



Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

| | |
|---------------------|---|
| Application Date/ID | 2013-03-07 (ITC-3444) |
| Certification No. | C0497 |
| Sponsor | Canon Inc. |
| TOE Name | Canon imageRUNNER ADVANCE C350/C250 Series 2600.1 model |
| TOE Version | 1.0 |
| PP Conformance | IEEE Std. 2600.1 TM -2009 |
| Assurance Package | EAL3 augmented with ALC_FLR.2 |
| Developer | Canon Inc. |
| Evaluation Facility | Mizuho Information & Research Institute, Inc. Information Security Evaluation Office |

This is to report that the evaluation result for the above TOE is certified as follows.

2016-02-25

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

Evaluation Criteria, etc.: The TOE 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

“Canon imageRUNNER ADVANCE C350/C250 Series 2600.1 model” 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 | 1 |
| 1.1 Product Overview | 1 |
| 1.1.1 Assurance Package | 1 |
| 1.1.2 TOE and Security Functionality | 1 |
| 1.1.2.1 Threats and Security Objectives | 2 |
| 1.1.2.2 Configuration and Assumptions | 2 |
| 1.1.3 Disclaimers | 2 |
| 1.2 Conduct of Evaluation | 2 |
| 1.3 Certification | 2 |
| 2. Identification | 3 |
| 3. Security Policy..... | 5 |
| 3.1 Security Function Policies | 6 |
| 3.1.1 Threats and Security Function Policies | 6 |
| 3.1.1.1 Threats | 6 |
| 3.1.1.2 Security Function Policies against Threats | 6 |
| 3.1.2 Organizational Security Policies and Security Function Policies | 7 |
| 3.1.2.1 Organizational Security Policies | 7 |
| 3.1.2.2 Security Function Policies to Organizational Security Policies | 8 |
| 4. Assumptions and Clarification of Scope | 10 |
| 4.1 Usage Assumptions | 10 |
| 4.2 Environmental Assumptions | 10 |
| 4.3 Clarification of Scope | 12 |
| 5. Architectural Information | 13 |
| 5.1 TOE Boundary and Components | 13 |
| 5.2 IT Environment | 14 |
| 6. Documentation | 15 |
| 7. Evaluation conducted by Evaluation Facility and Results..... | 16 |
| 7.1 Evaluation Facility | 16 |
| 7.2 Evaluation Approach | 16 |
| 7.3 Overview of Evaluation Activity | 16 |
| 7.4 IT Product Testing | 17 |
| 7.4.1 Developer Testing | 17 |
| 7.4.2 Evaluator Independent Testing | 20 |
| 7.4.3 Evaluator Penetration Testing | 23 |
| 7.5 Evaluated Configuration | 26 |
| 7.6 Evaluation Results..... | 27 |
| 7.7 Evaluator Comments/Recommendations | 27 |
| 8. Certification..... | 28 |

| | | |
|-----|---------------------------|----|
| 8.1 | Certification Result..... | 28 |
| 8.2 | Recommendations | 28 |
| 9. | Annexes..... | 29 |
| 10. | Security Target | 29 |
| 11. | Glossary..... | 30 |
| 12. | Bibliography..... | 32 |

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of “Canon imageRUNNER ADVANCE C350/C250 Series 2600.1 model Version 1.0” (hereinafter referred to as the “TOE”) developed by Canon Inc., and the evaluation of the TOE was finished on 2016-02 by Mizuho Information & Research Institute, Inc., Information Security Evaluation Office (hereinafter referred to as the “Evaluation Facility”). It is intended to report to the sponsor, Canon Inc., and provide security information to procurement entities and consumers who are interested in the TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the “ST”) that is provided along with this report. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes “procurement entities and general consumers who purchase the TOE” to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a multifunction printer (hereinafter referred to as “MFP”) that offers Copy, Print, Universal Send, Fax, and Internet Fax (hereinafter referred to as “I-fax”) capabilities.

The security functions provided by the TOE satisfy all security functional requirements, as required and defined in the Protection Profile for Hardcopy Devices, IEEE Std. 2600.1™ -2009 [14] (hereinafter referred to as the “PP”).

For these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package. The TOE assumes threats and assumptions as described in the following sections.

1.1.2.1 Threats and Security Objectives

The TOE assumes the following threats as described below and provides the functions to counter these threats.

The assets of the TOE, namely user document data and the data that have an effect on security functions, are susceptible to unauthorized disclosure or alteration through manipulation of the TOE, or through access to the TOE's network communications data.

To prevent such unauthorized disclosure or alteration of those assets, the TOE provides security functions such as identification and authentication, access control, and encryption.

1.1.2.2 Configuration and Assumptions

The evaluated products are assumed to be operated under the following configurations and assumptions.

It is assumed that the TOE will be located in an environment where physical components of the TOE and its interfaces are protected from unauthorized access. The TOE shall be properly configured and maintained according to the guidance documents.

1.1.3 Disclaimers

- The Identification and Authentication Function contained in the target of this evaluation does not apply to incoming print jobs. Although the protocol used in the submission of the print job contains an identification and authentication mechanism, that mechanism is outside the scope of this evaluation.

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 2016-02 based on functional requirements and assurance requirements of the TOE 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 Observation Reports prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The Certification Body confirmed that the TOE 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 TOE is identified as follows:

TOE Name: Canon imageRUNNER ADVANCE C350/C250 Series 2600.1 model

TOE Version: 1.0

Developer: Canon Inc.

The TOE consists of the following software, hardware, and licenses.

Note that the Japanese names are originally written in Japanese and translated into English.

Table 2-1 Components of the TOE

| Component Name | Description |
|---|--|
| (Japanese Name) Canon imageRUNNER ADVANCE C350/C250 Series (English Name) Canon imageRUNNER ADVANCE C350/C250 Series | Any of the following MFP: - iR-ADV C350F - iR-ADV C350iF - iR-ADV C350i - iR-ADV C350 - iR-ADV C250iF - iR-ADV C250i - iR-ADV C250 If “F” is contained in the last one or two characters of the product names above, a fax-board is included in the MFP. If the character “i” is contained, an additional license is included in the MFP. |
| (Japanese Name) iR-ADV Security Kit-J1 for IEEE 2600.1 Ver 1.00 (English Name) iR-ADV Security Kit-J1 for IEEE 2600.1 Common Criteria Ver 1.00 | It contains the control software and security kit license for “Canon imageRUNNER ADVANCE C350/C250 Series.” |

| Component Name | Description |
|---|---|
| (Japanese Name) HDD Data Encryption Kit-C (Canon MFP Security Chip 2.01) (English Name) HDD Data Encryption Kit-C (Canon MFP Security Chip 2.01) | Hardware which encrypts all data stored in the HDD. |
| (Japanese Name) SuperG3 FAX Board-AN1 (English Name) SuperG3 FAX Board-AN1 | A Fax Board that is attached to the MFP. It is included as standard equipment on the following “F” and “iF” models: - iR-ADV C350F - iR-ADV C350iF - iR-ADV C250iF |
| (Japanese Name) Access Management System (English Name) Access Management System | A license to activate Access Control Function in the control software. This license comes as standard equipment for MFPs sold in the United States and Canada. |

Users can verify that a product is the TOE, which is evaluated and certified, by the following means.

