Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-01-29 (ITC-0287)
Certification No.	C0277
Sponsor	RICOH COMPANY, LTD
Name of TOE	Remote Communication Gate A
Version of TOE	Machine Code (First 4 characters) : D459 Firmware Version : A1.18-C1.14-P1.12-K1.04
PP Conformance	None
Assurance Package	EAL3
Developer	RICOH COMPANY, LTD
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2010-10-22

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass

" Remote Communication Gate A " has been evaluated in accordance with the provision of the "IT Security Certification Procedure" 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 certification result in relation to IT Security Evaluation of "Remote Communication Gate A, Machine Code (First 4 characters) : D459 Firmware Version : A1.18-C1.14-P1.12-K1.04" (hereinafter referred to as "the TOE") developed by RICOH COMPANY, LTD, and evaluation of the TOE was finished on 2010-09-30 by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, RICOH COMPANY, LTD and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the Security Target (hereinafter referred to as "the ST") that is the appendix of this book together. Especially, the TOE security functional, the assurance requirements for TOE and rationale of sufficiency about those are specifically described in ST.

This certification report assumes "the consumer who brings in the remote diagnosis maintenance service for digital MFP manufactured by RICOH COMPANY, LTD" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

1.1 Product Overview

Overview of the TOE functions and operational conditions are as follows. Refer to Chapter 2 and below for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

The TOE is an IT device to be used for a service that remotely diagnoses and maintains digital MFPs and printers (hereinafter referred to as "device(s)") on a local area network (LAN) in general offices.

This remote diagnosis maintenance service (hereafter, "@Remote Service") provides the necessary maintenance functions for each device. The TOE sends the information received from the targeted devices that use the service to the maintenance centre, and the maintenance centre diagnoses the status of the devices based on the information. For providing @Remote Service, the TOE also intermediates the communication between the targeted devices and the maintenance centre.

In order to prevent leakage or tampering of assets to be protected such as the maintenance service information, etc. communication between the TOE and the devices, and the communication between the TOE and the Communication Server (hereafter, "CS") of the maintenance centre are protected by the SSL protocol.
Only pre-assigned operations are provided for successfully identified and authenticated users in order to prevent execution of the Security Management Functions by operation from anyone other than TOE users and general user's misoperation.

For this security functionality, the evaluation for the validity of the design policy and the correctness of the implementation is conducted in the scope of the assurance package. The next clause describes the assumed threats and assumptions in this TOE.

1.1.2.1 Threats and Security Objectives

This TOE counters threats with the following Security Functions:

In order to protect the communication data, which includes the maintenance service information as protected assets, from leakage or tampering by a third party on the Internet, the SSL protocol is used for the communication with CS. This enables the communication data to be secured and the data tampering to be detected.

The TOE authenticates the CS and restricts communication with a pseudo CS in order to counter against sending malicious programs into the LAN if the attacker set up the pseudo CS on the Internet. This ensures that the TOE communicates with a genuine CS provided by RICOH COMPANY, LTD.

There are threats that those who are not authorised TOE users access the TOE and general users accidentally perform the TOE operations which are permitted for administrators only. As a countermeasure against these threats, for remote operation of the TOE from a client computer's web browser, the TOE identifies and authenticates users prior to the remote operation and allows the users to remotely operate the TOE. The TOE ensures users' access to and only to protected assets permitted according to the role (general user or administrator).

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

This TOE is assumed to be used in the LAN environments such as general offices and it is managed through Web browsers of client computers on the LAN.

The TOE administrators, who have the necessary knowledge to securely manage and operate the TOE, physically protect the TOE, and the LAN environment is protected from the external attackers through the Internet. Also, network administrator shall instruct users not to change the communication information of the TOE on the LAN. The device administrator shall manage the maintenance of the devices connected to the LAN. Genuine devices shall be acquired and used.

The devices are categorised as an HTTPS-compatible device and an SNMP-compatible device depending on the compatible communication methods. Both the compatible devices are the scope of the remote diagnosis maintenance service.

The TOE administrator, network administrator, and device administrator shall not use their privileges maliciously.

For the maintenance of the TOE, the TOE administrator shall allow only the qualified Customer Engineer (hereafter, "CE") who is qualified by RICOH COMPANY, LTD. to maintain it.

1.1.3 Disclaimers

1. This TOE does not provide the following functions:
- The TOE does not provide the Communication Protection Function to use the SSL protocol in the Device Firmware Update Function on the communications between the TOE and HTTPS-compatible devices.
- The TOE does not provide the Communication Protection Function to use the SSL protocol on the communications between the TOE and SNMP-compatible devices, because SMNP-compatible devices rarely support SSL-protected SNMP.

2. In this TOE, the following is not the scope of this evaluation:
- Although this TOE has the Supplementary Functions such as IEEE802.1X Authentication Function and recording and displaying the security logs, these functions are not the scope of this evaluation.
- If updated with the RC Gate Firmware Update Function to the version except for A1.1.8-C1.14-P1.12-K1.04., the updated version is out of the scope of this evaluation assurance.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2010-09 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Reports prepared by Evaluation Facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure.

Certification oversight reviews are also prepared for those concerns found in the certification process.

Those concerns pointed out by the Certification Body are fully resolved, and the Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]).

The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and concluded fully certification activities.

2. Identification

The TOE is identified as follows;

Name of TOE	Remote Communication Gate A
Version of TOE	Machine Code (First four characters): D459 Firmware Version: A1.18-C1.14-P1.12-K1.04
Developer	RICOH COMPANY, LTD.

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

- Machine code of the TOE: check the first four characters of the machine code printed on the rating plate label (silver) on the hardware chassis.

- Firmware version of the TOE: check the login screen (top right side of the page) of the Remote Communication Gate A (hereafter, "RC Gate") via the client computer's Web browser.

3. Security Policy

This chapter describes security function policies and organisational security policies.

The TOE sends the information received from the devices installed on LAN in general offices to the maintenance centre on the external networks and the maintenance centre diagnoses the status of the devices based on the information, and it is used for the service to execute the maintenance required for each device. The TOE provides the following functions to securely use the service:

The TOE provides the functions to protect the communication data which includes the maintenance information flown over the external networks and the communication data flown over the LAN from leakage or tampering.

