CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9240-2005**
Product / system:	Remote Communication Unit Software Module of Remote Communication Gate Type BN1 & BM1, Version 3.18 summarized as Software Module of RC Gate, version 3.18
Product manufacturer:	Ricoh Company, Ltd. 1-3-6 Nakamagome, Ohta-ku Tokyo, 143-8555 Japan
Customer:	see above
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 1.1 as of 2005-09-16* Document-number: *20653678_TÜViT_023.02* Author: Harald Wacker
Result:	EAL3
Evaluation stipulations:	none
Certifier:	Joachim Faulhaber
Certification stipulations:	none

Essen, 2005-09-26

Dr. Christoph Sutter Joachim Faulhaber

Contents

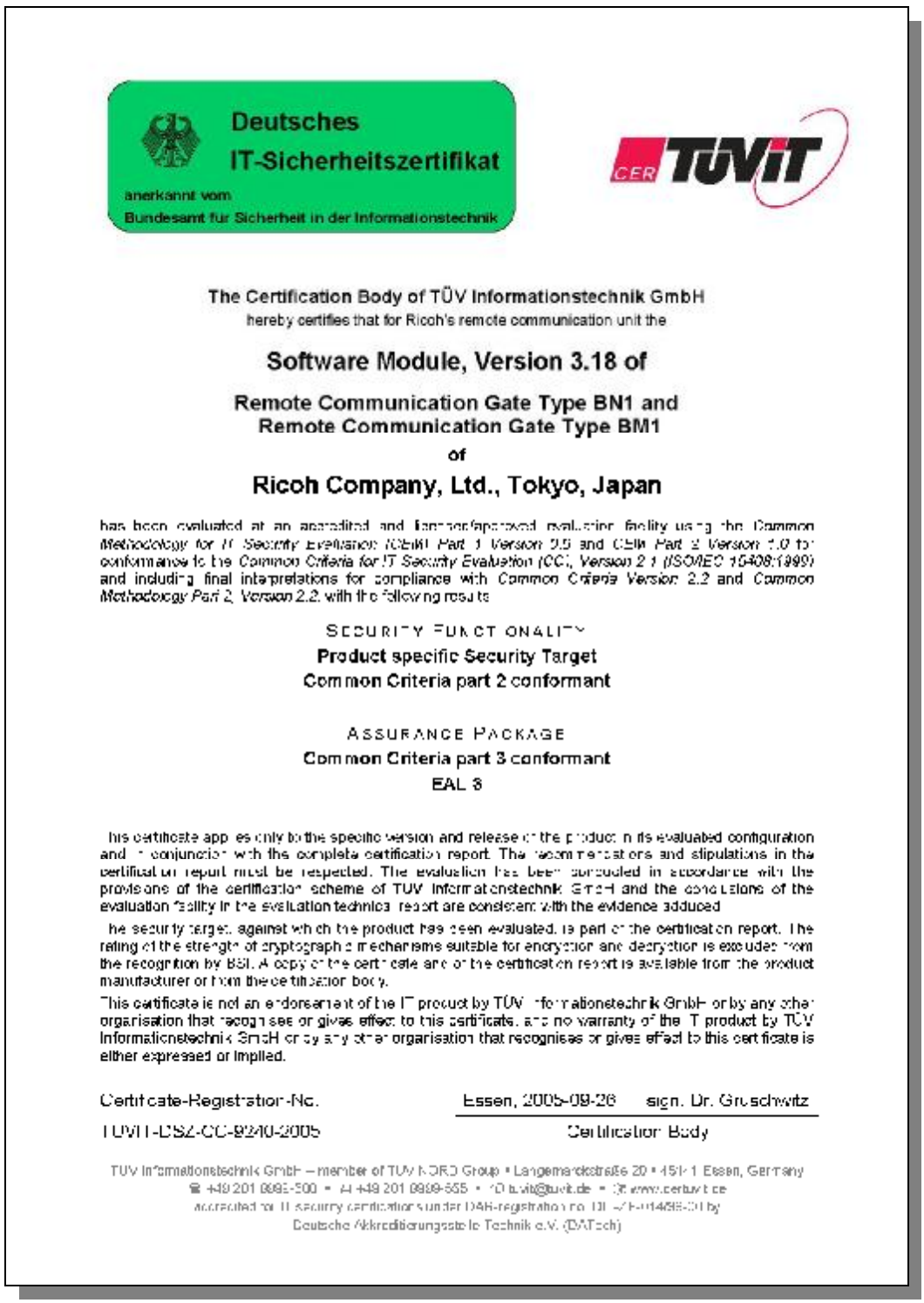
Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate



Deutsches
IT-Sicherheitszertifikat
anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

CER TÜViT

The Certification Body of TÜV Informationstechnik GmbH
hereby certifies that for Ricoh's remote communication unit the

Software Module, Version 3.18 of

Remote Communication Gate Type BN1 and
Remote Communication Gate Type BM1

of

Ricoh Company, Ltd., Tokyo, Japan

has been evaluated at an accredited and licensed/approved evaluation facility using the Common *Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and CEM *Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with *Common Criteria Version 2.2* and *Common Methodology Part 2, Version 2.2*, with the following results:

SECURITY FUNCTIONALITY
Product specific Security Target
Common Criteria part 2 conformant

ASSURANCE PACKAGE
Common Criteria part 3 conformant
EAL 3

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TUV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No.
TUVIT-DSZ-CC-9240-2005

Essen, 2005-09-26 sign. Dr. Grusschwitz
Certification Body

TUV Informationstechnik GmbH – member of TUV NORD Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-500 • 🖷 +49 201 8999-555 • ✉ it@tuvit.de • 🌐 www.certuvit.de
Accredited as IT security certification body under DAkkS-registration no. D-ZE-11436-01 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)

2 Certification Body – CERTÜViT

CERTÜViT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – member of TÜV NORD Group – was established in 1998 and offers a variety of services in the context of security evaluation and validation.

CERTÜViT was accredited in September 1999 for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (Dekitz)* now *Deutsche Akkreditierungsstelle Technik e.V. (DATech), Frankfurt/Main* under DAR-registration no. DAT-ZE-014/99-01 and performs its projects under a quality management system certified against ISO 9001 by *Germanischer Lloyd, Hamburg*.

CERTÜViT is accredited by *Bundesamt für Sicherheit in der Informationstechnik*[2] to issue the "German IT Security Certificate" which is recognised by BSI as equivalent to the "German IT Security Certificate" of BSI.

3 Specifications of the Certification Procedure

The certification body conducts the certification procedure according to the criteria laid down in the following:

- DIN EN 45011
- TÜViT Certification Scheme
- TÜViT Certification Conditions
- Regulations on the "German IT Security Certificate" issued by the BSI and accepted in the contract of BSI and TÜViT as of November 20, 2002.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.2, January 2004.
- Common Methodology for Information Technology Security Evaluation (CEM) part 1, version 0.6, January 1997.
- Common Methodology for Information Technology Security Evaluation (CEM) part 2, version 2.2, January 2004.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[1] in the following termed shortly TÜViT

[2] in the following termed shortly BSI

4 Recognition Agreements

In order to avoid multiple certification of the same product by different certification bodies a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC - under certain conditions was agreed. CERTÜViT certificates are German IT Security Certificates recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates but they are not part of these international agreements.

4.1 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4 was signed between the national participants of Australia and New Zealand, Austria, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, The Netherlands, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom and the United States.

4.2 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The arrangement on the mutual recognition of IT security certificates based on the CC was extended by these participants up to and including the evaluation assurance level EAL7.

5 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The product Software Module of RC Gate, version 3.18 has undergone the certification procedure at TÜViT certification body. It was an initial certification.

The evaluation of the product Software Module of RC Gate, version 3.18 was conducted by the evaluation body for IT-security of TÜViT and concluded on September 16, 2005. The TÜViT evaluation facility is recognised by BSI.

The sponsor as well as the developer is Ricoh Company, Ltd. Distributor of the product is Ricoh Company, Ltd.

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on September 26, 2005. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

This certification report applies only to the version of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

With regard to the meaning of the evaluation assurance levels (EAL) and the strength of function (SOF), please refer to part C of this report.

