Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

Protection Profile (PP)

Reception Date of Application (Reception Number)	2017-02-09 (ITC-7627)
Certification Identification	JISEC-C0553
Protection Profile Name/Identifier	Protection Profile for Hardcopy Devices
Protection Profile Version Number	1.0 dated September 10, 2015
Protection Profile Developer	IPA, NIAP, and the MFP Technical Community
Protection Profile Sponsor	Information-technology Promotion Agency, Japan (IPA)
Assurance Conformance	ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1
Name of IT Security Evaluation Facility	ECSEC Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above PP has been certified as follows.
2017-05-29

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center
Technology Headquarters

Evaluation Criteria, etc.: This PP is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass
"Protection Profile for Hardcopy Devices" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of the "Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015" [12] (hereinafter referred to as "the PP") developed by IPA, NIAP and the MFP Technical Community, and the evaluation of the PP was finished on 2017-04 by ECSEC Laboratory Inc., Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Information-technology Promotion Agency, Japan (IPA), and provide security information to procurement entities and consumers who are interested in the PP.

This Certification Report assumes "the developer who develops the products that conform to the PP and the procurement entities" to be readers. Note that this Certification Report presents the certification result based on assurance requirements to which the PP conforms, and does not guarantee an individual IT product itself.

Readers of this Certification Report are advised to read the PP along with this report. Especially, it describes details of security functional requirements, assurance requirements and security problems behind which the PP requires to the TOE.

1.1 Product Overview

An overview of the PP is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 PP Overview

The PP prescribes security requirements in regard to the Hardcopy Device (hereinafter referred to as the "HCD") which has basic functions of Scanning, Copying and Printing, etc.

The HCD that conforms to the PP (hereinafter referred to as the "TOE") provides one or more of the following basic functions; besides, it provides the Network communications to send or receive documents over a Local Area Network (LAN) and Administration functions to configure various settings and collect audit logs.

- Printing: converting (printing) an electronic document to hardcopy form
- Scanning: converting a hardcopy document to electronic form
- Copying: duplicating a hardcopy document

The TOE also provides the Fax communication and Document storage functions, etc., depending on the TOE configuration.

Besides these basic functions, the TOE provides security functions to protect the document data that are handled by the TOE and the security-relevant configuration data from disclosure and alteration.

In accordance with the different functional configurations (including security functions) for each TOE, the PP prescribes Mandatory Requirements for all the TOEs, Conditionally Mandatory Requirements or Selection-based Requirements for TOEs with specified conditions, and Optional Requirements provided as other options. The next section and subsequent sections show these security requirements.

1.1.1.1 Threats and Security Objectives

The PP assumes the following threats to the TOE and requires security functions to counter them.

For the User Document Data that are the protected assets of the TOE and the security setting information that has effects on security, there are threats of unauthorized disclosure and alteration caused by the operation of the TOE or by unauthorized access to the communication data on the network on which the TOE is installed.

To counter these threats, the TOE provides the security functions, such as User Identification and Authentication, Access Control, and Encryption.

Additionally, the TOE also provides security functions, such as Software Update Verification and Self-test functions, in order to counter the threats like the alteration of the TOE itself and the loss of security caused by malfunctions.

1.1.1.2 Configuration and Assumptions

The PP assumes that the TOE is operated under the following configuration and assumptions.

It is assumed that the TOE is operated under the environment where unauthorized physical access is limited and where the TOE is connected with the LAN protected from the external network. For the operation of the TOE, it shall be properly configured, maintained, and managed by the Administrator according to the guidance documents.

1.1.2 Disclaimers

The TOE is assumed to be operated under the environment shown in Section 1.1.1.2. The PP does not counter the threats related to direct attacks via the Internet or physical attacks to the TOE.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2017-04, based on functional requirements and assurance requirements of the PP according to the publicized documents, "IT Security Evaluation and Certification Scheme Document" [1], "Requirements for IT Security Certification" [2], and "Requirements for Approval of IT Security Evaluation Facility" [3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and the Observation Report prepared by the Evaluation Facility, as well as evaluation documentation, and confirmed that the PP evaluation was conducted in accordance with the prescribed procedure. The Certification Body confirmed that the PP evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The PP is identified as follows:

PP Name:	Protection Profile for Hardcopy Devices
PP Version:	1.0 dated September 10, 2015
	(Protection Profile for Hardcopy Devices – v1.0 Errata #1)
Developer:	IPA, NIAP, and the MFP Technical Community

3. Security Policy

This chapter describes security problems to be solved by the TOE that conforms to the PP and security functions to be implemented.