In order to prevent unauthorised persons from exploiting the TOE, the TOE provides the User Identification and Authentication Function and the function that allows the successfully authenticated users to access the maintenance information, configure and change the management function settings according to their roles.

The TOE provides a function for users to confirm that the firmware of the TOE is manufacturer-genuine and provided by RICOH COMPANY, LTD.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1. and to meet the organisational security policies shown in Chapter 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 for countermeasure against them.

This TOE classifies users into "administrator (TOE administrator)" and "general user".

The administrator (TOE administrator) installs and manages this TOE, and can change the RC Gate configurations and view the information collected from devices.
The general user is a user with a TOE user account (permitted by the administrator) who can view the information collected from devices using the client computer.

Table 3-1 Assumed Threats

Identifier	Threat
T.FAKE_CS (Spoofing on the Internet)	Attackers may launch a pseudo CS on the Internet that is not provided by RICOH COMPANY, LTD., install device firmware in the registered device, or send malicious programs such as a virus into the LAN.
T.INTERNET	Attackers may leak or tamper communication data sent

(Tampering of Communication Information on the Internet)	over the Internet when the TOE communicates with the CS. [Additional remarks] The communication data contains the maintenance service information such as billing information, failure information,, and firmware for updating.
T.ACCESS (Unauthorised Access)	Unauthorised TOE users may perform the TOE operation that is authorised only for general user or administrator. General user may accidentally exploit the Security Management Functions permitted for administrator.

3.1.1.2 Security Function Policies against Threats

This TOE applies the following security function policies to counter the threats shown in Table 3-1:

(1) Countermeasures against Threat, T.FAKE_CS
T.FAKE_CS is countered by the "Communication Protection Function between the RC Gate and CS".

The "Communication Protection Function between the RC Gate and CS" verifies the authentication of the CS with the certificate using the SSL protocol for the communication between the TOE and the CS. This allows the communications with only the genuine CS provided by RICOH COMPANY, LTD.

(2) Countermeasures against Threat, T.INTERNET
T.INTERNET is countered by the "Communication Protection Function between the RC Gate and CS".

The "Communication Protection Function between the RC Gate and CS" uses the SSL protocol to secure the communication data on the Internet and other communication paths between the TOE and the CS, and detects data tampering. This protects the communication data from leakage or tampering.

(3) Countermeasures against Threat, T.ACCESS
T.ACCESS is countered by the "User Identification and Authentication Function", "Security Management Functions", and "Access Control Function of Information Received from Devices".

The "User Identification and Authentication Function" implements the following countermeasures against threats:

- This function requires that users who attempt to remotely operate the TOE be identified and authenticated successfully.

- If a successfully authenticated user does not operate the computer for a certain period of time, the user is automatically logged off. With this functionality, unauthorised persons are less likely to remotely operate the TOE from the

computer.

- Passwords for user authentication must be secure so that the TOE makes it difficult to decode. Moreover the TOE doesn't give attackers sufficient time for Brute Force Attacks.

- To prevent users other than the administrator from changing the administrator's password, the users shall be re-authenticated before changing the administrator's password.

The "Security Management Functions" implements the following countermeasures against threats:

- Only administrators are allowed to use the Security Management Functions.

The "Access Control Function of Information Received from Devices" implements the following countermeasures against threats:

- This function restricts access to the information that can be viewed in accordance with user roles.

As mentioned above, only successfully identified and authenticated users are allowed to operate the TOE. Furthermore, the TOE is protected from unauthorised access by limiting the TOE functions that can be operated for each user role.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Table 3-2 shows the organisational security policies that are required for this TOE usage. Although these are not based on the concrete requirements or laws, the security policies are assumed by the developer, RICOH COMPANY, LTD., to be appropriate policies for organisations considering the installation of this TOE.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.ATR_DEVICE (Communication with HTTPS-compatible devices)	As for Machine Counter Notice Function, Service Call Function, and Supply Call Function, if the TOE communicates with the HTTPS-compatible device (a device that has the capability to communicate with the Communication Protection Function between the RC Gate and CS), measures shall be provided at communication start to confirm that the HTTPS-compatible devices are valid, and the communication information between the TOE and the HTTPS-compatible devices shall be protected.

P.SOFTWARE (Verifying the integrity of RC Gate Firmware)	Procedures shall be provided to confirm that the RC Gate Firmware built into the TOE is the genuine RC Gate Firmware provided by RICOH COMPANY, LTD.
P.PC_WEB (Communication with Computers)	For Web Function, tampering of information between computers and the TOE shall be detected and leakage of passwords shall be prevented.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to enforce the Organisational Security Policies shown in Table 3-2.

(1) **Means to support Organisational Security Policy "P.ATR_DEVICE".**
This organisational security policy will be achieved by implementing the "Communication Protection Function between the RC Gate and Devices".
The "Communication Protection Function between the RC Gate and Devices" verifies the correctness of the HTTPS-compatible devices with the certificate using the SSL protocol for communication between the TOE and the HTTPS-compatible devices in the Machine Counter Notice Function, the Service Call Function, and the Supply Call Function. Also, the Communication Protection Function between the RC Gate and Devices secures the communication data on the communication path, and detects data tampering.

(2) **Means to support Organisational Security Policy "P.SOFTWARE".**
This organisational security policy will be achieved by implementing the "RC Gate Firmware Validation Confirmation Function".
The "RC Gate Firmware Validation Confirmation Function" verifies the integrity of the executable codes of the RC Gate Firmware at the request of the authorised user, and it also verifies that it is the genuine RC Gate Firmware provided by RICOH COMPANY, LTD.

(3) **Means to support Organisational Security Policy "P.PC_WEB".**
This organisational security policy will be achieved by implementing the "Communication Protection Function between the RC Gate and Computers".
The "Communication Protection Function between the RC Gate and Computers" uses the SSL protocol for communication between the TOE and the client computers that are remotely controlled by users to secure the communication data on the communication paths and to detect data tampering.

No attackers are assumed for (1) and (3) because, as explained later, protection will be provided for the LAN environment against external attacks and other network management measures will be implemented by A.NETWORK, which is one of the assumptions and clarification of scope.
Also, no attackers are assumed for (2) because protection will be provided by the operational environment, according to A.ADMINSHIP.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and operational environments of this TOE, which will be valuable information for the assumed readers to use the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE.

