RICOH

Remote Communication Gate

Type N/L/BN1/BM1

Security Target

Hiroshi KAKII, Jun SATOH, Yasushi FUNAKI, Haruyuki HIRABAYASHI
RICOH COMPANY, LTD.
2006-06-07
Version 1.03

This document is a translation of the security target written in Japanese, which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

Document Revision History

Version	Date	Author	Description
0.10	2005-03-04	Kakii, Hirabayashi	First draft.
0.11	2005-03-06	Kakii, Funaki, Hirabayashi	Corrected typographical errors.
0.12	2005-04-18	Satoh, Hirabayashi	2.4 Physical boundary of the TOE ・ Revised contents and added physical structure figures. 2.5 Logical boundary of the TOE ・ Revised contents and added assets to Figure 4. 3.2 Assumptions ・ Added necessity of education and enlightenment to general users. 4.2.1 Objectives for the IT environment ・ Added that antivirus software is introduced. 4.2.2 Objectives for the non-IT environment ・ Added that administrator shall provide education and enlightenment activities to general users. 8.1 Security Objectives Rationale ・ Added A.LAN_USER to Table 9. ・ Added rationale for A.LAN_USER and OE.ADMIN.
0.13	2005-7-19	Kakii, Satoh	・ Organized product types ・ Specified assets ・ Revised the correspondence between assumptions (A), threats (T), and security objectives (O). ・ Standardised related terms ・ Redefined TOE.
0.14	2005-8-11	Kakii, Satoh	・ Reviewed the correspondence between assumptions (A), threats (T), and security objectives (O). ・ Reviewed positioning of OSP.
0.15	2005-9-6	Kakii, Satoh	・ Added contents about cryptographic algorithm
0.16	2005-9-8	Kakii, Satoh	・ Revised structure figures. ・ Organized list of product names.
0.17	2005-9-8	Funaki	8.2.4 Rationale for dependencies of security function requirements ・ Made an overall review. 8.2.5 Mutual support of security function requirements ・ Added contents. 5.1 Security Function Requirements ・ Revised description of dependencies of FCS_CKM.4.
0.18	2005-9-12	Satoh, Kakii	Revised descriptions of assets and assumptions.

			Revised FDP_ACF and FCS_COP. Added import information. Organized TSF data. Revised the table for correspondence between rationales.
0.19	2005-9-13	Satoh	Revised FCS_COP.
0.20	2005-9-26	Kakii, Satoh	Revised and made addition to the TOE names. Added versions. Standardised terms (decryption, HTTPS method, SMTP method, and RC Gate monitor).
0.21	2005-10-06	Kakii, Satoh	Reviewed the threats and made addition to OSP. Standardised terms (Web, TOE, and RC Gate). Revised and made addition to the assumptions and security for the environment.
0.22	2005-10-21	Kakii, Satoh	Standardised names and versions. Added the table for FDP_ACF.1 and rewrote the related descriptions. Rewrote the descriptions of time stamp. Revised and made addition to the descriptions of O.SIGNATURE. Excluded O.CIPHER from the Web security functions.
0.23	2005-10-26	Kakii, Satoh	Added contents of CC identification/conformity. Standardised terms: for LAN and for modem. Deleted latter part of the descriptions of T.FAKE_CS. Revised descriptions of OE.CS. Added contents of rationale for strength of function claims. Organized user data and TSF data (FDP_ACF, FMT_MTD) > Overall rewrite of rationales in section 8.
0.24	2005-11-04	Kakii, Satoh	Revised the organizational security policies. Revised the security function requirements (including FTP_ITC.1). Made some changes to the cover sheet, header and footer.
0.25	2005-11-09	Kakii, Satoh	8.1.1 “Rationale for security function requirements.” Made some changes. 8.2.1 “Rationale for TOE security functions.” Made some changes.
0.26	2005-11-24	Kakii, Satoh	Section 5.1: Made some changes to FCS_CKM and FCS_COP. Section 6.1: Made some changes to the description of security functions. Section 8.1.1: Made some changes to the rationale for security function requirements.
0.27	2005-11-30	Kakii, Satoh, Funaki	Section 5.1: Made some changes to FDP_ACF, FIA_ATD, FIA_UID and FMT_SMF, made addition to FMT_MSA, and deleted FMT_MOF.

			Section 6: Noted reference to section 8.2.1. Made some changes concerning the audit log. (Deleted A.TIME, O.AUDIT, OE.TIME, FMT_MTD.1Ta, FMT_MTD.1Tb, FMT_MTD.1Tc, FAU_GEN.1, FAU_SAR.1, FAU_STG.2, FPT_STM.1, and SF.AUDIT. Revised the rationales and other contents.)
0.28	2005-12-09	Kakii, Satoh, Funaki	Made some changes to UAU.7 and organized contents of assets, assumptions, threats, organizational security policies and summary of TOE specification.
0.29	2005-12-14	Kakii, Satoh	Made some changes to the descriptions of TOE, assumptions, objectives, security function requirements, summary of TOE specification, and rationales.
0.30	2005-12-20	Kakii, Satoh	Organized SF descriptions and definition of specific terms.
0.31	2006-01-06	Kakii, Satoh	Made some changes to FDP_ACF table in section 5.
0.32	2006-01-23	Kakii, Satoh, Funaki	5.2 Minimum strength of function claim Made some changes. 6.3 Strength of function claims Made some changes. 8.2.2 Rationale for minimum strength of function level Made some changes. 8.3.2 Rationale for strength of function claims Made some changes. 5.1 Security function requirements Made some changes. FDP_ACF.1, FIA_UAU.6, and FTA_MCS.2 6.1 Summary of TOE Specification SF.OPE_I&A and SF.OPE_AC
0.33	2006-01-24	Kakii, Satoh	Made some changes to the description of FIA_UAU.6.
0.34	2006-01-24	Kakii, Satoh	Made some changes to FIA_UAU.6 and the descriptions based on it, changed FTA_MCS.2 to 1, and made changes to section 8.3.3.
0.35	2006-01-25	Satoh, Kakii	Made some changes to FIA_UAU.6.
0.36	2006-01-26	Satoh, Kakii	Made some changes to the table and description of FMT_MTD.1 and FMT_SMF.1. Made some changes to description of mutual support.
0.37	2006-01-27	Satoh	Partially deleted FIA_UAU.7 from the table and description in section 6.2 and section 8.3.1. Made some changes to the mutual support.
0.38	2006-02-16	Kakii, Satoh	Changed the TOE version. Made some changes to the description of manual version.
0.39	2006-04-07	Kakii, Satoh, Funaki	Specified assets, reviewed the assumption A.NETWORK, standardised and redefined the related terms, made changes to the description of OSP, and deleted FTA_MCS.1.
1.00	2006-04-11	Kakii, Satoh,	Specified threats, added description of CE operation authority,

		Funaki	changed the version to 1.00 as the formal release version.
1.01	2006-05-02	Kakii, Satoh	Deleted A.BROWSER and its related part. Added contents of P.ACCESS and changed the related part.
1.02	2006-05-09	Kakii, Satoh	Made some changes to P.ACCESS and its related part. Made some changes to "Rationale for minimum strength of function level" and "Rationale for assurance requirements."
1.03	2006-06-07	Kakii, Satoh, Funaki	Deleted description of SF.OPE_I&A session. Standardised the version of related documentations.

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 ST Identification

Title:	Remote Communication Gate TypeN/L/BN1/BM1 Security Target
Version:	1.03
Date:	2006-06-07
Author:	Hiroshi KAKII, Jun SATOH, Yasushi FUNAKI, Haruyuki HIRABAYASHI Ricoh Company, Ltd.
Product Name:	Japan: Remote Communication Gate Type N, Remote Communication Gate Type L Other Countries: Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 *Note: Hereafter these products are called with a generic name "RC Gate".*
TOE Name:	[Japan] Remote Communication Gate Application Software (in Japanese) [Other Countries] Remote Communication Gate Application Software
TOE version:	3.34
Evaluation Assurance Level: EAL3	
CC identification:	CC version 2.1, ISO/IEC 15408:1999, JIS X 5070:2000; CCIMB Interpretations-0407
Keywords:	Remote service, image I/O device, internal network, external network, office

1.2 ST Overview

This Security Target (ST) describes the security specification of software module of the RC Gate. 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 a software module for RC Gate and has the following security functions:

- Identification and authentication of the operators to change settings of the RC Gate
- Access control of each operator
- Identification and authentication of CS and data encryption when directly communicating with the CS
- Data encryption when sending information to CS by e-mail

This product is an important element of maintenance of image I/O devices by remote service. The following three main services are provided:

1. Remote diagnosis and maintenance of image I/O devices

In remote diagnosis and maintenance, SC ("service call" to request maintenance service) is automatically sent to Ricoh's customer engineer (CE) in case of a failure of image I/O device. In addition, firmware and other components can be upgraded via Internet by remote control. This remote management system will save many cumbersome manual tasks.

