – possibly, though not necessarily, for the purposes of performing  
229 Remediation on that AR.  
230

231 **Metadata Access Point (MAP):** The role in the TNC framework of a broker/server to  
232 which metadata may be published and from which metadata may be searched and  
233 subscribed to using the IF-MAP protocol.  
234

235 **Metadata Access Point Client (MAPC):** The role in the TNC framework of an element  
236 which publishes metadata to or searches/subscribes to metadata from a MAP.  
237

238 **Metadata Access Point Server (MAPS):** The component of the MAP providing the  
239 function that allows other TNC components to publish, subscribe to, and search metadata.  
240

241 **Network Access Authority (NAA):** The NAA is the network layer function of the PDP  
242 that decides whether an NAR should be granted access to a network.  
243

244 **Network Access Enforcer (NAE):** The NAE is the network layer function of the PEP that  
245 consumes and enforces access control policies from an NAA.  
246

247 **Network Access Requestor (NAR):** The NAR is the component of the Access  
248 Requestor (AR) responsible for negotiating and establishing network access onto a given  
249 network. The NAR is expected to implement network layer protocols, covering security,  
250 message transport and others. In the context of 802.1X, the NAR can be identified as the  
251 Supplicant.  
252

253 **Platform Authentication:** The act of verifying both the proof-of-identity and integrity-  
254 status of a given platform.  
255

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

261  
262 **Policy Decision Point (PDP):** The PDP is an entity evaluating the status of a TNC Client  
263 (seeking network connectivity) and deciding upon some network-related action to be  
264 enforced by the PEP. The PDP embodies the security and integrity related policies  
265 governing the network.

266  
267 **Policy Enforcement Point (PEP):** The PEP is a component within the TNC Architecture  
268 that controls access to a protected network, whose policies are implemented through a  
269 Policy Decision Point (PDP). The PEP enforces the decision of the PDP.

270  
271 **Sensor:** The Sensor function monitors network activities and publishes information to the  
272 MAP via IF-MAP. Examples include: intrusion detection devices, network virus detection  
273 devices, layer 3 traffic monitors, and application traffic scanners.

274  
275 **TNC Client (TNCC):** The TNCC is the software component on the Access Requestor  
276 (AR) that aggregates integrity measurements (from IMCs), assists the management of the  
277 Integrity Check Handshakes and assists in the measurement and reporting of platform  
278 and IMC integrity.

279  
280 **TNC Server (TNCS):** The TNCS is the component on the PDP that manages the flow of  
281 messages between Integrity Measurement Collectors (IMC) and Integrity Measurement  
282 Verifiers (IMV), gathers recommendations from IMVs, and combines those  
283 recommendations (based on policy) into an overall TNCS Action Recommendation to the  
284 NAA.

285

286 **3. Requirements**

287 **3.1 Rationale for Title of Standard**

288 Provide a rationale for the standard.

289 **3.2 Use Cases**

290 Provide use cases for the standard.

291 **3.3 Out of Scope**

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

293 **3.4 Design Requirements**

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

295

## 296 **4. TNC Protocol Overview**

### 297 **4.1 TNC Architecture**

298 The TNC Architecture [TNC-ARCH] is intentionally general, in order to accommodate a  
299 wide variety of network devices, topologies and implementation configurations – it  
300 includes multiple roles, functions, and interfaces. A detailed discussion of the TNC  
301 Architecture is in Appendix A – TNC Architecture.  
302

### 303 **4.2 TNC Transport Protocol**

304 Put brief summary here of:

305 (a) IETF PT-EAP [PT-EAP] for assessment *\*before\** an IP address is assigned (the  
306 endpoint is joining the network);

307 (b) IETF PT-TLS [PT-TLS] for assessment *\*after\** an IP address is assigned (the endpoint  
308 is already on the network).  
309