According to the procedure written in the guidance documents, users operate the control panel of the MFP, and confirm the identification information of the TOE components displayed on the panel.

As described below, identification information which is different from the names in Table 2-1 is displayed for a part of components. It is also necessary to refer to the guidance documents for how to confirm the identification information.

- For “Canon imageRUNNER ADVANCE C350/250 Series” products, the names without the last one or two characters shown in the Table 2-1 will be displayed. Fax boards and additional options indicated by the last one or two characters of the names will be displayed separately.

(For example, in the case of iR-ADV C350iF, “iR-ADV C350” will be displayed as the product name, along with the name of the additional license which corresponds to “i” and the name of the fax board which corresponds to “F” in the names shown in the Table 2-1.)

- The display “iR-ADV Security Kit-J1 for IEEE 2600.1 Common Criteria Ver 1.00” is the display of the version of the control software and the license of the security kit.

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organizational security policies.

In addition to offering MFP capabilities such as Copy, Print, and Scan, the TOE is capable of storing user document data in its internal HDD device, and has the functionality for interacting with user terminals and various servers over the network.

The PP, to which the TOE is conformant, assumes an environment where a relatively high level of security is ensured and where accountability for actions is required, and specifies the security functional requirements for such an environment.

When using the MFP functions, the TOE offers security functions that satisfy the security functional requirements specified in the PP. These include user identification and authentication, access control, HDD data encryption and data erase functions, and cryptographic communication protocols, and protect user document data and setting data that have an effect on TOE security functions, which are TOE assets, from unauthorized disclosure and alteration.

In terms of the use of the TOE, the following roles are assumed.

- U.NORMAL
A User who is authorized to perform User Document Data processing functions of the TOE, such as Copy, Print, and Scan.
- U.ADMINISTRATOR
The TOE user in this role has special privileges that allow configuration of security functions.
- TOE Owner
A person or organizational entity responsible for protecting TOE assets and establishing related security policies.

The TOE assets are defined as follows.

- User Document Data
User Document Data consist of the information contained in a user's document.
- User Function Data
User Function Data are the information about a user's document or job to be processed by the TOE. This includes information such as print priority and print settings.
- TSF Confidential Data
TSF Confidential Data are data used by the security functions, and for which integrity and confidentiality must be preserved. This includes information such as user password, Box PIN, and audit logs. This does not, however, include cryptographic keys, since the user has no interface available to its access.
- TSF Protected Data
TSF Protected Data are data used by the security functions, and for which only integrity must be preserved. This includes information such as user identification and access privilege information.

3.1 Security Function Policies

The TOE provides the security functions to counter the threats shown in Section 3.1.1 and to satisfy the organizational security policies shown in Section 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the functions to counter them. These threats are the same as those specified in the PP.

Table 3-1 Assumed Threats

| Identifier | Threat |
|------------|---|
| T.DOC.DIS | User Document Data may be disclosed to unauthorized persons. |
| T.DOC.ALT | User Document Data may be altered by unauthorized persons. |
| T.FUNC.ALT | User Function Data may be altered by unauthorized persons. |
| T.PROT.ALT | TSF Protected Data may be altered by unauthorized persons. |
| T.CONF.DIS | TSF Confidential Data may be disclosed to unauthorized persons. |
| T.CONF.ALT | TSF Confidential Data may be altered by unauthorized persons. |

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1) Countermeasures against threat “T.DOC.DIS,” “T.DOC.ALT,” “T.FUNC.ALT”

These are threats to user data. The TOE counters the threats by the following functions: “User Authentication,” “Function Use Restriction,” “Job Output Restriction,” “HDD Data Erase,” “HDD Data Encryption,” and “LAN Data Protection.”

“User Authentication” and “Function Use Restriction” functions of the TOE allow only the authorized users to use the TOE functions. For details of these functions, refer to the description of P.USER_AUTHORIZATION in Section 3.1.2.2.

“Job Output Restriction” function of the TOE enforces access control when an identified and authenticated user performs the operation such as Print, Preview, Send to Network, Fax TX (send), Delete, Change Print Priority, and Change Print Settings on print jobs and fax/I-fax jobs stored in the TOE, thereby ensuring that only the owner of the documents or U.ADMINISTRATOR gains access to perform these operations. The TOE determines that the identified and authenticated user is the authorized document owner as follows:

- For documents submitted as print jobs, the identified and authenticated user is determined to be the owner of the document if his/her user name matches the user name information of the document specified upon submission of the print job.

- In the case of the document data received by fax/I-fax, the user is required to enter the correct box PIN when the user operates the document data. The box PIN is set by U.ADMINISTRATOR. When the U.ADMINISTRATOR accesses from the remote UI, the U.ADMINISTRATOR is determined to be the owner of the stored document data if the PIN entered to operate the Memory RX Inbox matches the pre-configured PIN for the Memory RX Inbox.

“HDD Data Erase” function of the TOE permanently erases the HDD area where the document data are stored, by overwriting with random data upon deleting the document data, to prevent the deleted document data from being read from the HDD.

“HDD Data Encryption” function of the TOE encrypts all data stored in the removable HDD of the TOE, and prevents the data from being disclosed or altered by tampering the detached HDD from the TOE. It uses the 256-bit AES encryption algorithm. Its cryptographic key is generated using the FIPS PUB 186-2 deterministic random number generator algorithm at start-up, and destroyed upon power-off.

“LAN Data Protection” function of the TOE uses the cryptographic communication protocol, IPsec, when the TOE communicates with other IT devices over the LAN, and protects the communicated data from unauthorized disclosure and alteration.

With the above functions, the TOE prevents unauthorized use of the TOE, unauthorized access to data stored in the HDD and communication data; thus, the TOE protects the data to be protected from unauthorized disclosure and alteration.