2. Periodic report of automated counter

As the copy counter and other counter data are automatically reported to the CS on a periodic basis, users no longer need to report the counter data. Introduction of this product enables completely automatic billing, and reduces cumbersome workload as well as billing mistakes and troublesome routine works.

3. Automatic report on nonregular supplies (toner, etc.)

As the remote diagnosis and maintenance system also reports the remaining toner level, users no longer need to call suppliers to order additional toner, or concern about forgetting to stock the toner and delayed supply. This means no more need of stock control and ordering hassles.

As you see from these features, it is inevitable to transmit accurate communication data between image I/O devices and CS, because accurate communication is required for error-free billing and service provision. As this system will use the Internet, appropriate defensive mechanism against compromise and tampering is necessary. Being a relay unit, RC Gate plays an extremely important role in operation of this service.

1.3 CC Conformance Claim

The TOE conforms to the function requirement-CC version 2.1, part 2 (ISO/IEC 15408-part2:1999(E)).

The TOE conforms to the assurance requirement-CC version 2.1 part 3 (ISO/IEC 15408-part3:1999(E)).

The TOE applies to CCIMB Interpretations-0407.

The evaluation assurance level conforms to EAL3.

There are no PPs claimed to which this ST conforms.

2 TOE Description

2.1 Product Type

The product type of RC Gate is a relay unit for remote service. Table 1 shows a list of product names.

Table 1: RC Gate Product Type List

Product name	Destination	Type	Code
Remote Communication Gate Type N	Japan	For LAN	A768-00
Remote Communication Gate Type L	Japan	For Modem	A769-00
Remote Communication Gate Type BN1	North America	For LAN	A768-17
Remote Communication Gate Type BM1	North America	For Modem	A769-17
Remote Communication Gate Type BN1	Europe	For LAN	A768-27
Remote Communication Gate Type BM1	Europe	For Modem	A769-27

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):

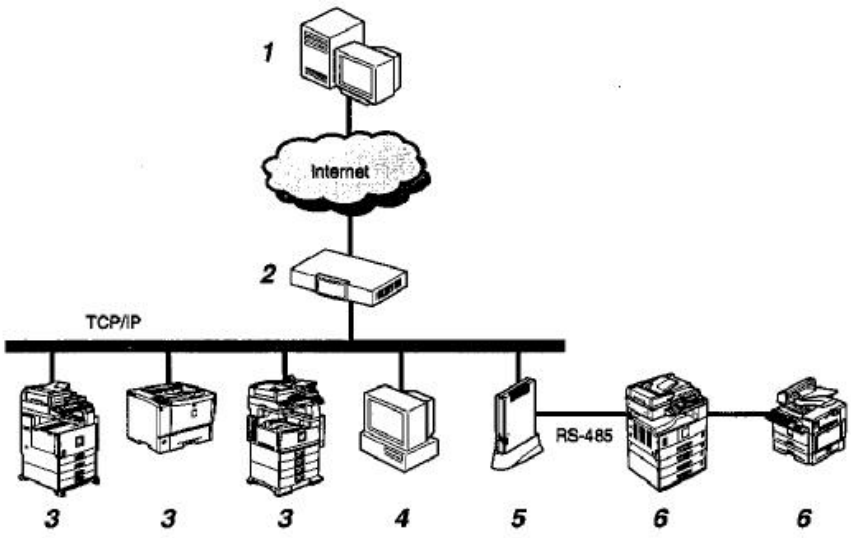


Figure 1: Network connection configuration of RC Gate Type N/BN1

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.

   * RC Gate Type N supports only HTTPS method for communication while RC GateTypeBN1 allows the user to select an option from the above two communication methods (HTTPS method and SMTP 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 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.

Unlike the aforesaid product for LAN, RC Gate Type L/BM1 is a product that supports modem connection which allows the communication with CS by "dial-up connection" via telephone line using a modem instead of accessing the Internet directly from the office's internal network. Dial-up connection uses a telephone line prepared for RC Gate or a line shared with the facsimile. Typical network environment of RC Gate Type L/BM1 is shown as follows (Figure 2):

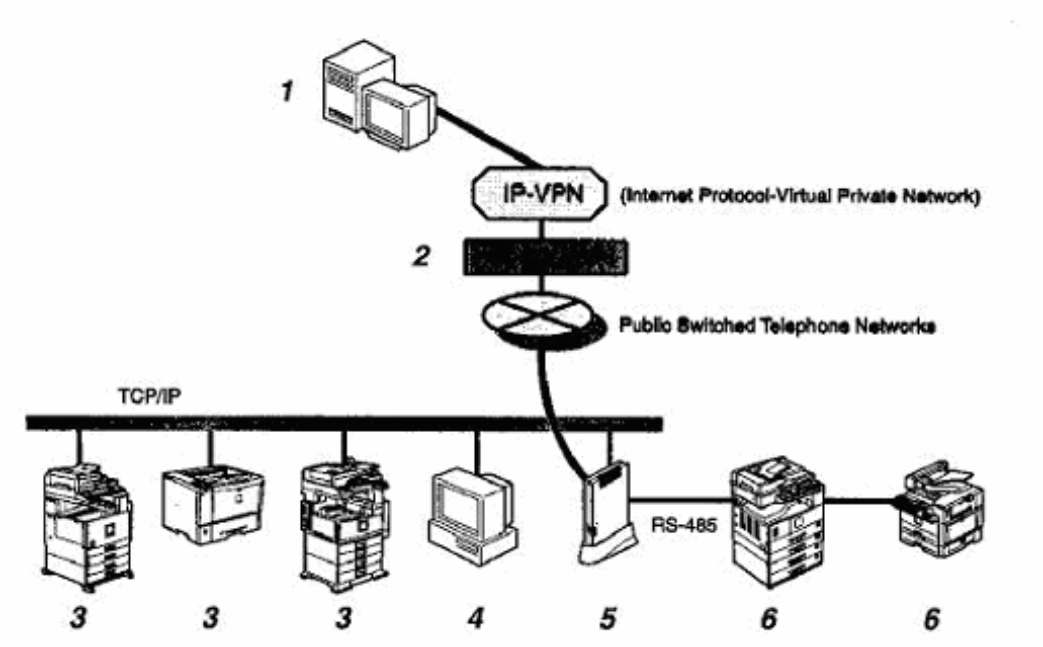


Figure 2: Network Connection Configuration of RC Gate Type L/BM1

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 function.

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.

2.2 RC Gate Operators

This section provides a list of the TOE operators. They are classified into the following authorities and each authority is distinctly separate from one another.

1) RC Gate Administrator
RC Gate administrator means the administrator on the customer side who maintains RC Gate (hereinafter referred to as "administrator"). The administrator can access various setting information of RC Gate through the input interface, and can configure various settings such as the proxy setting.

2) RC Gate Registrant
RC Gate registrant means a registrant on the customer side (hereinafter referred to as "registrant"). The registrants can register RC Gate and other devices through the input interface and have the Gate registered to CS.

3) CE
CE (Customer Engineer) means a trusted customer engineer who has duly received education to handle RC Gate and has been authorized by Ricoh on his/her capability to install RC Gate and handle its faults. CE can access almost all the setting information of RC Gate through the input interface at the customer's site. However, the administrator has the discretion to give CE the authority to access such information.

Authorities of administrator, registrant and CE are apparently distinguished in this document. Authorities for RC Gate are distinguished by the operator identification and authorization function of the TOE via Web input interface.

2.3 Other Persons Involved

Other persons involved with RC Gate are listed as follows:

1) Network Administrator
Network Administrator means the IT manager or other personnel responsible to manage the internal network of the customer with RC Gate.

2) RC Gate Manager
RC Gate Manager means the responsible personnel on the customer side for RC Gate installation contract exchanged between Ricoh and the customer.

2.4 Importance of security for RC Gate

Image I/O devices such as copier, facsimile and printer are connected to LAN environment today, and retain a lot of IT infrastructure information. Data collected by RC Gate includes information such as type of devices connected to the internal network as well as personal data like e-mail address of RC Gate administrator. It is undesirable to hold a risk of such important IT infrastructure information of a company catching the eyes of the public on an external network such as Internet. It is obviously undesirable to have such information stolen by a fake CS on external network as well.

In addition, as the counter data indicating the number of copied and printed documents collected by RC Gate is used for billing process, there exists a threat that the counter data may be tampered by malicious parties on external network. In the meanwhile, RC Gate can download firmware for image I/O devices from CS and transfer it to the relevant devices. There even is a risk to have such firmware tampered on the external network and let an illegal program sent in the devices. RC Gate shall prevent such potential security threats over external network.

2.5 Physical boundary of the TOE

RC Gate is a product provided in a special case container, and TOE is application software installed on it.

