January 6, 2014

Candidate Standard 5110.1-2014

The Printer Working Group

PWG Hardcopy Device Health Assessment Attributes

Status: Approved

Abstract: This standard defines a set of attributes for Hardcopy Devices (HCDs) that may be used in the various network health assessment protocols to measure the fitness of a HCD to attach to the network.

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

This document is available electronically at:
ftp://ftp.pwg.org/pub/pwg/candidates/cs-idsattributes11-20140106-5110.1.doc
ftp://ftp.pwg.org/pub/pwg/candidates/cs-idsattributes11-20140106-5110.1.pdf

Title: *PWG Hardcopy Device Health Assessment Attributes*

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

IDS Web Page:

http://www.pwg.org/ids

IDS Mailing List:

ids@pwg.org

Instructions for subscribing to the IDS mailing list can be found at the following link:

http://www.pwg.org/mailhelp.html

Those interested in this specification are encouraged to join the IDS Mailing List and to participate in any discussions clarifications or review of this specification. Not that, to reduce spam, the mailing list rejects mail from non-subscriber; you must subscribe to the mailing list to be able to send a question or comment to the mailing list.

Table of Contents

1. Introduction

Many corporate network and security administrators are beginning to deploy various security policy enforcement mechanisms that measure the "health" of a networked device being attached to the network infrastructure in addition to merely authenticating the user or device. The goal of these health assessment mechanisms is to provide a level of assurance that the device being granted access to network resources will do no harm to the network or other networked devices. For PCs, servers, etc.; these health assessment schemes allow the administrator to access the condition of the device's operating system, anti-virus program, personal firewall, and other attributes of the device to ensure that they are in compliance with the security policy for the network.

Currently, Hardcopy Devices do not participate in any of these protocols and are allowed to bypass health assessment when attaching to the network. In many health assessment schemes, this is merely the entry of the device's MAC or IP address into an exception table. This, however, results in a vulnerability in the network assessment scheme as it is fairly simple for the MAC or IP address of the excepted HCD to be spoofed by another device that would normally be subject to the health assessment.

2. Terminology

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

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

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.

Boolean – Boolean has the set of values (value space) required to support the mathematical concept of binary-valued logic:{true, false}. [XML-SCHEMA2]

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]

Integer – 32-bit unsigned value.

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

OctetArray – Variable number of octets containing binary data. [RFC5792]

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.

String – OctetArray that contains a human readable text encoded in UTF-8 [RFC3629] transformation format. [RFC5792]

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 Datatype Terminology

Normative definitions and semantics of the following standard abstract datatypes are imported from W3C XML Schema Part 2: Datatypes Second Edition [XML-SCHEMA2]. These XML datatypes in turn are normatively mapped by this specification to their corresponding SNMP MIB datatypes.

Table 1 – Standard Abstract Datatypes (XML, SNMP)

HCD Datatype	XML Datatype	XML Reference	SNMP Datatype	SNMP Reference	Description
Boolean	boolean	Section 3.3.2	TruthValue	[RFC2579]	binary true/false
OctetArray	hexBinary	Section 3.2.15	OCTET STRING	[RFC2578]	Variable or fixed length Array of octets. Array length must be specified as a separate integer entry in a protocol binding
Integer	int	Section 3.4.17	Integer32	[RFC2578]	signed 32-bit integer
String	string	Section 3.3.1	SnmpAdminString or DisplayString	[RFC3411] [RFC2579]	UTF-8 [RFC3629] - messages US-ASCII [ISO646] - keywords