310 Also put a brief summary here of the relevant TCG TNC transport specs.  
311

### 312 4.3 PB-TNC Message Syntax

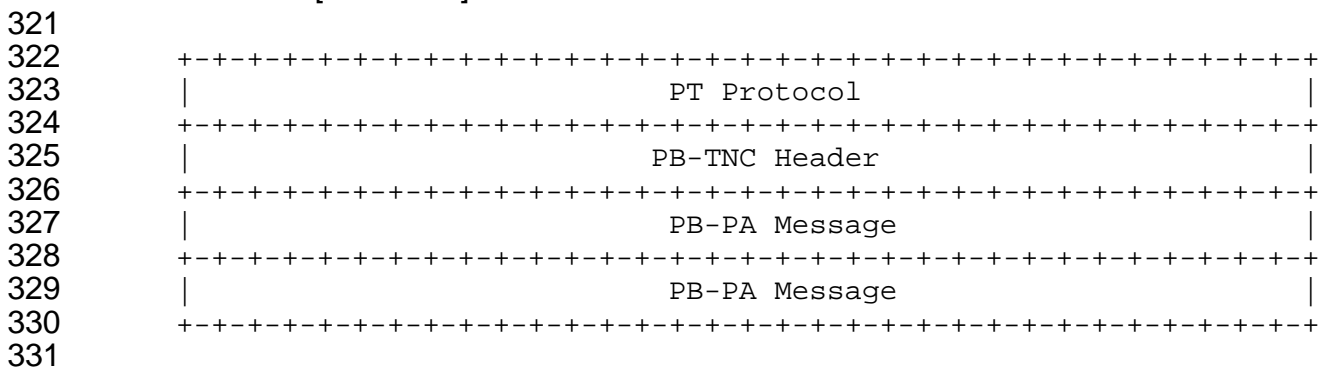
313 Put a brief summary here of:

314 (a) IETF PA-TNC [RFC5792] which is identical to TCG TNC IF-M: TLV Binding  
315 [TNC-IFM-TLV];

316 (b) IETF PB-TNC [RFC5793] which is identical to TCG TNC IF-TNCCS: TLV Binding  
317 [TNC-TNCCS-TLV].

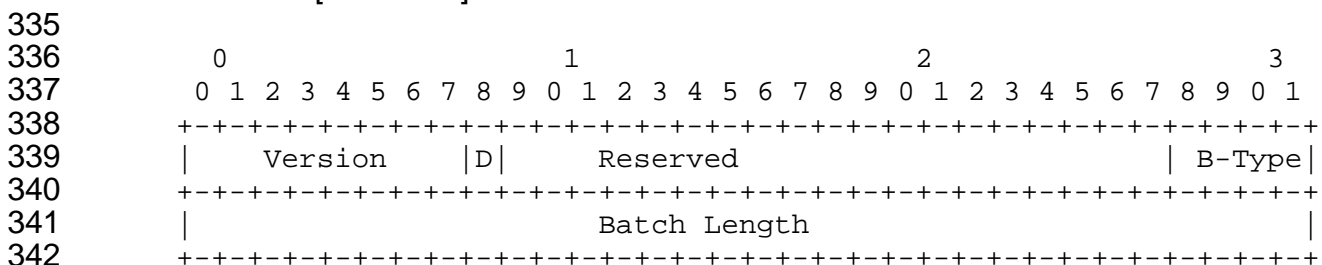
#### 318 4.3.1 PB-TNC Message Encapsulation

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



#### 332 4.3.2 PB-TNC Message Header Format

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



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

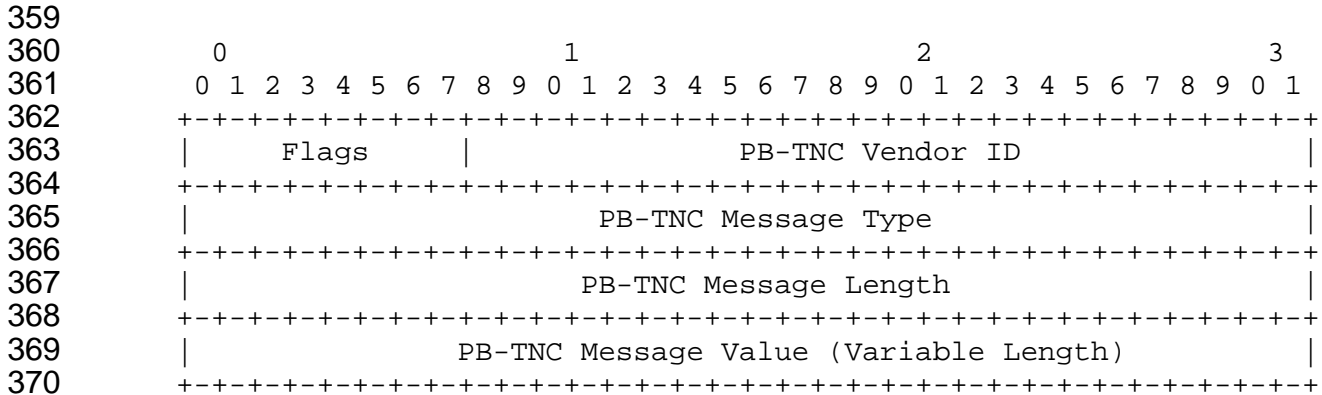
345  
346 **Directionality** (1 bit): Value MUST be 0 for a TNC Client request for [RFC5793]  
347 conformance.

