Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	August 31, 2006 (ITC-5049)
Certification No.	C0048
Sponsor	Ricoh Company, Ltd.
Name of TOE	Remote Communication Gate Application Software
Version of TOE	3.34
PP Conformance	None
Conformed Claim	EAL3
TOE Developer	Ricoh Company, Ltd.
Evaluation Facility	Mizuho Information & Research Institute Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
June 26, 2006

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center
Information-Technology Promotion Agency, Japan

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 2.1 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations (as of 01 December 2003)

Evaluation Result: Pass

"Remote Communication Gate Application Software" has been evaluated in accordance with the provision of the "IT Product 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

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “Remote Communication Gate Application Software” (hereinafter referred to as “the TOE”) conducted by Mizuho Information & Research Institute Center for Evaluation of Information Security (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, Ricoh company, Ltd..

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

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.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	(Japanese) Remote Communication Gate Type N Remote Communication Gate Type L (English) Remote Communication Gate Type BN1 Remote Communication Gate Type NM1
Version:	3.34
Developer:	Ricoh Company, Ltd.

1.2.2 Product Overview

TOE of this product is “RC Gate application software” (RC Gate stands for Remote Communication Gate Type N/L/BN1/BM1). RC Gate is used primarily in a business office and acts as a relay unit to connect image I/O devices and the remote server called “Communication Server (hereinafter referred to as “CS”)”. The data collected by the RC Gate is transferred to a trusted CS via Internet or telephone line (dial-up PPP connection). The TOE is reinforced to protect the information assets from Internet and Intranet threats by using encryption and CS identification and authentication.

1.2.3 TOE scope and TOE functions

(1) TOE operating environment
RC Gate exchanges data with CS from the office's internal network via Internet or telephone line. Typical network connection configuration of “RC Gate Type N/BN1” for LAN is as follows (Figure 1-1):

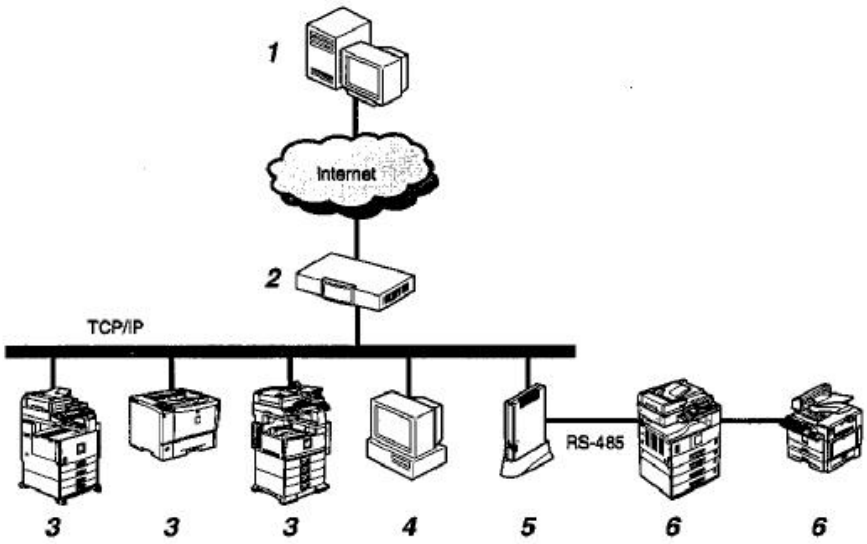


Figure 1-1: Network connection configuration of RC Gate (LAN Type)

Each device’s role is described as follows. The index numbers correspond to the numbers in Figure 1.

1. Communication Server (CS)
   The server with which RC Gate communicates via Internet is referred to as Communication Serer. It is abbreviated to CS as mentioned previously.

2. Proxy Server and Firewall
   Security system to protect office’s internal network environment from the external network.

3. Image I/O devices
   Image I/O devices, which support Ricoh’s remote service and those with MIB function.

4. PC for RC Gate
   PC to access RC Gate via Web browser.

5. Remote Communication Gate Type N/BN1
   RC Gate is a relay unit to maintain image I/O devices. It transmits the device information to CS and downloads firmware for the device from CS. There are two communication methods between RC Gate and CS:
   1) HTTPS method exchanges messages between CS as the HTTPS server and RC Gate as the HTTPS client.
   2) SMTP method sends messages in S/MIME from RC Gate toward CS via SMTP server.

6. The Image I/O devices maintained via serial communication bus (RS-485)
   Image I/O devices manufactured by Ricoh can also be maintained, by directly connecting them to RC Gate with the serial modular cable. The serial modular cable can connect up to five image I/O devices to one RC Gate.

