

1
2
3 **Charter of the PWG**
4 **Imaging Device Security (IDS)**
5 **Working Group (WG)**
6

7 **Status: Initial Draft**

8 **Copyright © 2017 Printer Working Group. All Rights Reserved.**

9 **<ftp://ftp.pwg.org/pub/pwg/ids/wd/ch-ids-charter-20170501.pdf>**

10
11 **IDS WG Chair:**

12 Alan Sukert (Xerox)

13
14 **IDS WG Vice-Chair:**

15 Position Open

16
17 **IDS WG Secretary:**

18 Alan Sukert (Xerox)

19
20 **IDS WG Document Editors:**

21 Ira McDonald (High North)

22
23
24 **Problem Statement:**

25
26 Modern Imaging and Hardcopy Devices¹ and Services may be allowed unrestrained access to and storage of secure
27 and controlled documents and resources exposing security and access considerations that are not fully addressed
28 within current standards.

- 29
30
- 31 • Imaging Devices provide and use services outside of the traditional concept of a local user or server on a
32 physical device. While current standards such as the IEEE 2600-2008 are focused on addressing issues
33 related to securing local Hardcopy Device functionality, there are currently no suitable Imaging Device
34 standards or recommendation for controlling or validating access to these extended services.

¹ IEEE 2600-2008 defines the term Hardcopy Device as: A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), “all-in-ones,” and other similar products. The definition of an Imaging Device includes that of a Hardcopy Device, but also may include hardware devices such as projectors or displays and software services or processes that perform imaging functionality such as Character Recognition or document format transformations.

- 35 • Imaging Devices provide services to Imaging Clients² running on various operating systems and can extend
36 these services as Cloud³ resources. Imaging Devices and Imaging Clients also use resources and Imaging
37 Services from the Cloud. There are no suitable Imaging Device standards or recommended methodologies
38 for authenticating and securing the Imaging Devices, Imaging Clients, and Imaging Services in a Cloud
39 environment.
40
- 41 • Imaging Devices and Imaging Services have no standard method to associate security information with an
42 Imaging Job and ensure that the security information is maintained throughout the Job lifetime.
43
- 44 • Enterprise networks are deploying network endpoint attachment and compliance protocols and tools to
45 measure and assess the health of devices on the network. These assessment protocols go beyond simply
46 checking that the device possesses the correct credentials to access the network to also monitoring and
47 assessing information such as operating system, security patches, antivirus definition levels etc. Hardcopy
48 Devices (Network Printers, Multi-Function Devices, Network Scanners, etc.) have not been widely
49 integrated into these new assessment protocol schemes, in part because there is no standardized set of
50 attributes that a health assessment server can measure for Hardcopy Devices.
51

52 The original goals of the Imaging Device Security Working Group were to address the above issues by developing
53 the necessary specifications and recommendations and to liaison with the Common Criteria MFP Technical
54 Community developing the new Hardcopy Device Protection Profile.⁴ The initial set of specifications that were to be
55 developed by this Working Group were:

- 56 • TNC Binding for IDS Health Attributes – Define health attributes transport using TNC.
57 • Remediation specification – Define standard methods to perform remediation of detected device health and
58 security defects.
59 • IDS Model – Define a common security model for PWG projects and working groups.
60 • IDS Identification, Authentication and Authorization – Define a set of standards and recommendations for
61 providing the credentials and information required to provide secure access to Imaging Devices, Services
62 and Clients.
63 • IDS Security Ticket schema – Define a standard schema for specifying, associating and maintaining
64 security information with an Imaging Job, Imaging Device or Imaging Client.
65

66 **At the 08/12/2015 IDS Face-to-Face Meeting the IDS Working Group (WG) decided that the Working Group**
67 **should** go into “hibernation” and be reactivated as needed should work on a spec be required. **The 11/19/2015**
68 Charter update reflected **ed** that decision. The rationale for this Working Group going into “hibernation” were:

- 69 • The IDS WG essentially completed its original goal of providing HCD specifics to network admission
70 schemes, by doing HCD-ATTR, HCD-NAP and HCD-TNC Bindings specs.
71 • There was an initial expectation that there would be a market demand for such network and endpoint
72 protection schemes, as well as some expansion of "near-continuous monitoring" like SCAP as promoted by
73 NIST, to which the IDS WG could contribute. However, the market demand hasn't gone much beyond
74 desktops and mobiles so there is nothing at this time for the IDS WG to contribute to in this area.
75 • For some of the other initially planned IDS WG activities, there hasn't been a sufficient business case to
76 justify the investment of participation at the current time.
77

78 Based on that decision, the new long-term deferred goals of the Imaging Device Security Working Group are to:

- 79 • Develop any new required specifications or recommendations to address the issues cited above as directed
80 by the PWG Steering Committee.

² Terms such as “Imaging Device” and “Imaging Service” used in this document are defined in the PWG MFD Model and Common Semantics document. The term “Imaging Client” is synonymous with the PWG Model term “Client”

³ The term “Cloud” is defined in the NIST Special Publication 800-145 (http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf)

⁴ The result of this Technical was the approved Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015.