Unless these assumptions are satisfied, the effective performance of the TOE Security Functions is not assured.

Administrators for this TOE are classified into "administrator (TOE administrator)", "network administrator", and "device administrator".
If this certification report simply mentions "administrator", it means the above TOE administrator.
"Network administrator" means an IT manager who is in charge of the customers' LAN where the TOE is installed.
"Device administrator" means a person in charge of the maintenance of the devices connected to the customers' LAN where the TOE is installed.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMINSHIP (Conditions of Administrator)	TOE administrator, network administrator, and device administrator shall not use their privileges maliciously.
A.TOE_ADMIN (Administration of the TOE)	The TOE administrator shall have the necessary knowledge and perform the administrative roles for the secure management and operation of the TOE in the administrators' work. The administrator shall also provide physical protection for the TOE.
A.NETWORK (Network Management)	The network administrator shall manage the LAN maintenance and instruct network users not to change the communication information of devices other than the HTTPS-compatible devices and the TOE. The network administrator shall also provide protection for the LAN environment from external attackers via the Internet. [Additional remarks] Devices other than the HTTPS-compatible devices indicate the SNMP-compatible devices that do not protect the communication with the TOE.
A.DEVICE (Device Management)	The device administrator shall manage the maintenance of the device connected to the LAN. The

	genuine and unmodified device shall be acquired and used.
A.CE (TOE Maintenance)	Only a qualified CE shall be able to maintain the TOE. [Additional remarks] To satisfy this assumption, the TOE administrator shall allow only a qualified CE only to maintain the TOE.

4.2 Environment Assumptions

This TOE is installed in general offices and connected to the internal networks, and it is used by client computers connected to the internal networks likewise. Figure 4-1 shows the general operational environment of this TOE.

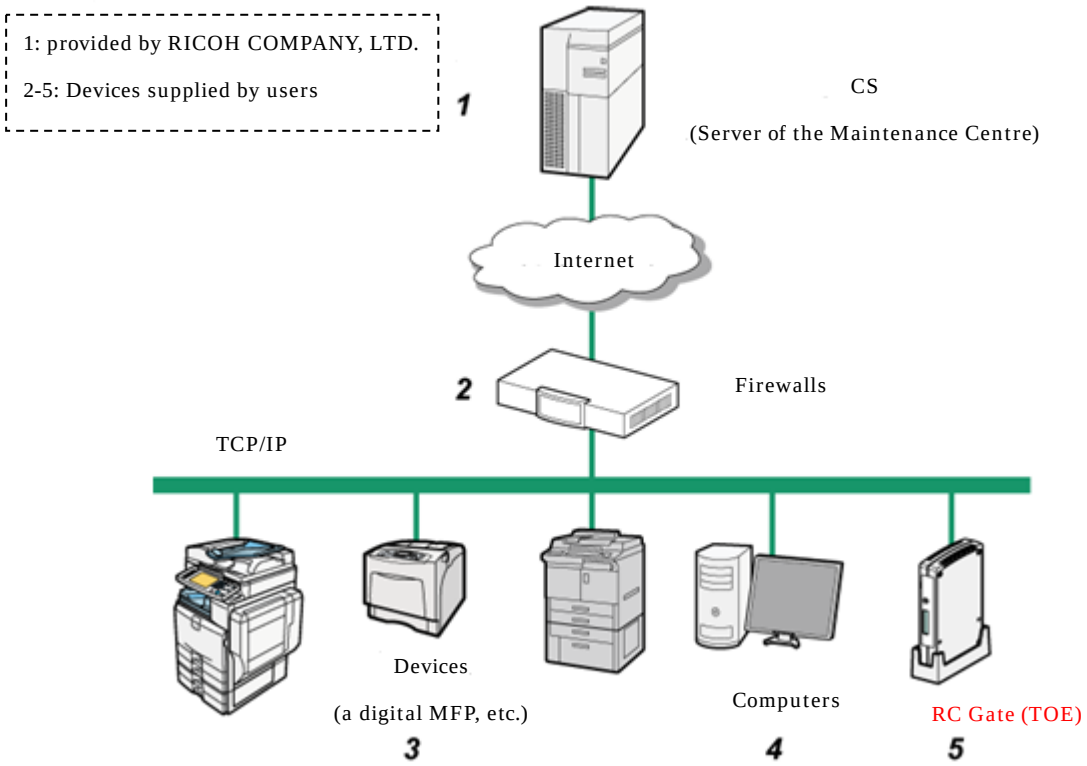

Figure 4-1 Operational Environment and Configuration

According to the number of Figure 4-1, the roles of each machine are explained as follows:

1. CS (Communication Server)
   A server located in the maintenance centre. The TOE requests to start communications and sends or receives the information for the maintenance service between the TOE and the CS.

2. Firewalls
   A security system to protect the office LAN environment from external networks.

3. Devices
   The "device" means either a digital MFP or a printer, both of which can communicate with the TOE connected to the office LAN environment. It is categorised according to its communication method with the TOE as either an HTTPS-compatible device or an SNMP-compatible device. The HTTPS-compatible device is a device that can communicate with the TOE using the "Communication Protection Function between the RC Gate and Devices", and the SNMP-compatible device is a device that is not an HTTPS-compatible device and that can communicate with the TOE by means of SNMP.

4. Computer
   A computer is connected to the office LAN environment. Users can remotely operate the TOE from a computer's Web browser. The Web browser should be Internet Explorer (Ver. 6.0 or above) with the Flash Player plugin (Ver. 9.0 or above).

5. RC Gate
   RC Gate is this TOE that is connected to the office LAN environment.

4.3 Clarification of scope

The developer does not assume that the Device Firmware Update Function protects the communication data on the communication path between the TOE and the HTTPS-compatible devices as the organisational security policies. Therefore, the Device Firmware Update Function does not provide Communication Protection Function by the SSL protocol.
Also the TOE provides no Communication Protection Functions using the SSL protocol on the communication between the TOE and the SNMP-compatible devices, because SMNP-compatible devices rarely support SSL-protected SNMP. For this reason, it is assumed that network administrators instruct network users not to change the communication information between the TOE and the SNMP-compatible devices in the operational environment of this TOE.