2.4 Acronyms

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

FTP – File Transfer Protocol

HCD – Hardcopy Device

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

IANA – Internet Assigned Numbers Authority

IETF – Internet Engineering Task Force

IP – Internet Protocol

IPP – Internet Printing Protocol

ISMS – Information Security Management System

IT – Information Technology

LAA – Locally Administered Address

LDAP – Lightweight Directory Access Protocol

MAC – Media Access Control

NTP – Network Time Protocol

PA-TNC – Posture Attribute – Trusted Network Connect

PC – Personal Computer

PSTN – Public Switched Telephone Network

RTC – Real Time Clock

PWG – Printer Working Group

SMI – Structure of Management Information

SSL – Secure Sockets Layer

UAA – Universally Administered Address

URI – Universal Resource Indicator

USB – Universal Serial Bus

UTF – Unicode Transformation Format

3. Requirements (Informative)

3.1 Rationale For HCD Health Assessment Attributes

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

3.2 Use Cases For HCD Health Assessment Attributes

3.2.1 Managed IT Environment Using Health Assessment Protocols For Desktops and Laptops

A corporate IT department has decided to implement a network health assessment infrastructure as part of a rollout of laptop and desktop refresh for the company's employees. The motivation behind the decision to implement an assessment protocol was driven by the increasing number of laptops used by employees that were used away from the office on unmanaged networks and only occasionally attached to the corporate network. These laptops could not automatically have their security patches, antivirus definitions etc. updated since they were not on the network when the administrator's system management software executed batch updates.

Because Hardcopy Devices do not support the network health assessment protocols, the IP address of each HCD is manually entered into an exception table with the health assessment scheme's configuration tool. Industrious employees have discovered that they can program their laptops with the same IP address as the area's shared printer and access the corporate network without having to manually install operating system patches and antivirus updates before being allowed access.

Having HCDs report attributes will remove the need for most exceptions and therefore decrease the chance of unprotected laptops spreading malware.

3.2.2 IT Environment That Requires Common Criteria Certification For Networked Devices

IT Security and Network administrators that follow specific Information Security Management System (ISMS) guidelines may require that all devices that attach to a network be certified via some external body, (e.g., Common Criteria). These certifications are usually only valid if the device is maintained in a particular configuration. For Hardcopy Devices, configuration parameters that may affect the status of a certification can include, but are not limited to:

— The specific level of firmware that is loaded into the HCD.

— The specific hardware ports that are enabled or disabled on the HCD.

— The specific network protocols that are enabled or disabled on the HCD.

— The specific port numbers that are enabled or disabled on the HCD.

— The specific services that are enabled on the HCD.

Any modification to these configuration parameters can result in the device no longer operating in its certified configuration.

3.2.3 IT Environment That Requires Policy Enforcement Certification For Networked Devices

Organizations may have a set of internal policies that must be satisfied before a device is allowed on the network. Often these policy requirements are configuration requirements and may not seem directly related to "health." However, from the following example, it may be seen that configuration settings may be important elements for assessing the fitness of a device to attach to the network.

Users have discovered that they can gain access to the network by acquiring the address of a device on the exception list and statically assigning this IP address to their computer. Their computer is now on the exception list and is granted access. To mitigate this breach, IT administrators decide corporate policy is that ALL devices must acquire their IP addresses from a DHCP server. The configuration setting that enables/disables DHCP becomes part of the Policy Enforcement health assessment.

Policy Enforcement can encompass a wide range of configuration settings. The relevance of these settings may also vary between organizations. Some additional configuration elements that could be part of a policy statement include, but are not limited to:

— Secure Time Source

— Valid X.509 certificate signed by corporate Certificate Authority

— MAC addresses – Universally Administered Address (UAA) versus Locally Administrated Address (LAA)

— Enabled/Disabled protocols -- for example, no FTP daemon, or support for HTTPS but not for HTTP.

— Installed features – for example, disallow printers with hard disks unless they support disk wiping.

— Authentication settings – Kerberos/LDAP configuration

— Network proxy configuration

— DNS server address(es)

It is also important to note that some policy related settings, like disabled protocols and installed features, may overlap with other health related evaluations.

3.3 Design Requirements For Attributes

1) The PWG HCD Health Assessment Attribute definitions are independent of any implementation of a specific network health assessment protocol.
2) The PWG HCD Health Assessment Attributes are abstracted to enable support for mappings to multiple network health assessment protocols.
3) The PWG HCD Health Assessment Attributes design allows vendor extensions.