(2) Countermeasures against threat “T.PROT.ALT,” “T.CONF.DIS,” “T.CONF.ALT”

These are threats to TSF data that affects the security functions. The TOE counters the threats by the following functions: “User Authentication,” “Management,” “HDD Data Encryption,” and “LAN Data Protection.”

“Management” function of the TOE allows only the authorized U.ADMINISTRATOR to manage user information and various configuration data. Note, however, that the authorized U.NORMAL can change their own passwords.

“User Authentication,” “HDD Data Encryption,” and “LAN Data Protection” work as described in (1).

With the above functions, the TOE prevents unauthorized use of the TOE, unauthorized access to data stored in the HDD and communication data; thus, the TOE protects the data to be protected from unauthorized disclosure and alteration.

3.1.2 Organizational Security Policies and Security Function Policies

3.1.2.1 Organizational Security Policies

The organizational security policies required in use of the TOE are shown in Table 3-2. These organizational security policies are the same as specified in the PP except for addition of P.HDD.ACCESS.AUTHORIZATION. P.HDD.ACCESS.AUTHORIZATION is augmented for the PP under the assumption that it would generally be required to use a removable HDD on the TOE.

Table 3-2 Organizational Security Policies

| Identifier | Organizational Security Policy |
|-----------------------------|---|
| P.USER.AUTHORIZATION | To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner. |
| P.SOFTWARE.VERIFICATION | To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF. |
| P.AUDIT.LOGGING | To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel. |
| P.INTERFACE.MANAGEMENT | To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment. |
| P. HDD.ACCESS.AUTHORIZATION | To prevent access TOE assets in the HDD with connecting the other HCDs, the TOE will have authorized access the HDD data. |

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the security functions to satisfy the organizational security policies shown in Table 3-2.

(1) Means for organizational security policy “P.USER.AUTHORIZATION”

This policy is realized by “User Authentication” and “Function Use Restriction” functions of the TOE.

“User Authentication” function of the TOE only permits the users who are successfully identified and authenticated to use the TOE. To enhance the identification and authentication mechanism, the TOE enforces a password policy to use passwords of a certain minimum length containing a mixture of character types, and a lockout policy whereby a lockout of certain duration is imposed upon a certain number of failed authentication attempts.

Incoming print jobs or fax/I-fax jobs are accepted without requiring identification and authentication. The resulting document data are stored within the TOE, and not automatically printed out or transmitted. To print out or transmit document data stored in the TOE, the users must operate the control panel of the TOE, which will require identification and authentication.

“Function Use Restriction” function of the TOE performs access restriction on the use of the TOE functions, so that only the identified and authorized users with appropriate permissions are permitted to use the functions. For access restriction, users are assigned “roles” which are bound to permission information. This information is used to determine whether the use of the function is permitted to each user or not.

With the above functions, the TOE ensures that only the authorized users are permitted to use the TOE.

- (2) Means for organizational security policy “P.SOFTWARE.VERIFICATION”

This policy is realized by “Self-Test” function of the TOE.

“Self-Test” function of the TOE checks the integrity of the cryptographic algorithm and the cryptographic key generation algorithm that are used by LAN Data Protection function, after decrypting the executable code which is encrypted and stored in the HDD, at start-up. Thereby the integrity of the executable code of the TOE security functions is ensured.

Note that the self-test function does not check all executable codes of the TOE security functions; however, the evaluator evaluates that if the integrity of the part of the TOE security functions is verified, the integrity of all other executable codes decrypted by the same mechanisms is also ensured.

- (3) Means for organizational security policy “P.AUDIT.LOGGING”

This policy is realized by “Audit Log” function of the TOE.

“Audit Log” function of the TOE generates and stores audit logs in the TOE’s HDD at the occurrence of security-relevant events when security functions are used. The stored audit logs can be viewed by an authorized U.ADMINISTRATOR only, via a Web browser.

- (4) Means for organizational security policy “P.INTERFACE.MANAGEMENT”

This policy is realized by “User Authentication” and “Forward Received Jobs” functions of the TOE.

“User Authentication” function of the TOE ensures that only identified and authenticated users are allowed to use the TOE. Additionally, a session will be terminated, if a user leaves the session inactive longer than the specified time.

“Forward Received Jobs” function of the TOE restricts data received from various interfaces to be directly forwarded to the LAN without prior processing by the TOE.

These functions prevent the unauthorized use of the interfaces of the TOE.

- (5) Means for organizational security policy “P.HDD.ACCESS.AUTHORIZATION”

This policy is realized by the Device Identification and Authentication function, which is part of “HDD Data Encryption” function of the TOE.

The Device Identification and Authentication function in the “HDD Data Encryption” function is provided by the HDD Data Encryption & Mirroring Board, one of the components of the TOE. The HDD Data Encryption & Mirroring Board acquires the device authentication ID from the MFP device when it is initially mounted. At each start-up, it uses this information for a challenge and response method to confirm the identity of the MFP device, and grants access to the HDD only if it successfully confirms that it is mounted on the authorized MFP device.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. These assumptions are the same as specified in the PP.

The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

| Identifier | Assumptions |
|------------------|--|
| A.ACCESS.MANAGED | The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE. |
| A.USER.TRAINING | TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures. |
| A.ADMIN.TRAINING | Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures. * The meaning of "correctly configure" includes the description specified in (1) and (2) of Section 8.2 "Recommendations." |
| A.ADMIN.TRUST | Administrators do not use their privileged access rights for malicious purposes. |

4.2 Environmental Assumptions

The TOE is an MFP designed to operate in a typical office environment, where the MFP is connected by an internal LAN, and the internal LAN is protected by Firewall, etc., from threats from the external network. The assumed operational environment of the TOE is shown in Figure 4-1.

TOE users can operate the TOE from its control panel, from a PC connected via USB, or from a PC connected to the LAN.