348  
349 **Reserved** (19 bits): Value MUST be 0 for [RFC5793] conformance.  
350

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

### 356 4.3.3 PB-TNC Message Format

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



371  
 372 **Flags** (8 bits): Value of this field affects processing of the associated message. Bit 0  
 373 (0x80) is the NOSKIP flag – if set to 1, then TNC Servers (Validators) MUST not process  
 374 this message if this Message Type is NOT supported. All other bits are reserved and  
 375 MUST be set to 0 for [RFC5793] conformance.

376  
 377 **Vendor ID** (24 bits): Value MUST be 24-bit SMI Private Enterprise Number of the party  
 378 who owns this Message Type namespace. Value MUST be 0 for IETF namespace,  
 379 21911 for TCG namespace, or 2699 for PWG namespace. Value of 0xfffff is reserved  
 380 and MUST not be used.

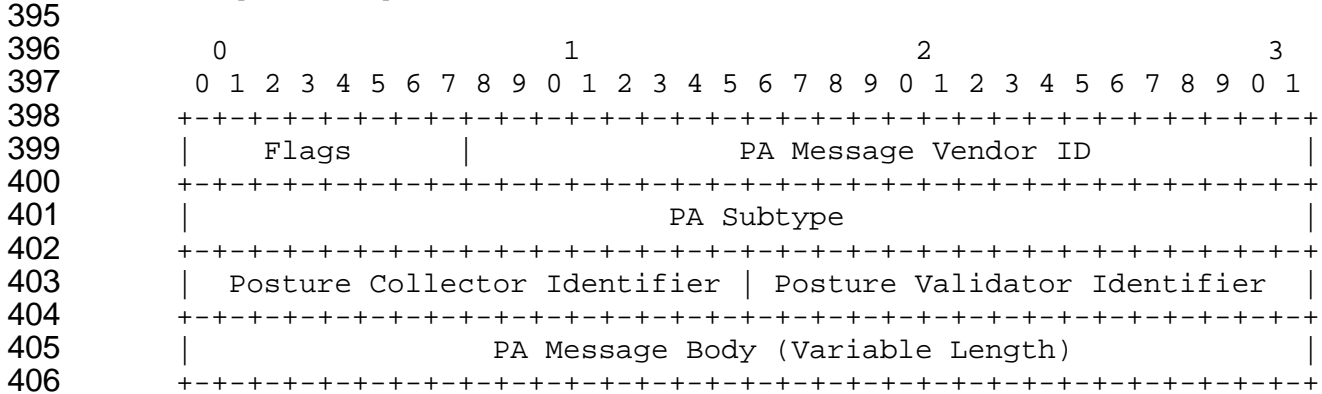
381  
 382 **Message Type** (32 bits): Value MUST be an IETF, TCG, or PWG standard message  
 383 type. Value of 0xffffffff is reserved and MUST not be used. IETF standard PB-TNC  
 384 message types are defined in section 4.3 of [RFC5793] and registered with IANA. A TNC  
 385 Client will send a PB-PA (1) message type.

386  
 387 **Message Length** (32 bits): Value is the length of the PB-TNC Message contained in the  
 388 Message Value field.

389  
 390 **Message Value** (variable length): Value specifies the contents of the PB-TNC Message.  
 391

### 392 4.3.4 PB-PA Message Type Format

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



408 **Flags** (8 bits): Value of this field affects the delivery of this message to the Posture  
409 Collectors. Bit 0 (0x80) is the EXCL (exclusive) flag – if set to 1, then the receiving  
410 Posture Broker Client SHOULD deliver this message only to the Posture Collector  
411 specified by the Posture Collector Identifier field – however if that Posture Collector has  
412 not expressed an interest in PA messages with this Vendor ID and PA Subtype, then the  
413 message SHOULD be silently discarded. All other bits are reserved and MUST be set to  
414 0 for [RFC5793] conformance.