6 Publication

The following Certification Results consist of pages B-1 to B-16. The product Software Module of RC Gate, version 3.18 will be included in the BSI list of certified products which is published at regular intervals (e. g. in the Internet at http://www.bsi.bund.de) and the TÜViT certification lists (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the Certification Result

1 Executive Summary

1.1 Target of Evaluation and Evaluation Background

The TOE is the “Software module of RC Gate V3.18” implemented in the product Remote Communication Gate Type BN1 and Remote Communication Gate Type BM1.

The product RC Gate acts as a relay unit, which collects operational data like alerts, status or counter information from networked laser printers or multifunctional printers (MFPs). Collected data is sent to a trusted management server via Internet or telephone line (Dial-up PPP connection). The trusted management server is called "Communication Server (CS)". During transmission the information is HTTPS or S/MIME secured. Once received, the data is processed and used to generate meter billing, printer supply orders and fleet utilization reports. Furthermore RC Gate supports the firmware update of networked laser printers and multifunctional printers (MFPs).

RC Gate identifies and authenticates different operators (administrator, registrant or CE). It controls operations performed by the operator and identifies and authenticates CS before communication takes place.

RC Gate exports and imports encrypted information when HTTPS method is selected and exports encrypted E-mail information to CS when SMTP method is selected.

Additionally RC Gate records three types of audit log: access log, communication log and system log.

RC Gate consists of the main board with CPU, flash memory, LAN Ethernet circuit, RS485 and the interface of power supply. RC Gate type BM1 differs from BN1 by an additional modem board, which provides an interface to the telephone line. Optional wireless LAN card can be attached to RC Gate, but the wireless option is out of scope of the TOE.

The software part of the RC Gate consists of:

- embedded Linux operating system (RC Gate OS V1.11, based on MontaVista Linux) – out of scope of the TOE
- Data Base Management System (DBMS) – out of scope of the TOE,
- Communication Management Module – out of scope of the TOE,
- SMTP Communication Module – out of scope of the TOE,
- as well as the software parts of the TOE
    - Device Management Module,
    - Log Management Module,
    - Web Management Module, and
    - CS Management Module

The sponsor, vendor and distributor is “Ricoh Company, Ltd., 1-3-6 Nakamagome, Ohta-ku, Tokyo, 143-8555 Japan“

The TOE was evaluated against the claims of the Security Target[3] (attached in part D) by the “*evaluation body of TÜV Informationstechnik GmbH*” (TÜViT). The evaluation was completed on September 16, 2005. TÜViT’s evaluation body is recognised by BSI.

1.2 Assurance Package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 3 (Evaluation Assurance Level 3).

1.3 Strength of Functions

The TOE‘s strength of functions is rated “basic” (SOF-basic). The strength of functions rating does not include cryptographic algorithms for encryption and decryption. For more details see also chapter 9 of this report.

1.4 Functionality

The TOE’s security requirements have exclusively been taken from CC part 2 (i.e. the set is CC part 2 conformant) [CC]. Chapter 9 lists the security functional requirements in detail. They are met by suitable IT security functions realized by the TOE:

SF.OPE_I&A: TSF identifies and authenticates operator (Administrator, Registrant and CE) prior to the operation listed below. When authentication is succeeded, TSF assigns a role (Administrator, Registrant and CE) to the operator.

While the operator is entering password, the asterisks are shown instead of password characters.

If the wrong password is entered three consecutive times, TSF reject identification and authentication for one minute.

The operator (Administrator, Registrant and CE) can change his own password. The length of new password should be at least 8 and at most 13 characters. If the length of the new password is not in the range, the new password is rejected.

SF.OPE_AC: TSF controls operations performed by the operator based on the operator's identification information and method to communicate with CS. When direct HTTPS method, dialup HTTPS method, or

[3] hereinafter called ST

SMTP method is used to communicate with CS, operators can access to the information based on [ST], Table 4.

SF.CS_I&A: TSF identifies and authenticates CS before communicates with CS by HTTPS. When the identification and authentication is succeeded, it is allowed to export or import information to/from CS.

For authentication of CS, TSF uses the HTTPS mutual authentication mechanism.

SF.CS_HTTPS: TSF can export and import information listed in [ST], Table 5 to/from CS by using HTTPS protocol.

TSF authenticates CS before export or import information. When CS is successfully authenticated, TSF encrypts the information to export, and decrypts the imported information. Furthermore, CS is able to perform the allowed operations as specified/stated in [ST], table 4 after a successful authentication.

SF.CS_SMIME: TSF can export information listed in [ST], Table 5 to CS by E-Mail. When TSF export information to CS by using E-Mail, TSF encrypts E-Mail message by S/MIME. TSF encrypts the message by the public key of CS to prevent other than CS to read the message.

SF.AUDIT: TSF records 3 types of audit log: access log, communication log and system log. The events listed in Table 7 [ST] are recorded to each audit log, and the information listed in [ST], Table 9 are included in the records.

When size of each audit log exceeds 64 Kbytes, the oldest record is overwritten with new record.

The operator successfully authenticated by SF.OPE_I&A is allowed to read access log and communication log. Only CE successfully authenticated by SF.OPE_I&A is allowed to read system log. They cannot modify those audit logs.

1.5 Summary of Threats and Organisational Security Policies (OSPs)

The assets the TOE intends to protect are

- Certificates for RC Gate
- Passwords for each operator
- Audit logs
- Setting information for RC Gate
- Collected information of image I/O devices
- Firmware to update image I/O device

- Certificates for image I/O device

The threats as defined in the security target are:

T.WEB: Assets in RC Gate may be read, modified or destroyed by employees or external attackers.

T.CS_COMM: Leackage of, or tampering at Internet or telephone line, when RC Gate communicates CS directly.

T.CS_MAIL: Leackage of, or tampering with information at Internet, when mail method is used.

T.FAKE_CS: A fake CS may be built in Internet or telephone network when RC Gate communications with CS.

The TOE complies with the following organisational security policy (OSP):

OSP.AUDIT: TOE shall write/create logs for audit or maintenance.

A more detailed description of the threats and OSPs, which were assumed for the evaluation are specified in the ST which is attached as part D of this certification report.

1.6 Special Configuration Requirements

The TOE is delivered as one fixed configuration and no further generation takes place after delivery to the customer.

1.7 Assumptions about the Operating Environment

The assumptions about the environment of use of the TOE and about the intended usage of the TOE cover physical and personnel aspects.

It is assumed that RC Gate is placed in a physical secure place. Multifuntional printers and laser printers are genuine products. The network is properly managed and the CE is well trained. Furthermore CE, administrator, registrant and the communication server can be trusted.

Further assumptions on secure usage are detailed in the ST which is attached as part D of this certification report.

1.8 Independence of the Certifier

Within the last two years, the certifier did not render any consulting- or other services for the company ordering the certification and there was no relationship between them which might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product which forms the basis of the certification.

1.9 Disclaimers

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept with regard to generation, configuration and operation as detailed in this certification report. This certificate is not an endorsement of the IT product by the TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

Beside guidance documentation (see chapter 6) the RC Gate box with preinstalled operating system and TOE are delivered to the user and marked with the developer's identifiers:

TOE:	**Software module of RC Gate V3.18**	
Product **(TOE platform):**	**Remote Communication Gate Type BN1**	
	Code Europe:	A76827
	Code North America	A76817
	Remote Communication Gate Type BM1	
	Code Europe:	A76927
	Code North America:	A76917
Operating system of the TOE platform:	RC Gate OS V1.11 (based on MontaVista Linux)	

The evaluated TOE version can be uniquely identified by comparison of the information presented on RC Gate Login page (browser GUI/browser window) with validation

information's provided by the developer on the web site for RC Gate, e.g. "`firmware 3.18-1.11`".

The first figure denotes the version of the TOE and the second figure denotes the version of the underlying operating system.

3 Security Policy

The security policy is described in section 5.1 [ST] as "Role Based Access Control-SFP" and deals with the following subjects:

- Operator (Administrator, Registrant or CE)
- Communication Server (CS)

who can perform the following operations

`-R--`: can see setting items existence can view its current value.
`--W-`: can see setting items existence
can change its value (but cannot necessarily view the current and under-change value of the item as only '*' characters are shown if not in combination with -RW-)
`A---`: can add (create) new setting items
can delete setting items
`---E`: can execute a function
`----`: can not see setting items existence
can not view or change or the value of the setting item

on setting items (objects), as defined in table 4 in [ST]

Security policy is described more detailed in the ST which is attached as part D of this certification report.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

It is assumed that the local network is properly managed and that RC Gate is physically protected. Administrator, Registrant and Customer engineer (CE) are trustworthy.