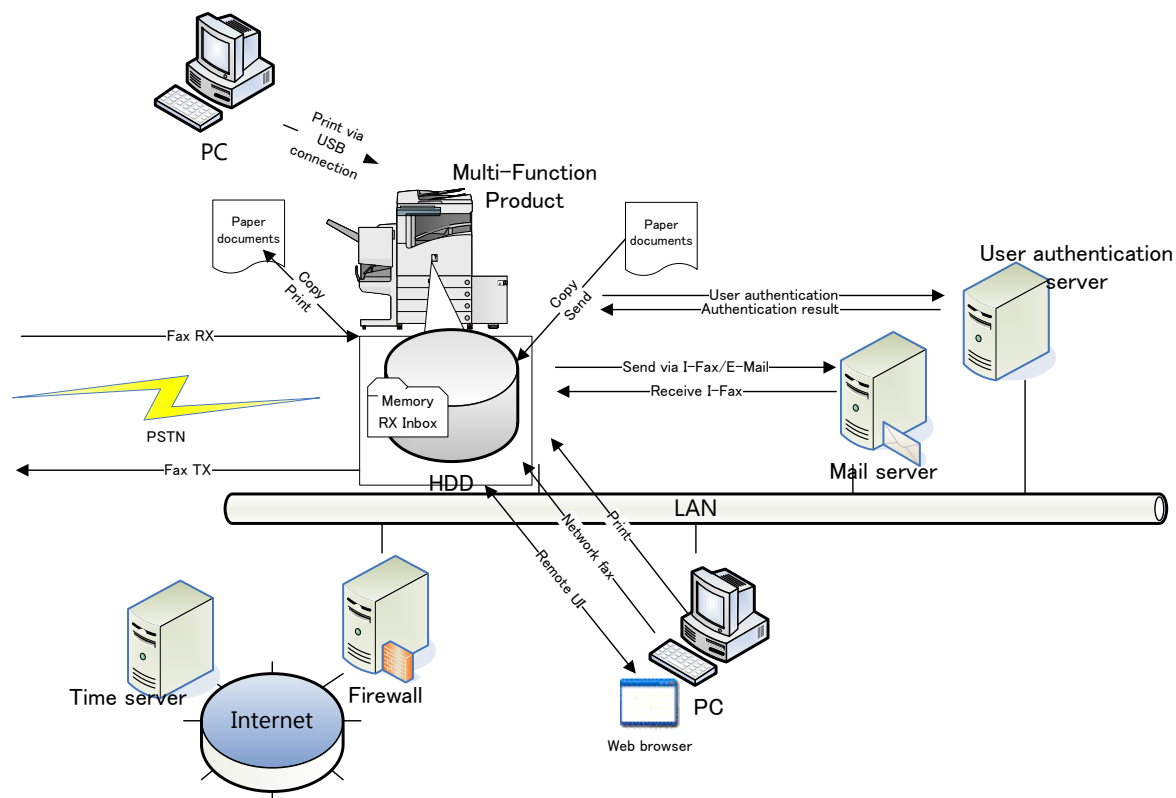


Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following components.

(1) PC

It is a generic PC used by a user to connect to the TOE, via USB or internal LAN. This evaluation was performed using the following software.

- Printer driver: the following printer drivers were used for this evaluation.
 - Canon UFR II Printer Driver Version 21.45
 - Canon PS Printer Driver Version 21.45
 - Canon PCL6 Printer Driver Version 21.45
- Web browser: Microsoft Internet Explorer 8

(2) User Authentication Server

The TOE supports two methods of “User Authentication” of the TOE described in Chapter 3: “Internal Authentication” where authentication takes place using user information stored within the TOE, and “External Authentication” where authentication takes place using user information stored in an external server.

The User Authentication Server is the server that is necessary for the TOE when using “External Authentication,” and the authentication protocol to be used is either Kerberos or LDAP.

This evaluation was performed using eDirectory 8.8 SP7 as the authentication server software for LDAP authentication and Active Directory Domain Service as the authentication server software for Kerberos authentication.

(3) Mail Server

A Server is installed as required to facilitate the I-fax capability of the MFP.

(4) Time Server

It is the NTP service commonly provided over the Internet. As long as the environment allows, it is recommended that a time server be configured in the TOE, to synchronize the time in the MFP that is used as the time stamp of audit logs. Otherwise, the time that is configured and maintained by the TOE's Management function is used instead.

Note that the reliability of hardware and associated software shown in this configuration is outside the scope of this evaluation (they are assumed to have sufficient reliability).

4.3 Clarification of Scope

In this evaluation, it is considered that the security functional requirements for the identification and authentication specified in the PP regarding the MFP's Print function do not apply to the operations on submitting print jobs; rather, they apply only to the operations on document data accumulated in the MFP, created by the submitted print jobs. As such, the following security functions are considered outside the scope of this evaluation.

- (1) The TOE supports various print protocols for the submission of print jobs. Some protocols have their own identification and authentication mechanisms, and those mechanisms are outside the scope of this evaluation. Examples of this include the identification and authentication mechanism in the IPP protocol or in the FTP protocol for FTP print.
- (2) When submitting a print job to the TOE through a print driver, the user is asked to provide the user name and PIN. This input is not used by the identification and authentication function. A PIN is associated with each document data submitted as a print job, and the user must provide the correct PIN in order to print that data from the control panel (this is known as "Secured Print"). This behavior is outside the scope of this evaluation.

The user name is not authenticated for its validity, but is simply associated with the submitted print job. The user name is used by the access restriction function for the target of evaluation.

5. Architectural Information

This chapter explains the scope of the TOE and its main components (subsystem).

5.1 TOE Boundary and Components

The configuration of the MFP or TOE as well as the IT environment other than the MFP is shown in Figure 5-1. In Figure 5-1, the TOE is shown within the bold line box marked as the TOE. User Authentication Server, Mail Server, PC, Time Server and User are not included in the TOE.