- 81 • Provide any errata to approved specifications developed by the Imaging Device Security Working Group as
82 directed by the PWG Steering Committee.
83 • Liaison with any international Technical Committees formed to update or replace the new Protection
84 Profile for Hardcopy Devices.

85
86 **This charter update reflects an expanded role of the IDS WG in performing a liaison function with the**
87 **Multifunction Printer (MFP) Technical Committee (TC) and any other TCs related to hardcopy devices. This**
88 **liaison role is important as it allows IDS members to review and comment on what the MFP TC is doing,**
89 **provide a different perspective on the issues vendors are facing in trying to conform with this new Protection**
90 **Profile and monitor future activities related to formation of an international TC to develop a collaborative**
91 **Protection Profile for hardcopy devices.**

92

93 **Out-of-scope:**

94

- 95 • OOS-1 Define new encryption algorithms
- 96 • OOS-2 Define new transport protocols
- 97 • OOS-3 Define new application protocols
- 98 • OOS-4 Define new hash functions or digital signatures
- 99 • OOS-5 Define new network endpoint attachment protocols
- 100 • OOS-6 Define new security protocols
- 101 • OOS-7 Define new security token, or public key certificate formats

102

103 **Objectives:**

104

- 105 • OBJ-1 Define an extended set of attributes for Imaging Devices that may include device configuration
106 attributes to be used for policy enforcement
- 107 • OBJ-2 Define a TNC transport binding for health assessment.
- 108 • OBJ-3 Define a common Security Model specification for reference by other PWG specifications.
- 109 • OBJ-4 Define a set of recommendations for identifying, authenticating and authorizing Imaging Devices,
110 Imaging Client, and Imaging Services.
- 111 • OBJ-5 Define a schema for security attributes and a Security Ticket to be associated with Imaging Jobs,
112 Users, Services and Devices.
- 113 • **OBJ-6 Provide liaison with the Multifunction Printer Technical Committee and any international**
114 **Technical Committees formed to update or replace the new Protection Profile for Hardcopy Devices.**

115

116 **Milestones:**

117

118 **Charter Stage:**

119

- 120 • CH-1 Initial working draft of updated IDS WG charter – DONE
- 121 • CH-2 Interim/Stable working draft of updated IDS WG charter – Nov 2015
- 122 • CH-3 PWG Formal Approval of updated IDS WG charter – Dec 2015
- 123 • **CH-4 PWG SC Formal Approval of updated IDS WG Charter – Apr 2017**

124

125 **Definition Stage:**

126

- 127 • BIND-1 Prototype Working draft of the TNC binding of the Hardcopy Device Health attributes - DONE
- 128 • BIND-2 PWG Last Call of the TNC binding of the Hardcopy Device Health attributes – DONE
- 129 • REM-1 Initial working draft of Remediation specification - DONE
- 130 • SEC-1 Initial working draft of IDS Security Ticket Schema model - DONE
- 131 • MODEL-1 Initial working draft of IDS Model specification – DONE

- 132 • IAA-1 Initial working draft of IDS Identification, Authentication and Authorization specification –
- 133 DONE
- 134 • REM-2 Prototype working draft of Remediation specification – See Note 1
- 135 • SEC-2 Prototype working draft of IDS Security Ticket Schema model – See Note 1
- 136 • MODEL-2 Prototype working draft of IDS Model specification – See Note 1
- 137 • IAA-2 Prototype working draft of IDS Identification, Authentication and Authorization specification –
- 138 See Note 1
- 139 • REM-3 PWG Last Call of Remediation specification – See Note 1
- 140 • SEC-3 PWG Last Call of IDS Security Ticket Schema model – See Note 1
- 141 • MODEL-3 PWG Last Call of IDS Model specification – See Note 1
- 142 • IAA-3 PWG Last Call of IDS Identification, Authentication and Authorization specification - See Note
- 143 1
- 144

145 **Implementation Stage:**

- 146
- 147 • INTEROP-1 Interoperability testing of the TNC Health Assessment – See Note 1
- 148 • INTEROP-2 Interoperability testing of the IDS Security Ticket – See Note 1
- 149 • INTEROP-3 Interoperability testing of the Remediation specification - See Note 1
- 150

151 **Maintenance Stage:**

- 152
- 153 • MAINT-1 Maintenance of PWG 5110.1-2013: PWG Hardcopy Device Health Assessment Attributes –
- 154 Note 2
- 155 • MAINT-2 Maintenance of PWG 5110.2-2013: PWG Hardcopy Device Health Assessment Network
- 156 Access Protection Protocol Binding – See Note 2
- 157 • MAINT-3 Maintenance of PWG 5110.2-2013: PWG Hardcopy Device Health Assessment Network
- 158 Access Protection Protocol Binding – See Note 2
- 159 • MAINT-4 Maintenance of TNC Binding of the Hardcopy Device Health attributes – See Note 2
- 160

161 **NOTE 1:** This document has been archived. Continuation of work on the document will be as directed by the PWG

162 Steering Committee.

163

164 **NOTE 2:** This document has been archived. Responsibility for errata updates of these documents will be

165 performed at the discretion of the PWG Steering Committee.

166

167