4.2 Environmental Assumptions

The specific conditions listed below are assumed to exist in the TOE environment. These assumptions include essential environmental constraints on the use of the TOE.

A.PHYSICAL	The TOE is physically protected
A.DEVICE	Laser printers and multifunctional printers are trusted
A.NETWORK	Network is properly managed by responsible persons
A.CE	Customer Engineer (CE) is trusted
A.ADMIN	Administrator and Registrant are trusted
A.CS	Communication Server is properly managed by responsible company and persons.

4.3 Clarification of Scope

Access to RC Gate via the web interface is not necessarily located within the customer/end user network. It is up to the customer to prevent such access from the internet and to have administration locally.

5 Architectural Information

The TOE consists of the following modules:

- CS Management Module
- Device Management Module
- Log Management Module
- Web Management Module

CS Management module performs CS identification and data exchange. Cryptographic function is included in this module. Certificates are read via *Web Management Module*.

Device Management Module manages laser printers and multifunctional printers. Main function of this module is collecting information of these devices.

Log Management Module provides log management function. Each module such as *CS, Web and Device Management Module* send the logging event to *Log Management Module*. This module reads system time from OS to create audit event. Log files are saved in SD memory.

The *Web Management Module* provides the Web interface and performs operator identification and authentication. Flash memory is used for storing certificates (these certificates are read by *Web Management Module* when RC Gate starts up).

6 Documentation

The following documentation is provided with the product by the developer to the consumer:

- Safety Information & Setup Guide (either European, North America or Asia version), 2005-06-22
- Remote Communication Gate Type BN1/BM1 Operating Instructions (either European, North America or Asia version), 2005-07-01, **(available via Internet, URL given in above mentioned document)**
- Remote Communication Gate Type BN1/BM1 (Machine Code: A768/A769) Service Manual, 2005-05-24, **(provided to customer engineer only)**

7 IT Product Testing

The developer's strategy was to test the TOE against the specification of all security enforcing functions detailed in the functional specifications and in the high-level design. Furthermore the developer's test cases were conducted with the goal to confirm that the TOE meets the security functional requirements.

The test cases reported (approx. 80 different test cases/test steps)

- completely cover the security functions (altogether: 6),
- correspond to the external interfaces (altogether: 10) of the TOE defined in the functional specification,
- correspond also to the defined subsystems (altogether: 7) as defined in the high-level design and
- completely cover the 4 modules (chapt. 5), the TOE consists of.

The developer specified, conducted and documented suitable functional tests for the security functions. The test results obtained for all of the performed tests turned out to be as expected. No errors or other flaws occurred with regard to the security functionalities and the TOE subsystems. Consequently, the test results demonstrate that the behaviour of the security functions is as specified.

The evaluator’s independent testing as well as penetration tests were partly performed in the developer’s testing environment and partly at TÜViT GmbH, information security department, in Essen. The same platforms and tools as for the developer tests were used.

The evaluator's objective regarding this aspect was to test the functionality of the TOE as described in the functional specifications and the high-level design, and to verify the developer's test results. The evaluator’s sample of developer tests covers all TSF.

The results of the specified and conducted independent evaluator tests confirm the TOE functionality. The TOE security functions were found to behave as specified.

Penetration testing has been conducted by repeating 19 developer tests and 39 evaluator tests (including independent, penetration and confirmation tests of non-exploitability of

vulnerabilities). The penetration testing conducted confirms that all the obvious vulnerabilities were considered and that the vulnerabilities identified are non-exploitable by attackers with low attack potential in the intended operational environment of the TOE, if taking into consideration all the measures the user is informed about.

8 Evaluated Configuration

The TOE is delivered in one fixed configuration and no further generation takes place. Therefore the evaluated configuration is identical to the TOE, which can be identified as described in chapter 2 of this certification report:

"firmware 3.18-1.11"

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by TÜViT's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS].

The verdicts for the CC, part 3 assurance classes and components (according to EAL3 and the class ASE for the Security Target Evaluation) are summarised in the following table:

EAL3 assurance classes and components		**Verdict**
Security Target evaluation	**CC Class ASE**	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	n.a.[4]
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration Management	**CC Class ACM**	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and operation	**CC Class ADO**	PASS
Delivery procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	**CC Class ADV**	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	**CC Class AGD**	PASS

[4] n.a. = not applicable

Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	**CC Class ALC**	PASS
Identification of security measures	ALC_DVS.1	PASS
Tests	**CC Class ATE**	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	**CC Class AVA**	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

No Protection Profile (PP) compliance claims were made in the ST. Thus, the component ASE_PPC.1 is not applicable. All other assurance components were assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the security target is considered to be Part 3 conformant.

The security target, chapter 5 claims, that the TOE will fulfil the following TOE security functional requirements, which were exclusively taken from [CC] part 2:

Component ID	Component title
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1 (a)	Audit review
FAU_SAR.1 (b)	Audit review
FAU_STG.2	Guarantees of audit data availability
FCS_COP.1	Cryptographic operations
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ITC.1	Import of user data without security attributes
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication

Component ID	Component title
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Timing of identification
FMT_MTD.1	Management of TST data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps
FTP_ITC.1	Inter-TSF trusted channel

The evaluation performed in accordance to EAL3 has shown that the TOE security functional requirements are correctly realised by the TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE will meet the security objectives claimed in the ST.

The evaluation has shown that the TOE will fulfil the claimed strength of function SOF-basic for the probabilistic and permutational mechanisms (account name/password based authentication), implemented in security function SF.OPE_I&A.

The sponsor must advise the certification authority about any modification of the TOE or its guidance documentation. The certification authority will then check whether the certification results are still valid and, if necessary, initiate all further steps concerning a re-evaluation. The results of the evaluation are only applicable to "*Software Module of RC Gate,version 3.18*". The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

10 Evaluation stipulations, comments and recommendations

With reference to a potential vulnerability found during penetration testing the following hint important to the end user / customer was provided by the developer on the web site for RC Gate as supplement to *Service Manual* and *Operating Instructions*:

- *(…) RC Gate must be always connected to a UPS (uninterruptible power supply system) to prevent the log files from getting lost by a power cut. One week's logs are lost at worst-case scenario. (…)*

- *(…) Before power down/deactivation of RC Gate, please log on as registrant and perform a restart procedure by clicking "Restart" button on RC Gate monitor to save latest logs. After a short time, the yellow and green LEDs come to remain lit, then you can shut off the power supply. (…)*

11 Certification stipulations and notes

The hints given to the end user / customer, referenced in chap. 10, shall be taken into account in operating RC Gate.

12 Security Target

The security target for "*Software Module of RC Gate,version 3.18*" as of 2005-08-15, version 1.0 is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ADM	Administrator Guidance
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CE	Customer Engineer
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
CM	Configuration Management
EAL	Evaluation Assurance Level
FSP	Functional Specification
HLD	High-level Design
IF	Interface
IGS	Installation, Generation and Start-up
MFP	Multifunctional Printer
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface

SOF	Strength of Function
SS	Sub-system
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces
TSP	TOE Security Policy
USR	User Guidance
VLA	Vulnerability Analysis

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from Part3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[AIS] Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004,
Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 1: Introduction and general model, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, Version 2.2, January 2004

[ETR] Evaluation Technical Report, version 1.1, 2005-09-16, TÜV Informationstechnik GmbH, document-number: 20653678_TÜViT_023.02

[ST] Security Target for “Remote Communication Gate Type BN1, Remote Communication Gate Type BM1”, Version 1.0, 2005-08-15

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- conformance results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance results

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

> **Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2.
>
> **Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.

plus one of the following:

> **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3.
>
> **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

> ***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
>
> ***Package name* Augmented** - A PP or TOE is an augmentation of a predefined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.“

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

> ***PP Conformant*** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in *Table 1*.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 1: Assurance family breakdown and mapping

Evaluation assurance levels (chapter 6)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances.

Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview

„Table 2 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration Management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and Operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_IMT					**1**	**2**	***3***
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance Documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life Cycle Support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability Assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Table 2: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested

“EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay. An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested

"EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited."

Evaluation assurance level 3 (EAL3) - methodically tested and checked

"EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed

"EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL5) - semiformally designed and tested

"EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested

“EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested

“EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF)

AVA_SOF Strength of TOE security functions

“Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large.”

Three levels exist: SOF-basic, SOF-medium, and SOF-high.