415  
416 **PA Message Vendor ID** (24 bits): Value MUST be 24-bit SMI Private Enterprise Number  
417 of the party who owns this Attribute Type namespace. Value MUST be 0 for IETF  
418 namespace, 0x5597 (21911) for TCG namespace, or 0x0A8B (2699) for PWG  
419 namespace. Value of 0xfffff is reserved and MUST not be used.

420  
421 **PA Subtype** (32 bits): Value identifies the type of PA message contained in the PA  
422 Message Body field. IANA maintains a registry of PA subtypes. New vendor-specific PA  
423 subtypes (those used with a non-zero PA Message Vendor ID) may be defined and  
424 employed by vendors without IETF or IANA involvement. Value of 0xfffff is reserved and  
425 MUST not be used.

426  
427 **Posture Collector Identifier** (16 bits): Value of this field contains the identifier of the  
428 Posture Collector associated with this PA message. The Posture Broker Client MUST  
429 assign one or more Posture Collector Identifier values (but not 0xffff) to each Posture  
430 Collector involved in a message exchange.

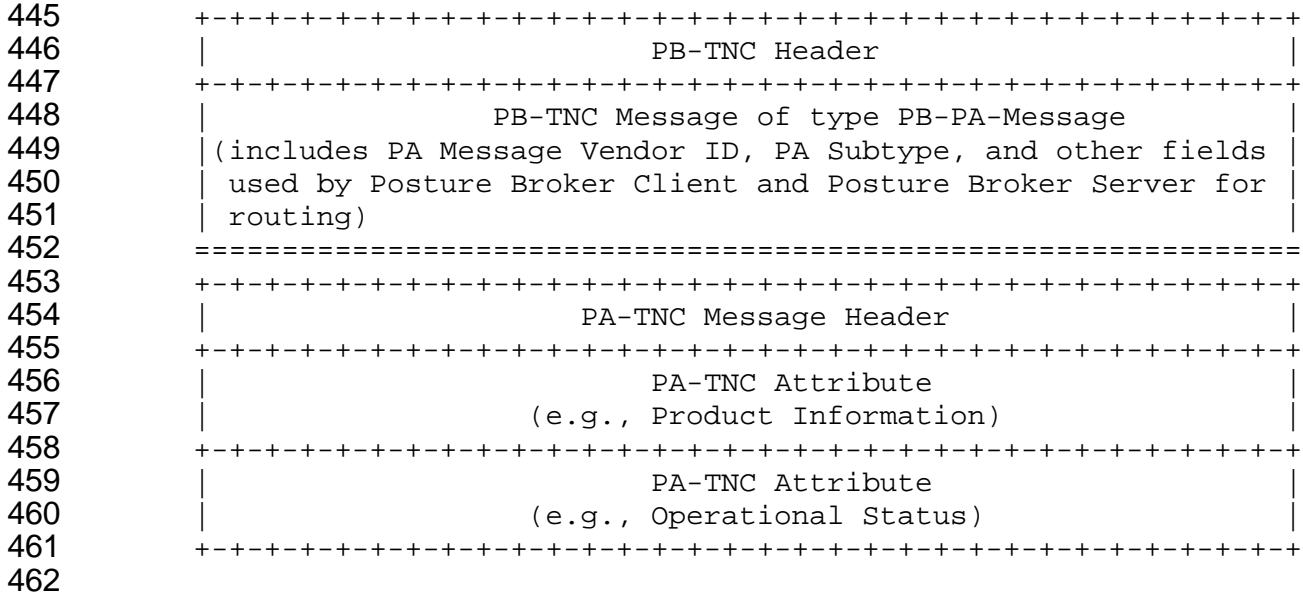
431  
432 **Posture Validator Identifier** (16 bits): Value of this field contains the identifier of the  
433 Posture Validator associated with this PA message. The Posture Broker Server MUST  
434 assign a unique Posture Validator Identifier value (but not 0xffff) to each Posture Validator  
435 involved in a message exchange.