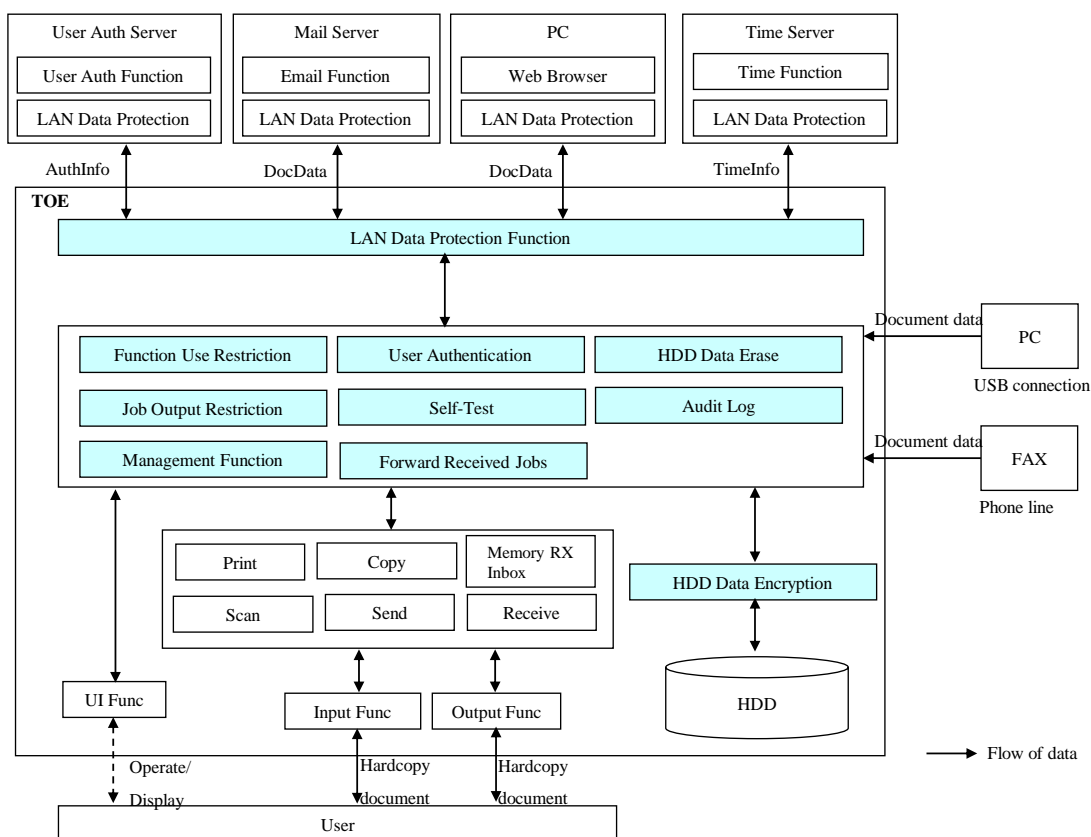


Figure 5-1 TOE Boundary

In Figure 5-1, the components shown in blue box within the TOE are the security functions of the TOE described in Chapter 3, and the remaining components shown in white box within the TOE are the basic functions of the MFP. For details on the basic MFP functions, see Glossary in Chapter 11.

Users of the TOE operate the TOE from its control panel (“UI Func” in Figure 5-1), from a PC connected to the LAN using a Web browser (“Web Browser” contained in “PC” in Figure 5-1), or from a PC connected via LAN or USB using a print driver (indicated only as the “PC” and a print driver is not illustrated in Figure 5-1).

The security functions of the TOE are applied when the user uses basic MFP functions. The following describes the relation between the security functions and the basic MFP functions.

- (1) When a user submits a print job from a PC connected via LAN or USB, or when a fax/I-fax job is received, the jobs are accepted without requiring identification and authentication, and the resulting document data are stored within the TOE. The user may perform operations on the document data in the TOE later, using the control panel or from a Web browser.

When the user attempts to access the basic MFP functions from the control panel or from a Web browser, “User Authentication” and “Function Use Restriction” functions are applied, so that only authorized users are allowed to use the TOE. Subsequently, when the user attempts to execute an operation on a document data stored in the TOE, “Job Output Restriction” function is applied, so that only the owner of the document data or the Administrator is allowed to operate the document data.

When the user attempts to use “Management” function or the function to browse audit logs provided by “Audit Log” function from the control panel or a Web browser, “User Authentication” function is applied, so that only the identified and authenticated users with Administrator privileges can gain access to the TOE.

Note that audit logs are generated by “Audit Log” function when these security functions are used.

- (2) In the use described in (1) above, “HDD Data Encryption” function is applied to all data stored in the internal HDD device, and “HDD Data Erase” function is applied when document data are deleted.
- (3) In the use described in (1) above, “LAN Data Protection” function is applied when the TOE communicates with other IT devices over the LAN. In addition, “Forward Received Jobs” function restricts data received from various interfaces to be forwarded without any TOE security functions applied.

5.2 IT Environment

When the external authentication method is used for “User Authentication” function of the TOE, Kerberos or LDAP protocol is used to query the information contained in the User Authentication Server to perform user identification and authentication. User account information is registered in the User Authentication Server through the management function of the User Authentication Server.

The time information recorded on the TOE’s audit logs is provided by the TOE. The time information of the TOE is set and maintained by the Management function of the TOE, or can be synchronized with an external time server using the NTP protocol.

The TOE uses IPsec protocol to communicate with other external IT devices over the network. As such, those external IT devices need to have IPsec protocol configured as well.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

(Japanese name)

- imageRUNNER ADVANCE C350/C250 Series 2600.1 model e-Manual CD [FT6-0943 (000)]
 - This CD includes the following two documents:
 - imageRUNNER ADVANCE C350F e-Manual
 - ACCESS MANAGEMENT SYSTEM Individual Management Configuration Administrator Guide
- iR-ADV Security Kit-J1 for IEEE 2600.1 Administrator Guide [FT6-0941 (000)]
- Before Using the iR-ADV Security Kit-J1 for IEEE 2600.1 [FT6-0942 (000)]
- HDD Data Encryption Kit User's Guide [FT5-2437 (020)]

(English name)

- imageRUNNER ADVANCE C350/C250 Series 2600.1 model e-Manual CD (USE Version) [FT6-0946 (000)]
 - This CD includes the following two documents:
 - imageRUNNER ADVANCE C350iF/C250iF e-Manual
 - ACCESS MANAGEMENT SYSTEM Individual Management Configuration Administrator Guide
- imageRUNNER ADVANCE C350/C250 Series 2600.1 model e-Manual CD (APE Version) [FT6-0947 (000)]
 - This CD includes the following two documents:
 - imageRUNNER ADVANCE C350i/C250i e-Manual
 - ACCESS MANAGEMENT SYSTEM Individual Management Configuration Administrator Guide
- iR-ADV Security Kit-J1 for IEEE 2600.1 Common Criteria Certification Administrator Guide [FT6-0944 (000)]
- Before Using the iR-ADV Security Kit-J1 for IEEE 2600.1 Common Criteria Certification [FT6-0945 (000)]
- HDD Data Encryption Kit Reference Guide [FT5-3328 (010)]

(Supplementary note)

“APE” in the above identification of documents represents a product for Australia, Singapore, and Hong Kong. “USE,” on the other hand, represents a product for other regions than those “APE” countries.

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Mizuho Information & Research Institute, Inc., Information Security Evaluation Office 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 is agreed on mutual recognition with 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.

7.2 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 summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.3 Overview of Evaluation Activity

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

The evaluation has started on 2013-03 and concluded upon completion of the Evaluation Technical Report dated 2016-02. 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. Additionally, the evaluators directly visited the development and manufacturing sites on 2015-02, 2015-08, and 2015-11, and examined procedural status conducted in relation to each work unit for configuration management, delivery and development security, by investigating records and interviewing staff. Furthermore, the evaluators conducted the sampling checks of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2015-06, 2015-07, and 2016-01.

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

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As a result of the evidence shown in the process of the evaluation and the verification results of the testing performed by the developer, the evaluator performed the reproducibility testing, additional testing, and penetration testing based on vulnerability assessments judged to be necessary.