5. Architectural Information

This chapter explains the purposes and the relation about the scope of this TOE and the main component.

5.1 TOE boundary and component

The TOE consists of the entire hardware of RC Gate and the equipped firmware, and it consists of configuration items shown in Figure 5-1.

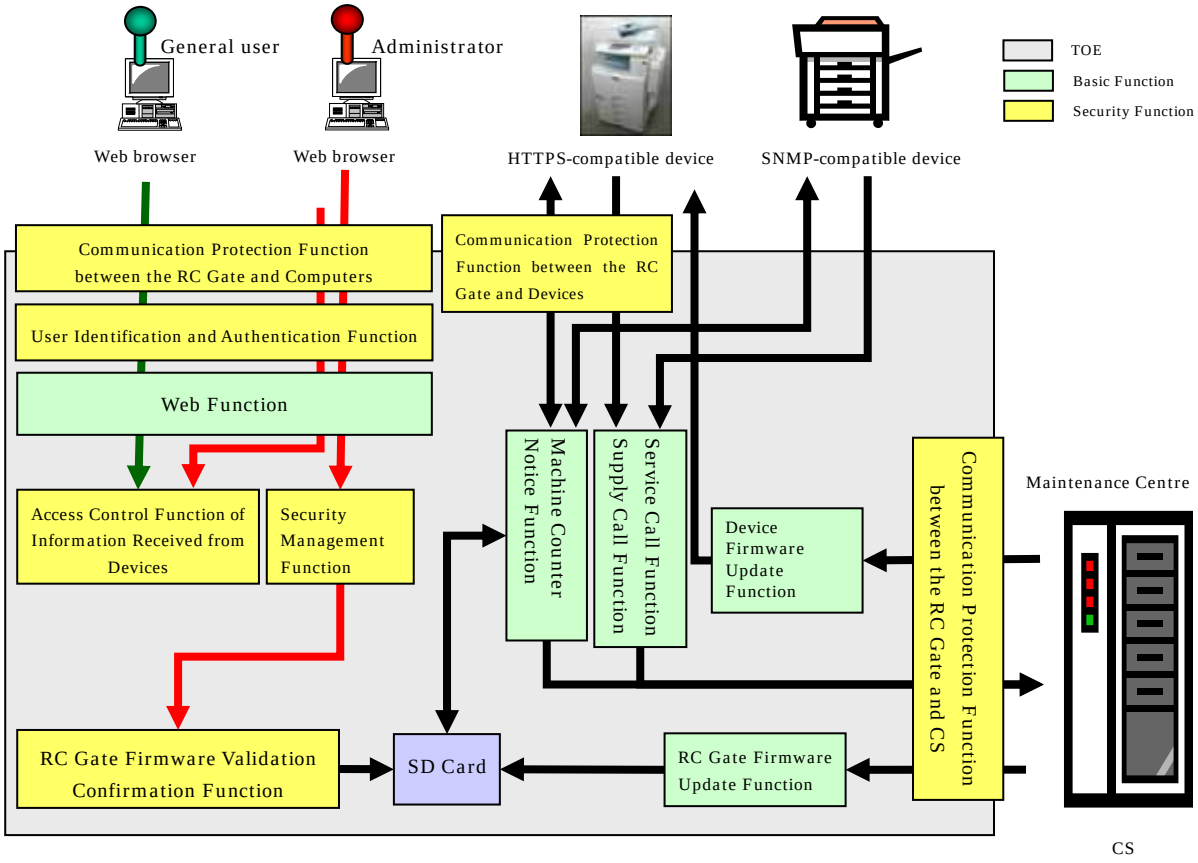

Figure 5.1 TOE boundary

The TOE consists of the Basic Functions and the Security Functions as functional components. The following shows the overview of the Basic Functions provided by @Remote Service and the relevant Security Functions.

Machine Counter Notice Function

A function that allows the TOE to periodically notify the CS about the machine counter information (number of print pages counted for each device) received from the registered device. The counter values are used for billing information.

The communication between the TOE and the HTTPS-compatible devices uses the SSL protocol by the "Communication Protection Function between the RC Gate and Devices" as the organisational security policies.

The communication between the TOE and CS uses the SSL protocol and protect the communication data from leakage or tampering by the "Communication Protection Function between the RC Gate and CS".

Service Call Function

A function that allows the TOE to report to the CS the device failure information received from the registered device.
The communication between the TOE and the HTTPS-compatible devices uses the SSL protocol by the "Communication Protection Function between the RC Gate and Devices" as organisational security policies.
The communication between the TOE and CS uses the SSL protocol and protect the communication data from leakage or tampering by the "Communication Protection Function between the RC Gate and CS".

Supply Call Function

A function that allows the TOE to notify the CS about the supply information (remaining toner and paper) received from the registered device.
The communication between the TOE and the HTTPS-compatible devices uses the SSL protocol by the "Communication Protection Function between the RC Gate and CS" as the organisational security policies.
The communication between the TOE and CS uses the SSL protocol and protect the communication data from leakage or tampering by the "Communication Protection Function between the RC Gate and CS".

Device Firmware Update Function

A function that allows the TOE to update the firmware of the registered HTTPS-compatible device with the device firmware received from the CS.
The communication between the TOE and CS uses the SSL protocol and protect the communication data from leakage or tampering by the "Communication Protection Function between the RC Gate and CS".
Only if the device firmware update permission settings are enabled by the "Security Management Functions", the device firmware can be updated.

RC Gate Firmware Update Function

A function that allows the TOE to update the RC Gate's firmware with the RC Gate Firmware received from the CS.
The communication between the TOE and CS uses the SSL protocol and protect the communication data from leakage or tampering by the "Communication Protection Function between the RC Gate and CS".
Only if the RC Gate firmware update permission settings are enabled by the "Security Management Functions", the RC Gate firmware can be updated.
(Notes): If the version is updated with this function except for the version of A1.1.8-C1.14-P1.12-K1.04., it is outside the scope of this evaluation and is not assured.

Web Function

A function that allows users to remotely operate the TOE. Users access the TOE via a computer's Web browser.

As the organisational security policies, the communications between the TOE and computers use the SSL protocol by the "Communication Protection Function between the RC Gate and Computers".