4. HCD Health Assessment Attributes

This section contains the definitions and functional descriptions of the Health Assessment Attributes for Hardcopy Devices.

4.1 General Attribute Definitions and Semantics

These attributes in the following table are the base set of attributes for HCDs that can be used to identify and measure the health of the HCD. The binding of these attributes into specific health assessment protocols is specified in other Printer Working Group documents.

HCD Health Assessment Attribute Name	(DataType)
Description	
CertificationState	(OctetArray)
The CertificationState attribute is a vendor-specific variable length field that uniquely identifies the state of a particular set of configuration settings in the HCD that are included as part of a certification process (e.g., Common Criteria certification). 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 attribute. Note: An example implementation of this attribute could be a cryptographically secure hash of the configuration (e.g., firmware version, port filter settings, protocols enabled/disabled etc.) that must be set to a specific state as part of the certification process.	
ConfigurationState	(OctetArray)
The ConfigurationState attribute is an administratively configured, vendor-specific variable length field that uniquely identifies the state of any configuration settings in the HCD that are included in creation of the attribute. 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 attributes value. The configuration settings included as part of this attribute SHOULD be administratively configurable. Note: An example implementation of this attribute could be a cryptographically secure hash of the configuration settings. ***Implementer Note:*** *The ConfigurationState attribute is intended to provide a method for a system administrator (site local, device, etc.) to snap-shot a specific device configuration state. Examples of configuration information included in this attribute may include such items as default settings for duplex, media type, color mode, language, etc.; enabled or disabled services or features such as Fax, IPP, SSL support etc.; and encryption parameters for storage or network transports. In conjunction with a system health validation agent, this value can be used to determine if the configuration has changed in any way from the last snap-shot. No standardized values or behavior is defined by the PWG, only the ability to detect a change. Any access control restrictions that may be triggered by a change in this attribute are vendor or administrator defined. While a specific vendor may wish to provide mediation support for this attribute, no remediation support is defined or required by this standard.*	
DefaultPasswordEnabled	(Boolean)
The DefaultPasswordEnabled attribute is a Boolean field that indicates that one or more of the devices' administrator passwords or other credentials, such as self-signed certificates, are currently using factory default values and have not been changed.. (false = no default passwords)	
FirewallSetting	(OctetArray)
The FirewallSetting attribute is an octet field of variable length that indicates the state (open/closed) of each IP protocol port on the device. Note: An example binding of this attribute follows the format for the Port Filter attribute type in [RFC5792] section 4.2.6.	
FirmwareName	(String)