Typical network environment of RC Gate modem type is shown as follows (Figure 1-2):

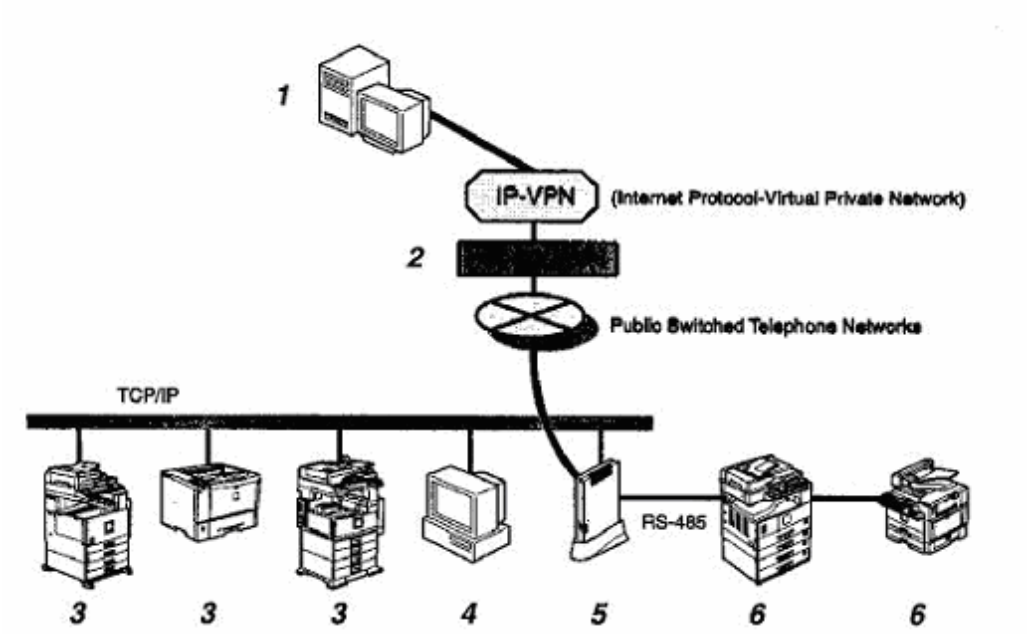


Figure 1-2: Network Connection Configuration of RC Gate (Modem Type)

1. Communication Server
   The server with which RC Gate communicates is referred to as Communication Serer. This is physically identical to CS for communication via Internet.

2. Access Point
   Access point for dial-up connection via telephone line. The access point for RC Gate is pre-installed so that RC Gate can access the nearest local access point.
3. Image I/O devices
   Image I/O devices, which support Ricoh's remote service or MIB functions.

4. PC for RC Gate
   PC to access RC Gate via Web browser.

5. Remote Communication Gate Type L/BM1
   RC Gate is a relay unit to maintain image I/O devices. It transmits the device information to CS, but does not download firmware for the devices from CS. There is only one communication method between RC Gate and CS:
   1) HTTPS method exchanges messages between CS as the HTTPS server and RC Gate as the HTTPS client.

   RC Gate Type L/BM1 only supports HTTPS method.

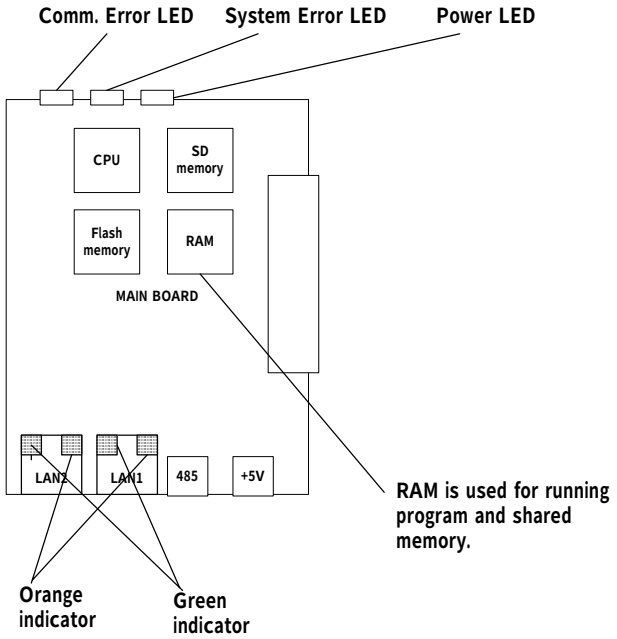
6. The Image I/O devices maintained via serial communication bus (RS-485)
   Image I/O devices manufactured by Ricoh can also be maintained by their direct connection to RC Gate with the serial modular cable. The serial modular cable can connect up to five image I/O devices to one RC Gate.