Only the successfully identified and authenticated, and permitted TOE users are allowed to use the Web Function by the "User Identification and Authentication Function".

The "Security Management Functions" and "RC Gate Firmware Validation Confirmation Function" are provided for only Administrator of the TOE users. The Administrator executes these functions using the Web browser from computers.

As for viewing the information received from the device stored in SD Card using the Web browser, the information that can be viewed by each user role (administrator and general user) is controlled by the "Access Control Function of Information Received from Devices".

5.2 IT Environment

Users can remotely operate the TOE from the Web browser of computers that are connected to the LAN environments. The Web browser should be Internet Explorer (Ver. 6.0 – 8.0) with the Flash Player plugin (Ver. 9.0 – 10.0).

6. Documentation

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

Guidance documents for Japan
- Remote Communication Gate A Safety Information (written in Japanese) (D459-8500A)
- Remote Communication Gate A Setup Guide (written in Japanese) (D459-8504A)
- Remote Communication Gate A Operating Instructions (written in Japanese) (D459-8501A)

Guidance documents for overseas countries
- Remote Communication Gate A Safety Information/Setup Guide (D459-8510A)
- Remote Communication Gate A Safety Information/Setup Guide (D459-8530A)
- Remote Communication Gate A Setup Guide (D459-8503A)
- Remote Communication Gate A Operating Instructions (D459-8502A)

As For Remote Communication Gate A Safety Information/Setup Guide, the difference between (D459-8510A) and (D459-8530A) is due to difference regulation in each country.

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3.

Details for evaluation activities are reported in the Evaluation Technical Report.

In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

The history of evaluation conducted was present in the Evaluation Technical Report as follows;

Evaluation has started on 2010-02 and concluded by completion the Evaluation Technical Report dated 2010-09.

The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted.

Additionally, the evaluator directly visited the development and manufacturing sites on 2010-04 and 2010-05 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff interview.

Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-05.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to the developer.

These concerns were reviewed by the developer and all concerns were solved eventually.

Concerns that the Certification Body found about the evaluation process was described as a certification oversight review, and it was sent to Evaluation Facility.

After Evaluation Facility and the developer examined it, these concerns were reflected in the evaluation report.

7.3 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had executed.

Based on the evidence shown by the process of the evaluation and those confirmed validity, the evaluator executed the sampling testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer executed and the testing documentation of actual testing results.

It explains the content of the developer testing evaluated by the evaluator as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configurations used by the developer and Table 7-1 shows the hardware and software configurations.

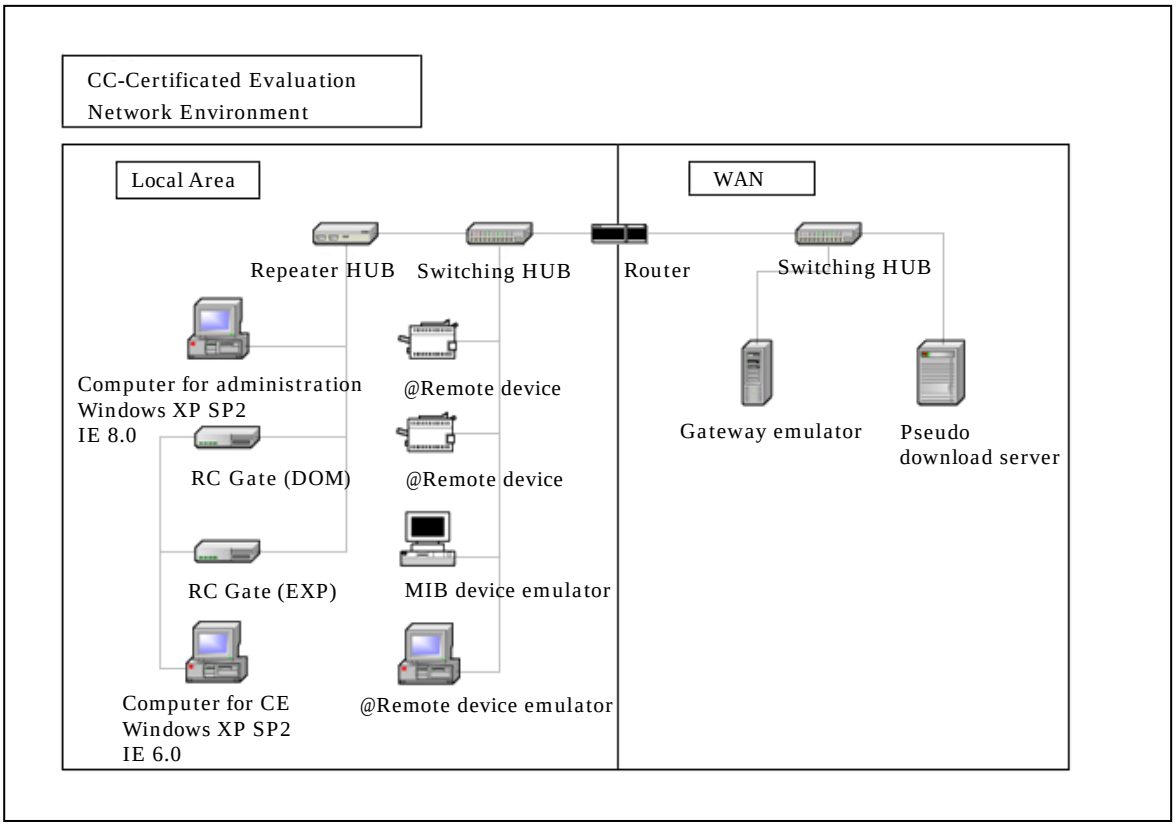

Figure 7-1 Configuration of the Developer Testing

Table 7-1 Hardware and Software Configurations

Hardware Type		Quantities	Specifications
RC Gate		2	Devices for testing (Japanese version/English version)
Gateway emulator		1	Gateway emulator (V1.07)
Devices	HTTPS-compatible device (@Remote device)	1	RICOH imagio MP C3500
			RICOH Aficio 3025
	@Remote device emulator (HTTPS-compatible device emulator)	1	@Remote device emulator (supplied with the Gateway emulator)
	MIB device emulator (SNMP-compatible device emulator)	1	MIB tool
Router		1	LAN/WAN 10BASE-T/100BASE-TX
Network environment		1	Private network environment
SD Card		2	Formatted by the initialisation tool
Pseudo download server		1	Server for TOE and device firmware release (Download the firmware from this Web server for executing the TOE and the Device Firmware Update Function)
Client computers		2	Computer for administration OS: Windows XP Professional SP2 Browser: Internet Explorer 8 Flash Player: Flash Player 10 Computer for CE OS: Windows XP Professional SP2 Browser: Internet Explorer 6 Flash Player: Flash Player 10