HCD Health Assessment Attribute Name	(DataType)
Description	
The FirmwareName attribute is a variable length string that specifies the name attributed to the firmware that is contained in the HCD. This attribute may present multiple values to represent different names of firmware for different system components	
FirmwarePatches	(String)
The FirmwarePatches attribute is a variable length string that describes the patch(s) that have been applied to the firmware in the HCD. All patches must be listed in the order in which they were applied, beginning with the first patch applied and ending with the last patch applied. Patch values MUST be delimited by a Carriage Return/Line Feed pair (0x0D0A). This attribute may present multiple values to represent different instances of firmware patches for different system components. Note: Any firmware patches applied to the HCD MUST NOT result in a change in the FirmwareVersion attribute.	
FirmwareStringVersion	(String)
The FirmwareStringVersion attribute is variable length string that can uniquely describe the current version of firmware loaded in the device. This attribute may present multiple values to represent different versions of firmware for different system components	
FirmwareVersion	(OctetArray)
The FirmwareVersion attribute is a 16 octet field that can uniquely describe the current version of firmware loaded in the device. Note: An example binding of this attribute may follow the format for the Numeric Version in [RFC5792] section 4.2.3. This attribute may present multiple values to represent different versions of firmware for different system components.	
ForwardingEnabled	(Boolean)
The ForwardingEnabled attribute is a Boolean field that indicates whether any external-facing interface is being used as a bridge, route, or proxy from any other external-facing interface including itself. (false = no forwarding enabled) Note: An example of this may be a USB, Infrared, 802.11, Bluetooth, or PSTN Fax interface being bridged to the Ethernet interface allowing devices that have not been subject to the health assessment measurement to access the Ethernet network.	
MachineTypeModel	(String)
The MachineTypeModel attribute is a variable length string that indicates the particular machine type and model of the device. This attribute is generally common to all devices in a particular generation of that device. Example: “SomeCompany PhotoSmart 500”	
PSTNFaxEnabled	(Boolean)
The PSTNFaxEnabled attribute is a Boolean field that indicates if the PSTN fax interface or other modem interface on the device is enabled. (true = Fax enabled. false = Fax Disabled or not present)	
ResidentApplicationName	(String)
The ResidentApplicationName attribute is a variable length string that specifies the name attributed to a resident application that is currently installed on the HCD.	
ResidentApplicationPatches	(String)
The ResidentApplicationPatches attribute is a variable length string that describes the patch(s) that have been applied to a resident application in the HCD. All patches must be listed in the order in which they were applied, beginning with the first patch applied and ending with the last patch applied. Patch values MUST be delimited by a Carriage Return/Line Feed pair (0x0D0A). This attribute may present multiple values to represent different instances of software patches for different applications. Note: Any application patches applied to the HCD MUST result in a change in the ResidentApplicationVersion attribute.	
ResidentApplicationStringVersion	(String)
The ResidentApplicationStringVersion attribute is variable length string that can uniquely describe the current version of an installed resident application in the device.	
ResidentApplicationVersion	(OctetArray)
The ResidentApplicationVersion attribute is a 16 octet field that can uniquely describe the current version of an installed resident application in the device. Note: An example binding of this attribute may follow the format for the Numeric Version in [RFC5792] section 4.2.3.	

HCD Health Assessment Attribute Name	(DataType)
Description	
TimeSource	(String)
The TimeSource attribute is a variable length string that indicates where the device acquires its time setting. Regardless of the time source, the HCD shall provide administrative protection for its internal time. Examples of this attribute include: ("onboard" for a resident RTC or a Hostname or URI string for a network time source) Usage Considerations: Many security mechanisms rely on accurate time to enforce security. Examples include validity periods on X.509 certificates and Kerberos Tickets. As such, it is important to know that the device's internal clock(s) acquire time in a secure manner. If the time source is not secure, it could lead to denial of service (set time outside the validity period) and/or allow unauthorized access (set time to within validity period.) There are several ways to acquire the time including Network Time Protocol (NTP) and explicitly set by the user via some user interface. NTP has the ability to utilize encryption and integrity checks using pre-shared keys. The user interface to the clock can be protected using passwords. It is important to note that internal time of day clocks are often used in devices and may utilize a bus structure, such as I2C. In such cases, the bus used MUST NOT be accessible externally from the device.	
UserApplicationEnabled	(Boolean)
The UserApplicationEnabled attribute is a Boolean field that indicates whether the HCD supports (or currently has enabled) the ability to download or execute applications intended to dynamically downloaded by users and executed on the device. (false = not enabled)	
UserApplicationPersistenceEnabled	(Boolean)
The UserApplicationPersistenceEnabled attribute is a Boolean field that indicates whether user-downloadable applications can persist outside the boundary of a single job. (false = not enabled)	
UserApplicationName	(String)
The UserApplicationName attribute is a variable length string that specifies the name attributed to a dynamic user-downloadable and executable application that is currently installed on the HCD. Note: Since these applications are dynamic, a re-assessment of the device may be required after each download.	
UserApplicationPatches	(String)
The UserApplicationPatches attribute is a variable length string that describes the patch(s) that have been applied to a user-downloadable application in the HCD. All patches must be listed in the order in which they were applied, beginning with the first patch applied and ending with the last patch applied. Patch values MUST be delimited by a Carriage Return/Line Feed pair (0x0D0A). This attribute may present multiple values to represent different instances of software patches for different applications. Note: Any user-downloadable application patches applied to the HCD MUST result in a change in the UserApplicationVersion attribute.	
UserApplicationStringVersion	(String)
The UserApplicationStringVersion attribute is variable length string that can uniquely describe the current version of an installed user-downloadable application in the device.	
UserApplicationVersion	(OctetArray)
The UserApplicationVersion attribute is a 16 octet field that can uniquely describe the current version of an installed user-downloadable application in the device. Note: An example binding of this attribute may follow the format for the Numeric Version in [RFC5792] section 4.2.3.	
VendorName	(String)
The VendorName attribute is a variable length string that indicates the name of the manufacturer of the HCD.	
VendorSMICode	(Integer)
The VendorSMICode is a 24 bit unsigned integer that contains a globally unique SMI Network Management Private Enterprise Code of the vendor, as defined by IANA.	
AttributesNaturalLanguage	(String)
The AttributeNaturalLanguage is a variable length string containing the language code that indicates the local language used for all HCD string attribute values. The value is specified as defined in [RFC5646].	