Vulnerability analysis (AVA_VLA)

AVA_VLA Vulnerability analysis

"Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE."

Application notes

"A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.

The intent of the developer analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment for the TOE and that the TOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that requires a minimum of understanding of the TOE, skill, technical sophistication, and resources. These might be suggested by the TSF interface description. Obvious vulnerabilities include those in the public domain, details of which should be known to a developer or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer identify those vulnerabilities in a structured and repeatable way, as opposed to identifying them in an ad-hoc fashion. The associated evidence that the search for vulnerabilities was systematic should include identification of all TOE documentation upon which the search for flaws was based.

Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential. To accomplish this intent, the evaluator first assesses the exploitability of all identified vulnerabilities. This is accomplished by conducting penetration testing. The evaluator should assume the role of an attacker with a low (for AVA_VLA.2), moderate (for

AVA_VLA.3) or high (for AVA_VLA.4) attack potential when attempting to penetrate the TOE. Any exploitation of vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to the AVA_VLA.*.2C elements) in the context of the components AVA_VLA.2 through AVA_VLA.4.”

Part D

Security Target

Attached is the Security Target for “Remote Communication Gate Type BN1, Remote Communication Gate Type BM1”

Author: Hiroshi KAKII, Atsushi SATOH, Tomoaki ENOKIDA, Masahiro ITOH, Chitose MIURA, Haruyuki HIRABAYASHI, Jun SATOH, Ricoh Company, Ltd.

Date: 2005-08-15

Version:1.0

Security Target for

Remote Communication Gate Type BN1, Remote Communication Gate Type BM1

Author: Hiroshi KAKII, Atsushi SATOH, Tomoaki ENOKIDA, Masahiro ITOH, Chitose MIURA, Haruyuki HIRABAYASHI, Jun SATOH
Ricoh Company, Ltd.
Date: 2005-08-15
Version: 1.0

Document Revision History

Version	Date	Author	Description
1.0	2005-08-15	Hiroshi KAKII, Atsushi SATOH, Tomoaki ENOKIDA, Masohiro ITOH, Chitose MIURA, Haruyuki HIRABAYSHI, Jun SATOH	Adjusted version(s) and date(s) of all reference(s)

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 ST Identification

Title:	Security Target for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version:	1.0
Date:	2005-08-15
Author:	Hiroshi KAKII, Atsushi SATOH, Tomoaki ENOKIDA, Masahiro ITOH, Chitose MIURA, Haruyuki HIRABAYASHI, Jun SATOH Ricoh Company, Ltd.
Product:	Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 *Note: Hereafter these products are called with a generic name "RC Gate".*
TOE:	Software module of RC Gate V3.18
CC used:	ISO/IEC 15408:1999(E) Furthermore all relevant final interpretations until creation of this documentation were also considered.
Keywords:	Remote service, copier, printer, network, office, security

1.2 ST Overview

This Security Target (ST) describes the security specification of software module of the Remote Communication Gate (RC Gate). RC Gate is used mainly in business office and acts as a relay unit to which the user's image I/O devices (e.g. Copiers, Multi-Functional Printers) are connected. RC Gate collects data on mentioned devices connected to it through the LAN or directly. Collected data are received by a trusted management server via Internet or telephone line (Dial-up PPP connection). The trusted management server is called "Communication Server (CS)". The TOE is the Software module of RC Gate and works as following security features:

- Prevention of unauthorized disclosure and modification of the information on the inner memory of RC Gate.
- Prevention of unauthorised disclosure and modification of the information via internet, intranet and/or telephone line.
- Prevention of receiving/sending information from/to a non-authorized CS

There are three broad features of this system[1]:
(an overview of the involved components/systems is shown by the following figure 1)

[1] System means here the configuration of elements in the network with RC Gate as a central element.

1. Reduced Image I/O device Downtime

Image I/O device downtime is dramatically reduced through remote maintenance. Specifically, remote maintenance cuts downtime by sending service calls automatically to Ricoh's service technician. In addition, to further cut on time and expense, many upgrades (firmware, etc.) can be performed remotely too - services only made possible through connection to the Internet. This means customers/end users can operate without worrying about incomplete jobs or being tied to maintenance or repairs; companies are freed from time-consuming duties and additional downtime expense.

2. Automated Counter Checking

Remote counter monitoring means the user no longer has to manually report counter figures. This system offers an improvement in the form of remote, automated counter checking. This system allows billing to be better timed. User workload is reduced and so too (the previously inevitable) billing mistakes, red tape routine, and associated complications.

3.Ordering Supplies (toner, etc.)

Remote system notifies remaining amount of supplies like toner to CS - image I/O device downtime is reduced, and the user no longer has to worry about re-order telephone calls, forgotten stock, supply control and so on, now that monitoring and dispatch is fully user-independent.

Therefore, RC Gate becomes a significant device in this system, as the information between the user image I/O devices and CS shall be stringently correct. For example, wrongheaded image I/O device information shall bring some wrongheaded accounting or service for users.

1.3 ISO/IEC 15408 Conformance Claim

The TOE is **conformant** to ISO/IEC 15408-2:1999(E).

The TOE is **conformant** to ISO/IEC 15408-3:1999(E), assurance level **EAL3**.

There are no PPs claimed to which this ST is conformant.

2 TOE Description

2.1 Product Type

The product type of RC Gate, listed in Table 1, is a communication box manufactured by Ricoh. All of those product names are described in 1.1 ST Identification and detailed explanation about the products is described later. Application software is installed in a trusted factory and assembled in another trusted factory.

Table 1: Product name and code of RC Gate

Product name	Destination	
	Europe	North America
Remote Communication Gate Type BN1	A76827	A76817
Remote Communication Gate Type BM1	A76927	A76917

When the office network is connected to the Internet, RC Gate uses this network to send and receive data from CS. Typical network environment is as follows:

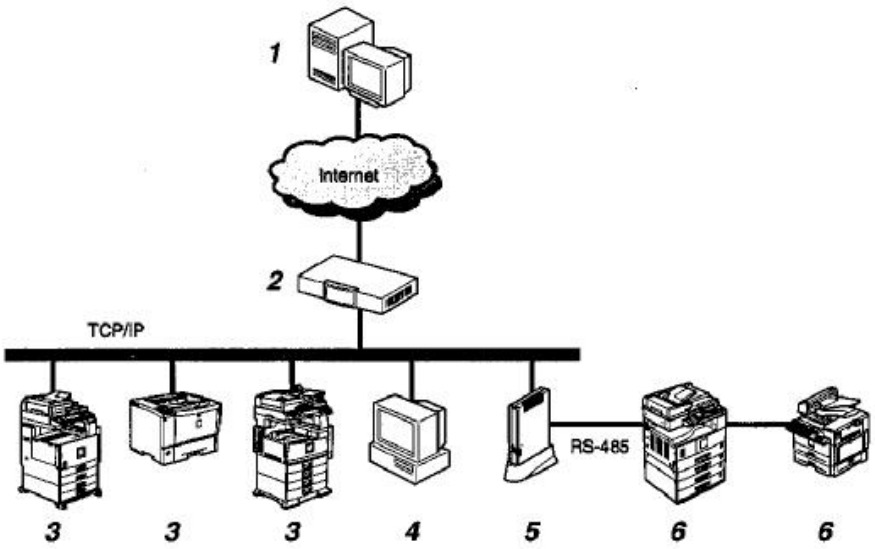


Figure 1:Network environment of RC Gate Type BN1

* RS-485 stands for TIA/EIA-485.

1. Communication Server (CS)

Information for various services will be sent to CS from RC Gate.

2. Proxy Server and Firewall

Security system for the network environment should be established.

3. Image I/O Devices managed via IP network

RC Gate can manage image I/O devices and laser printers, which support MIB information or Ricoh's remote service.

4. PC for Administration

Communication between RC Gate and RC Gate Monitor is based on the https-protocol.

Note: The so-called RC Gate Monitor is a web based access, which is not necessarily located within the customer/end user network (protected intranet).

5. This Equipment (Remote Communication Gate Type BN1)

Various pieces of information of the image I/O devices managed by RC Gate are sent to 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 from RC Gate toward CS via SMTP server.

6. The Image I/O Devices managed via serial communication bus (TIA/EIA-485)

Image I/O devices manufactured by Ricoh can also be managed, by directly connecting them to RC Gate with the serial modular cable. A maximum of five image I/O devices can be connected to one RC Gate.