7.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of the actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

The TOEs used in the developer testing are iR-ADV C350F and iR-ADV C350iF models with the same TOE identification described in Chapter 2.

The evaluator evaluated that it is sufficient to test each representative model only for the models with additional license and for the models without additional license. This is because, except for the additional license for the models indicated by the character “i” at the end of their names, the differences between the MFP models are hardware performances such as scanning and printing speeds, and there is no difference in the behavior of the security functions. Note that the evaluator tested other MFP models that were not tested by the developer to verify machine independence. For details, see Section 7.4.2 “Evaluator Independent Testing.”

Details of the non-TOE components of the developer testing environment are given in Table 7-1. The configuration for this testing is the operational environment of the TOE as described in Figure 4-1, except for the following differences. Besides these differences, this configuration is identical to the configuration specified in the ST, and the evaluator evaluates that these differences do not affect the purpose, which is to test the TOE's functions.

- Although included in the description in the ST, no firewall is used in the testing environment since it was not connected to the Internet.
- The fax machine is connected to the fax board via a pseudo-exchanger instead of the public switched telephone network (PSTN).
- Either “User Authentication Server 1” or “User Authentication Server 2” is used as the User Authentication Server, depending on the protocol used for external authentication.
- The Internet Time Server is substituted with the software on the “Time Server.”
- The optional fax board (2nd line) is attached to the MFP.

Table 7-1 Devices used for the Developer Testing

| Device Name | Description |
|------------------------------|---|
| PC | The user's PC. <ul style="list-style-type: none"> - OS: Windows 7 Professional - Web browser: Internet Explorer 8 - Printer driver: Canon UFR II Printer Driver Version 21.45 |
| User Authentication Server 1 | It serves as the authentication server (Kerberos) used in external authentication server. <ul style="list-style-type: none"> - PC with Windows Server 2008 Enterprise SP1 installed - Authentication server software: Active Directory Domain Services (Comes with the OS) |
| User Authentication Server 2 | It serves as the authentication server (LDAP) used in external authentication. <ul style="list-style-type: none"> - PC with Windows Sever 2003 Standard Edition SP2 installed - Authentication server software: eDirectory 8.8 SP7 |
| Time Server | <ul style="list-style-type: none"> - PC with Windows Server 2008 Enterprise SP1 installed - Time server software: Windows TIME (Comes with the OS) |
| Mail Server | It is used as the server for I-fax transmissions. <ul style="list-style-type: none"> - PC with Windows Server 2003 Standard Edition SP2 installed - Mail Server software: Microsoft POP3 Service (comes with the OS) Simple Mail Transfer Protocol (comes with the OS) |
| Fax Board | Optional fax board for the 2nd line. It expands the number of fax lines to two. (One line is used in the case of Canon Super G3 FAX Board-AN1 only, which is part of the TOE.) <ul style="list-style-type: none"> - Canon Super G3 FAX Board-AN1 |
| Fax Machine | The fax machine (not shown) at the free end of the telephone line in Figure 4-1. In the testing, it is connected to the fax board via a pseudo-exchanger. <ul style="list-style-type: none"> - iR-ADV C250iF |

2) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

- (1) By operating the user interfaces such as control panel, Web browser, and printer driver, the developer confirms the output messages of the user interfaces, the TOE's behavior, and the contents of audit logs.

- (2) To confirm the HDD Data Erase function, the developer uses the HDD protocol analyzer to read the deleted contents of the HDD to confirm that the contents are overwritten with the specified data.
- (3) To confirm the HDD Data Encryption function, the developer compares the encrypted data stored in the HDD with the result of the data encrypted by another tool, and confirms that the TOE implements the cryptographic algorithm according to the specification. For the cryptographic key generation, the developer also compares the results of random numbers that were generated using various seed values with the known data, and confirms that the TOE implements the cryptographic key generation algorithm according to the specification.
- (4) To confirm the IPsec function, the developer confirms that IPsec communication is established with the PC and that IPsec communication properly functions. The developer also confirms that the cryptographic communication protocol is applied according to the specification by using a network analyzer.
- (5) To confirm the Device Identification and Authentication function of the HDD Data Encryption Kit, the developer checks its behavior when mounted on the MFP with the correct ID as well as when mounted on a MFP with an incorrect ID.
- (6) For the configuration with the optional fax board for the 2nd line attached, the developer conducted the same testing as performed on the configuration without the optional fax board for the 2nd line attached, in order to confirm that there is no difference in these two configurations other than the number of the fax lines.

<Developer Testing Tools>

The tools used for the developer testing are shown in Table 7-2 below.

Table 7-2 Developer Testing Tools

| Tool Name | Description |
|--|--|
| LeCroy Sierra M6-4 (SAS-M006-804-X) | It is a tool that monitors the bus connected to the HDD and analyzes input/output data. |
| LeCroy SATA Protocol Suite Ver.4.00 build 385 | It is a tool that analyzes the data captured by the HDD Protocol Analyzer. |
| Network Analyzer Wireshark Ver. 1.12.4 | It is a tool that monitors and analyzes data communicated over the LAN. |
| Encryption Library Fujitsu AES library for FR Ver. 1.0 | It is used to compare encrypted data in order to check the accurate implementation of the encryption algorithm. |
| TamperIE 1.0.1.13 | It is a tool that mediates the communication from the Web browser to the Web server and that refers and changes the communication data between them. |

| Tool Name | Description |
|----------------------------------|--|
| Fiddler Web Debugger V2.5.0.0 | <p>It is a tool that mediates the communication from the Web browser to the Web server and that refers and changes the communication data between them.</p> <p>It has higher capability than TamperIE and is used to observe the communication data, which are the responses from the Web server to the Web browser.</p> |

<Content of the Performed Developer Testing>

It was confirmed that the security functions to be applied to various input parameters operate according to the specification by operating the basic MFP functions and security management functions from various interfaces. It was also confirmed that all acceptable setting values for the evaluated configuration, such as internal or external authentication settings, operate according to the specification.

b. Scope of the Performed Developer Testing

The developer testing was performed on 358 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been sufficiently tested. By the depth analysis, it was verified that all subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

The evaluator confirmed the approach of the performed developer testing and the legitimacy of tested items, and confirmed the consistency between the testing approach described in the testing plan and the actual testing approach. The evaluator confirmed the consistencies between the testing results expected by the developer and the actual testing results performed by the developer.

7.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of the security functions by the test items extracted from the developer testing, and the evaluator performed the evaluator independent testing (hereinafter referred to as the “independent testing”) to gain further assurance that security functions are certainly implemented, based on the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The configuration of the testing performed by the evaluator is the same as the configuration of the developer testing.