436  
 437 **PA Message Body** (variable length): Value specifies the contents of the PB-PA  
 438 Message.  
 439

440 **4.4 PA-TNC Message Syntax**

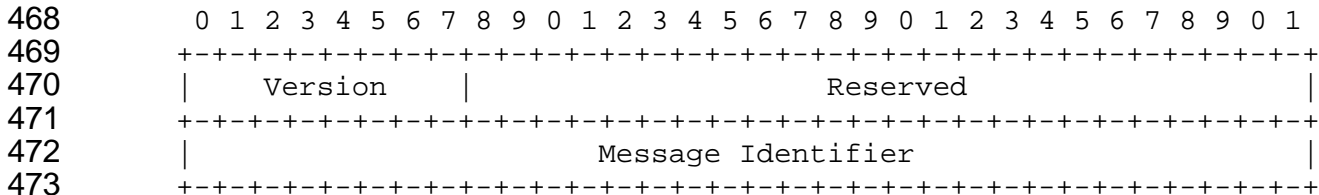
441 **4.4.1 Overview of PB-TNC Message with PA-TNC Message**

442 The following PA-TNC message within a PB-TNC message format diagram is excerpted  
 443 from section 3.2 IETF PA-TNC [RFC5792]:  
 444



463 **4.4.2 PA-TNC Message Header Format**

464 The following PA-TNC message header format diagram is excerpted from section 3.6 of  
 465 IETF PA-TNC [RFC5792]:  
 466



475 **Version** (8 bits): Value MUST be 1 for [RFC5792] conformance.  
 476

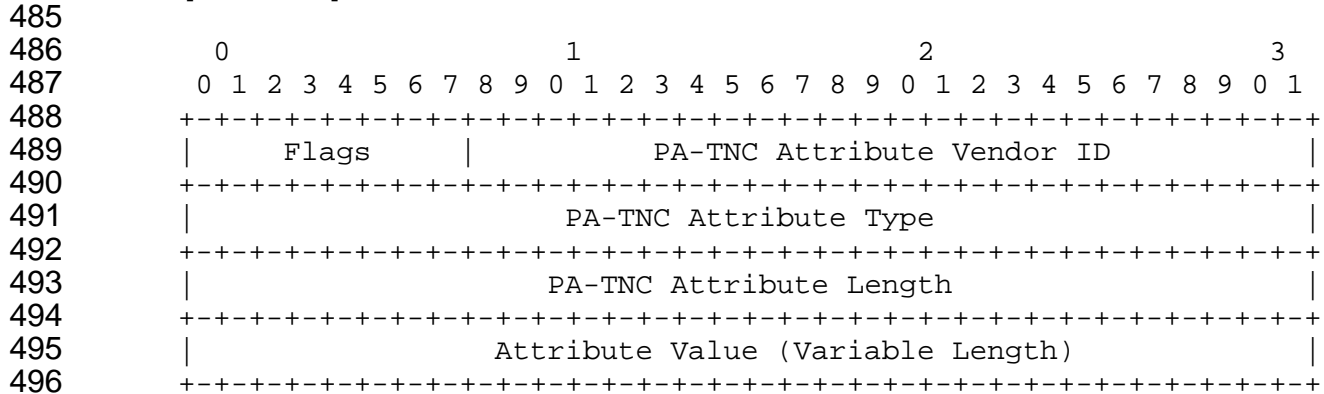


477 **Reserved** (24 bits): Value MUST be 0 for [RFC5792] conformance.

478  
479 **Message Identifier** (32 bits): Value uniquely identifies this message within this  
480 assessment.  
481

#### 482 4.4.3 PA-TNC Attribute Format

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



497  
498 **Flags** (8 bits): Value of this field affects processing of the associated attribute. Bit 0  
499 (0x80) is the NOSKIP flag – if set to 1, then TNC Servers (Validators) MUST not process  
500 any attribute in the PA-TNC message if this attribute is NOT supported. All other bits are  
501 reserved and MUST be set to 0 for [RFC5792] conformance.

502  
503 **Vendor ID** (24 bits): Value MUST be 24-bit SMI Private Enterprise Number of the party  
504 who owns this Attribute Type namespace. Value MUST be 0 for IETF namespace,  
505 0x5597 (21911) for TCG namespace, or 0x0A8B (2699) for PWG namespace. Value of  
506 0xffffffff is reserved and MUST not be used.

507  
508 **Attribute Type** (32 bits): Value is the type of the attribute in the Attribute Value field.  
509 Value of 0xffffffff is reserved and MUST not be used.

510  
511 **Attribute Length** (32 bits): Value is the length in octets of the entire PA-TNC attribute,  
512 including the PA-TNC Attribute Header – therefore, the value MUST always be at least 12.

513  
514 **Attribute Value** (variable length): Value specifies the contents of the PA-TNC attribute.

515

## 516 **5. HCD Statement of Health for TNC Protocol**

517 This section defines how the specified Hardcopy Device Health Assessment Attributes  
518 [HCD-ATR] are to be used with the TNC Protocol, in particular with IETF PB-TNC  
519 [RFC5793] carrying IETF PA-TNC [RFC5792] messages.