(2) TOE scope and overview of the functions
RC Gate is a product provided in a special case container, and the TOE is application

software installed on it.
RC Gate acts as a relay unit for the internal network communication with image I/O devices and the external network communication with CS. It is designed with the assumption to be used mainly in an office with general LAN environment.
Main functions of RC Gate as hardware are assembled on the main board (Figure 1-3). The main board has CPU, flash memory, Ethernet line, RS485 and the power supply unit on it. Type L/BM1 has a modem board connected in addition to the main board. The modem board has a telephone line interface. Hardware details of RC Gate are described as follows:

Software of RC Gate Type N/L/BN1/BM1 mainly consists of the application software and operating system (hereinafter referred to as OS). The TOE is limited to application software and does not include an OS. There is a point to notice that the same software is used for Type N/L/BN1/BM1. The TOE is stored in the SD memory as a program to execute software. When power is supplied to RC Gate, the TOE is loaded from the SD memory to RAM, and launched automatically.

Type N/BN1



Type L/BM1

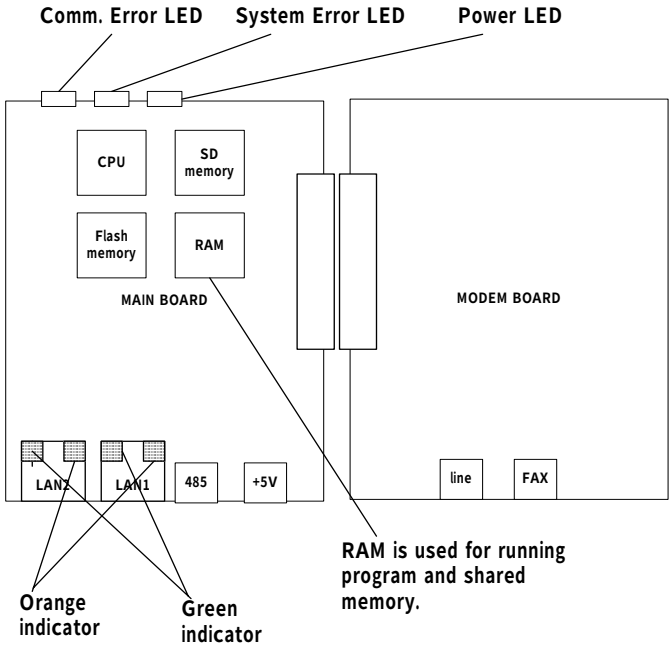


Figure 1-3: Physical structure of RC Gate

RC Gate consists of hardware and software components. The software components consist of OS and application software. The OS is an embedded Linux operating system ported for RC Gate based on MontaVista Linux, and referred to as RC Gate OS. The OS is out of the TOE. Wireless LAN card can be installed on RC Gate as an option, but the OS is out of the TOE even when in connection with the wireless LAN option. The functions of the TOE are described as follows, referring to Figure 1-4. The TOE's security functions are; operator identification and authentication provided by the application software, access control, CS identification and authentication for HTTPS, and S/MIME mailing.

The TOE identifies and authenticates operators and controls their access via the Web interface. The operator identification and authentication is made possible by combination of the operator type and password. Passwords are hashed using the encryption library in the TOE and stored in the SD memory. The TOE saves the identified and authenticated operator information in its internal memory and controls access of operators during the session in accordance with the accessible items assigned to each operator based on the saved operator data.

CS identification and authentication is realized using HTTPS technology. The TOE judges the validity of public key certificates by validating the public key certificate sent from CS to RC Gate and CS route certificate held by the RC Gate. It also validates the details of the public key certificate determined as valid in order to ensure the uniqueness of CS. CS route certificate is written into the flash memory in RC Gate at the factory before it is shipped, and extracted to the shared memory by the TOE when starting RC Gate. Communication to CS is triggered by the periodic report schedule in the TOE or error report from an image I/O device. The TOE encrypts and decrypts data using the encryption library when exchanging information with CS.

In SMTP communication, mails from RC Gate to CS are transmitted in S/MIME. CS public key certificate required in this process is directly written in the application software. Data transmission to CS is triggered by the periodic report schedule in the

TOE. The encryption library is used to convert the transmit data into S/MIME. The S/MIME mailing function is available only when RC Gate product type is Type BN1 and the communication method is SMTP.