4.2 Attribute Grouping and Multiple Attribute Values

Some HCD attributes may be repeated to provide values for multiple instances of a system entity. Some attributes may naturally fall into a cohesive collection or grouping of attribute sets. An IDS HCD binding implementation MUST maintain these attribute relationships within the limits and capabilities of the binding protocol.

5. Conformance

5.1 Binding Conformance

Any binding that supports the attributes defined in Section 4.1 *General Attribute Definitions and Semantics* MUST support multiple instances of the Name, Version, and Patch attributes related to user and resident applications.

5.2 HCD Conformance

This section contains the implementation requirements for HCDs that support Hardcopy Device Health Attributes. In addition, Section 4.1 *General Attribute Definitions and Semantics* contains additional required behaviors and interactions for these attributes.

5.2.1 Mandatory Attributes

HCDs that claim conformance to this specification MUST support the following set of attributes:

- AttributeNaturalLanguage
- DefaultPasswordEnabled
- FirewallSetting
- FirmwareName
- FirmwarePatches
- FirmwareStringVersion
- FirmwareVersion
- ForwardingEnabled
- MachineTypeModel
- PSTNFaxEnabled
- TimeSource
- UserApplicationEnabled
- UserApplicationPersistenceEnabled
- VendorName
- VendorSMICode

5.2.2 Conditionally Mandatory Attributes

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

5.2.2.1 User Application Attributes

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

- UserApplicationName
- UserApplicationPatches

- UserApplicationStringVersion
- UserApplicationVersion

5.2.2.2 Resident Application Attributes

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

- ResidentApplicationName
- ResidentApplicationPatches
- ResidentApplicationStringVersion
- ResidentApplicationVersion

5.2.3 Optional Attributes

Support for the following attributes is OPTIONAL for an HCD.

- ConfigurationState
- CertificationState

6. IANA and PWG Considerations

The XML Schema for the PWG Semantic Model/2.0 [PWGSM20] MUST include the HCD Health Assessment Attributes described in Section 4 . All HCD Health Assessment Attributes are members of the System object of the PWG Semantic Model [PWGSM]. The following table represents the mapping between HCD Attributes and the PWG Semantic Model:

HCD Name	SM Name	Data Type
AttributesNaturalLanguage	NaturalLanguageConfigured	String
MachineTypeModel	MachineTypeModel	String
VendorName	VendorName	String
VendorSMICode	VendorSMICode	Integer
DefaultPasswordEnabled	DefaultPasswordEnabled	Boolean
FirewallSetting	FirewallSetting	OctetString|base64Binary
ForwardingEnabled	ForwardingEnabled	Boolean
TimeSource	TimeSource	String
PSTNFaxEnabled	PSTNFaxEnabled	Boolean
FirmwareName	Firmware:FirmwareName	String
FirmwarePatches	Firmware:FirmwarePatches	String
FirmwareStringVersion	Firmware:FirmwareStringVersion	String
FirmwareVersion	Firmware:FirmwareVersion	OctetString|base64Binary
ResidentApplicationName	ResidentApplication:ResidentApplicationName	String
ResidentApplicationPatches	ResidentApplication:ResidentApplicationPatches	String
ResidentApplicationStringVersion	ResidentApplication:ResidentApplicationStringVersion	String
ResidentApplicationVersion	ResidentApplication:ResidentApplicationVersion	OctetString|base64Binary
UserApplicationEnabled	UserApplicationEnabled	Boolean
UserApplicationPersistenceEnabled	UserApplicationPersistenceEnabled	Boolean
UserApplicationName	UserApplication:UserApplicationName	String
UserApplicationPatches	UserApplication:UserApplicationPatches	String
UserApplicationStringVersion	UserApplication:UserApplicationStringVersion	String
UserApplicationVersion	UserApplication:UserApplicationVersion	OctetString|base64Binary
CertificationState	CertificationState	OctetString|base64Binary
ConfigurationState	ConfigurationState	OctetString|base64Binary

7. Internationalization Considerations

The attributes that are defined in this specification are intended to be used as part of a network assessment protocol and conform to the IETF Policy on Character Sets and Languages [RFC2277] in that all string attributes are UTF-8 encoded.

8. Security Considerations

This specification does not define any specific security mechanism for the protection of the confidentiality and integrity of the attributes, however, assessment protocols that use these attributes SHOULD provide integrity protection and confidentiality of the attributes.

9. Normative References

[RFC2119]	S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels" (RFC 2119), IETF, March 1997, available at http://www.ietf.org/rfc/rfc2119.txt
[RFC2277]	H. Alvestrand, "IETF Policy on Character Sets and Languages" (RFC 2277), IETF, January 1998, available at http://www.ietf.org/rfc/rfc2277.txt
[RFC2578]	K. McCloghrie, D. Perkins, J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)" (RFC 2578), IETF, April 1999, available at http://www.ietf.org/rfc/rfc2578.txt
[RFC2579]	K. McCloghrie, D. Perkins, , J. Schoenwaelder, "Textual Conventions for SMIv2 " (RFC 2579), IETF, April 1999, available at http://www.ietf.org/rfc/rfc2579.txt
[RFC3411]	D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks " (RFC 3411), IETF, December 2002, available at http://www.ietf.org/rfc/rfc3411.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
[RFC5646]	A.Philips, M. Davis "Tags for Identifying Language" (RFC 5646), IETF, September 2009, available at http://w ww.ietf.org/rfc/rfc5646.txt
[PWGSM]	MFD Model and Common Semantics (ftp://ftp.pwg.org/pub/pwg/candidates/cs-sm20-mfdmodel10-20110415-5108.1.pdf)

10. Informative References

[IEEE2600]	IEEE 2600-2008 IEEE Standard for Information Technology: Hardcopy Device and System Security
[RFC5792]	PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)
[XML-SCHEMA2]	XML Schema Part 2: Datatypes Second Edition: http://www.w3.org/TR/xmlschema-2/

11. Authors' Addresses

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

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

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

Randy Turner – Amalfi Systems
Lee Farrell
Rick Landau
Glen Petrie – Epson
Ira McDonald – High North
Harry Lewis – Ricoh
Dave Whitehead – Independent Contractor
Nancy Chen – Oki Data
Ron Bergman
Brian Smithson – Ricoh
Shah Bhatti
Peter Cybuck
Joe Murdock – Sharp
Ron Nevo – Samsung
Craig Whittle – Sharp
Bill Wagner – TIC
Sameer Yami
Pete Zehler – Xerox
Alan Sukert - Xerox