### 520 **5.1 Mandatory Attributes**

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

#### 523 **5.1.1 AttributesNaturalLanguage**

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

526  
527 Flags: 0x00 (SKIP)  
528 Vendor ID: 0x0A8B (2699 – PWG)  
529 Attribute Type: 0x01 (1)  
530 Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)  
531 Attribute Value: A variable length natural language tag that conforms to [RFC5646]  
532

#### 533 **5.1.2 MachineTypeModel**

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

536  
537 Flags: 0x00 (SKIP)  
538 Vendor ID: 0x0A8B (2699 – PWG)  
539 Attribute Type: 0x02 (2)  
540 Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)  
541 Attribute Value: A variable length string containing the machine type and model of this  
542 device, which SHOULD be consistent with the values of: (a) sysDescr in IETF MIB-II  
543 [RFC1213]; and (b) hrDeviceDescr in IETF Host Resources MIB v2 [RFC2790] for the row  
544 with hrDeviceType equal to hrDevicePrinter.  
545

#### 546 **5.1.3 VendorName**

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

549 Flags: 0x00 (SKIP)  
550 Vendor ID: 0x0A8B (2699 – PWG)  
551 Attribute Type: 0x03 (3)  
552 Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)  
553 Attribute Value: A variable length string containing the manufacturer name of this device,  
554 which SHOULD be consistent with the values of: (a) sysDescr in IETF MIB-II [RFC1213];  
555 and (b) hrDeviceDescr in IETF Host Resources MIB v2 [RFC2790] for the row with  
556 hrDeviceType equal to hrDevicePrinter.

#### 557 **5.1.4 VendorSMICode**

558 This integer attribute specifies the globally unique 24-bit SMI code assigned by IANA of  
559 the manufacturer this device, which SHOULD be consistent with the value of sysObjectID  
560 in IETF MIB-II [RFC1213]. The PA-TNC Attribute fields (see section 4.4.3) are set to:

561  
562 Flags: 0x00 (SKIP)  
563 Vendor ID: 0x0A8B (2699 – PWG)  
564 Attribute Type: 0x04 (4)  
565 Attribute Length: 0x0F (decimal 12 plus length of attribute value)  
566 Attribute Value (32-bits): fixed length 8-bit reserved flags followed by 24-bit SMI code of  
567 the manufacturer of this device (unpadded).

#### 568 **5.1.5 DefaultPasswordEnabled**

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

573  
574 This boolean attribute specifies whether or not any factory default administrator  
575 passwords or other credentials are currently set on this device. If set to to '0' (false), then  
576 no administrator passwords or other credentials are set to factory defaults. The PA-TNC  
577 Attribute fields (see section 4.4.3) are set to:

578  
579 Flags: 0x00 (SKIP)  
580 Vendor ID: 0x0A8B (2699 – PWG)  
581 Attribute Type: 0x14 (20)  
582 Attribute Length: 0x10 (decimal 12 plus length of attribute value)  
583 Attribute Value (32-bits): fixed length integer field contains either '0' or '1'.

584 **5.1.6 FirewallSetting**

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

588

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

591

592 Flags: 0x00 (SKIP)

593 Vendor ID: 0x0A8B (2699 – PWG)

594 Attribute Type: 0x15 (21)

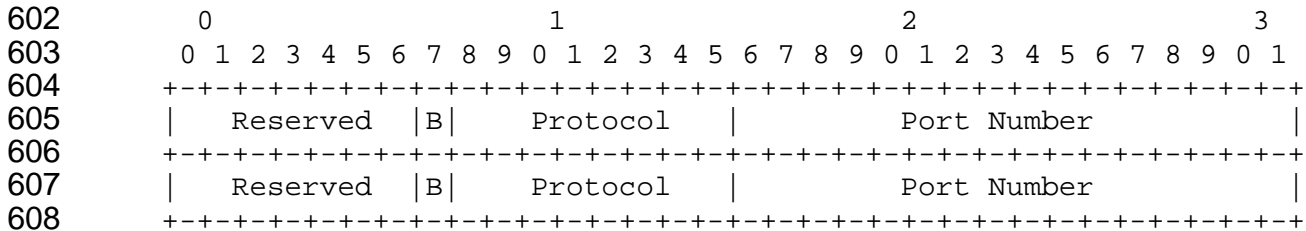
595 Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)

596 Attribute Value: A variable length firewall setting array that conforms to the following  
 597 encoding.

598

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

601



609

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

612

613 **B Flag** (Blocked or Allowed Port): This single-bit field specifies whether the following port  
 614 is blocked or allowed. This bit MUST be set to 1 if the protocol and port combination is  
 615 blocked. Otherwise, this field MUST be set to 0. Posture Collectors MUST NOT provide  
 616 a mixed list of blocked and non-blocked ports for a particular protocol.