If the office network environment cannot access the Internet directly, RC Gate can communicate with CS using a modem type (Type BM1). Here, this is called "Dial-up." For the Dial-up, facsimile line or telephone line prepared for RC Gate can be used.

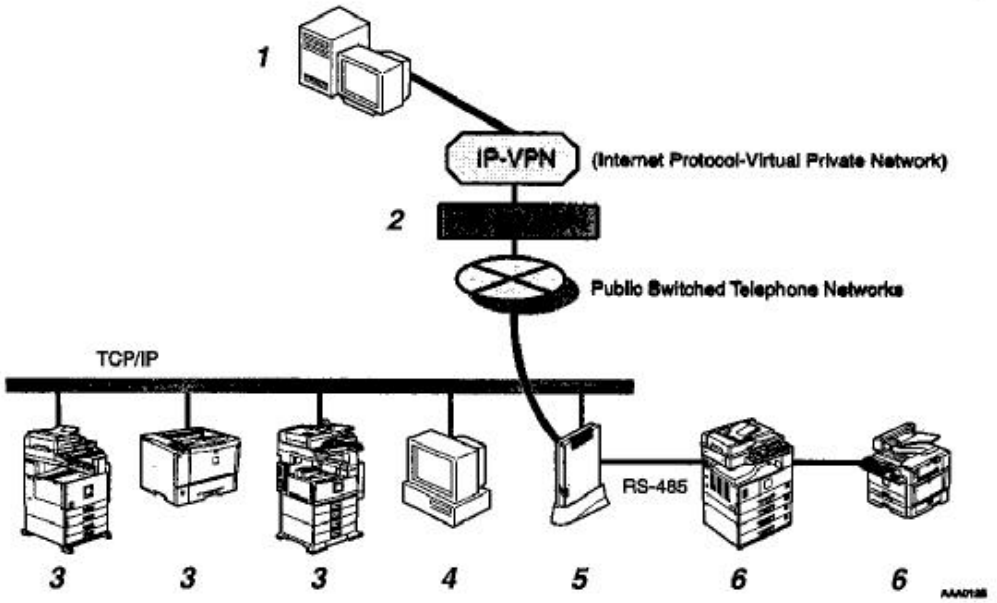


Figure 2:Network environment of RC Gate Type BM1

* RS-485 stands for TIA/EIA-485.

1. Communication Server

Information for various services will be sent to CS from RC Gate.

2. Access Point

The nearest access point of the area RC Gate is used, is pre-installed.

3. Image I/O Devices managed via IP network

RC Gate can manage image I/O devices and laser printers, which support MIB information or Ricoh's remote service.

4. PC for Administration

Administrating RC Gate via PC Web browser, called "RC Gate Monitor".

5. This Equipment (Remote Communication Gate Type BM1)

Various pieces of information of the image I/O devices managed by RC Gate are sent to CS.

There is 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. Firmware download and mail system cannot used in this type because of data transfer speed.

6. The Image I/O Devices managed via serial communication bus (TIA/EIA-485)

Image I/O devices manufactured by Ricoh can also be managed, by directly connecting them to RC Gate with the serial modular cable. A maximum of five image I/O devices can be connected to one RC Gate.

In this system security functionality of RC Gate consists of six functions as follows:

1. RC Gate identifies and authenticates the different operators (administrator, registrant or CE). Communication between RC Gate and RC Gate Monitor is based on the https-protocol
2. RC Gate controls operations performed by the operator.
3. RC Gate identifies and authenticates CS before communicates with CS by HTTPS method.
4. RC Gate shall export and import encrypted information when HTTPS method is selected.
5. RC Gate shall export encrypted E-mail information to CS when SMTP method is selected.
6. RC Gate records three types of audit log: access log, communication log and system log.

2.2 Persons concerned

The followings are concerned persons of TOE. The person concerned is separated by authority to show in the following. Every each authority is separated.

1) Administrator

RC Gate administrator can access for various setting information of RC Gate. He/She is a manager of a customer managing RC Gate to be concrete. He/She can access RC Gate through RC Gate monitor, and setting of proxy is possible.

2) Registrant

RC Gate registrant has authority to register RC Gate on CS. Registration Wizard is available on the RC Gate monitor.

Application Note:

Registrant authority is opened up to above administrator. However, in case of user's request CE (Customer Engineer) to put up next is entrusted to this authority.

3) CE

CE (Customer Engineer) can access information of RC Gate via RC Gate monitor to maintain it, or to investigate it in an obstacle. He/She is a trusted person authorized by RICOH or affiliate companies. He/She shall receive education of RC Gate and read "Service Manual" thoroughly.

CE port (the outside LAN port of RC Gate) is normally used. Administrator can prohibit CE from accessing TOE using Administrator setting menu.

Authority of the administrator, the registrant and the CE is divided in this ST definitely. These authority separations depend on a user selection in login by RC Gate monitor.

2.3 Importance of security for RC Gate

It becomes important to protect all information at the office. Image I/O devices like copier, facsimile or printer almost have many information. These data such as copy counter, toner remaining amount and accident information are available for accounting and maintenance. Especially counter data are used for accounting, so we have to prevent many threats such as illegal counter alternation; non-authorized CS. RC Gate is responsible for prevention of these thinkable damages. Software module is executed on RC Gate exclusive hardware. The software is written into suitable media as SD memory card. Main function of this software is recognition of Image I/O devices and sending correct data toward CS using SSL (Secure Socket Layer) or S/MIME technology.

Image I/O device downtime is dramatically reduced through remote maintenance. RC Gate is ready for receiving SC (stand for "Service Call", call for maintenance service) initiated from Image I/O devices manufactured by Ricoh, and call CS immediately. Specifically, remote maintenance cuts downtime by sending such calls automatically to CE. Remote counter monitoring means the user no longer has to manually report counter figure. This mode supports identification of the machine maintained and gets correct counters of that machine. This system (system overview is shown by figure 1 and 2) offers an improvement in the form of remote, automated counter checking. This system allows billing to be better timed. User workload is reduced and so too (the previously inevitable) billing mistakes, red tape routine, and associated complications. Remote system provides toner remaining amount data to our service company - image I/O device downtime is reduced, as the user no longer has to worry about re-order telephone calls, forgotten stock, supply control and so on, now that monitoring and dispatch is fully user-independent.

RC Gate becomes a significant device in this system, as the information between the user image I/O devices and the server shall be stringently correct. For example, a wrongheaded image I/O device information shall bring some wrongheaded accounting or service for our customers.

2.4 Physical boundary of the TOE

RC Gate acts as an intermediary between the image I/O device and CS, e.g. intermediation network communication appliance. It is used mostly in general LAN-constructed office. Common hardware part of RC Gate is main board on which CPU, Flash memory, LAN Ethernet circuit, RS485 and the interface of power supply. RC Gate type BM1 consists of main board and modem board. Modem board has the interfaces for telephone line. The hardware specification of RC Gate Type BN1 and BM1 is shown as follows:

- CPU: Correspond to TX4925XB-200
- ROM: 4MB
- RAM: 64MB
- SD memory card: 32MB
- NIC: 10BASE-T/100Base-TX
- Front Indication: Green LED indicates power supply, Orange LED indicates communication status and Red LED indicates system status.
- LAN Indication: Orange LED indicates communication speed e.g. 100/10Mbps and Green LED indicates link status.

Software part of RC Gate Type BN1 and BM1 consists of application software and its Operation System (OS). Between Type BN1 and BM1, there is no difference in software component. TOE is the application software module of RC Gate. OS is out of TOE.

2.5 Logical boundary of the TOE

RC Gate consists of hardware and software parts. The software part consists of OS, DBMS, Communication Management Module, Device Management Module, Log Management Module, Web Management Module, CS Management Module and SMTP Communication Module. The OS is embedded Linux operating system (Hereafter “RC Gate OS”). OS, DBMS, Communication Management Module and SMTP Communication Module are out of the TOE. Optional wireless LAN card can be attached to RC Gate, but the wireless option is out of the TOE. SD memory card sockets and Flash Memory are embedded on the main hardware board.

- Communication Management Module is the main controller of communication, which also schedules the communication timing to CS or image I/O device according to the setting information for RC Gate.
- DBMS provides data management function and interfaces of SD memory.
- SD memory stores collected information, settings or firmware and certificates for devices. Image I/O device information is stored in SD memory through DBMS.
- SMTP Communication Module sends mail information to external SMTP server.