As a log management function not concerned with security, the system time of OS is used as the time data for log. Log files are written in the SD memory. The recorded log data include the access log, communication log and system log.

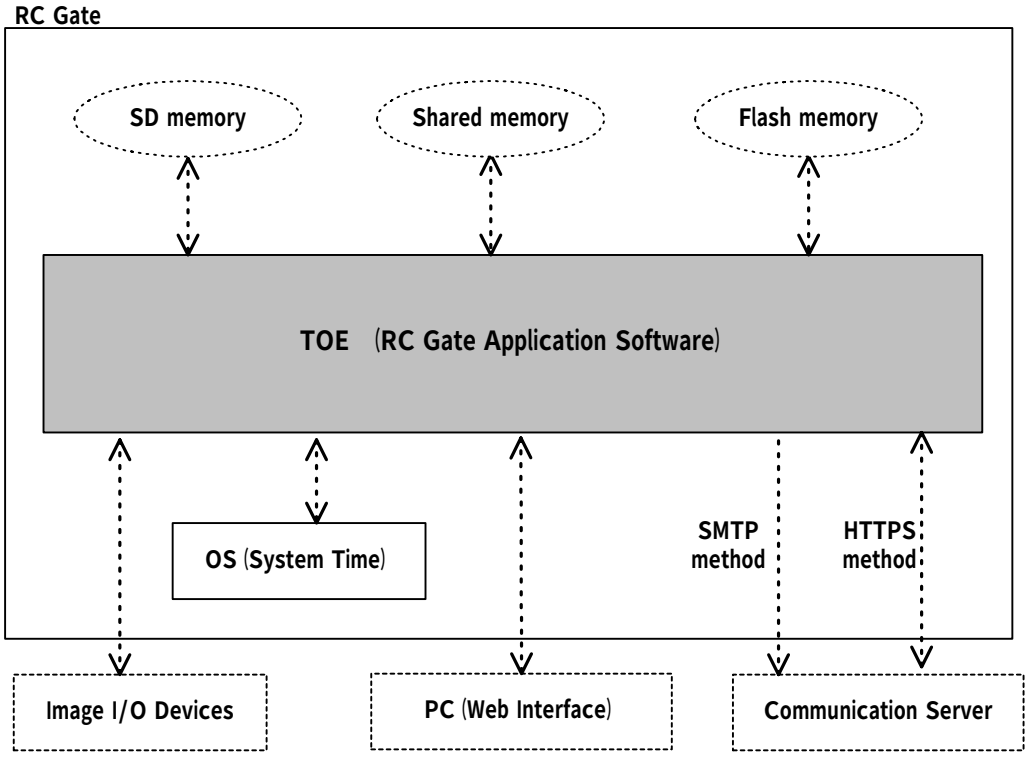


Figure 4: Logical boundary of RC Gate and the TOE

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "Remote Communication Gate Type

N/L/BN1/BM1 Security Target Version 1.03" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex C of CC Part 1 (either of [5], [8], [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9], [12] or [15]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10], [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in "Remote Communication Gate Application Software Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [22]. Further, evaluation methodology should comply with the CEM Part 2 (either of [17], [18] or [19]). In addition, the each part of CC and CEM shall include contents of interpretations (either of [20] or [21]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated June, 2006 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.
In the TOE environment assumable attack target is maintenance and management information via external network. It does not directly affect financial assets of the customer. This means the attack capability is "low level." because of the motivation. The organizational security policies claim the strength of function for SOF-Basic based on password policy. Therefore, SOF-Basic can be considered appropriate for the minimum strength of function level for the TOE for the reason of attacker's level and the organizational security policies

1.5.4 Security Functions

Security functions of the TOE are as follow.

- Identification and authentication of the operators
Operator's identifier and password ensures identification and authentication of the operators.

- Access control of each operator
Operator who is authenticated can access the matching items by access control.

- Identification and authentication of CS in HTTPS method
The TOE identifies and authenticates CS before it communicates data with CS over https by examining the public key certificate sent from CS and the corresponding route certificate to confirm the certificate's validity and by checking details of the public key certificate. The TOE performs cryptographic operations in the communication.

- S/MIME mail sending
In SMTP method communication, the e-mail sending information is encrypted by S/MIME format.

1.5.5 Threat

This TOE assumes such threats presented in Table 1-1 and provides functions for countermeasure to them.

