Common Criteria Recognition Arrangement

## Development Board

## CCDB HCD cPP WG



**Title:** Hardcopy Device (HCD) Essential Security Requirements

**Maintained by:** TBD（CCDB Work Group for Hardcopy Devices）

**Version:** 0.6 draft

**Date of issue:** *2018-September-13*

**Supersedes:**

# Status

Developers of Hardcopy Devices have developed an Essential Security Requirements (ESR) document for the development of a Hardcopy Devices (HCD) collaborative Protection Profile. Even though there is currently no cPP for Hardcopy Devices, there is a related protection profiles “Protection Profile for Hardcopy Devices” developed by the Multifunction Printers Technical Community with representatives from industry, Japanese and U.S Government agencies (Information-technology Promotion Agency and the National Information Assurance Partnership), Common Criteria Test Laboratories, and international Common Criteria schemes. That PP should be interpreted by the iTC as contributing to the development of an HCD cPP. The related PP focused on facilitating efficient procurement of Commercial Off-The-Shelf (COTS) Hardcopy Devices (HCDs) using the Common Criteria (CC) methodology for information technology security evaluation but lacked the existence as a cPP for global recognition.

TBD（The CCDB Working Group approves this draft of the ESR for distribution to the international Technical Community. The CCDB WG consists of representatives of the following CCRA Participants: names of nations.)

# Background and Purpose

The following provides a high-level set of security requirements that a Hardcopy Device, (hereafter referred to as an HCD) will satisfy when evaluated against the collaborative Protection Profile (cPP) written for such technology. In addition to stating what properties the HCD will minimally exhibit, the ESR also expresses functionalities that could be optionally considered as extensions, but go beyond the expected baseline. Furthermore, the ESR identifies aspects that are definitely outside the desired scope so as to limit the final set of security functional requirements specified in the cPP, as well as the assurance activities performed during the course of evaluation. The reason behind this scoping of the HCD's capabilities to be specified in the cPP is to ensure that objectives and repeatable assurance activities can be captured in the cPP while still delivering a cPP in a timely manner. Another factor is to ensure the security functionality prescribed is not well beyond the current best practices and is achievable by multiple developer products.

Having said that, this ESR allows for the specification of an optional capability - sending and receiving documents over PSTN using standard facsimile protocols, storing and retrieving electronic documents in the HCD, and updating the HCD's software (e.g. Patches or releases).

The HCD does not have to provide a means for updating software, but if it does, a conforming Security Target (ST) will include the requirements that ensure it will do so in a trusted manner.

The expectation is that the HCD will employ cryptographic means to provide the necessary protection of user data, the strength of which lies in the quality of the cryptographic algorithms and the entropy of the authentication factor (e.g. Password, passphrase). The HCD will encrypt the user data as it is stored in the HCD, and decrypt the data as it is retrieved from the HCD. The HCD will also encrypt user data as it is transferred to and from the HCD to ensure that such data transfer is done via a secure communication channel.

In addition to protecting the user data, the HCD is also responsible for ensuring the resident software cannot be modified by un-authorised entities through the logical interface. This is to ensure the HCD cannot be compromised by malware as a delivery mechanism to spread the malware. The intent here is to ensure the HCD cannot be compromised by malware running on a computer, which could then use the HCD as a delivery mechanism to spread the malware. This protection ensures “unauthorized” modifications – modifications or replacement of any arbitrary system files, including configuration files or critical data, such as a digital certificate, cannot be performed through the logical interface. As stated above, it may be possible for a developer to build the HCD that allows for software updates. The software updates for the HCD must be done in a controlled and trusted manner that employs a form of cryptography, such as a digital signature.

The cryptographic mechanisms (e.g., algorithms, key sizes) must not exhibit publicly known vulnerabilities or weaknesses, and are subject to approval by the appropriate cryptographic authorities, which are represented by the national schemes committing to the ESR and the procurement of the HCD compliant with the resulting cPP.

The HCD is responsible for ensuring audit logs are generated so that security-relevant events and HCD use can be monitored by authorized personnel. The HCD must generate audit logs and securely transmit them to an External IT entity for storage. Optionally, audit logs may also be stored in the HCD where they can be reviewed by an Administrator.