The TOEs tested by the evaluator are iR-ADV C350F, iR-ADV C350iF, or iR-ADV C250iF among the models with the same TOE identification as described in Chapter 2.

The independent testing was performed in the same environment as TOE configuration

identified in the ST.

Note that the components and testing tools used in the independent testing environment were the same as those used in the developer testing. Their validity confirmation and behavior tests were performed by the evaluator.

2) Summary of Independent Testing

A summary of the performed independent testing is as follows.

a. Independent Testing Viewpoints

The evaluator devised the independent testing in terms of the following viewpoints, based on the developer testing and the provided evaluation documentation, in order for the evaluator him/herself to demonstrate that the TOE security functions work as specified.

<Independent Testing Viewpoints>

- (1) By testing other models that were not tested by the developer, the evaluator confirms that the differences between models are those of hardware performance (i.e., processing speed) only, and the differences do not affect the behavior of the security functions.
- (2) In terms of the sampling of the developer testing, the evaluator performs the same testing as the developer testing performed, by extracting test items so that all TSFIs and security functions are included.
- (3) In the developer testing, there are some interfaces that were not rigorously tested to examine the behavior of the security functions, so the evaluator confirms the behavior of the parameters that were not yet tested.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

Using the same approach as that of the developer testing, the same testing and the testing with changed parameters were conducted.

<Independent Testing Tools>

The same testing tool as that of the developer testing was used.

<Content of the Performed Independent Testing >

Table 7-3 shows viewpoints of the independent testing conducted by the evaluator with the corresponding testing contents. Note that while the developer testing covered all setting values, the evaluator testing was performed using the default setting values that were set immediately after completing all installation procedures.

Table 7-3 Independent Testing Performed

| Viewpoint of independent testing | Outline of independent testing |
|---|---|
| (1), (2) | Based on the viewpoints, test items were extracted from the developer testing, and the same tests were repeated to determine that the same results can be obtained in the independent testing. Out of a total of 358 test items, 137 test items were tested. |
| (3) | The evaluator confirmed that the behavior of the threshold values of the length of the user password, box PIN, or password for machine maintenance was according to the specification. |
| (3) | The TOE provides multiple roles available as U.NORMAL. The evaluator confirmed that whatever the role a user was assigned for U.NORMAL, the user would not be able to use the management functions intended only for U.ADMINISTRATOR according to the specification. |
| (3) | <p>The evaluator confirmed that the behavior was as expected, when a secured print job is submitted using a user name that is not registered in the TOE.</p> <p>(i.e., The Administrator can browse or delete all secured print jobs. A non-Administrator cannot operate because the access is denied as the user name will not match.)</p> |
| (3) | The evaluator confirmed that a log of the transmission error was generated according to the specification, when the LAN cable was unplugged while a document stored in a box was being transmitted to the network. |
| (3) | The evaluator confirmed that the HDD Data Erase function properly operated, even when fax transmission was interrupted due to a problem outside the TOE. |
| (3) | The evaluator confirmed that no IPsec connection was established, when IPsec was not properly configured (i.e., no encryption, or a weak cryptographic algorithm was specified) on the connected PC. |
| (3) | The evaluator confirmed that a special function for maintenance would not become available by the specific operation that does not need identification and authentication. |
| (3) | When using different Secured Print settings from the developer testing, the evaluator confirmed that the user authentication function would not be affected. |
| (3) | In the tests to change the input from Web browser to Web server (TOE) using tools, the evaluator confirmed that input checks were properly conducted by adding a negative number as an input, which was considered as an incorrect value, when the type and number of the input characters were different from those used in the developer testing. |

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed the consistencies between the expected behavior and all the testing results.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the “penetration testing”) on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation. The penetration testing performed by the evaluator is explained below.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

Note that for cryptographic keys, the evaluator determines that attackers with the assumed attack potential cannot obtain or guess the cryptographic key, based on the mechanism used at the TOE start-up to generate the cryptographic key and the analysis of the developer testing for that mechanism.

- (1) There is a concern corresponding to the TOE regarding the publicly available vulnerability information, such as the possibility of unauthorized use of network service, various vulnerabilities on the Web.
- (2) There is a concern in Web interfaces that identification and authentication or access control mechanisms may be bypassed if the URL is directly specified or session management information is guessed.
- (3) There is a possibility that the information on the TOE is acquired or tampered without authorization by exploiting the language used for the print job.
- (4) There is a concern that the TOE unexpectedly operates when powered OFF/ON during start-up or shut-down.
- (5) There is a concern that the TOE operates unexpectedly when the same document data is simultaneously accessed from the control panel and from a Web browser.
- (6) There is a concern that the TOE unexpectedly operates when the TOE’s resources such as disk space are exhausted.
- (7) There is a concern that a security may be compromised when the TOE is activated with a special operation for maintenance if some operation is made in that state.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The penetration testing was conducted in the same environment as the evaluator independent testing. The TOEs used as the target of this test are iR-ADV C350F or iR-ADV C350iF.

The penetration testing was performed by using an additional PC with the penetration testing tools. Details of the tools used are provided in Table 7-4 as follows. The specification confirmation, behavior tests, and calibration for these tools were performed by the evaluator.

Table 7-4 Penetration Testing Tools

| Tool Name | Description |
|----------------------------|---|
| PC for penetration testing | A PC running Internet Explorer 8 and the following penetration testing tools. |
| (1) Nessus 6.5.4 | A tool that detects network service vulnerabilities. Vulnerability data is current as of January 21, 2016. |
| (2) nmap 6.47 | A tool that detects available network services. |
| (3) Nikto 2.1.5 | A tool that detects Web server vulnerabilities. Vulnerability data is current as of July 7, 2015. |
| (4) OWASP ZAP 2.4.0 | A tool that detects Web application vulnerabilities. |
| (5) TamperIE 1.0.1.13 | A tool that mediates communication from the Web browser (PC) to the Web server (TOE) to browse or alter communication data. TamperIE enables to change the communication data into arbitrary data with no restriction from the Web browser and send to Web server. |

<Contents of the Performed Penetration Testing>

Table 7-5 shows an outline of the penetration testing for the vulnerability of concern.