The TOE provides the necessary basic functions as the HCD and generally has functions to store User Document Data inside the TOE and to communicate with user terminals and various servers through the network. When using these functions, the TOE provides security functions to prevent User Document Data and configuration data from unauthorized disclosure and alteration and to securely operate the TOE itself.

The PP defines the Assets to be protected by the security functions as below; at the same time, User Roles are also required to be defined for the TOE. Note that the definitions can be added for both Assets and User Roles as necessary for each TOE.

Assets

(User Data)

D.USER.DOC: User Document Data

D.USER.JOB: User Job Data

(TSF Data)

D.TSF.PROT (Protected TSF Data): TSF Data, which may be read by any user but must be protected from unauthorized alteration and deletion.

D.TSF.CONF (Confidential TSF Data): TSF Data, which may neither be read nor altered or deleted except by authorized users.

User Roles

U.NORMAL: Normal Users who are identified and authenticated and do not have an administrative role.

U.ADMIN: Administrators who are identified and authenticated and have an administrative role.

3.1 Threats

The TOE that conforms to the PP assumes the threats shown in Table 3-1 and provides the functions as countermeasures against them.

Table 3-1 Assumed Threats

Identifier	Threat
T.UNAUTHORIZED_ ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.

T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_ UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.2 Organizational Security Policies

Organizational security policies required in use of the TOE that conforms to the PP are shown in Table 3-2.

Table 3-2 Organizational Security Policies

Identifier	Organizational Security Policy
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION (conditionally mandatory)	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL (conditionally mandatory) * This security policy is applied along with P.STORAGE_ENCRYPTION.	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW (conditionally mandatory)	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.

P.PURGE_DATA (optional)	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.

3.3 Security Objectives

The TOE that conforms to the PP implements the security functions as outlined below, against the security problems described in Sections 3.1 and 3.2.

3.3.1 User Identification and Authentication Function

The TOE provides a function to perform identification and authentication of users who access to the TOE by using trusted External IT Entities, such as authentication servers or mechanisms provided by the TOE itself. Successfully authenticated users are granted the authority in accordance with their roles, and are permitted to use the TOE.

3.3.2 Access Control Function

The TOE enforces access controls to protect User Data and TSF Data based on the User Roles and authorities against the user's request on handling. Specific rules for access controls are clearly prescribed for each TOE, but the PP requires the following as fundamental policies.

- [D.USER.DOC] that is managed inside the TOE can neither be read nor modified or deleted by users except for its Owner or an Administrator.
- [D.USER.JOB] that is managed inside the TOE can neither be modified nor deleted by users except for its Owner or an Administrator.
- For [D.TSF.PROT], users except for its Owner or an Administrator are prohibited from modifying.
- For [D.TSF.CONF], users except for its Owner or an Administrator are prohibited from reading or modifying.

3.3.3 Encrypted Communication Function

The TOE provides a function to protect user terminals and network communications between various servers from unauthorized access to communication data, replay attacks, and source/destination spoofing. Specific protection measures, communication protocols, and cryptographic suites, etc., are specifically prescribed for each TOE.

3.3.4 Self-test

The TOE performs self-tests during start-up in order to verify by itself that the security functions are operating properly.

3.3.5 Audit Function

When auditable security events occur, the TOE provides a function to generate audit logs that consist of event type, date and time of the event, and its result, and to send them to an External IT Entity, such as an audit server. The communication path to send them is protected as with other network communications. In addition, generated audit logs are securely managed inside the TOE, which may provide a function for authorized users to read.

3.3.6 Update Function

The TOE provides a function to verify the authenticity of software updates in order to protect the TOE itself from being altered by unauthorized software when updating itself. Only if this verification succeeds, the software update is performed.