617

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

620

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

### 625 5.1.7 ForwardingEnabled

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

630  
631 This boolean attribute specifies whether this device is forwarding traffic between any  
632 network interfaces. If set to to '0' (false), then this device MUST NOT forward any traffic  
633 between any network interfaces (including so-called loopback in and out of the same  
634 network interface). Note that these are the rigorous semantics specified for Forwarding  
635 Enabled in section 4.2.11 of [RFC5792]. The PA-TNC Attribute fields (see section 4.4.3)  
636 are set to:

637  
638 Flags: 0x00 (SKIP)  
639 Vendor ID: 0x0A8B (2699 – PWG)  
640 Attribute Type: 0x16 (22)  
641 Attribute Length: 0x10 (decimal 12 plus length of attribute value)  
642 Attribute Value (32-bits): fixed length integer field contains either '0' or '1'.

### 643 5.1.8 FirmwareName

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

646  
647 Flags: 0x00 (SKIP)  
648 Vendor ID: 0x0A8B (2699 – PWG)  
649 Attribute Type: 0x3C (60)  
650 Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)  
651 Attribute Value: A variable length string containing the firmware name for this device.

### 652 5.1.9 FirmwarePatches

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

655  
656 Flags: 0x00 (SKIP)  
657 Vendor ID: 0x0A8B (2699 – PWG)  
658 Attribute Type: 0x3D (61)  
659 Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)  
660 Attribute Value: A variable length string containing the list of all firmware patches (from  
661 the oldest to the newest) for this device.

### 662 **5.1.10 FirmwareStringVersion**

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

665  
666 Flags: 0x00 (SKIP)  
667 Vendor ID: 0x0A8B (2699 – PWG)  
668 Attribute Type: 0x3E (62)  
669 Attribute Length: 0x0C+length (decimal 12 plus length of attribute value)  
670 Attribute Value: A variable length string containing the firmware string version for this  
671 device.

### 672 **5.1.11 FirmwareVersion**

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

676  
677 Flags: 0x00 (SKIP)  
678 Vendor ID: 0x0A8B (2699 – PWG)  
679 Attribute Type: 0x3F (63)  
680 Attribute Length: 0x1C+length (decimal 12 plus length of attribute value)  
681 Attribute Value (16 bits): A fixed length octet string containing the firmware build version  
682 for this device, which MAY conform to section 4.2.3 “Numeric Version” of IETF PA-TNC  
683 [RFC5292].

### 684 **5.1.12 UserApplicationEnabled**

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

690  
691 Flags: 0x00 (SKIP)  
692 Vendor ID: 0x0A8B (2699 – PWG)  
693 Attribute Type: 0x64 (100)  
694 Attribute Length: 0x10 (decimal 12 plus length of attribute value)  
695 Attribute Value (32-bits): fixed length integer field contains either ‘0’ or ‘1’.

### 696 **5.1.13 UserApplicationPersistenceEnabled**

697 This boolean attribute specifies whether or not the ability is supported and currently  
698 enabled for user dynamically downloaded applications to persist outside the boundaries of

699 a single Job on this device. If set to to '0' (false), then user dynamically downloaded  
700 applications MUST deleted when their associated original Job reaches completion. The  
701 PA-TNC Attribute fields (see section 4.4.3) are set to:

702

703 Flags: 0x00 (SKIP)

704 Vendor ID: 0x0A8B (2699 – PWG)

705 Attribute Type: 0x65 (101)

706 Attribute Length: 0x10 (decimal 12 plus length of attribute value)

707 Attribute Value (32-bits): fixed length integer field contains either '0' or '1'.

708

## 709 **5.2 Conditionally Mandatory Attributes**

710 [to be supplied]

## 711 **5.3 Optional Attributes**

712 [to be supplied]