The HCD provides for user identification, authentication, and authorization to ensure that the functions of the HCD are accessible only to Users who have been authorized to access the HCD. User  
identification and authentication is also forms the basis for access control and administrative roles and helps associate security-relevant events and HCD use with specific Users. Identification and authentication may be performed by the HCD or by an external server. Role-based access controls also ensure that the ability to configure the security settings of the HCD is available only to users who have been authorized with an Administrator role.

# Use case

HCDs support job functions to convert hardcopy documents into digital form (scanning), convert digital documents into hardcopy form (printing), duplicate hardcopy documents (copying), or transmit documents over a PSTN connection (PSTN faxing). Hardcopy documents typically take the form of paper, but can take other forms (e.g. transparencies). For the purpose of this cPP, a conforming HCD must support at least one of the job functions printing, scanning, or copying and must support the functions network communications and administration. The job functions supported by the HCD and the network communications and administration functions are “Required Uses” of a conforming HCD and are mandatory functions. A conforming HCD may also support “Conditionally Mandatory Uses”. Conditionally Mandatory Uses are optional functions, the presence of which in a HCD is not required for conformance, but which must meet conditionally mandatory requirements if they are present in an HCD.

* **Required Uses**

The required Uses that shall be present in a conforming HCD are:

**One or more of the following:**

1. Printing: converting an electronic document to hardcopy form, or
2. Scanning: converting a hardcopy document to electronic form, or
3. Copying: duplicating a hardcopy document,

--- and ---

**Network communications**: sending or receiving documents over a Local Area Network (LAN),

--- and ---

**Administration**: configuring, auditing, and verifying the security of the HCD.

In other words, a conforming HCD must support at least one of the Required Uses scanning, printing, or copying, and must support the Required Uses network communications and administration.

* **Conditionally Mandatory Uses**

Conditionally Mandatory Uses that may be present in a conforming HCD are:

**PSTN faxing**: sending and receiving documents over the public switched telephone network (PSTN) using standard facsimile protocols

**Storage and retrieval**: storing electronic documents and retrieving them at a later time

**Field-Replaceable Nonvolatile Storage**: storing documents or confidential system information on Field-Replaceable Nonvolatile Storage Devices.

To conform, the HCD must meet requirements associated with these functions if they are present in the TOE.

* **Optional Uses**

Optional Uses that may be present in a conforming HCD are:

**Internal Audit Log Storage**: storing audit logs in the HCD

**Image Overwrite**: Actively overwriting residual image data at the conclusion of an image processing job

**Purge Data**: Purging all customer-supplied data from the HCD in preparation for redeployment, decommissioning, or other change in environment.

OR

**Required Use Cases**

The security-relevant use cases for Required Uses of a conforming HCD are:

1. One or more of the following:
2. **Printing**: A Network User sends a Document from an External IT Entity to the HCD over a LAN with instructions for printing. The HCD has the capability to protect the User’s Document from unauthorized disclosure or alteration while it is in transit to the HCD, in Temporary Storage in the HCD, and before printed output is released to a User.
3. **Scanning**: A Local User initiates scanning a Document on the HCD and the HCD sends the digital image to an External IT Entity. The HCD has the capability to protect the User’s Document from unauthorized disclosure or alteration while it is in Temporary Storage in the HCD and while it is in transit to the External IT Entity.
4. **Copying**: A Local User scans a Document on the HCD and the HCD prints the Document. The HCD has the capability to protect the User’s Document from unauthorized disclosure and alteration while it is in Temporary Storage in the HCD.
5. **Configuration**: A Local or Network User with administrative privileges configures the security settings of the HCD. The HCD has the capability to assign Users to roles that distinguish Users who can perform administrative functions from Users who can perform User functions. The HCD also has the capability to protect its security settings from unauthorized disclosure and alteration when they are stored in the HCD and in transit to or from an External IT Entity
6. **Auditing**: Authorized personnel monitor security-relevant events in an audit log. The HCD generates audit log records when security-relevant events occur. It is mandatory that the HCD is able to securely transmit audit logs to an External IT Entity for storage, and the HCD has the capability to protect it from unauthorized disclosure or alteration while in transit to the External IT Entity.
7. **Verifying software updates**: Authorized personnel install updated software on the HCD. The HCD ensures that only authorized personnel are permitted to install software, has the capability to help the installer to verify the authenticity of the software update.
8. **Verifying HCD function**: The HCD checks itself for malfunctions by performing a self-test each time that it is powered on.