As for the devices used to conduct the testing, there are some differences between the devices, the CS, the software of the client computers, and the components identified in the ST. However, the devices are considered to be identical to the configurations in the ST by the following reasons:

1. Device:
Testing uses the emulator software which emulates the same communication functions as the actual devices, and the HTTPS-compatible devices and SNMP-compatible devices. Since the emulator used for the testing can emulate the identical communication protocols to the HTTPS-compatible devices and SNMP-compatible devices, the devices operated in the testing environment are identical with those in the ST.

2. CS:
The ST stipulates that the CS is installed in the maintenance centre and the TOE starts the communications to send or receive the information for the maintenance service between the TOE and CS. In the testing environment, a Gateway emulator is used as a substitute for the CS. Also, a pseudo download server is used as the server for firmware release of the TOE and the devices in order to download the firmware.
Although the Gateway emulator is not the actual CS, evaluators confirmed that the functionalities of the Gateway emulator and the pseudo download server are identical to the configurations of the ST when viewing from the TOE. Because the Gateway emulator emulates the CS from the communication protocols, and the pseudo download server also contains the functionality to emulate the functionalities of the server for firmware release of the actually used TOE and devices.

3. Software of client computers
Two client computers of terminals for administrator and CE are used for the testing. Although each computer has the different version of Internet Explorer, since all the in/output items and the check functions provided by the Web browser's screen are provided by Flash files (Application software), the items are not affected by the version of Internet Explorer.
As for Flash Player, Flash Player 10 is solely used and this TOE is not affected by the version because it does not use the functions changed/added from Flash Player 9.
As described above, since the testing is conducted with all the software (Internet Explorer (6.0 or above), Flash Player (9.0 or above)) described in the ST, the software examined in the testing environment is consistent with the one in the ST.

2) Summary of Developer Testing
Summary of the developer testing is as follows:

a. Developer Testing Outline
Outline of the developer testing is as follows:
<Developer Testing Approach>
The developer testing was conducted using the following two approaches:

1. Testing approaches using external interfaces:
The testing procedure consisted of stimulation of the external interfaces and visual observation of the results by the operation of Web browser and directly operating the buttons on computers connected to the TOE.
The input for the external interfaces means pushing the buttons, and the buttons or parameters specified in the entry fields displayed on the browser. The responses from the external interfaces mean that messages will appear in the Web browser's screen or LCDs.
These tests consisted of the following executed tests of each external interface:
exclusive control test at simultaneous execution of processing,
test when input parameter is outside of the allowable range and within the range,
test when process ends normally and when terminating abnormally

If the behaviors of the modules vary depending on the initial conditions and the input parameters, the testing was conducted for each of the initial conditions and the input parameters.

2. Testing approaches for testing items that no external interfaces can be used for:
The behaviors that cannot be observed by the external interfaces were tested by alternative approaches using analysis tools and emulators. The outline of the main alternative approaches applied is as follows:
- The communication with the SSL protocol
Whether or not providing the communications to use the SSL protocol on the communication paths was checked by the order and contents of the line packets for which a packet capture analysis tool (Wireshark) was used.
- The responses to the actions such as communication initiation or termination
Whether or not the communications was initiated or terminated was checked by the log contents of the Gateway emulator outputted for each request from the TOE.

<Tools for the developer testing>
Table 7-2 shows the tools used for the developer testing. Wireshark is designed mainly for network management. It is an open source tool and is generally and widely used for packet analysis. Like Wireshark, Winpcap is also designed mainly for network management and is a generally used packet capture library.

Table 7-2 Developer Testing Tools

No	Tool Name	Ver.	Function	Operational Environment
1	Wireshark	1.0.5	Packet analysis	Windows
2	WinPcap	4.1.1	Packet capture library	Windows

<Content of execution of the developer testing>
For the related functions to the external interfaces, the test results shown in the error messages and screen displays according to the users' stimulation were compared with the expected test results.
In the communications with the SSL protocol between the TOE and CS, devices, and client computers, both the order of line packets and the contents were checked by the packet capture analysis tool (Wireshark).
To confirm that the Firmware Validation Confirmation Function is properly terminated, the display media such as LED and LCD, and the Web browser were observed so that the behavior of the function was indirectly checked, and this observation was compared with the expected test results.

b. Scope of Execution of the Developer Testing
The developers tested 194 items.
The implementation of a coverage analysis verified that all Security Functions and external interfaces specified in the functional specifications were fully tested. Also, the implementation of a depth analysis verified that all subsystems and subsystem interfaces specified in the TOE design specifications were fully tested.

c. Result
It was confirmed that the expected results of the developer testing matched the actual test

results. The evaluators confirmed the approaches of the developer testing and the validity of the tested items, and also confirmed that both the approaches and results matched the test plans.

7.3.2 Evaluator Independent Testing

The evaluators conducted the independent testing for reconfirmation of the Security Functions whose implementation can be ensured, referring to the materials shown in the evaluation process.

An overview of the independent testing performed by the evaluators is as follows:

1) Independent Testing Environment
The evaluators' test configurations were identical with those of the developer testing.
Figure 7-1 shows the evaluators' test configurations.

2) Summary of Independent Testing
The evaluator independent testing includes sampling the results of the developer testing and conducting the evaluator independent testing that the evaluators devised.
Details of the independent testing performed by the evaluators are as follows:

a. Independent Testing Viewpoints

<Sampling Testing Viewpoints>
The evaluators sampled 47 out of 194 items of the developer testing regarding the following viewpoints:
1. At least one interface test was sampled for interfaces of all Security Functions.
2. In this TOE, the test case for Web interface was selected to enforce the test more than other interfaces, because the greater part of Security Functions are related to this interface and it is complex.
3. In case of implementing the two types of the normal and abnormal testings for one testing, the abnormal testing was sampled because the normal testing was implicitly conducted in other testings.
4. The independent testing does not cover the sampling items that are regarded as the same functions can be tested by changing parameters or testing approaches.