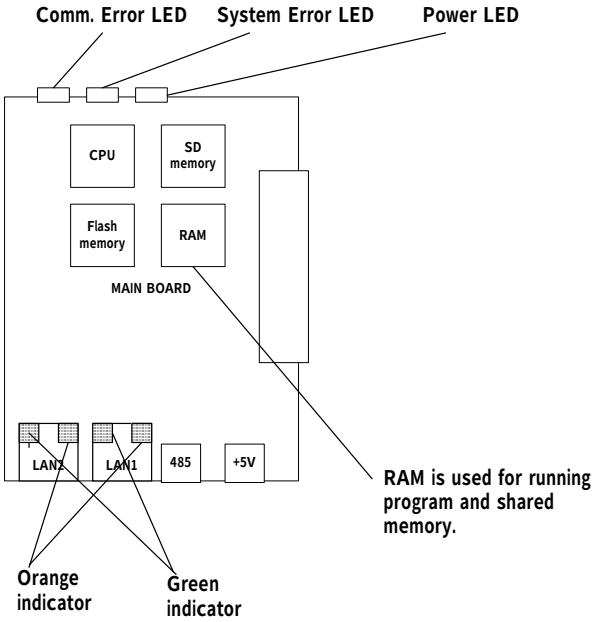
RC Gate acts as a relay unit for the internal network communication with image I/O devices and the external network communication with CS. It is designed with the assumption to be used mainly in an office with general LAN environment.

Main functions of RC Gate as hardware are assembled on the main board (Figure 3). The main board has CPU, flash memory, eithernet line, RS485 and the power supply unit on it. RC Gate 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:

- CPU: TX4925XB-200
- ROM: 4MB
- RAM: 64MB
- SD memory: 32MB
- NIC: 10Base-T/100Base-TX
- Front indicators: Power LED (green), System Error LED (red), Communication Error LED (orange)
- LAN indicators: Orange indicator Turns on when the transmission speed is 100Mbps and turns off when the transmission speed is 10Mbps or connection is not made.), and green indicator Turns on when sending or receiving data.)

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.

RC Gate Type N/BN1 (A768-00/17/27)



RC Gate Type L/BM1 (A769-00/17/27)

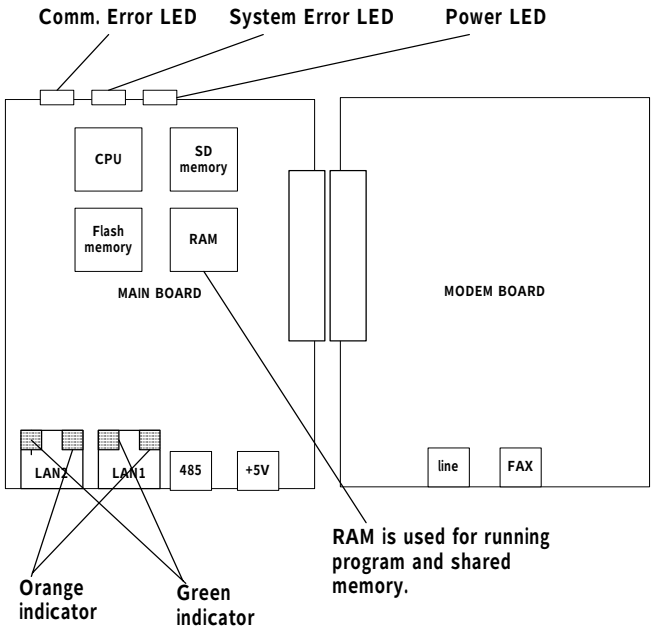


Figure 3: Physical structure of RC Gate Type N/L/BN1/BM1

2.6 Logical boundary of the TOE

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 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.

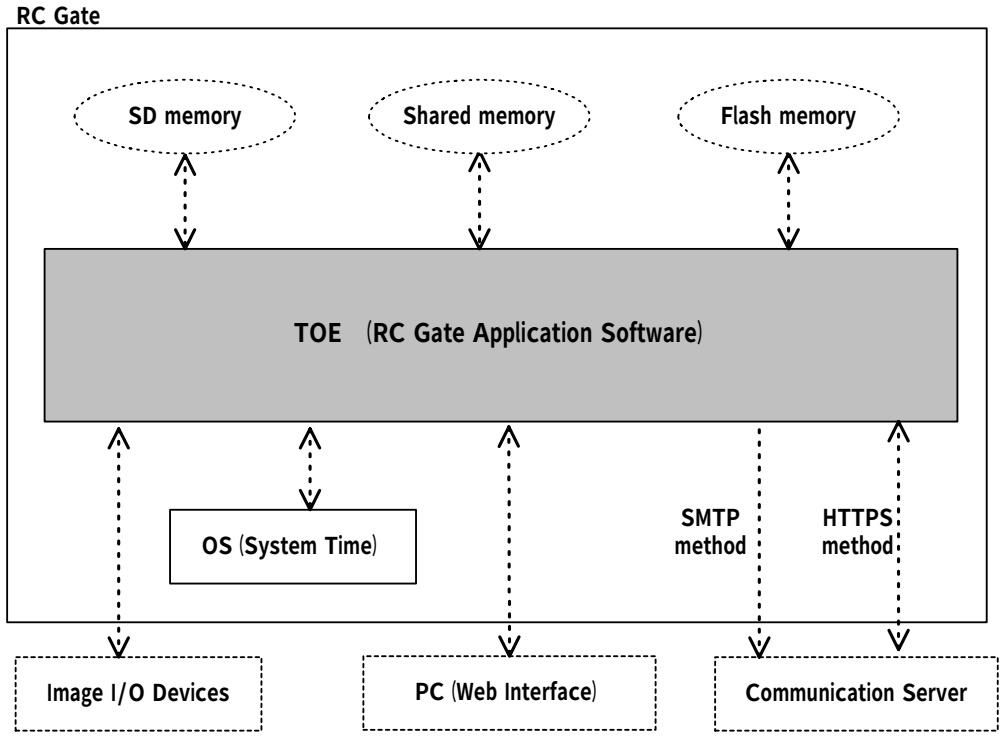


Figure 4: RC Gate Type N/L/BN1/BM1 and TOE

2.7 Definition of Specific Terms

For clear understanding of this ST, Table 2 provides definition of specific terms.

Table 2: Specific terms related to RC Gate

Term	Definition
Administrator	An administrator is authorised to perform administrative operations of RC Gate.
Registrant	A registrant is authorised to register RC Gate to CS.
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 company.
Operator	Operators mean administrator, registrant and CE in this document.
Firewall	Network server to protect assets in an internal network from the external network.
Flash memory	Flash memory is non-volatile memory which is a memory device fixed on board.

Term	Definition
SD memory	SD memory stands for Secure Digital memory. It is used to store information of image I/O devices and the RC Gate application itself.
Shared memory	Shared memory is non-volatile memory which is a memory device fixed on board.
Image I/O device	Image I/O device is a collective term for copier, printer, facsimile, and multi-functional device with such functions.
Linux	Linux is a UNIX compatible OS and is a freeware with high portability. RC Gate works on the embedded RC Gate OS ported based on the Linux provided by MontaVista Software, Inc.
MIB	MIB stands for Management Information Base. RC Gate can collect data from internal network devices supporting MIB. RC Gate shall handle MIB1 prescribed as RFC 1156.
External network	External network means the Internet or other public line network which are used as the communication route between RC Gate and CS.
Internal network	Internal network means the network inside the office with RC Gate installed. It is usually a LAN environment established as the intranet in the office.
Master key	Master key is the key for cryptography, which uses the same key for encryption and decryption.
PKI	PKI (Public Key Infrastructure) is a public key cryptosystem, a digital key technology used for secure communication.
Private key	Private key is a secret key coupled with a public key, and used to encrypt and decrypt data.
Public key	Public key is disclosed to the communication partner, and is used for PKI certification.
RC Gate	RC Gate stands for Remote Communication Gate. RC Gate is a relay unit to enable communication between image I/O devices and CS.
RS-485	RS-485 is a serial communication standard standardized by the Electronic Industries Alliance (EIA), and is superior to RS-422. While RS-422 supports multi-dropped connection allowing multiple-to-one, RS-485 supports the bus type multipoint connection, and allows multiple-to-multiple connection with up to 32 devices. This product allows you to connect up to 5 image I/O devices.
HTTPS	While HTTP is a protocol used to communicate data between Web servers and clients, HTTPS has additional functions; certification by SSL, data integrity assurance and data encryption feature.
S/MIME	S/MIME is one of the standards to realize e-mail security. It uses the master key cryptosystem, public key cryptosystem and the hash function to encrypt e-mails and detect tampering.

3 TOE Security Environment

3.1 Assets

The TOE shall protect the following assets;

- Setting data in RC Gate (RC Gate network setting, RC Gate administrator's e-mail address, RC Gate communication method, and image I/O device setting data),
- Collected image I/O device data (counter values, remaining toner level, etc.), and
- The user data for the image I/O devices (firmware for image I/O devices and key sets of image I/O devices)

Those data include information such as the type of devices connected to the internal network as well as personal data like e-mail address of RC Gate administrator. It is undesirable for such important IT infrastructure information of a company to be leaked out through the external network such as the Internet.

In relation to the assets, CS route certificate, CS public key certificate (for S/MIME) and operator passwords are stored in RC Gate as the TSF data.