713

714

715 **6. Conformance Requirements**

716 Provide a list of conformance requirements for the standard.

717 **7. Internationalization Considerations**

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

720 **8. Security Considerations**

721 Provide security considerations for this specification.

722 **9. IANA Considerations**

723 Provide IANA registration information for this specification.

724



725 **10. References**

726 **10.1 Normative References**

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

729 **10.2 Informative References**

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

732 **11. Editor's Address**

733

734 **Ira McDonald**

735 High North Inc

Email: [blueroofmusic@gmail.com](mailto:blueroofmusic@gmail.com)

736 PO Box 221

737 Grand Marais, MI 49839

Phone: +1-906-494-2434

738 USA

739

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

742

Joe Murdock

Sharp

Brian Smithson

Ricoh

Jerry Thrasher

Lexmark

743

744

## 745 **12. Appendix A – TNC Architecture**

### 746 **12.1.1 TNC Roles**

747 The TNC Architecture defines the following two required roles:

748

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

751

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

754

755 The TNC Architecture defines the following three optional roles:

756

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

759

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

762

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

### 765 **12.1.2 TNC Layers**

766 The TNC Architecture defines the following three abstract layers:

767

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

772

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

777

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

### 782 12.1.3 TNC Functions

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

785  
786 The required Access Requestor (AR) consists of the following functions: Network Access  
787 Requestor (NAR), TNC Client (TNCC), and Integrity Measurement Collector (IMC).

788  
789 The required Policy Decision Point (PDP) consists of the following functions: Network  
790 Access Authority (NAA), TNC Server (TNCS), and Integrity Measurement Verifier (IMV).

791  
792 The optional Policy Enforcement Point (PEP) consists of the following function: Network  
793 Access Enforcer (NAE).

794  
795 The optional Metadata Access Point (MAP) consists of the following function: Metadata  
796 Access Point Server (MAPS).

797  
798 The optional MAP Client consists of the following functions: Flow Controller and Sensor.

### 799 12.1.4 TNC Interfaces

800 The TNC Architecture defines the following interfaces:

801  
802 **Integrity Measurement Collector Interface (IF-IMC):** The interface between Integrity  
803 Measurement Collectors (IMCs) and a TNC Client (TNCC).

804  
805 **Integrity Measurement Verifier Interface (IF-IMV):** The interface between Integrity  
806 Measurement Verifier (IMVs) and a TNC Server (TNCS).

807  
808 **TNC Client-Server Interface (IF-TNCCS):** The interface between the TNC Client (TNCC)  
809 and the TNC Server (TNCS) as it pertains to the exchange of integrity measurement data.

810  
811  
812 **Vendor-Specific IMC-IMV Messages (IF-M):** The interface that pertains to vendor-  
813 specific information exchange that may occur between IMCs and IMVs.

814  
815 **Network Authorization Transport Protocol (IF-T):** The interface that pertains to the  
816 transportation of messages between the AR element and the PDP element.

817  
818 **Platform Trust Services Interface (IF-PTS):** The interface that provides platform trust  
819 services to ensure that TNC components are trustworthy.

820

821 **Policy Enforcement Point Interface (IF-PEP):** The interface that allows the PDP to  
822 communicate with the PEP, especially allowing the PDP to instruct the PEP to isolate the  
823 AR during remediation and later grant it full network access once remediation is complete.  
824

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

### 831 **12.1.5 TNC Support Profiles**

832 The TNC family of specifications includes support profiles for aspects of network access control which are  
833 related to, but do not fall directly under, the TNC Architecture. In particular is the following:  
834

835 **Clientless Endpoint Support Profile (CESP) [TNC-CESP]:** Outlines an approach and  
836 enforcement mechanisms to ensure interoperability and enforce compliance in  
837 environments where some endpoints lack a TNC Client. Many existing endpoints do not –  
838 or cannot – run a TNC Client to provide integrity information, yet still require access to a  
839 protected network.  
840

## 841 **13. Appendix X – Change History**

### 842 **13.1 5 December 2011**

843 Editorial – Changed status to Interim Draft.

844 Editorial – Added one-line Abstract and Introduction as placeholders.

845 Editorial – Moved TNC Architecture details (not necessary to understanding this  
846 document) from mainline section 4.1 to new Appendix A – TNC Architecture, per IDS WG  
847 review.

848 Editorial – Revised section 4.3.4 to add field definitions for PB-PA message type format,  
849 per IDS WG review.

850 Editorial – Revised section 5.1 to add all HCD mandatory attributes, per IDS WG review  
851 and updated HCD spec.

### 852 **13.2 4 August 2011**

853 Initial version.