# Charter of the PWG Imaging Device Security (IDS) Working Group (WG)

**Status: Approved**



**ftp://ftp.pwg.org/pub/pwg/ids/charter/ch-ids-charter-20110503.pdf**

## IDS WG Chairs:

Joe Murdock (Sharp), Brian Smithson (Ricoh)

## IDS WG Secretary:

Brian Smithson (Ricoh)

## IDS WG Document Editors:

Joe Murdock (Sharp), Brian Smithson (Ricoh), Michael Sweet (Apple), Ira McDonald (High North), Jerry Thrasher (Lexmark), Bill Wagner (TIC), Ron Nevo (Samsung)

## Mailing Lists and Documents:

PWG General Discussion: pwg@pwg.org
Imaging Device Security WG Discussion: ids@pwg.org
To Subscribe: http://www.pwg.org/mailhelp.html
IDS WG Documents: ftp://ftp.pwg.org/pub/pwg/ids
IDS Wiki page: http://pwg-wiki.wikispaces.com/Imaging+Device+Security+WG

## Problem Statement:

Modern Imaging and Hardcopy Devices[1] may be allowed unrestrained access to and storage of secure and controlled documents and resources exposing security and access considerations that are not fully addressed within current standards.

- Imaging Devices provide and use services outside of the traditional concept of a local user or server on a physical device. While current standards such as the IEEE 2600-2008 are focused on addressing issues

[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.

related to securing local Hardcopy Device functionality, there are currently no suitable Imaging Device standards or recommendation for controlling or validating access to these extended services.

- Imaging Devices provide services to Imaging Clients[2] running on various operating systems and can extend these services as Cloud[3] resources. Imaging Devices and Imaging Clients also use resources and Imaging Services from the Cloud. There are no suitable Imaging Device standards or recommended methodologies for authenticating and securing the Imaging Devices, Imaging Clients, and Imaging Services in a Cloud environment.

- Imaging Devices and Imaging Services have no standard method to associate security information with an Imaging Job and ensure that the security information is maintained throughout the Job lifetime.

- Security Information and Event Management (SIEM) systems are being deployed in enterprise and government environments to provide continuous monitoring and analysis of security-related system log entries and other events. Imaging Devices have no industry standard format or set of values defined for to provide this information in a manner easily gathered and analyzed by SIEM tools.

- Enterprise networks are deploying network endpoint attachment protocols and tools to measure and assess the health of devices on the network. These assessment protocols go beyond simply checking that the device possesses the correct credentials to access the network to also assessing information such as operating system, security patches, antivirus definition levels etc. Hardcopy Devices (Network Printers, Multi-Function Devices, Network Scanners, etc.) have not been widely integrated into these new assessment protocol schemes, in part because there is no standardized set of attributes that a health assessment server can measure for Hardcopy Devices.

The goal of the Imaging Device Security Working Group is to address these issues by developing the following specifications and recommendations:

- Imaging Device Health Attributes - Define a set of common health assessment attributes for Imaging Devices
  - Binding Specifications – Define health attributes binding to the most common health assessment protocols.
  - Remediation specification – Define standard methods to perform remediation of detected device health failures.
- IDS Model and Requirements – Define a set of common security model for PWG projects and working groups.
- IDS Identification, Authentication and Authorization - Define a set of standards and recommendations for providing the credentials and information required to provide secure access to Imaging Devices, Services and Clients.
- IDS Security Ticket – Define a standard method for specifying, associating and maintaining security information with an Imaging Job, Imaging Device or Imaging Client.
- IDS Log - Define standards and recommendations for common log information.

Our goal 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.

## Out-of-scope:

[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)

- OOS-1 Define new encryption algorithms
- OOS-2 Define new transport protocols
- OOS-3 Define new application protocols
- OOS-4 Define new hash functions or digital signatures
- OOS-5 Define new network endpoint attachment protocols
- OOS-6 Define new security protocols
- OOS-7 Define new security token, or public key certificate formats

## Objectives:

- OBJ-1 Define a minimal required set of attributes that can be used to assess a Imaging Device's "fitness" to attach to a network
- OBJ-2 Define an extended set of attributes for Imaging Devices that may include device configuration attributes to be used for policy enforcement
- OBJ-3 Define a set of bindings to a limited set of network endpoint attachment protocols.
- OBJ-4 Define a set of recommendations for identifying and authenticating Imaging Devices, Imaging Client, and Imaging Services.
- OBJ-5 Define a set of standard security attributes and a Security Ticket to be associated with Imaging Jobs, Users, Services and Devices
- OBJ-6 Define a common log format and set of values to facilitate automated log and security event analysis

## Milestones:

### Charter Stage:

- CH-1 Initial working draft of IDS WG charter – Jan. 2008 - DONE
- CH-2 Interim/Stable working draft of IDS WG charter – Jan. 2008 - DONE
- CH-3 PWG Formal Approval of original IDS WG charter – Feb. 2008 - DONE
- CH-4 Interim/Stable working drafts of IDS WG charter for new security work – April 2011 - DONE
- CH-5 PWG Formal Approval of revised IDS WG charter revision – May 2011 - DONE

### Definition Stage:

- USE-1 Initial education on the specific network assessment protocols and development of use cases and requirements – Q1 2008 - DONE
- ATTR-1 Development of draft proposals for attributes to be included in the required minimal set to be measured – Q2 2008 - DONE
- ATTR-2 Development of draft proposals for attributes to be included in the extended set(s) of attributes – Q2 2008 - DONE
- ATTR-3 Finalization of the standardized set of attributes for Hardcopy Devices – Q3 2008 - DONE
- BIND-1 Development of the draft bindings of the Hardcopy Device attributes to the network assessment protocols – Q3 2008 - DONE
- BIND-2 Finalization of the bindings of the standardized set of attributes for Hardcopy Devices to the network assessment protocols – TBD
- REM-1 Initial working draft of NAC Remediation specification – August 2010 - Done
- LOG-1 Initial working draft of IDS Common Log specification – August 2010 - Done
- SEC-1 Initial working draft of IDS Security Ticket Schema model – Dec 2010 - Done
- MODEL-1 Initial working draft of IDS Model specification – Q3 2011
- IAA-1 Initial working draft of IDS Identification, Authentication and Authorization specification – Q2 2011
- REM-2 Prototype working draft of NAC Remediation specification – Q3 2011

- LOG-2 Prototype working draft of IDS Common Log specification – Q3 2011
- SEC-2 Prototype working draft of IDS Security Ticket Schema model – Q2 2011
- MODEL-2 Prototype working draft of IDS Model specification – Q4 2011
- IAA-2 Prototype working draft of IDS Identification, Authentication and Authorization specification – Q3 2011
- REM-3 PWG Last Call of NAC Remediation specification – Q4 2011
- LOG-3 PWG Last Call of IDS Common Log specification – Q3 2011
- SEC-3 PWG Last Call of IDS Security Ticket Schema model – Q3 2011
- MODEL-3 PWG Last Call of IDS Model specification – Q1 2012
- IAA-3 PWG Last Call of IDS Identification, Authentication and Authorization specification - Q1 2012

## Implementation Stage:

- INTEROP-1 Testing of the IDS Security Ticket as part of interoperability testing of Cloud Imaging working groups - Q2 2012
- INTEROP-2 Validation of common log data format across multiple implementations – Q1 2012