- Web Management Module performs operator identification and authentication. This module also provides Web interface.
- Flash memory is used for storing certificates. These certificates are read by Web Management Module when RC Gate starts up.
- CS Management module performs CS identification, authentication and data exchange. Cryptographic function is included in this module. Certificates are read via Web Management Module.
- Log Management Module provides log management function. Each module such as CS, Web and Device Management Module send the logging event to Log Management Module. This module reads system time from OS to create audit event. Log files are saved in SD memory.
- Device Management Module manages image I/O devices (includes copier, printer, facsimile, and multi-functional device). Main function of this module is collecting information of Image I/O devices.

RC Gate

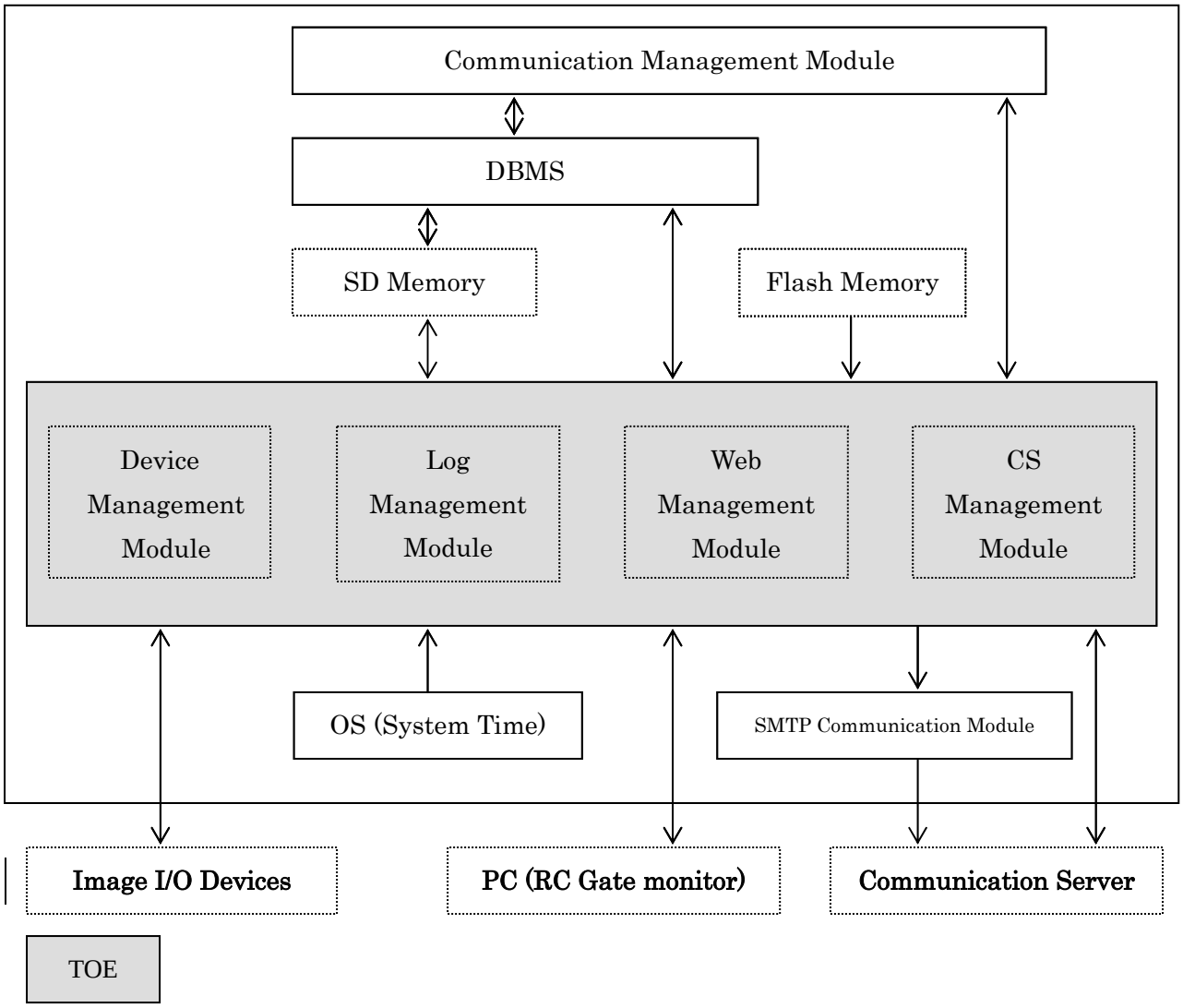


Figure 3: RC Gate and the TOE

2.6 Definition of Specific Terms

For clear understanding of this ST, the meanings of specific terms are defined as shown in Table 2.

Table 2: Specific terms related to the RC Gate

Term	Definition
Administrator	Administrator is the trusted person who is authorised to perform the administrative operations of the RC Gate.
CE	CE, Customer Engineer, is the person who performs maintenance operation of the RC Gate. The CEs are employees of Ricoh or its affiliated company.
Certificates for RC Gate	Public/Private key for the RC Gate and the root key for CS and Image I/O device.
Certificates for image I/O device	Public/Private key for the image I/O device and the root key for RC Gate.
Firewall	A set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.
Flash memory	Flash memory is non-volatile memory, which is a fixed memory device on board.
Image I/O device	Image I/O device, which includes copier, printer, facsimile, and multi-functional device.
Linux	UNIX compatible OS; is freeware and high portability. RC Gate is working on "RC Gate OS" based on MontaVista Linux supplied by MontaVista Software, Inc.
MIB	Management Information Base. Network machinery managed with SNMP is information to show in order to tell RC Gate about a state of oneself outside. There is MIB2 prescribed with MIB1 and RFC 1213 prescribed as RFC 1156, and RC Gate shall treat MIB2 and MIB1.
Master key	Master key is a symmetric key: used by Certificate Manager[2] to encrypt/decrypt information.
Operator	There are three kinds of operators; Administrator, Registrant and CE.
PKI	Public Key Infrastructure, which is a digital key technology used for secure communication.
Private key	Private key is used to encrypt/decrypt information association with public key.
Public key	Public key is using to identify communication apparatus.

[2] Certificate Manager is part of an OpenSSL library and used from CS Management Module.

Term	Definition
RC Gate	Remote Communication Gate is the communication box between image I/O devices and the Communication Server.
RC Gate monitor	WEB interface of RC Gate, operator has access to RC Gate using this interface.
Registrant	Registrant is the trusted person who is authorised to set up operations of the RC Gate.
SD memory card	SD memory card is Secure Digital memory card, which is a highly sophisticated memory device about the size of a postage stamp and it is used for providing the TOE or other applications for the image I/O device

3 TOE Security Environment

3.1 Subjects and Assets

Subjects in context with the defined TOE:

- Operator (especially the Administrator, the Registrant and the Customer engineer, which is also abbr. as CE)
- Communication server (also abbr. as CS)
- Attacker (also called unauthorized person, unauthorized operator, outer evil person); Furthermore, the attacker can also be a mimicked/faked communication server, which is also called Fake CS, none authorized CS or pseudo CS.

The assets that the TOE intends to protect are as follows:

Table 3: Assets that the TOE intends to protect

TOE / user – data	Asset	In particular, IT-security is focused on …	
		confidentiality	Integrity/availability
TOE	Certificates for RC Gate		X
TOE	Passwords for each operator	X	X
TOE	Audit logs (access information, communication information, system information)	X	X
User	Setting information for RC Gate	X	X
User	Collected information of image I/O devices		X
User	Firmware to update image I/O device		X
User	Certificates for image I/O device		X

3.2 Assumptions

In this section, the assumptions concerning the environment of the TOE are identified and described.

A.PHYSICAL **It is assumed that the TOE is physically protected.**

RC Gate with its TOE is set in a place of safety such as business office. Therefore the TOE containing the assets is indirectly protected, because an accessible user with evil intent cannot access RC Gate respectively modify the TOE unobserved.

A.DEVICE **It is assumed that image I/O devices are trusted.**

Image I/O devices are genuine products. Illegal applications are not installed on image I/O devices. In addition, firmware on image I/O devices is not tampered.

A.NETWORK **It is assumed that the network is properly managed by responsible person.**

The network, which RC Gate and image I/O devices belong to, is properly managed by responsible persons. Furthermore, the network is protected from outer attack via Internet by establishing a firewall and running virus protection programs.