3.3.7 Storage Encryption Function

The Storage Encryption Function is a function provided when the TOE stores [D.USER.DOC] or [D.TSF.CONF] in the Field-Replaceable Storage Devices. The stored data will be encrypted by the internationally accepted cryptographic algorithms that are specified for each TOE. The cryptographic key used in this function and key materials used when generating the cryptographic key are protected from unauthorized access and are stored in a different area where the above Storage Devices are stored.

3.3.8 FAX-Network Separation Function

The FAX-Network Separation Function is a function provided when the TOE supports FAX communications, and it is intended to prohibit access to the LAN via the PSTN used in the FAX communications. This function prohibits communications using the PSTN except for sending/receiving [D.USER.DOC] using a FAX protocol, in order to protect unauthorized access to the LAN that is connected to the TOE.

3.3.9 Data Clearing and Purging Function

This function consists of two functions; a function that the TOE overwrites the residual unnecessary information inside the TOE, upon completion or cancellation of a Document Processing job, with specified data; and a function that the TOE purges the User Data and TSF Data stored in the TOE to make them unavailable by the operation of Administrators. These functions are defined as optional requirements in the PP, and whether the functions are provided or not is specified for each TOE.

4. Assumptions and Clarification of Scope

In this chapter, the assumptions to operate the TOE that conforms to the PP are shown in Table 4-1. The effective performances of the TOE security functions are not assured unless these assumptions are upheld.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

5. Evaluation conducted by Evaluation Facility and Results

5.1 Evaluation Facility

ECSEC Laboratory Inc., Evaluation Center that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

5.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the PP overview as well as the content of the evaluation and the verdict of each work unit in the CEM.

5.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2017-02 and concluded upon completion of the Evaluation Technical Report dated 2017-04. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted.

Concerns found in the evaluation activities for each work unit were all issued as the Observation Report, and it was reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

5.4 Evaluation Results

The evaluator had concluded that the PP satisfies all work units prescribed in the CEM by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- Security functional requirements: Common Criteria Part 2 extended
- Security assurance requirements: Common Criteria Part 3 conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.1, APE_ECD.1, APE_REQ.1

5.5 Evaluator Comments/Recommendations

This evaluation is conducted by applying the "Protection Profile for Hardcopy Devices - v1.0 Errata #1" [13] (hereinafter referred to as the "Errata") to the PP. It should be noted that the overall evaluation result without applying the Errata fails to pass the evaluation.

6. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.

2. Contents pointed out in the Observation Report shall properly be solved.

3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

4 Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

6.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Report, and related evaluation documentation, the Certification Body determined that the PP satisfies the assurance components of APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.1, APE_ECD.1, and APE_REQ.1 in the CC Part 3.

6.2 Recommendations

- As described in Section "1.1.1 PP Overview," there are cases in the PP where security requirements differ depending on TOE configurations. Therefore, it should be noted the procurement entities which purchase the TOE that conforms to the PP need to confirm if the necessary security functions are implemented in the TOE to be purchased on the basis of its functional configuration.

- Note that, as described in Section "5.5 Evaluator Comments/Recommendations," the Errata [13] containing error corrections shall be applied when using the PP as the certified PP.

7. Annexes

There is no annex.

8. Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

LAN	An abbreviation of Local Area Network.
MFP	An abbreviation of Multifunction Printer, or Multifunction Peripheral.
PSTN	An abbreviation of Public Switched Telephone Networks.

The definitions of terms used in this report are listed below.

Document Processing	Printing, scanning, or copying a document.
Field-Replaceable (unit)	The smallest subassembly that can be swapped in the field to repair a fault. (minimum unit of parts)

9. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001, (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002, (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003, (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004, (Japanese Version 1.0, November 2012)

[12] Protection Profile for Hardcopy Devices, 1.0 dated September 10, 2015, MFP Technical Community

[13] Protection Profile for Hardcopy Devices - v1.0 Errata #1 (https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_errata.pdf)

[14] PP Evaluation Technical Report, Version 2.0, April 26, 2017, ECSEC Laboratory Evaluation Center