Table 4 presents such assets and their locations while Table 5 provides a list of the TSF data and their locations.

Table 3: Assets and their locations inside RC Gate

No.	Assets	SD memory	Flash memory
1	Setting data inside RC Gate	X	
2	Collected information on image I/O devices	X	
3	Image I/O device data	X	

X: Present

Table 4: TSF data and their locations inside RC Gate

No.	TSF data	SD memory	Flash memory
1	CS route certificate		X
2	CS public key certificate (for S/MIME)	X	
3	Operator password	X	

X: Present

3.2 Assumptions

This section explains assumptions of the TOE.

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.

3.3 Threats

This section presents the threats to be countered by the TOE and its environment.

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.

3.4 Organizational Security Policies

This section discusses organizational security policies concerning the TOE.

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.

4 Security Objectives

4.1 Security Objectives for the TOE

This section describes the security objectives for the threats and organizational security policies.

O.OPE_I&A **The TOE ensures to provide the administrator with the function to manage the operators who can access the TOE data by identification and authorization and to prohibit access of CEs.**

When someone accesses the TOE via Web interface, the TOE identifies the operator (administrator, registrant or CE) and ensures that the operator can access the setting data inside RC Gate according to the operator's role. The TOE assures the administrator of the function to prohibit access of CEs. Passwords shall be used for access control and the password policy shall have sufficient strength of function to satisfy the SOF-basic.

O.CS_ID **The TOE ensures that RC Gate communicates with correct CS.**

The TOE ensures communication with correct CS 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.

O.T_CH **The TOE shall build a trusted channel for direct communication with CS and ensures no data leak and the data integrity.**

Trusted channel shall be established when the TOE communicates CS.

O.CIPHER **The TOE ensures that the transmitted data does not leak when sending e-mails to CS.**

When the TOE sends e-mails to CS, it shall encrypt the e-mail data and ensure that the data does not leak.

O.SIGNATURE **The TOE ensures data integrity in communication with CS.**

When the TOE sends e-mails to CS, it ensures that hash values are added to detect any e-mail tampering (for data integrity assurance).

4.2 Security Objectives for the Environment

4.2.1 Security objectives for the environment

This section explains the security objectives for the environment against the threats or for the assumptions described in Chapter 3.

OE.PHYSICAL **The TOE shall be physically protected.**

The trusted administrator shall set the TOE at a safe place in a non-open space to prevent malicious parties from physically accessing RC Gate.

OE.NETWORK **The TOE shall be protected in a safe internal network environment.**

Trusted personnel shall take charge of the internal network management of the office with RC Gate installed. Such personnel shall monitor the internal network to make sure it is working properly. If the TOE uses the Internet, the personnel shall establish “Firewall” to protect the internal network from outside attackers.

OE.CE **TOE shall be maintained by trusted CEs.**

CEs shall belong to Ricoh or its affiliated company, have carefully read and understood the maintenance documents (service manual), and duly maintain RC Gate. The CE shall be duly trained and fully informed of RC Gate. 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.

OE.ADMIN **The TOE shall be managed and operated by trusted administrator and registrant.**

RC Gate manager shall select reliable personnel for administrator and registrant. Selected administrator and registrants shall carefully read and understand the user’s documents (setup guide and operating instruction or user’s manual), and manage and operate RC Gate 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.

OE.CS **CS shall be properly operated by a trusted company.**

In order to have a trusted company operate CS, Ricoh shall select a suitable operational company and sign a contract with it. Ricoh shall also establish management and operation regulations for proper operation and maintenance of CS, and the company shall carry out operation of CS in accordance with such regulations.

5 IT Security Requirements

5.1 TOE Security Function Requirements

This section presents function requirements of the TOE to meet the security objectives. Parts with "assignment" or "selection" defined in [CC] are indicated by **[boldface and brackets]** while parts with "refinement" are indicated by **boldface and underline.** Parts with "repeat" are indicated by brackets and alphabetic suffix like "(a)."

FDP_ACC.1 Subset access control

Hierarchical to:	No other components
FDP_ACC.1.1	The TSF shall enforce the **[assignment: RC Gate operator access control policy]** on **[assignment: list of subjects, objects and operations between subjects and objects provided in Table 5].**
Dependencies:	FDP_ACF.1 Security attribute based access control

Table 5: Subjects, Objects and the Operations

Subjects	Objects	Operations between subjects and objects
Administrator process	Administrator's setting items (CE operation authority is not included in the setting items.)	Viewing and modifying
Registrant process	Registrant's setting items	Viewing and modifying
CE process	CE's setting items	Viewing and modifying

FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components
FDP_ACF.1.1	The TSF shall enforce the **[assignment: RC Gate operator access control policy]** to objects based on the following: **[assignment: list of subjects and objects, and the security attributes for each of them provided in Table 6]**
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: rules provided as follows:]** **1. Administrator process acting as operator with administrator's identity will be allowed to manipulate the setting data in RC Gate assigned to administrators.** **2. Registrant process acting as operator with registrant's identity will be allowed to manipulate the setting data in RC Gate assigned to registrants.** **3. CE process acting as operator with CE's identity or CE's operation authority will be allowed to manipulate the setting data in RC Gate assigned to CE.**
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: N/A].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[assignment: no additional rules]**.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

Table 6: Subjects, Objects and the Security Attributes

Category	Subjects or Objects	Security Attributes
Subject	Administrator process	Administrator's identity
Subject	Registrant process	Registrant's identity
Subject	CE process	CE's identity and CE's operation authority
Object	Setting items	Setting items' identity

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components

FTP_ITC.1.1 Inter-TSF trusted channel requires that the TSF provide a trusted communication channel between itself and another trusted IT product.

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **[selection: TSF]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[assignment: list of functions provided in Table 7]**.

Dependencies: No dependencies

Note: This requirement is applied only for direct communication, and not for communication via e-mail.

Table 7: List of functions requiring a trusted channel

Function	Data handled by the left function
Data export to CS	Collected information on image I/O devices
	Setting data in the RC Gate
Data import from CS	Data for image I/O devices such as firmware (programs) for image I/O devices
	Setting data in the RC Gate

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm provided in Table 8]** and specified

cryptographic key sizes **[assignment: cryptographic key sizes provided in Table 8]** that meet the following: **[assignment: standards provided in Table 8]**.

Dependencies: [FCS_CKM.2 Cryptographic key distribution

or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Table 8: List for Cryptographic Key Generation

Cryptographic key generation	Standard	Cryptographic key generation algorithm	Key size
Generation of data cryptographic keys	ANSI X9.31	Generation of RSA pseudo random number	168 bits

FCS_COP.1(a) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform **[assignment: cryptographic operations provided in Table 9]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm provided in Table 9]** and cryptographic key sizes **[assignment: cryptographic key sizes provided in Table 9]** that meet the following: **[assignment: standards in the list of cryptographic operations provided in Table 9]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes

or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Table 9: List of Cryptographic operations (1)

Cryptographic operation	Standard	Cryptographic algorithm	Key size
Data encryption	FIPS PUB 46-3	3DES	168 bits

FCS_COP.1(b) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform **[assignment: cryptographic operations provided in Table 10]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm provided in Table 10]** and cryptographic key sizes **[assignment: cryptographic key sizes provided in Table 10]** that meet the following: **[assignment: standards in the list of cryptographic operations provided in Table 10]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes

or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Table 10: List of Cryptographic operations (2)

Cryptographic operation	Standard	Cryptographic algorithm	Key size
Encryption of cryptographic keys	PKCS#1	RSA	512 bits

FCS_COP.1(c) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform **[assignment: cryptographic operations provided in Table 11]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm provided in Table 11]** and cryptographic key sizes **[assignment: cryptographic key sizes provided in Table 11]** that meet the following: **[assignment: standards in the list of cryptographic operations provided in Table 11]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes

or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Table 11: List of Cryptographic operations (3)

Cryptographic operation	Standard	Cryptographic algorithm	Key size
Data hashing	FIPS PUB 180-1	SHA1	N/A

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when **[selection: [assignment: 3 (positive integer number)]** unsuccessful authentication attempts occur related to **[assignment: continuous input of incorrect operator passwords via Web browser]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: reject access via Web browser for one minute]**.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment: CE operation authority]**.
Dependencies:	No dependencies

FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet **[assignment: ASCII code (0x20-0x5F, 0x61-0x7A) of 8 or more characters]**.
Dependencies:	No dependencies

FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification

FIA_UAU.6 Re-authenticating

Hierarchical to:	No other components.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions **[assignment:** **1. An administrator requests to modify the administrator's password** **2. A registrant requests to modify the registrant's password** **3. A CE requests to modify the CE's password** **]**
Dependencies:	No dependencies

FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1
FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.
Dependencies:	No dependencies

FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.

FMT_MSA.1.1 The TSF shall enforce the **[assignment: RC Gate operator access control policy]** to restrict the ability to **[selection: modify]** the security attributes **[assignment: CE operation authority]** to **[assignment: administrator].**

Dependencies: [FDP_ACC.1 Subset access control

or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1(a) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: modify]** the **[assignment: administrator password]** to **[assignment: administrator]**.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Note: All operators have their own password.