A.CE **It is assumed that Customer Engineer is trusted.**

The customer engineer (CE) is well trained and can be trusted. He/She belongs to Ricoh or a Ricoh's affiliate company and reads the maintenance documentation thoroughly, responds appropriately to RC Gate. He/She does not change the configuration of RC Gate, does not carry out the RC Gate and does not install programs into RC Gate without permission of user administrator. Furthermore, the customer engineer will keep his/her password secret.

A.ADMIN **It is assumed that both Administrator and Registrant are trusted.**

The user administrator and registrant can be trusted. Administrator and registrant may be same person. He/She reads the user's documentations (Set up Guide and Operating Instructions) thoroughly, responds appropriately to RC Gate. He/She can set and change the configuration of RC Gate. Furthermore, the administrator and/or registrant will keep his/her password secret.

A.CS **It is assumed that Communication Server is properly managed by responsible company and persons.**

The communication server is trusted. Responsible persons shall manage CS properly.

3.3 Threats

In this section, the threats that will be countered by the TOE or its environment are identified and described.

T.WEB **Assets in RC Gate may be read, modified or destroyed by employees or external attackers.**

The assets inside RC Gate as defined could be attacked through web interface by an employee and/or an attacker, especially by attack attempts from intranet and/or internet.

T.CS_COMM **Leakage of, or tampering with information at Internet or telephone line, when RC Gate communicates CS directly.**

An attacker may disclose and/or modify the data (relevant assets as defined in chapter 3.1 before), which are sent/received between RC Gate and CS via Internet or telephone line directly. The attacker may be an evil person wandering around Internet or monitoring line in secret.

T.CS_MAIL **Leakage of, or tampering with information at Internet, when mail method is used.**

An attacker may disclose and/or modify information in mails (relevant assets as defined in chapter 3.1 before), which is sent from RC Gate toward CS via Internet. The attacker may be an evil person wandering around Internet.

T.FAKE_CS **A fake CS may be built in Internet or telephone network when RC Gate communicates with CS.**

An attacker may build a fake CS (non-authorized CS). In addition, he/she may get the information data (relevant assets as defined in chapter 3.1 before), which is sent/received between RC Gate and the fake CS via Internet or telephone line. The attacker may be an evil person wandering around Internet or telephone network.

3.4 Organisational Security Policies

In this section, the organisational security policies concerning the TOE are identified and described.

OSP.AUDIT **TOE shall write/create logs for audit or maintenance.**

There are the following three types of log information:

- access information	(Login authentication)
- communicating information	(Sending information to CS and image I/O device; Receiving information from CS and image I/O device)
- system information	(Start-up of the TOE; Shutdown of the TOE; Process information)

These defined types of log information should contain date and time of each event. Furthermore, the access information and communicating information should be steady checked by administrator, registrant, and CE. Additionally, the system information should be checked by CE and/or CS.

4 Security Objectives

4.1 Security Objectives for the TOE

In this section, the security objectives of the TOE that cover the aspects of the threats and OSP in section 3.3 are described.

O.OPE_I&A **The TOE must identify and authenticate the operator.**

When someone accesses the TOE via Web Interface, the TOE must unambiguously identify one of the following operators (administrator, registrant and/or customer engineer) via secured password login. After successfully operator identification and authentication, the TOE will give the specified/allowed access rights to the operator.

O.CS_ID **The TOE must ensure that RC Gate shall communicate with the correct CS.**

The TOE will ensure that CS shall be strictly correct one. RC Gate compares a unique ID of CS to the information of electrical certification. Therefore, no other server can access the TOE.

O.A_RIGHTS **The TOE must control access to the assets by appropriate access rights.**

After successfully operator identification and authentication (O.OPE_I&A or O.CS_ID), the TOE will give the specified/allowed access rights to respectively control the access rights to the administrator, registrant, customer engineer or communication server (CS) as stated in [ST], Table 4.

O.TRUST_NET **The TOE must ensure a trusted communication between RC Gate and CS.**

For the communication between RC Gate and CS, a trusted channel (HTTPS communication) has to be used (focused on the identification and authentication protocol mechanisms).

O.CIPHER **The TOE must ensure that communications are done through encrypted channel.**

When RC Gate is accessed by an operator via its web user interface or RC Gate is communicating with CS directly, those data is encrypted/decrypted using HTTPS technology/method.
When RC Gate sends mail toward CS, the mail is encrypted/using SMIME technology.

O.AC_AUDIT **TOE must ensure that access information shall be logged.**

When RC Gate is accessed via RC Gate monitor, access information must be logged by the TOE.

The logged access information can only be read out (not modified) by the administrator, registrant or CE (as stated/specified in [ST], Table 4). Therefore, illegal access can be detected by way of analysing this log.

O.COM_AUDIT TOE must ensure that communicating information shall be logged.

When RC Gate communicates with CS or with image I/O devices, all specified communication information's has to be logged.
The logged communication information's can only be read out (not modified) by the administrator, registrant and CE.
Therefore, illegal communication can be detected by way of analysing this log.

O.SYS_AUDIT TOE must ensure that system information shall be logged.

When RC Gate is running, system information must be logged. Therefore, CE can analyse the information in case of software accident. Audit data are only readable by CE and CS.

4.2 Security Objectives for the Environment

In the following “responsible persons” refer to operators.

4.2.1 Security objectives for the IT environment

OE.TIME **Responsible persons who should watch RC Gate working correctly will keep correct time for RC Gate.**

Responsible persons should watch that RC Gate is working correctly and well regarding the presented/used time. Audit logs, which will be created, are using this time.

4.2.2 Security objectives for the non-IT environment

In this section, the security objectives of the non-IT environment that cover the aspects of the assumptions described in section 3.

OE.PHYSICAL **The TOE and assets are physically protected.**

Responsible person should set the RC Gate in stable place as an accessible user with evil intent cannot access RC Gate physically and confirm that they are working correctly.

OE.DEVICE **Responsible persons shall watch the image I/O device working correctly.**

Responsible persons who should watch the image I/O device confirm that they are working correctly. Especially the image I/O device that RC Gate manages explicitly should up and run well.

OE.NETWORK **Responsible persons who should watch the office network working correctly will ensure that office network system is trusted.**

Responsible persons should watch the office network working correctly and well. When the TOE is using under circumstance of Internet, "Firewall" and virus protecting programs shall be established.

OE.CE **The maintenance of RC Gate shall carry out by CE who is an employee of Ricoh or a Ricoh’s affiliate company.**

CE is well trained and well informed about RC Gate. He/She reads the maintenance documentation and user documentation thoroughly; therefore, he/she can respond appropriately to RC Gate. The CE has to check the time and date regularly among others and correct these, if necessary. Furthermore, the CE has to keep his/her password secret.

OE.ADMIN **Those responsible for the TOE shall assign the reliable administrator and registrant, and train them appropriately.**

Reliable persons are assigned as Administrator and Registrant of the TOE. Administrator and Registrant should read the user's document thoroughly; therefore, they can respond appropriately to RC Gate as an Administrator and Registrant. The Administrator and Registrant has to check the time and date regularly among others and correct these, if necessary. Furthermore, the Administrator has to keep his/her password secret.

OE.CS **CS shall ensure that the identification information is maintained correctly.**

CS is the only and unique server for RC Gate, so CS shall be trusted and the identification information for HTTPS method and SMTP method shall be maintained correctly. The CS has to check the time and date regularly among others and correct these, if necessary.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

In this section, the functional requirements of the TOE to achieve the security objectives identified in section 4.1 are described. The parts against which the assignment and selection operations defined in [CC] are performed are identified with **[bold letters and brackets]**.

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:**
Subject: operator (Administrator, Registrant or CE) or CS,
Object: setting item,
Operation:
-R--: can see setting items existence, can view its current value.
--W-: can see setting items existence, can change its value (but cannot necessarily view the current and under-change value of the item as only '*' characters are shown if not in combination with -RW-)
A---: can add (create) new setting items, can delete setting items
---E: can execute a function
----: can not see setting items existence, can not view or change or the value of the setting item].

Dependencies:

FDP_ACF.1 Security attribute based access control

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:**
subjects: operator or CS
Objects: setting items respectively assets as defined in chapter 3.1
Subject attributes: - operator ID and CS ID
- Communication method (direct HTTPS, dialup HTTPS, SMTP)
Object attributes: list of allowed operations.