Table 1-1 Assumed Threats

Identifier	Threat
T.CS_COMM	Information leak or illegal alternation may take place via the Internet or telephone line when RC Gate directly communicates CS. Malicious attackers on the external network may use protocol analyzer on Internet or telephone line to illegally access the communication data (assets: setting data inside RC Gate, collected information on image I/O devices and the image I/O device data) directly transmitted between RC Gate and CS. They may also alter such communication data to make the receiver receive data different from what the sender sent.
T.CS_MAIL	Information leak or illegal alternation may take place via the Internet when RC Gate uses e-mail to communicate with CS. Malicious attackers on the external network may use protocol analyzer on Internet to illegally access the e-mail data (assets: setting data inside RC Gate and collected information on image I/O devices) sent from RC Gate to CS. They may also alter such e-mails to make the receiver receive e-mails different from what the sender had sent.

T.FAKE_CS	A fake CS for spoofing may be set up and take on the position of CS to communicate with RC Gate and send in improper data or steal the user's assets. Malicious attackers may set up a fake CS, and the fake CS's administrator may obtain the user's assets such as collected information on image I/O devices via Internet or telephone line.

1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-2.

Table 1-2 Organisational Security Policy

Identifier	Organisational Security Policy
P.ACCESS	The personnel allowed to access and operate security devices shall be restricted to the operators responsible to manage such devices. Only the particular operators responsible to manage devices shall be able to access the TOE. The administrator shall be provided with the function to prohibit access of CEs. Passwords shall be used for access control and the password policy shall have sufficient strength of functions to satisfy the SOF-basic.

1.5.7 Configuration Requirements

Remote Communication Gate Type N/L/BN1/BM1 is a product provided in a special case container, and TOE is application software pre-installed on SD memory card. The TOE communicates with image I/O devices using original protocol or MIB. Therefore, the TOE managing target makes it a condition that these compliant devices connect internal network.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.PHYSICAL	It is assumed that the TOE and assets are physically protected. It is assumed that no malicious parties can physically access the TOE, assets and the TSF data. In other words, nobody shall be able to physically damage or tamper the TOE, assets or the TSF data. And no malicious parties shall be able to open the

	case of RC Gate and remove the memory in it.
A.NETWORK	It is assumed that the internal network is protected from the external network. It is assumed that the internal network on which RC Gate and image I/O devices operate is protected by outsiders who try to attack it through Internet.
A.CE	It is assumed that trusted customer engineers (CEs) duly carry out their duties based on their authority. CEs shall be properly trained and trusted. CEs shall not change the configuration of RC Gate, take out RC Gate, or install any unnecessary program on it without permission of the user's administrator. Combination of one-byte alphabetic characters (upper and lower case), numeric characters and specified symbols shall be used for a password. No easily guessable passwords shall be used.
A.ADMIN	It is assumed that trusted administrator and registrant duly carry out their duties based on their authority. It is assumed that trusted personnel shall take up duties of the administrator and registrant. Same person may be assigned to both administrator and registrant, but he/she shall be able to set and change the configuration of RC Gate and maintain RC Gate so it will work properly. Combination of one-byte alphabetic characters (upper and lower case), numeric characters and specified symbols shall be used for a password. Passwords shall be changed at least once every six months. No easily guessable passwords shall be used.
A.CS	It is assumed that CS is properly managed by a trusted company It is assumed that CS is managed by a trusted company, and the company operates and maintains CS properly.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

Product name	Destination	Guidance	ID Code
Remote Communication Gate Type N	Japan	Remote Communication Gate Type N/L Safety Information and Setup Guide(in Japanese)	A768-8559
Remote Communication Gate Type L	Japan		
Remote Communication Gate Type BN1	North America	Remote Communication Gate TypeBN1/BM1 Safety Information and	A768-8605B

Remote Communication Gate Type BM1	North America	Setup Guide(North American version)	
Remote Communication Gate Type BN1	Europe	Remote Communication Gate TypeBN1/BM1 Safety Information and Setup Guide(European version)	A768-8603B
Remote Communication Gate Type BM1	Europe		

Note: Administrator's guidance is open on Internet web server. The guidance is downloaded via Internet using SSL communication technology.

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM Part 2 in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM Part 2.

2.2 Overview of Evaluation Conducted

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

Evaluation has started on September, 2005 and concluded by completion the Evaluation Technical Report dated June, 2006. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on July, 2005 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on January, 2006.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1) Test Environment

Test configuration performed by the developer is showed in the Figure 2-1(A)-(C). Test tools are listed in Table 2.