**Conditionally Mandatory Use Cases**

Security-relevant use cases for Conditionally Mandatory Uses (if present) of a conforming HCD may include:

**Sending PSTN faxes**: A Local User scans a Document on the HCD, or a Network User sends a Document from an External IT Entity to the HCD; the User provides instructions for sending it to a remote PSTN fax destination; the HCD sends a facsimile of the Document over the PSTN to the PSTN fax destination using standard PSTN fax protocols. The HCD has the capability to protect the Network User’s Document from unauthorized disclosure and alteration while in transit on the LAN. The HCD also has the capability to protect the User’s Document from unauthorized disclosure and alteration while in Temporary Storage in the HCD.

**Receiving PSTN faxes**: A remote PSTN fax sender sends a facsimile of a Document over the PSTN to the HCD using standard PSTN fax protocols. The HCD has the capability to protect received PSTN faxes from unauthorized disclosure and alteration while it is present in the HCD. Further, the HCD has the capability to ensure that the PSTN fax modem is not used to access the LAN.

**Storing and retrieving Documents**: A Local or Network User instructs the HCD to store or retrieve an electronic Document in the HCD. The sources and destinations of such Documents may be any of the other operations such as scanning, printing, or PSTN faxing. The HCD has the capability to protect such Documents from unauthorized disclosure and alteration while in transit and in storage in the HCD.

**Field-Replaceable Nonvolatile Storage Devices**: Authorized personnel remove the HCD from service in its Operational Environment to perform preventative maintenance, repairs, or other servicing-related operations. The HCD has the capability to protect documents or confidential system information that may be present in Field-Replaceable Nonvolatile Storage Devices from exposure if such a device is removed from the HCD.

**Optional Use Cases**

Security-relevant use cases for Optional Uses (if present) of a conforming HCD may include:

**Internal Audit Log Storage**: If the audit log can also be stored in the HCD, the HCD has the capability to protect its audit log from unauthorized disclosure and alteration

**Image Overwrite**: At the conclusion of an image processing job, residual image data may be present in the HCD. The HCD has the capability to actively overwrite such image data.

**Redeploying or Decommissioning the HCD**: Authorized personnel remove the HCD from service in its Operational Environment to move it to a different Operational Environment, to permanently remove it from operation, or otherwise change its ownership. The HCD has the capability to make all customer data that may be present in the HCD unavailable for recovery if it is removed from the Operational Environment.

# Resources to be protected

* User Document Data processed in the HCD (against unauthorised disclosure, modification or deletion).
* User Job Data related to documents in the HCD (against unauthorised modification or deletion).
* Communication Data on the network (against unauthorised disclosure or modification).
* TSF Protected Data such as User’s ID related to security configuration and monitoring of the HCD (against unauthorised modification or deletion).
* TSF Confidential Data such as User’s Password related to security configuration or administration of the HCD (against unauthorised disclosure, modification or deletion).
* Software in the HCD (against unauthorised modification or deletion).
* Audit Records obtained in order to trace generation of illegal actions (against unauthorised modification or deletion).

# Attacker's Access

* An attacker may attempt to retrieve or modify User Data or settings of security functions through one of the interfaces provided by the HCD or through physical access to media such as Storage Devices in the HCD.
* An attacker may modify the system files of the HCD through one of the logical interfaces. (An attacker may modify the system files through physical attacks which is out of scope for this ESR.)
* An attacker may recover User Document Data which is not removed physically and remains in the HCD which was returned at lease end or decommissioned.
* An attacker may compromise the security of the HCD by monitoring or manipulating network communications.
* An attacker may masquerade as an authorised user in order to attempt unauthorised access.
* An attacker may attempt to modify or replace the HCD software in order to gain unauthorised access to information in the HCD, or to attack other systems on the LAN.
* An attacker may attempt to modify or remove the audit data.