<Evaluator Independent Testing Viewpoints>
The independent testing performed by the evaluators was as follows:
1. For the Web interfaces, the testing items that changed the parameters were added to the items that have insufficient types of the parameters (e.g. values entered as the password, etc.).
2. No tests to simultaneously check the security functionalities were included in the developer testing, so the test was added to the independent testing.
3. Since there are verification approaches for the interfaces or functionalities other than those that developers implemented in the developer testing, other approaches were added to the independent testing due to insufficient verification for the operations in such methods.
4. There are various types of exception procedures for each interface, so that if an exceptional procedure was not tested in the developer testing, it was added to the independent testing.
5. Since the developer testing did not fully check data entry using both single-byte and two bytes characters in the English version of the TOE, the test was added to the independent testing.
6. The functional specifications state the permutational and probabilistic

mechanisms of passwords. To check that this function can meet the expectations and assumptions, the test was added to the independent testing.

b. Independent Testing Outline
An overview of the independent testing of the evaluators is as follows:

<Independent Testing Approach>
The independent testing was conducted applying the same approaches used for the developer testing.

<Tools for the independent testing>
The independent testing was conducted using the tools that are specified in Table 7-2 that were used for the developer testing.

<Content of execution of the independent testing>
For the independent testing conducted by the evaluators, the outlines of the 47 sampling tests and sampling items of the developer testing are specified in Table 7-3, and the outlines of the independent testing of the evaluators are specified in Table 7-4.

Table 7-3 Outlines of the Developer Testing and Sampling Items

Outlines of the developer testing	Number of sampling items
Checked the User Identification and Authentication Function (administrator).	4
Checked the Communication Test Call Function (SSL communication).	2
Checked the Communication Function between Devices and the TOE (SSL communication).	6
Checked the accessible functions only by administrator.	1
Checked the function to store the internal data.	2
Checked the Checking Function of Firmware Validation.	3
Checked the CE Access Permission Function.	2
Checked the Restriction Function to update the RC Gate Firmware.	3
Checked the Restriction Function to update the device firmware.	3
Checked the Access Control Function (Counter list).	13
Checked the Communication Function between the TOE and CS (SSL communication) (Service/Supply Call).	8

Table 7-4 Outlines of the Evaluator Independent Testing

Viewpoints of the independent testing	Outlines of the evaluator independent testing
1	Confirmed an entry parameters check for the Time Change Function.
2	Checked the operations of the simultaneous login with the same username.
3	Checked the functionalities of abnormal operations such as the behaviours of the user sessions when turning off the power of the TOE.
4	Checked the operations when changing/deleting the account information of general user while the general user is logged in.
5	Checked the operations when entering characters for multiple languages in the user registration.
6	Checked the various character configurations for password in case of the unavailable characters.

c. Result
All the evaluator independent testing was correctly completed, and the behaviors of the TOE were verified. The evaluators confirmed that all test results were in conformity with the expected behaviors.

7.3.3 Evaluator Penetration Testing

The evaluator devised and conducted the necessary evaluator penetration testing about the possibility of exploitable concern at assumed environment of use and attack level.

It explains the penetration testing executed by the evaluator as follows:

1) Summary of the Evaluator Penetration Testing
Summary of the penetration testing executed by the evaluator is as follows:

a. Vulnerability of concern
The evaluator searched into the provided evidence and the public domain information for the evaluator potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

Table 7-5 Vulnerability of concern

Vulnerability identifier	Contents
1	Security functions may be bypassed to leak or tamper the protected assets of the TOE by initiating network services that are not described in the design materials.

2	Although this TOE provides each service by Java Servlet, the identification and authentication and the access control may be bypassed if Java Servlet that does not check the session information exists.
3	In the communication interface (Web Server Function) of this TOE with the devices, the Security Functions of the TOE may be bypassed to leak or tamper protected assets if accidentally connected from client computers via Web browser.
4	Entering SQL codes into the input items of Web browser may result in unanticipated operations performed by the TOE. For this, the protected assets may be leaked or tampered.
5	Entering illegal characters such as scripts in the input box of Web browser may result in unassumed operations of the TOE. For this, the protected assets may be leaked or tampered.
6	The protected assets of the TOE and the information that may cause the attacks may be leaked by abusing the input specified in the URL of Web browser.

b. Evaluator Penetration Testing Outline

The evaluator executed the following evaluator penetration testing to identify possibly exploitable vulnerabilities.

<Evaluator Penetration Testing Environment>
The evaluators' test configurations were identical with those of the developer testing. Figure 7-1 shows the evaluators' test configurations.

Table 7-6 shows the used tools for details.
Regarding Wireshark, the evaluator penetration testing differs from the developer testing. Also, although the multiple versions are used depending on terminals, the difference occurs only in user interfaces and there is no result difference by using different versions due to the same functionalities to capture the packets.

Table 7-6 Penetration Testing Tools

No.	Tool name	Version	Functions	Operational environment
1	Wireshark	0.9.9.7	Packet analysis	Windows
		1.2.8		
2	WinPcap	4.1.1	Packet capture library	Windows
3	NMAP	5.21	Port Scan Tool	Windows
4	Paros	3.2.13	Proxy-type vulnerability verification tools	Windows

<Execution of vulnerability testing>

For anticipated vulnerabilities identified in Table 7-5 to search for potential vulnerabilities, Table 7-7 shows the penetration testing that corresponds to this. The evaluator executed the following penetration testing to identify possibly exploitable vulnerabilities.