FMT_MTD.1(b) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: modify]** the **[assignment: registrant password]** to **[assignment: registrant]**.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Note: All operators have their own password.

FMT_MTD.1(c) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: modify]** the **[assignment: CE password]** to **[assignment: CE]**.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Note: All operators have their own password.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[assignment: security management functions provided in Table 12]**.

Dependencies: No Dependencies

Table 12: Security Management Functions

Security Management Functions
Administrator's function to manage CE access authority
Administrator's function to modify administrator password
Registrant's function to modify registrant password
CE's function to modify CE password

FMT_SMR.1(a) Security roles (a)

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: administrator]**.

FMT_SMR.1.2 The TSF shall associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1(b) Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: registrant]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1(c) Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: CE]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1	TSF domain separation
Hierarchical to:	No other components.
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.
Dependencies:	No dependencies

5.2 Minimum Strength of Function (SOF) Claim

The minimum strength level claimed for the TOE is **SOF-Basic**.

The TOE security function requirements using probabilistic or permutational mechanism are listed as follows.

- FIA_SOS.1 (Verification of secrets)
- FIA_UAU.2 (User authentication before any action)
- FIA_UAU.6 (Re-authenticating)

The strength level is SOF-Basic.

Please note that the strength of cryptographic algorithm is not included in this strength of functions.

5.3 TOE Security Assurance Requirements

The assurance components for the TOE are shown in Table 13. It is the set of components defined by the evaluation assurance level **EAL3** and no other requirements have been augmented.

Table 13: TOE security assurance requirements (EAL3)

Assurance Class	Assurance Component	
Configuration management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE's CM coverage
Distribution and operation	ADO_DEL.1	Distribution procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcement high-level design
	ADV_RCR.1	Informal handling demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage

Assurance Class	Assurance Component	
	ATE_DPT.1	Test: high-level design
	ATE_FUN.1	Functional test
	ATE_IND.2	Independent test – sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Evaluation of strength of TOE security functions
	AVA_VLA.1	Developer vulnerability analysis

5.4 Security Function Requirements for the IT Environment

There is no security function requirements which shall be met by the TOE's IT environment.

5.5 Security Assurance Requirements for the IT Environment

There is no security assurance requirements which shall be met by the TOE's IT environment.

6 Summary of TOE Specification

6.1 Summary of TOE Specification

SF.OPE_I&A

The TOE identifies and authenticates operators (administrator, registrant and CE) when they log in via Web interface. Each operator selects an operator type and inputs a password. The TOE judges the validity of the operator's authority based on the operators and passwords information it has, and allows the operator to view and/or change the data in RC Gate only if it determines he/she is an authorized operator. If incorrect password is input three consecutive times, the TOE rejects access via Web interface for one minute.

When an operator wants to modify the password, the TOE requires his/her current password to be input. The new password shall consist of 8 or more characters. Any new password not meeting this condition is rejected.

SF.OPE_AC

The TOE gives operators (administrator, registrant and CE) authority to access the setting data in RC Gate according to their role. If the CE operation authority is set to "not permitted," the TOE does not permit the CE to access the setting data in RC Gate. The TOE allows only the administrator to specify the CE operation authority.

SF.CS_HTTPS

The TOE uses the HTTPS certification mechanism to authenticate CS. 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. If CS is successfully identified and authenticated, RC Gate allows the functions provided in Table 14, that is, data export to CS and data import from CS. If the identification and authentication fails, it rejects data export and import with CS.

When CS authentication is successful, the TOE encrypts the data to export to CS and decrypts the data imported from CS.

Data integrity is ensured by data hashing in this communication.

The TOE performs cryptographic operations in accordance with the standard, cryptographic algorithm and cryptographic key sizes provided in Table 15. It also generates cryptographic keys in accordance with the standard, cryptographic key generation algorithm and cryptographic key sizes provided in Table 16.

Table 14: Data Export and Import Functions

Function	Data handled by the left function
Data export to CS	Collected information on image I/O devices
	Setting data in RC Gate
Data import from CS	Data for image I/O devices such as firmware (programs) for image I/O devices
	Setting data in RC Gate

Table 15: List of Cryptographic Operations

Cryptographic operation	Standard	Cryptographic algorithm	Key size
Data encryption	FIPS PUB 46-3	3DES	168 bits
Data decryption	FIPS PUB 46-3	3DES	168 bits
MAC data generation for integrity	FIPS PUB 198	HMAC	N/A
MAC data validation for integrity	FIPS PUB 198	HMAC	N/A
Key exchange (key encryption and decryption)	PKCS#1	RSA	512 bits

Table 16: List for Cryptographic Key Generation

Cryptographic key generation	Standard	Cryptographic key generation algorithm	Key size
Generation of data encryption keys	ANSI X9.31	Generation of RSA pseudo random number	168 bits
Generation of data decryption keys	ANSI X9.31	Generation of RSA pseudo random number	168 bits

SF.CS_SMIME

When the TOE exports the data provided in Table 17 to CS via e-mail, it encrypts the e-mail data using S/MIME. To prevent the message from being read by anybody except CS, the TOE encrypts the message using CS's public key.

It also adds hash values for tampering detection to ensure integrity of the e-mail.

The TOE performs cryptographic operations in accordance with the standard, cryptographic algorithm and cryptographic key sizes provided in Table 18. It also generates cryptographic keys in accordance with the standard, cryptographic key generation algorithm and cryptographic key sizes provided in Table 19.

Table 17: Data Export Functions

Function	Data handled by the left function
Data export to CS	Collected information on image I/O devices
	Setting data in RC Gate

Table 18: List of Cryptographic Operations

Cryptographic operation	Standard	Cryptographic algorithm	Key size
Data cryptography	FIPS PUB 46-3	3DES	168 bits
Encryption of cryptographic keys	PKCS#1	RSA	512 bits
Data hashing	FIPS PUB 180-1	SHA1	N/A

Table 19: List for Cryptographic Key Generation

Cryptographic key generation	Standard	Cryptographic key generation algorithm	Key size
Generation of data encryption keys	ANSI X9.31	Generation of RSA pseudo random number	168 bits

6.2 Correspondence between Security Functions and Functional Requirements

Table 20 shows the correspondence between security functions and functional requirements. The "X" marks in the table indicate that the security function meets the functional requirement.

Table 20: Correspondence between Security Functions and Function Requirements

	SF.OPE_I&A	SF.OPE_AC	SF.CS_HTTPS	SF.CS_SMIME
FDP_ACC.1		X		
FDP_ACF.1		X		
FTP_ITC.1			X	
FCS_CKM.1				X
FCS_COP.1(a)				X
FCS_COP.1(b)				X
FCS_COP.1(c)				X
FIA_AFL.1	X			
FIA_ATD.1		X		
FIA_SOS.1	X			
FIA_UAU.2	X			
FIA_UAU.6	X			
FIA_UID.2	X			
FMT_MSA.1		X		
FMT_MTD.1(a)	X			
FMT_MTD.1(b)	X			
FMT_MTD.1(c)	X			
FMT_SMF.1	X	X		
FMT_SMR.1(a)	X			
FMT_SMR.1(b)	X			

FMT_SMR.1(c)	X			
FPT_RVM.1	X			
FPT_SEP.1		X		

SF.OPE_I&A meets the following 13 functional requirements; FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.6, FIA_UID.2, FMT_MTD.1(a), FMT_MTD.1(b), FMT_MTD.1(c), FMT_SMF.1, FMT_SMR.1(a), FMT_SMR.1(b), FMT_SMR.1(c), and FPT_RVM.1.

SF.OPE_AC meets the following 6 functional requirements; FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FMT_MSA.1, FMT_SMF.1, and FPT_SEP.1.

SF.CS_HTTPS meets the following 1 functional requirement; FTP_ITC.1.

SF.CS_SMIME meets the following 4 functional requirements; FCS_CKM.1, FCS_COP.1(a), FCS_COP.1(b), and FCS_COP.1(c).

This indicates that each security function meets at least one functional requirement.

6.3 Strength of Function Claims

The security functions realized by probabilistic or permutational mechanism are SF.OPE_I&A, SF.CS_HTTPS, and SF.CS_SMIME. However, we specify SF.OPE_I&A, the password mechanism as the target of SOF rating, and exclude SF.CS_HTTPS and SF.CS_SMIME because they are realized by the cryptographic mechanism.

The strength of function level of SF.OPE_I&A is SOF-Basic.