OR

* An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the HCD through one of the HCD’s interfaces.
* An attacker may gain Unauthorized Access to TSF Data in the HCD through one of the HCD’s interfaces.
* An attacker may cause the installation of unauthorized software on the HCD.
* An attacker may access data in transit or otherwise compromise the security of the HCD by monitoring or manipulating network communication.
* A malfunction of the TSF may cause loss of security if the HCD is permitted to operate while in a degraded state.

# Attacker's Resource

* The attacker may take sufficient times for finding vulnerabilities or developing attack methods. It is assumed that the knowledge level of expected attacker may be possible as a layman through an expert.
* There is numerous PC software providing HCD users with a variety of applications delivered by each HCD vendor. Such software could be a target of reverse engineering and a source of information available for the attackers.
* It is expected that the attacker will find it difficult to attempt attacks frequently in the expected operational environment. But if the attacker is a malicious user, the attacker may attempt to attack frequently by means of multiple kinds of remote access tools via LAN.
* The tools used for attacks are expected to be tools that are free or non-free according to the knowledge levels of the attackers.
* There are many customer engineers who had already retired from the vendors, and the confidential information may exist on the Internet. It is possible for the attackers to use this confidential information which has not been managed in a secure manner.

# Boundary of the Devices

Physical boundary of hardware and software of the HCD shall be defined as followings:

* All security functions are included and executed within the physical boundary of the HCD.
* If it is possible to connect the external storage devices via USB interfaces, the external storage devices and its data are out of scope of the TOE.

OR

The physical boundary of the TOE is the entire HCD product. Options and add-ons that are not security relevant, such as finishers, do not need to be included in the TOE. If it is possible for users to connect personal storage devices (such as portable flash memory devices) to the HCD, those devices and data contained within them are out of scope of the TOE and interfaces to connect such devices should be disabled.

The logical boundary of the TOE includes all security functions related to the Required Uses of the HCD, all Conditionally Mandatory Uses, and all Optional Uses that are to be included in the evaluation.

# Essential Security Requirements（ESR）

* The User shall be authorised by means of identification and authentication as a user before executing the HCD administration functions or the document processing functions which require the resources of the HCD.
* The HCD shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
  + User Document Data can be accessed only by the Document owner. Administrators are able to delete User Document Data.
  + User Job Data can be modified only by the job owner or an Administrator.
  + TSF Protected Data can be modified only by an administrator, or a Normal User who is associated with that Data.
  + TSF Confidential Data can be modified only by an Administrator or a Normal User who is associated with that Data.
* HCD shall enforce that only authorised Administrators are permitted to perform administrator functions.
* HCD shall provide mechanisms to verify the authenticity of software updates.
* HCD shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorised access, replay and source/destination spoofing.
* HCD shall generate audit data, and store them in the HCD or send them to a trusted External IT Entity.
* HCD shall test some subset of its security functionality to detect the malfunction.

OR

* HCD shall perform authorization of Users in accordance with security policies
* HCD shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles
* HCD shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
  + User Document Data can be accessed only by the Document owner or an Administrator.
  + User Job Data can be read by any User but can be modified only by the Job Owner or an Administrator.
  + Protected TSF Data are data that can be read by any User but can be modified only by an Administrator or (in certain cases) a Normal User who is the owner of or otherwise associated with that data.
  + Confidential TSF Data are data that can only be accessed by an Administrator or (in certain cases) a Normal User who is the owner of or otherwise associated with that data.
* HCD shall ensure that only authorized Administrators are permitted to perform administrator functions.
* HCD shall provide mechanisms to verify the authenticity of software updates.
* HCD shall test some subset of its security functionality to help ensure that subset is operating properly.
* HCD shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.
* HCD shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the HCD.

# Assumptions

* Physical security, commensurate with the value of the HCD and the data it stores or processes, is assumed to be provided by the environment.
* The Operational Environment is assumed to protect the HCD from direct, public access to its LAN interface.
* Administrators of the HCD are trusted to administrate the HCD according to site security policies.
* Authorised Users are trained to use the HCD according to site security policies.

# Optional Extensions

* If the HCD provides a PSTN fax function, then the HCD shall ensure logical separation of the PSTN and the LAN.
* If the HCD stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.

# Out of Scope for Evaluation

* Resistance against physical attacks of the HCD directly from outside are not to be considered.
* Anti-malware checks on User Data transferred to and from the HCD.