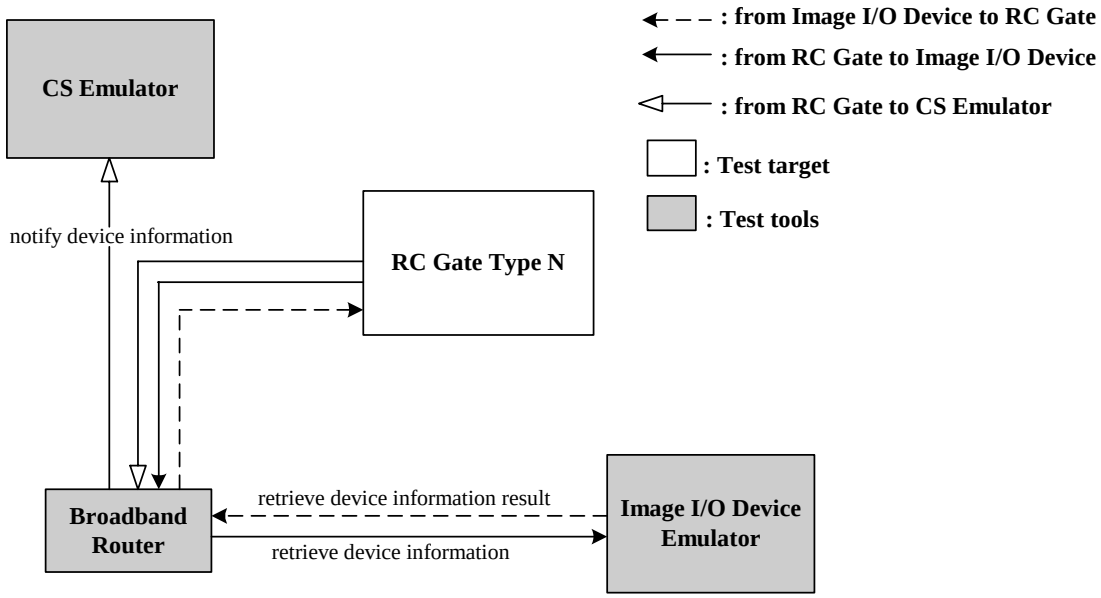


Figure2-1(A) Testing environment for RC Gate Type N/BN1 in HTTPS method

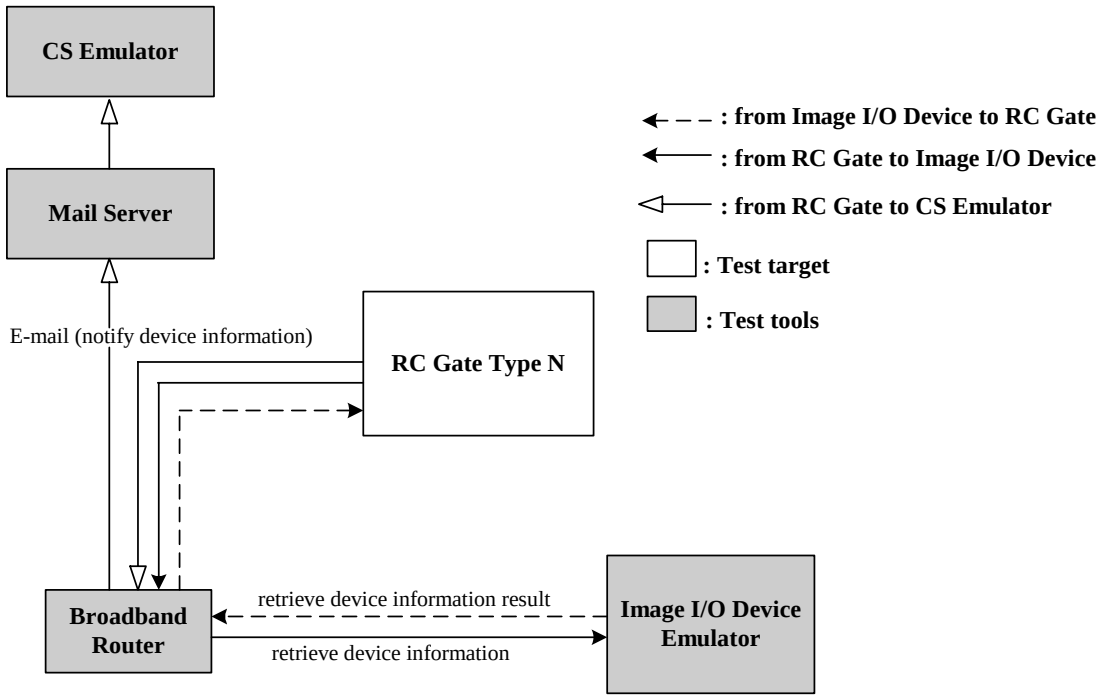


Figure 2-1(B) Testing environment for RC Gate Type N/BN1 in SMTP method

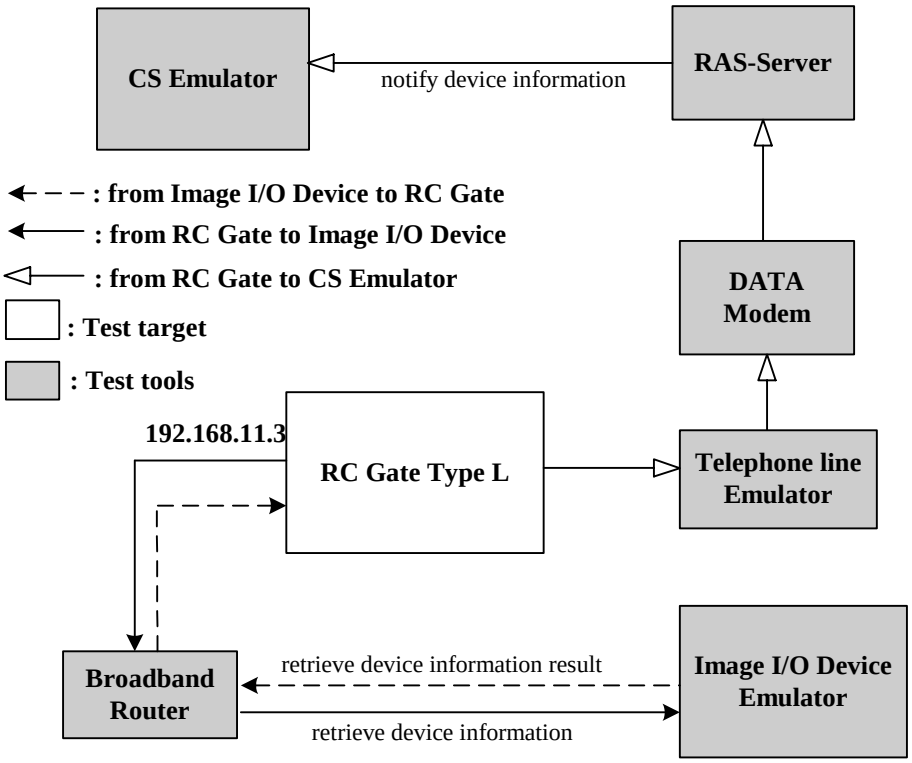


Figure 2-1(C) Testing environment for RC Gate Type L/BM1 in HTTPS method

Table 2 List of testing tools

Category	items
CS Emulator	Hardware: HITACHI PC8DK4-PA08P1C00 (PC/AT compatible) OS: Windows 2000 Professional (Version 5.00.2195) Emulator: CS Emulator software (Version 1.05) Mail Server: sendmail (Version 8.8.8)
Image I/O device	Digital MFP: RICOH Aficio 3025
RAS Server	Hardware: akia MICROBOOK 56 (PC/AT compatible) OS: Windows 2000 Advanced Server (Version 5.00.2195) RAS Server: Windows 2000 Advanced Server dial-up server software (Version 5.00.2134) Facsimile/Data modem: OMRON ME5614E2 Broadband router: BUFFALO BBR-4HG Telephone line Emulator: NEWTECH PASOPHONY
Analyzing Tools and others	Browser for RC Gate: Internet Explorer (Version 6.0.2800.1106) Network protocol monitor: EtherReal (Version 0.9.16)

	SSL analysing software: SSL Dump (Version 0.9b3) S/MIME analysing software: OpenSSL(Version 0.9.8a) Port scanning software: nmap (Version 1.3.1) WEB capturing software: Achilles (Version 0.27) Mail client software: Outlook Express 6 (Version 6.00.2800.1106)

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a) Test configuration

Test configuration performed by the developer is showed in the Figure 2-1. There are three types of testing environment listed below. In addition, developer's testing is carried out in the same TOE testing environment as TOE configuration identified in ST.

1. Testing environment for RC Gate Type N/BN1 in HTTPS method (Figure2-1 (A))
   Connecting and communication testing in HTTPS method is performed between RC gate and CS via network interface of RC Gate (Testing target) using testing tools.

2. Testing environment for RC Gate Type N/BN1 in SMTP method (Figure 2-1 (B))
   Communication testing in SMTP method is performed between RC gate and CS via network interface of RC Gate (Testing target) using testing tools.

3. Testing environment for RC Gate Type L/BM1 in HTTPS method (Figure 2-1 (C))
   Connecting and communication testing with dial-up emulating environment in HTTPS method is performed between RC gate and CS via line interface of RC Gate (Testing target) using testing tools.

b) Testing Approach

Following method is selected to perform testing. This testing method has a commonality through all testing.