6.4 Assurance Measures

The following documents are provided as the assurance measures:

Remote Communication Gate TypeN/L/BN1/BM1 Security Target
Version 1.03, 2006-06-07

Functional Specification for Remote Communication Gate Type N/L/BN1/BM1
Version 0.23, 2006-04-11

High-level design for Remote Communication Gate Type N/L/BN1/BM1
Version 0.16, 2006-04-11

Representation Guide for Remote Communication Gate Type N/L/BN1/BM1
Version 0.15, 2006-04-11

Remote Communication Gate TypeN/L Safety Information and Setup Guide
A768-8559, 2006-01-31

Remote Communication Gate TypeN/L Operating Instructions
A768-8558, 2006-02-08

Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (European version)
A768-8603B, 2006-01-30

Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (North American version)
A768-8605B, 2006-01-31

Remote Communication Gate Type BN1/BM1 Operating Instructions (European version)
A768-8604B, 2006-02-03

Remote Communication Gate Type BN1/BM1 Operating Instructions (North American version)
A768-8606B, 2006-02-03

Test Documentation for Remote Communication Gate Type N/L/BN1/BM1
Version 0.19, 2006-04-11

Strength of Function Analysis for Remote Communication Gate Type N/L/BN1/BM1
Version 0.11, 2006-03-08

Vulnerability Analysis for Remote Communication Gate Type N/L/BN1/BM1
Version 0.14, 2006-03-16

Configuration Management Plan for Remote Communication Gate Type N/L/BN1/BM1
Version 0.21, 2006-04-11

Configuration List for Remote Communication Gate Type N/L/BN1/BM1
Version 0.20, 2006-06-07

Development Security Plan for Remote Communication Gate Type N/L/BN1/BM1
Version 0.14, 2005-12-15

Delivery Procedure for Remote Communication Gate Type N/L/BN1/BM1
Version 0.11, 2005-11-28

Installation, Generation, and Start-up Procedures for Remote Communication Gate Type N/L/BN1/BM1
Version 0.11, 2005-11-01

Service Manual for Remote Communication Gate TypeN/L/NB/LB
Version 1.3, 2006-02-08

Remote Communication Gate Type BN1/BM1 (Machine Code: A768/A769) SERVICE MANUAL
1.0 revised, 2005-05-24 & Technical Bulletin No.RA768002, 2006-02-07

7 PP Claims

There are no Protection Profiles to which this ST conforms.

8 Rationale

8.1 Security Objectives Rationale

In this section, it is demonstrated that the security objectives described in section 4 follow and cover all aspects identified in the security environment of section.

Table 21 shows that each security objective covers at least one threat or assumption, and that each threat and assumption is countered or realized by at least one security objective.

Table 21: Correspondence between Security Needs and Security Objectives

	O.OPE_I&A	O.CS_ID	O.T_CH	O.CIPHER	O.SIGNATURE	OE.PHYSIAL	OE.NETWORK	OE.CE	OE.ADMIN	OE.CS
T.CS_COMM			X							
T.CS_MAIL				X	X					
T.FAKE_CS		X								
P.ACCESS	X									
A.PHYSICAL						X				
A.NETWORK							X			
A.CE								X		
A.ADMIN									X	
A.CS										X

T.CS_COMM is countered by O.T_CH, because communication data between the TOE and CS is assured by O.T_CH.

T.CS_MAIL is countered by O.CIPHER and O.SIGNATURE, because it is ensured that e-mail data sent to CS is encrypted by O.CIPHER. The encrypted e-mail data can be decrypted only by CS's private key. Also, O.SIGNATURE's hash values for tampering detection enable the TOE to detect any illegal alternation.

T.FAKE_CS is countered by O.CS_ID, because the TOE ensures communication with the correct CS by examining the public key certificate sent from CS and the corresponding route certificate to confirm the certificate's validity and by checking the expiration date and details of the public key certificate.

P.ACCESS is implemented by O.OPE_I&A, because O.OPE_I&A makes it a policy to allow the operation only to the specified operators by authenticating operators (administrator, registrant and CE) with passwords. Also, the policy provides

that the administrator shall have the function to prohibit access of CEs by giving CE operation authority to the administrator. In addition, passwords are used for access control and the password policy shall have sufficient strength of function to satisfy the SOF-basic.

A.PHYSICAL is realized by OE.PHYSICAL because it is ensured that storage media and the information stored in it are protected from outside malicious parties.

A.NETWORK is realized by OE.NETWORK, because it is ensured that the internal network works appropriately and the LAN environment is protected from external attacks by firewall.

A.CE is realized by OE.CE, because it is ensured that the user commissions a proper dealer to repair RC Gate and a reliable CE comes to carry out the maintenance. CE is a person authorized by Ricoh or an appropriate company and makes efforts to maintain RC Gate in order.

A.ADMIN is realized by OE.ADMIN, because it is ensured that the administrator and registrant have carefully read and understood the user's manual and are capable of proper maintenance of RC Gate.

A.CS is realized by OE.CS, because Ricoh will select a suitable management firm and sign a contract with it to have a trusted company operate CS. In addition, Ricoh will establish management and operation regulations for proper operation and maintenance of CS, and the selected management firm shall carry out operation of CS in accordance with such regulations.

8.2 Security Requirements Rationale

8.2.1 Rationale for security function requirements

In this section, it is demonstrated that the security function requirements achieve the security objectives. Among the security objectives for the environment, OE.NETWORK, OE.PHYSICAL, OE.CE, OE.ADMIN, and OE.CS are for operations. Table 22 shows that the TOE security function requirements cover the security objectives for the TOE.

Table 22: Correspondence between Security Objectives and Functional Requirements

	FDP_ACC.1	FDP_ACF.1	FTP_ITC.1	FCS_CKM.1	FCS_COP.1(a)	FCS_COP.1(b)	FCS_COP.1(c)	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.2	FIA_UAU.6	FIA_UID.2	FMT_MSA.1	FMT_MTD.1(a)	FMT_MTD.1(b)	FMT_MTD.1(c)	FMT_SMF.1	FMT_SMR.1(a)	FMT_SMR.1(b)	FMT_SMR.1(c)	FPT_RVM.1	FPT_SEP.1
O.OPE_I&A	X	X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
O.CS_ID			X																				

O.T_CH			X																		
O.CIPHER				X	X	X															
O.SIGNATURE							X														

O.OPE_I&A is achieved by FDP_ACC.1, FDP_ACF.1, FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.6, FIA_UID.2, FMT_MSA.1, FMT_MTD.1(a), FMT_MTD.1(b), FMT_MTD.1(c), FMT_SMF.1, FMT_SMR.1(a), FMT_SMR.1(b), FMT_SMR.1(c), FPT_RVM.1, and FPT_SEP.1, because of the following reasons:

FDP_ACC.1 controls access of operators and ensures that only authorized operators can access the TOE data.

FDP_ACF.1 manages the operations allowed to each operator according to their respective access authority as well as the objects to be handled in such operations.

FIA_AFL.1 detects consecutive authentication errors and rejects the access when unsuccessful attempts are made 3 consecutive times.

FIA_ATD.1 maintains the access control by the service (CE).

FIA_SOS.1 ensures that the passwords used for authentication meet the ASCII code of 8 or more characters (0x20-0x5F, 0x61-0x7A).

FIA_UAU.2 ensures that unauthorized person can not access the TOE.

FIA_UAU.6 re-authenticates operators when they try to modify their password.

FIA_UID.2 ensures that users can not access the TOE data unless they are identified.

FMT_MSA.1 restricts the ability to manage the permission of CE operation authority to administrator.

FMT_MTD.1(a) restricts the ability to modify administrator password to administrator.

FMT_MTD.1(b) restricts the ability to modify registrant password to registrant.

FMT_MTD.1(c) restricts the ability to modify CE password to CE.

FMT_SMF.1 manages the security management requirements provided in Table 12.

FMT_SMR.1(a) maintains the role of administrator.

FMT_SMR.1(b) maintains the role of registrant.

FMT_SMR.1(c) maintains the role of CE.

The above functions are satisfied by protecting data from interference and tampering by other untrusted subjects, which is made possible by FPT_RVM.1 to keep TSP not bypassed and FPT_SEP.1 to separate and maintain the security domains.

O.CS_ID is achieved by FTP_ITC.1, because FTP_ITC.1 provides a communication channel which identifies CS for communication between the TOE and CS, and therefore the TOE will never connect to a fake CS.

O.T_CH is achieved by FTP_ITC.1, because FTP_ITC.1 establishes a trusted channel for communication between the TOE and CS, encrypts the communication data, and detects tampering of transmitted data (which ensures integrity).

O.CIPHER is achieved by FCS_CKM.1, FCS_COP.1(a), and FCS_COP.1(b), because FCS_CKM.1 enables the TOE to generate cryptographic keys for e-mail data, FCS_COP.1(a) encrypts e-mail data, and FCS_COP.1(b) encrypts cryptographic keys.

O.SIGNATURE is achieved by FCS_COP.1(c), because FCS_COP.1(c) generates hash values for communication data.

8.2.2 Rationale for minimum strength of function level

This TOE is a commercial product and is maintenance software to provide remote service for image I/O devices. The TOE is installed in an office, and sends image I/O device data to CS via external network. In an office environment with the TOE installed, it realizes the strength of function for SOF-Basic based on the organizational security policies. RC Gate only handles maintenance data of image I/O devices and does not directly manage financial assets of the customer. This means that there exists no attackers of middle or high level on the external network and the attack capability is "low level."