Table 7-7 Outlines of the Evaluator Penetration Testing

Vulnerability identifier	Outlines of the penetration testing
1	Performed the testing to confirm that ports other than the ones that the TOE provides cannot be accessed by using Port Scan Tool (NMAP).
2	Performed the testing of attempting to access directly from Web browser for the accessible Java Servlet from the external in order to ensure that the checking function of the session information is operated.
3	Performed the testing to confirm that the protected assets are not leaked or tampered by the user access to interfaces for devices via Web browser.
4	Performed the testing to confirm the identification and authentication is not bypassed and the unpermitted protected assets cannot be accessed after entering characters including SQL in the input items of Web browser.
5	Performed the testing to confirm no operations to breach the Security Functions after entering the illegal characters such as scripts in the input items of Web browser.
6	For Web Server Function of the TOE, performed the testing to confirm the directory traversal does not occur by giving entry that anticipate directory traversal. Performed the testing to confirm there is no specified input in the URL of Web browser.

c. Result
The executed evaluator penetration testing did not find any vulnerability exploitable by attackers with the assumed attack potential.

7.4 Evaluated Configuration

In this evaluation, the evaluation configurations shown in Figure 7-1 were applied to the developer testing, the evaluator independent testing, and the evaluator penetration testing. The setting values recommended in the guidance are specified for the initialisation of the TOE at the beginning of the evaluation.
As for the devices used in the testing, there were some differences between devices, CS, the

software of client computers and the components identified in the ST. However, the evaluators determined it is appropriate that the devices are considered as being identical to the configurations in the ST (see "7.3.1 Developer Testing").

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance: none

- Security functional requirements: Common Criteria Part 2 Conformant

- 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

The result of the evaluation is applied to the composed by corresponding TOE to the identification described in the chapter 2.

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

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

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

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

3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Rationale of 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.

Concerns found in certification process were prepared as certification oversight reviews and were sent to Evaluation Facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this certification report.

8.1 Certification Result

As a result of verification of submitted Evaluation Technical Report, Observation Reports and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL3 in the CC part 3.

8.2 Recommendations

Since developers provides the function to confirm the validity of device firmware itself as indicated by the organisational security policies, the communication between the TOE and HTTPS-compatible devices are not assumed to protect the communication information in the device firmware Update Function. Consumers need to be cautious about organisational security policies that the developers assumed.

The firmware version of the TOE in this evaluation is A1.18-C1.14-P1.12-K1.04. When updating the version except for the above-mentioned ones of the firmware with the RC Gate Firmware Update Function, consumers need to know that it will not be the evaluated and certificated product.

As described in "1.1.3 Disclaimer", other functions that are out of the CC-certified scope exist in this TOE. Therefore, consumers need to consider the introduction of the remote analysis maintenance service to use this TOE.

9. Annexes

There is no annex.

10. Security Target

Security Target[12] of the TOE is provided within a separate document of this certification report.

Remote Communication Gate A Security Target Version 1.00 (2010-09-27) RICOH COMPANY, LTD

11. Glossary

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

CS	Communication Server
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MIB	Management Information Base
OS	Operating System
RC Gate	Remote Communication Gate A
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer

The definition of terms used in this report is listed below.

@Remote	A commercial name of this remote service using this TOE.
CE (Customer Engineers)	A person who is educated to handle and maintain the TOE. For maintenance, the CE can operate the TOE via the interface for the CE from a computer's Web browser.
Communication Protection Function between the RC Gate and CS	A function that allows the TOE to restrict the communication destination in order to communicate via the Internet only for CS and furthermore, to securely keep the communication data between the TOE and CS mutually and to detect data tampering.
Communication Protection Function between the RC Gate and Devices	A function to detect communication data tampering. This function can be mutually used by the TOE and the registered HTTPS-compatible devices for communication between them if the Service Call Function, the Machine Counter Notice Function, and the Supply Call Function are enabled.
Communication	A function secures the communication data between the

Protection Function between the RC Gate and Computers	RC Gate and Computer on the Web Function.
RC Gate Firmware Update Function	A function that allows the TOE to update the RC Gate's firmware with RC Gate Firmware received from the CS.
RC Gate Firmware Validation Confirmation Function	A function that allows the TOE to confirm that Application, Software Common Parts, Platform, and OS are officially provided by the manufacturers at the request of the user.
Web Function	A function that allows users to remotely operate the TOE. Users access the TOE via a computer's Web browser.
Service Call Function	A function that allows the TOE to report the device failure information received from the registered device to the CS. Based on the report, the maintenance centre analyses and handles the cause of the failure.
Supply Call Function	A function that allows the TOE to notify the CS about the supply information (remaining toner and paper) received from the registered device. Based on the report, the maintenance centre supplies toner and paper.
Security Management Function	A Web-based TOE function that allows only administrators to execute management authorities for the TOE.
Device Firmware Update Function	A function that allows the TOE to update the firmware of the registered HTTPS-compatible device by the device firmware received from the CS.
Device administrator	A person who manages the maintenance of the device connected to the LAN where the TOE is installed.
Access Control Function of Device Receiving Information	A function that allows the TOE to restrict the authorised users' access to the device receiving information. The TOE allows successfully identified and authenticated users to access the device receiving information authorised for the user roles.
Network administrator	A person who manages the LAN where the TOE is installed.
Network user	Network user means the generic name of users who access the users' LAN environment where the TOE is installed. It also includes users who have no TOE user accounts.
General user	A person who is given the TOE user account by administrator and can view the information collected from the devices by using computers.
Administrator (TOE	An administrator who introduces and manages this TOE, and can change the RC Gate configurations and

administrator)	view the information collected from devices.
Machine Counter Notice Information	A function that allows the TOE to periodically notify the CS about the machine counter information (number of print pages counted for each device) received from the registered device. The counter values are used for billing information.
User	A generic name of administrator and general user.
User Identification and Authentication Function	A function that allows the TOE to provide only the authorised users for the TOE (administrator, general user) with the Web Function. The TOE requires entering the information (hereafter referred to as account information) to identify and authenticate users who attempt to use the Web Function. When users enter the account information, only successfully identified and authenticated users can operate the TOE.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[2] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[3] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 3, July 2009, CCMB-2009-07-001 (Japanese Version 1.0, December 2009)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 3, July 2009, CCMB-2009-07-002 (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 3, July 2009, CCMB-2009-07-003 (Japanese Version 1.0, December 2009)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 3, July 2009, CCMB-2009-07-004 (Japanese Version 1.0, December 2009)

[12] Remote Communication Gate A Security Target Version 1.00 Sep 27, 2010 RICOH COMPANY, LTD

[13] Remote Communication Gate A Evaluation Technical Report Version 1.1, Sep 30, 2010, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center