1. Concerning functions that have operable external interface for operator, developer confirms the functions by hand

2. Concerning functions that don't have operable external interface for operator, developer uses tools and confirms the functions by capturing and analysing the communication data.

c) Scope of Testing Performed

Developer performed 17 testing items.
Coverage analysis, which judged all security functions described in the function specification and external interface were tested fully, was performed by

developer. Depth analysis, which judged all subsystem and subsystem interface were tested fully, was performed.

d) Result

Developer's testing results was the same as expected one. Evaluator confirmed that developer's testing method and items were applicable and testing method and testing results were conformed to the expected behaviours in testing plans.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Evaluator's testing environment is the same as developer's one.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Evaluator's testing configurations are shown in Figure2-1. Evaluator's testing is carried out in the same TOE testing environment as TOE configuration identified in ST.

b. Testing Approach

Developer's testing method is adopted to perform testing in a similar manner.

c. Scope of Testing Performed

Evaluator's 7 own testing items and developer's 11 testing items sampled from developer's testing, i.e. 18 testing items in total were performed. Selection criterion is as follows:

1. Concerning evaluator's original testing criterion

- Web interface testing which is used very often.
- Password testing which is included authentication mechanism.
- Developer's testing, which is less frequently used.

2. Concerning developer's sampling testing criterion
- Testing items which cover all security functions.

d. Result

All evaluator testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM Part 2 by submitting the Evaluation Technical Report.

3. Conduct of Certification

The following certification was conducted 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 review, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL3 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations 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
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

The glossaries used in this report are listed below.

CE	A CE (Customer Engineer) is authorized to perform operations for inspection and maintenance of RC Gate when its problem occurred. CEs are employees of Ricoh or its affiliated companies.
CE operation authority flag	Only the administrator is allowed to specify the CE operation authority. If the CE operation authority flag is set to "permitted," the TOE permits the CE to access the setting data in RC Gate.
CGI	CGI stands for Common Gateway Interface. CGI is a Web server program activated by the request from Web interface.
CS	CS stands for Communication Server. CS is the server to which RC Gate sends its collected data from the I/O devices.
DBMS	DBMS stands for Database Management System. This database software manages all of I/O devices' setting information and collected data by RC Gates.
MFP	MFP stands for Multi Function Printer, which is a multi-functional digital printing device.
MIB	MIB stands for Management Information Base. RC Gate can collect image I/O devices' information from the devices that support MIB. There are MIB1 prescribed as RFC1156 and MIB2 prescribed as RFC1213. RC Gate can treat both MIB1 and MIB2.
PKI	PKI stands for Public Key Infrastructure and is a public key cryptosystem. PKI is used as a digital key technology for the secure communication.
RC Gate	RC Gate is a generic name for Remote Communication Gate Type N, Type L, Type BN1 and Type BM1.

SD memory SD memory stands for Secure Digital memory, which is provided in the shape of small cards. SD memory is used to store information of image I/O devices and the RC Gate application itself. And also it is used to provide the application.

SSL SSL stands for Secure Sockets layer.

6. Bibliography

[1] Remote Communication Gate Type N/L/BN1/BM1 Security Target Version 1.03 (June 07, 2006) Ricoh Company Ltd.

[2] IT Security Evaluation and Certification Scheme, July 2005, Information-Technology Promotion Agency, Japan EC-01

[3] IT Security Certification Procedure, July 2005, Information-Technology Promotion Agency, Japan EC-03

[4] Evaluation Facility Approval Procedure, July 2005, Information-Technology Promotion Agency, Japan EC-05

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-00-031

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031 (Translation Version 1.2 January 2001)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (Translation Version 1.2 January 2001)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (Translation Version 1.2 January 2001)

[11] ISO/IEC 15408-1:1999 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1:2000 - Security techniques - Evaluation criteria for IT security - Part 1: General Rules and general model

[15] JIS X 5070-2:2000 - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[16] JIS X 5070-3:2000 - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999

[18] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999 (Translation Version 1.0 February 2001)

[19] JIS TR X 0049: 2001 – Common Methodology for Information Technology Security Evaluation

[20] CCIMB Interpretations (as of 01 December 2003)

[21] CCIMB Interpretations (as of 01 December 2003) (Translation Version 1.0 August 2004)

[22] Remote Communication Gate Application Software Evaluation Technical Report Version 05000481-01-R03-04, June 07, 2006, Mizuho Information & Research Institute