Therefore, SOF-Basic can be considered appropriate for the minimum strength of function level for the TOE.

8.2.3 Rationale for assurance requirements

As RC Gate only manages data from image I/O devices and does not directly manage financial assets, excessive protection mechanism is not required for TOE. However, Ricoh considers it is important to cover assurance for implementation of the security functions by analysing the security measures in the TOE developmental stage. Implementation and analysis of developers test based on the functional specification and high-level design of the security functions, which means the high-level design evaluation (ADV_HLD.2), is sufficient to demonstrate the accuracy. Analysis of apparent vulnerability (AVA_VLA.1) is sufficient for general needs. It is also important to achieve security assurance from development security (ALC_DVS.1) by evaluating the development environment and management of developed deliverables. For the reasons stated above, EAL3 can be considered appropriate as the estimation assurance level for this TOE.

8.2.4 Rationale for dependencies of security function requirements

Table 23 shows the rationale for dependencies of the security function requirements. This table provides the security requirements, which the TOE security function requirements depend on, along with the number of the TOE security function requirements. For those with no dependency, its rationale is explained below the table.

Table 23: Dependencies of security function requirements

No.	TOE security function requirement	Security requirement to depend on	No. for reference
1	FDP_ACC.1	FDP_ACF.1	2
2	FDP_ACF.1	FDP_ACC.1	1
		FMT_MSA.3	Unnecessary: Refer to (1) below.
3	FTP_ITC.1	N/A	—
4	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	5
		FCS_CKM.4	Unnecessary: Refer to (2) below.
		FMT_MSA.2	Unnecessary: Refer to (2) below.

5	FCS_COP.1(a)	FDP_ITC.1 or FCS_CKM.1	4
		FCS_CKM.4	Unnecessary: Refer to (3) below.
		FMT_MSA.2	Unnecessary: Refer to (3) below.
	FCS_COP.1(b)	FDP_ITC.1 or FCS_CKM.1	Unnecessary: Refer to (4) below.
		FCS_CKM.4	Unnecessary: Refer to (4) below.
		FMT_MSA.2	Unnecessary: Refer to (4) below.
	FCS_COP.1(c)	FDP_ITC.1 or FCS_CKM.1	Unnecessary: Refer to (5) below.
		FCS_CKM.4	Unnecessary: Refer to (5) below.
		FMT_MSA.2	Unnecessary: Refer to (5) below.
6	FIA_AFL.1	FIA_UAU.1	9
7	FIA_ATD.1	N/A	—
8	FIA_SOS.1	N/A	—
9	FIA_UAU.2	FIA_UID.1	11
10	FIA_UAU.6	N/A	—
11	FIA_UID.2	N/A	—
12	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	1
		FMT_SMF.1	14
		FMT_SMR.1	15
13	FMT_MTD.1(a) FMT_MTD.1(b) FMT_MTD.1(c)	FMT_SMF.1	14
		FMT_SMR.1	15
14	FMT_SMF.1	N/A	—
15	FMT_SMR.1(a) FMT_SMR.1(b) FMT_SMR.1(c)	FIA_UID.1	11
16	FPT_RVM.1	N/A	—
17	FPT_SEP.1	N/A	—

(1) **Rationale for no dependency of FDP_ACF.1 on FMT_MSA.3**

As access to the TOE setting data is restricted to administrator, registrant and CE, it can not be changed. FMT_MSA.3 is therefore unnecessary.

(2) **Rationale for no dependency of FCS_CKM.1 on FCS_CKM.4 and FMT_MSA.2**

E-mail data from TOE to CS is encrypted with a cryptographic key generated by the TOE. The life cycle of this key is short because cryptographic keys are generated and used for cryptographic operation when e-mails are sent to CS, which means a cryptographic key is generated each time an e-mail is sent out. It is therefore unnecessary to maintain a cryptographic key for a long period, or to have secure security attributes. FMT_MSA.2 is therefore unnecessary.

Cryptographic keys are encrypted by FCS_COP.1(b) when they are delivered to CS. FCS_CKM.4 is also unnecessary because there is no such process as to deliver the key to anywhere but CS or to replace the key.

(3) **Rationale for no dependency of FCS_COP.1(a) on FCS_CKM.4 and FMT_MSA.2**
FMT_MSA.2 and FCS_CKM.4 are unnecessary as well for the same reason as explained in (2).

(4) **Rationale for no dependency of FCS_COP.1(b) on [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4 and FMT_MSA.2**
Concerning the encryption of cryptographic keys for e-mail data, [FDP_ITC.1 or FCS_CKM.1] and FMT_MSA.2 for generation and management of cryptographic keys are realized in the manufacturing process, not in the use process of RC Gate, and therefore the dependency relation is not necessary. As the keys discussed here are public key certificates of CS, the TOE does not need to destruct them, which makes FCS_CKM.4 unnecessary as well.

(5) **Rationale for no dependency of FCS_COP.1(c) on [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, and FMT_MSA.2**
FCS_COP.1(c) is for hashing e-mail data and does not use cryptographic keys. This means it does not require key management such as generation and destruction of cryptographic keys and key security attributes, and therefore function requirements of [FDP_ITC.1 or FCS_CKM.1], FMT_MSA.2, and FCS_CKM.4 are unnecessary.

8.2.5 Mutual support of security function requirements

This section examines the mutual support of security function requirements.

Table 24: Mutual Support of Security Function Requirements

No.	Function Requirement	Bypass	Interference	Deactivation
1	FDP_ACC.1	N/A	N/A	N/A
2	FDP_ACF.1	FIA_UAU.2	FMT_MSA.1 FPT_SEP.1	N/A
3	FTP_ITC.1	N/A	N/A	N/A
4	FCS_CKM.1	N/A	N/A	N/A
5	FCS_COP.1(a)	N/A	N/A	N/A
6	FCS_COP.1(b)	N/A	N/A	N/A
7	FCS_COP.1(c)	N/A	N/A	N/A
8	FIA_AFL.1	N/A	N/A	N/A
9	FIA_ATD.1	N/A	N/A	N/A
10	FIA_SOS.1	N/A	N/A	N/A
11	FIA_UAU.2	FPT_RVM.1	FMT_MTD.1(a), FMT_MTD.1(b) FMT_MTD.1(c)	N/A

12	FIA_UAU.6	FPT_RVM.1	N/A	N/A
13	FIA_UID.2	N/A	N/A	N/A
14	FMT_MSA.1	N/A	N/A	N/A
15	FMT_MTD.1(a)	N/A	N/A	N/A
16	FMT_MTD.1(b)	N/A	N/A	N/A
17	FMT_MTD.1(c)	N/A	N/A	N/A
18	FMT_SMF.1	N/A	N/A	N/A
19	FMT_SMR.1(a)	N/A	N/A	N/A
20	FMT_SMR.1(b)	N/A	N/A	N/A
21	FMT_SMR.1(c)	N/A	N/A	N/A
22	FPT_RVM.1	N/A	N/A	N/A
23	FPT_SEP.1	N/A	N/A	N/A

[Bypass]

FDP_ACF.1 requires that unique operator be identified and authenticated, which is implemented by FIA_UAU.2.

FIA_UAU.2 shall be enforced before the operator controls the setting items through Web, which is implemented by FPT_RVM.1.

FIA_UAU.6 shall be enforced before the operator modifies the password, which is implemented by FPT_RVM.1.

[Interference]

FDP_ACF.1 controls access based on the security attributes of the subjects and objects. Among the security attributes of the subjects and objects, only the CE operation authority is changeable. Access to the CE operation authority is restricted to administrator by FMT_MSA.1, and it is protected from interference. Also, it is satisfied by separating and maintaining the security domain to protect data from interference and tampering by other untrusted subjects, which is ensured by FPT_SEP.1.

FIA_UAU.2 conducts authentication by passwords to prevent the setting items from being manipulated by anybody except operators assigned to administrator, registrant or CE. FMT_MTD.1(a), FMT_MTD.1(b), and FMT_MTD.1(c) protects passwords from illegal alternation by restricting the ability to modify passwords to administrator, registrant and CE respectively.

8.3 Rationale for Summary of TOE Specification

8.3.1 Rationale for TOE security functions

In this section, it is demonstrated that the security functions realize the security function requirements.

Table 25 shows that each security function for the TOE covers at least one of TOE security function requirements, and that each TOE security function requirement is covered with at least one of security functions for the TOE.