Table 7-5 Outline of the Penetration Testing

| Vulnerability of Concern | Outline of the Penetration Testing |
|---------------------------------|--|
| (1) | <ul style="list-style-type: none"> - Using Nessus and nmap on the TOE, the evaluator searched for any open ports and vulnerabilities, and confirmed that no unexpected ports were open and that no publicly-known vulnerabilities exist on the open ports. - Using Nikto and OWASP ZAP, the evaluator searched for vulnerabilities in the TOE's Web server function, and confirmed there were no publicly-known vulnerabilities. |

| Vulnerability of Concern | Outline of the Penetration Testing |
|--------------------------|--|
| (2) | <ul style="list-style-type: none"> - In the Web browser's login screen, the evaluator attempted bypass login by directly specifying the URL without login, and confirmed that login could not be bypassed. - During login from the Web browser to the TOE, the evaluator obtained multiple session information using TamperIE, and confirmed those were random numbers that could not be guessed by an attacker possessing the assumed attack potential. |
| (3) | <ul style="list-style-type: none"> - A job with a concern for the acquisition and/or tampering of data without authorization was created based on the grammar of the language used for print jobs and sent to the TOE. It was confirmed that no acquisition and/or tampering of the data without authorization was possible. |
| (4) | <ul style="list-style-type: none"> - It was confirmed that when the TOE was powered OFF during start-up, the TOE shut down properly showing no abnormal behavior. - It was also confirmed that when the TOE was powered ON during shutdown, the TOE started up after shutting down, showing no abnormal behavior. |
| (5) | <ul style="list-style-type: none"> - It was confirmed that when the same document was accessed simultaneously from the control panel and a Web browser, one with the intent to delete the document, the other to merge and save under the same file name, the former delete operation and the latter save operation succeeded, showing no abnormal behavior. |
| (6) | <ul style="list-style-type: none"> - The evaluator attempted the operation that the number of registered users or secured print jobs exceeded the upper limit, and confirmed that it resulted in error, showing no abnormal behavior. <p>(It is also assumed that there is a concern for the exhaustion of disk space as a result of receiving excessive amount of fax data; however, it was tested as a part of the developer testing, so it was not tested in the penetration testing.)</p> |
| (7) | <ul style="list-style-type: none"> - When the TOE was activated with a special operation for maintenance, the evaluator attempted various operations possible from the operation panel and network and confirmed that no abnormal behavior was observed. |

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

The conditions for the evaluated configuration of the TOE in this evaluation are as described in the guidance documents, and users must follow the guidance documents to set up the TOE. Some of the TOE settings values include enabling/disabling of the security functions, and there are some fixed values in this evaluation. If any setting values that affect security are changed to the value that is advised not to set in the guidance documents, then the MFP with those settings is no longer regarded as the evaluated configuration.

7.6 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance:

2600.1, Protection Profile for Hardcopy Devices, Operational Environment A (IEEE Std. 2600.1TM-2009)

SFR packages conformance defined in the above PP:

- 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A: Conformant
- 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A: Conformant
- 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A: Conformant
- 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A: Conformant
- 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A: Conformant
- 2600.1-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A: Augmented
- 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A: Augmented
- 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.

- All assurance components of EAL3 package
- Additional assurance component ALC_FLR.2

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.7 Evaluator Comments/Recommendations

No particular recommendations for users (procurement entities) are provided by the evaluator.

8. 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 Reports shall be adequate.
2. Contents pointed out in the Observation Reports 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.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports, and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

- (1) In terms of the security functional requirements specified in the PP, this evaluation acknowledges that the requirements for identification and authentication do not apply to incoming print jobs. Consumers expecting identification and authentication to be enforced for incoming print jobs are therefore advised to take note that the TOE specification may not be consistent with their needs.
- (2) When “external authentication” is used in the TOE, Kerberos or LDAP can be used to communicate with the user authentication server. Where this is the case, the assurance provided by this evaluation specifically applies only when Kerberos with Active Directory Domain Services or LDAP with eDirectory 8.8 SP7 is used as the authentication server software.

9. Annexes

There is no annex.

10. Security Target

The Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

Canon imageRUNNER ADVANCE C350/C250 Series 2600.1 model Security Target,
Version 1.09 (September 28, 2015) Canon Inc.

11. 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 |
| TSE | TOE Security Functionality |

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

| | |
|-----|-----------------------|
| MFP | Multifunction Product |
| HCD | A Hardcopy Device |

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

| | |
|--------------------------|---|
| Box PIN | PIN used for access to Memory RX inbox where document data are stored. It is used to control access to document data. |
| Copy function | It produces duplicates of the hardcopy documents by scanning and printing. |
| 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, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones," and other similar products. |
| I-fax | Short for Internet Fax, which uses the Internet to receive and send fax documents, instead of telephone line. |
| Input function | A function to input hardcopy documents into the TOE. |
| Memory RX Inbox | A space to store fax/I-fax documents received in electronic form. |
| Memory RX Inbox function | It allows fax/I-fax documents received in electronic form to be stored in Memory RX Inbox, and provides functionalities such as printing, sending and deleting the documents stored in the Memory RX Inbox. |
| Output function | It allows the TOE to output hardcopy documents. |

| | |
|--------------------------------|--|
| Print function | It produces a hardcopy document from its electronic form stored in the TOE. |
| Print Setting | It contains various print setting options for selecting color/monochrome, paper type, and duplex printing, etc. |
| Receive function | It allows I-fax documents received in electronic form to be printed in hardcopy form, or transmitted in electronic form. |
| Scan function | It allows the conversion of data from its hardcopy form to its electronic form, to create document data. |
| Secured Print | PIN-based printing function of the TOE. |
| Send (Universal Send) function | It allows scanned document data or document data stored in a box to be received for transmission to an email address, shared folder on a PC, or I-fax transmission. |
| TOE Owner | A person or organizational entity responsible for protecting TOE assets and establishing related security policies. |
| TSF Confidential Data | Assets for which either disclosure or alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE. |
| TSF Protected Data | Assets for which alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable. |
| U.ADMINISTRATOR | A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP. |
| UI function | It allows users to operate the TOE from the control panel, and the TOE to display information on the control panel. |
| U.NORMAL | A User who is authorized to perform User Document Data processing functions of the TOE. |
| User Document Data | The asset that consists of the information contained in a user's document. |
| User Function Data | The asset that consists of the information about a user's document or job to be processed by the TOE. |

12. 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] Canon imageRUNNER ADVANCE C350/C250 Series 2600.1 model Security Target, Version 1.09, September 28, 2015, Canon Inc.
- [13] Canon imageRUNNER ADVANCE C350/C250 Series 2600.1 model Evaluation Technical Report, Version 4.0, (118844-03-R004-04) February 5, 2016, Mizuho Information & Research Institute, Inc. Information Security Evaluation Office
- [14] IEEE Std. 2600.1™ -2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009