Table 25: Correspondence between Function Requirements and Security Functions

	SF.OPE_I&A	SF.OPE_AC	SF.CS_HTTPS	SF.CS_SMIME
FDP_ACC.1		X		
FDP_ACF.1		X		
FTP_ITC.1			X	
FCS_CKM.1				X
FCS_COP.1(a)				X
FCS_COP.1(b)				X
FCS_COP.1(c)				X
FIA_AFL.1	X			
FIA_ATD.1		X		
FIA_SOS.1	X			
FIA_UAU.2	X			
FIA_UAU.6	X			
FIA_UID.2	X			
FMT_MSA.1		X		
FMT_MTD.1(a)	X			
FMT_MTD.1(b)	X			
FMT_MTD.1(c)	X			
FMT_SMF.1	X	X		
FMT_SMR.1(a)	X			
FMT_SMR.1(b)	X			
FMT_SMR.1(c)	X			
FPT_RVM.1	X			
FPT_SEP.1		X		

FDP_ACC.1

FDP_ACC.1 is satisfied because SF.OPE_AC controls access based on the access list.

FDP_ACF.1

FDP_ACF.1 is satisfied because SF.OPE_AC controls accessible information for each operator.

FTP_ITC.1

FTP_ITC.1 is satisfied because SF.CS_HTTPS ensures communication over HTTPS between the RC Gate and CS.

FCS_CKM.1

FCS_CKM.1 is satisfied because SF.CS_SMIME generates cryptographic keys for 168 bits 3DES by generating RSA pseudo random numbers to encrypt data.

FCS_COP.1(a)

FCS_COP.1(a) is satisfied because SF.CS_SMIME encrypts data to be sent to CS.

FCS_COP.1(b)

FCS_COP.1(b) is satisfied because SF.CS_SMIME encrypts cryptographic keys with RSA when they are sent to CS.

FCS_COP.1(c)

FCS_COP.1(c) is satisfied because SF.CS_SMIME uses it to hash data.

FIA_AFL.1

FIA_AFL.1 is satisfied because SF.OPE_I&A makes the TSF reject access for one minute if operator password input fails three consecutive times.

FIA_ATD.1

FIA_ATD.1 is satisfied by SF.OPE_AC because it maintains the CE operation authority in the TOE and uses it to give operation authority to operators.

FIA_SOS.1

FIA_SOS.1 is satisfied because SF.OPE_I&A requires a password of 8 or more characters to be input when registering a new password.

FIA_UAU.2

FIA_UAU.2 is satisfied because SF.OPE_I&A identifies and authenticates operators with passwords when they start accessing data via Web browser.

FIA_UAU.6

FIA_UAU.6 is satisfied because SF.OPE_I&A requires the current password to be input when each operator tries to modify the password.

FIA_UID.2

FIA_UID.2 is satisfied because SF.OPE_I&A identifies operators (administrator, registrant and CE) before they start operation.

FMT_MSA.1

FMT_MSA.1 is satisfied because SF.OPE_AC restricts the ability to set the CE operation authority (permitted/not permitted) to administrator.

FMT_MTD.1(a)

FMT_MTD.1(a) is satisfied because SF.OPE_I&A restricts the ability to modify administrator password to administrator.

FMT_MTD.1(b)

FMT_MTD.1(b) is satisfied because SF.OPE_I&A restricts the ability to modify registrant password to registrant.

FMT_MTD.1(c)

FMT_MTD.1(c) is satisfied because SF.OPE_I&A restricts the ability to modify CE password to CE.

FMT_SMF.1

FMT_SMF.1 is satisfied because SF.OPE_I&A and SF.OPE_AC maintain the security management functions provided in Table 12.

Among the security management functions, SF.OPE_I&A provides the function for administrator to modify the administrator password, function for registrant to modify the registrant password, and function for CE to modify the CE password, while SF.OPE_AC provides the function for administrator to control the CE access authority.

FMT_SMR.1(a)

FIA_SMR.1 is satisfied because SF.OPE_I&A identifies administrator to assign its authority to perform operations.

FMT_SMR.1(b)

FIA_SMR.1 is satisfied because SF.OPE_I&A identifies registrant to assign its authority to perform operations.

FMT_SMR.1(c)

FIA_SMR.1 is satisfied because SF.OPE_I&A identifies CE to assign its authority to perform operations.

FPT_RVM.1

FPT_RVM.1 is satisfied because it is ensured that SF.OPE_I&A be enforced

FPT_SEP.1

FPT_SEP.1 is satisfied because SF.OPE_AC separates and maintains the security domains to protect data from interference and tampering by other untrusted subjects.

8.3.2 Rationale for strength of function claims

Three security functions (SF.OPE_I&A, SF.CS_HTTPS, and SF.CS_SMIME) have probabilistic or permutational mechanism. However, the strength of cryptographic algorithm is not applied to CC. The strength of function only applies to probabilistic or permutational mechanism, which is not for cryptography. Therefore, only SF.OPE_I&A has the strength of function for SOF-Basic.

Functions using cryptographic algorithm (SF.CS_HTTPS and SF.CS_SMIME) are excluded from the SOF rating. The minimum strength of function level for the TOE is SOF-Basic.

It is apparent that these claims are consistent.

8.3.3 Rationale for combination of security functions

The four security functions cover all the security function requirements. Each of these security functions satisfies the corresponding TOE security function requirements independently. There is no such security function to satisfy TOE security function requirements by working together.

8.3.4 Rationale for assurance measures

Table 26 shows that all assurance requirements for class ASE and EAL 3 are covered by corresponding assurance measures.

Table 26: Correspondence between Assurance Requirements and Assurance Measures

Assurance Class	Assurance Component	Assurance Measure
ASE: Security Target evaluation	ASE_DES.1 ASE_ENV.1 ASE_INT.1 ASE_OBJ.1 ASE_PPC.1 ASE_REQ.1 ASE_SRE.1 ASE_TSS.1	Remote Communication Gate TypeN/L/BN1/BM1 Security Target Version 1.03, 2006-06-07
ACM: Configuration management	ACM_CAP.3 ACM_SCP.1	Configuration Management Plan for Remote Communication Gate Type N/L/BN1/BM1 Version 0.21, 2006-04-11 Configuration List for Remote Communication Gate Type N/L/BN1/BM1 Version 0.20, 2006-06-07
ADO: Delivery and operation	ADO_DEL.1 ADO_IGS.1	Delivery Procedure for Remote Communication Gate Type N/L/BN1/BM1 Version 0.11, 2005-11-28 Installation, Generation, and Start-up Procedures Installation, Generation, and Start-up Procedures for Remote Communication Gate Type N/L/BN1/BM1 Version 0.11, 2005-11-01

Assurance Class	Assurance Component	Assurance Measure
ADV: Development	ADV_FSP.1	Functional Specification Functional Specification for Remote Communication Gate Type N/L/BN1/BM1 Version 0.23, 2006-04-11
	ADV_HLD.2	High-level design for Remote Communication Gate Type N/L/BN1/BM1High-level design for Remote Communication Gate Type N/L/BN1/BM1 Version 0.16, 2006-04-11
	ADV_RCR.1	Representation Guide for Remote Communication Gate Type N/L/BN1/BM1 Version 0.15, 2006-04-11
AGD: Guidance documents	AGD_ADM.1 AGD_USR.1	Remote Communication Gate TypeN/L Safety Information and Setup Guide A768-8559, 2006-01-31 Remote Communication Gate TypeN/L Operating Instructions A768-8558, 2006-02-08 Service Manual for Service Manual for Remote Communication Gate TypeN/L/NB/LB Version 1.3, 2006-02-08 Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (European version) A768-8603B, 2006-01-30 Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (North American version) A768-8605B, 2006-01-31 Remote Communication Gate Type BN1/BM1 Operating Instructions (European version) A768-8604B, 2006-02-03 Remote Communication Gate Type BN1/BM1 Operating Instructions (North American version) A768-8606B, 2006-02-03 Remote Communication Gate Type BN1/BM1 (Machine Code: A768/A769) SERVICE MANUAL 1.0 revised, 2005-05-24 & Technical Bulletin No.RA768002, 2006-02-07
ALC: Life cycle support	ALC_DVS.1	Development Security Plan for Remote Communication Gate Type N/L/BN1/BM1 Version 0.14, 2005-12-15
ATE: Tests	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_INT.2	Test Documentation for Test Documentation for Remote Communication Gate Type N/L/BN1/BM1 Version 0.19, 2006-04-11

Assurance Class	Assurance Component	Assurance Measure
AVA: Vulnerability assessment	AVA_MSU.1	Remote Communication Gate TypeN/L Safety Information and Setup Guide A768-8559, 2006-01-31 Remote Communication Gate TypeN/L Operating Instructions A768-8558, 2006-02-08
	AVA_SOF.1	Strength of Function Analysis for Strength of Function Analysis for Remote Communication Gate Type N/L/BN1/BM1 Version 0.11, 2006-03-08
	AVA_VLA.1	Vulnerability Analysis for Remote Communication Gate Type N/L/BN1/BM1 Vulnerability Analysis for Remote Communication Gate Type N/L/BN1/BM1 Version 0.14, 2006-03-16

8.4 PP Claims Rationale

There are no Protection Profiles to which this ST conforms.

9 Annex

9.1 Abbreviation

CC	Common Criteria
CE	Customer Engineer
CS	Communication Server
LAN	Local Area Network
OS	Operating System
PP	Protection Profile
SC	Service Call
SF	Security Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function