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:**
The operation is allowed according to the rules given in Table 4.].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[assignment: none]**.

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 4: Setting items and allowed operations

`-R--:` can see setting items existence
can view its current value.

`--W-:` can see setting items existence
can change its value (but cannot necessarily view the current and under-change value of the item as only '*' characters are shown if not in combination with `-RW-`)

`A---:` can add (create) new setting items
can delete setting items

`---E:` `can execute a function`

`----:` can not see setting items existence
can not view or change or the value of the setting item

Setting items	Allowed operations for each operator and access method											
	Administrator			Registrant			CE			CS		
	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP
RC Gate Settings-Basic												
RC Gate Setting-Basic parameters 1	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	----
RC Gate Setting-Basic parameters 2	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	----	----	----
RC Gate Setting-Basic parameters 3	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	-RW-	-RW-	----
RC Gate Setting-Basic parameters 4	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	----	----	----
Language	----	----	----	----	----	----	-R--	-R--	-R--	-RW-	-RW-	----
Time zone	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	----
Date / Time	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	----
RC Gate Setting-Basic parameters 5	----	----	----	-R--	-R--	-R--	-R--	-R--	-R--	-RW-	-RW-	----
Auth key version	----	----	----	----	----	----	-R--	-R--	----	----	----	----

Setting items	Allowed operations for each operator and access method											
	Administrator			Registrant			CE			CS		
	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP
RC Gate Settings-Network												
Maintenance Port IP address	-R--	-R--	-R--	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	----
Other Maintenance Port parameters	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	----
LAN Port MAC address	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	----
Other LAN Port parameters	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	----
Ethernet speed	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	----	----	----
DNS server parameters	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	--W-	--W-	--W-	----	----	----
RC Gate Settings-E-mail												
E-mail parameters 1	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	----
Communication Server E-mail address	----	----	----	----	----	----	----	----	-RW-	----	----	----
RC Gate admin's E-mail address	-R--	-R--	-RW-	-R--	-R--	-RW-	----	----	-RW-	-RW-	-RW-	----
E-mail parameters 2	-RW-	-RW-	-RW-	----	----	----	-RW-	-RW-	-RW-	----	----	----
SMTP / POP server												
server parameters 1	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	--W-	--W-	--W-	----	----	----
server parameters 2	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	----	----	----
password	--W-	--W-	--W-	--W-	--W-	--W-	--W-	--W-	--W-	----	----	----
RC Gate Settings-Communication Method												
Communication method	----	----	-R--	----	----	-R--	-R--	-R--	-R--	-R--	-R--	----
Internet connection method	----	----	----	----	----	----	-R--	-R--	----	-R--	-R--	----
Other communication method parameters	----	----	----	----	----	----	-RW-	-RW-	----	-RW-	-RW-	----
RC Gate Settings-Net Connection Settings-Connection Details												
Internet connection method	-R--	----	----	-R--	----	----	-R--	-R--	----	-R--	-R--	----
Proxy password	--W-	----	----	--W-	----	----	--W-	--W-	----	--W-	--W-	----
Proxy server parameters	-RW-	----	----	-RW-	----	----	-RW-	-RW-	----	--W-	--W-	----
RC Gate Settings-Net Connection Settings-Dial-up												
Dial-up internet connection method	----	-R--	----	----	-R--	----	----	-R--	----	----	-R--	----
Access point parameter 1	----	-R--	----	----	-RW-	----	----	-RW-	----	----	-RW-	----
Access point text	----	----	----	----	----	----	----	-RW-	----	----	----	----
Dialing Line parameters	----	-R--	----	----	-RW-	----	----	-RW-	----	----	-RW-	----

Setting items	Allowed operations for each operator and access method											
	Administrator			Registrant			CE			CS		
	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP
Modem parameters	----	----	----	----	----	----	----	-RW-	----	----	-RW-	----
Auto Discovery-Auto Discovery Settings												
Auto Discovery permit	-RW-	-RW-	----	-RW-	-RW-	----	----	----	----	----	----	----
Auto Discovery server address	----	----	----	----	----	----	-R--	-R--	----	-RW-	-RW-	----
Max. E-mail size	----	----	-RW-	----	----	-RW-	----	----	-R--	----	----	----
Auto Discovery start schedule, SNMP community name	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	-RW-	----
Auto Discovery Range parameters	ARW-	ARW-	ARW-	ARW-	ARW-	ARW-	ARW-	ARW-	ARW-	----	----	----
Device Management-Common management												
Information Retrieval settings	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	-RW-	-RW-	----
Devices to repeat search (HTTP and SNMP)	-RW-	-RW-	----	----	----	----	-RW-	-RW-	----	-RW-	-RW-	----
Other Network Connection settings	-R--	-R--	----	----	----	----	-R--	-R--	----	-RW-	-RW-	----
RS-485 Connection parameters	-R--	-R--	----	----	----	----	-R--	-R--	----	-RW-	-RW-	----
Device Management-Connection Details												
Device retry parameters	----	----	----	----	----	----	-R--	-R--	----	-RW-	-RW-	----
Device Management-Registered Device List												
M-R Device List parameters 1	-RW-	-RW-	----	-RW-	-RW-	----	-RW-	-RW-	----	-RW-	-RW-	----
Device name	-R--	-R--	----	-RW-	-RW-	----	-RW-	-RW-	----	-RW-	-RW-	----
SNMP community name	-R--	-R--	----	-RW-	-RW-	----	-R--	-R--	----	-RW-	-RW-	----
M-R Device List parameters 2	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----
M-R Device List parameters 3	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	-RW-	-RW-	----
Method to assign IP address	----	----	----	-RW-	-RW-	----	-RW-	-RW-	----	-RW-	-RW-	----
Machine administrator's E-mail address	-RW-	-RW-	----	-RW-	-RW-	----	--W-	--W-	----	-RW-	-RW-	----
M-R Device List parameters 4	-R--	-R--	----	-R--	-R--	----	-RW-	-RW-	----	-RW-	-RW-	----

Setting items	Allowed operations for each operator and access method											
	Administrator			Registrant			CE			CS		
	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP
Device Management-Notify												
Device Management-Notify parameters	----	----	----	----	----	----	-R--	-R--	----	-RW-	-RW-	----
Device Management-Update Device Firmware												
Device Firmware parameters 1	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	--W-	--W-	----
Device Firmware parameters 2	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	----	----	----
Device Firmware functions	-RW-	-RW-	----	-RW-	-RW-	----	-RW-	-RW-	----	----	----	----
Maintenance-Restart												
Restart function	----	----	----	---E	---E	---E	---E	---E	---E	---E	---E	----
Maintenance-Communication Server Calls-Service Test Call												
Service Test Call function	----	----	----	---E	---E	----	---E	---E	----	----	----	----
Log	----	----	----	-R--	-R--	----	-R--	-R--	----	-RW-	-RW-	----
Maintenance-Communication Server Calls-Device Check Req.Call												
Device Check Req.Call functions	---E	---E	----	---E	---E	----	---E	---E	----	----	----	----
Message	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	----	----	----
Maintenance-Restore												
Restore parameters	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	----	----	----
Maintenance-Log-Log setup												
Maintenance Log parameters	----	----	----	----	----	----	-R--	-R--	-R--	-RW-	-RW-	----
Maintenance Log collection level	----	----	----	----	----	----	-RW-	-RW-	-RW-	-RW-	-RW-	----
Maintenance-Log-System Log												
Maintenance System Log	----	----	----	----	----	----	-R--	-R--	-R--	-R--	-R--	----
Maintenance Communication Log	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	----	----	----
Maintenance-Memory												
Maintenance-Memory parameters	----	----	----	----	----	----	-R--	-R--	-R--	-R--	-R--	----
Maintenance-Service Call												
Maintenance-Service Call parameters 1	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	----

Setting items	Allowed operations for each operator and access method											
	Administrator			Registrant			CE			CS		
	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP	direct HTTPS	dialup HTTPS	SMTP
Maintenance-Service Call parameters 2	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----
Maintenance-System Status												
Maintenance-System Status parameters	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----	-R--	-R--	----
Security-Password												
CurrentUser	----	----	----	----	----	----	--W-	--W-	--W-	----	----	----
Password	--W-	--W-	--W-	--W-	--W-	--W-	--W-	--W-	--W-	----	----	----
Security-Permissions												
Permit access by service	-RW-	-RW-	-RW-	----	----	----	----	----	----	----	----	----
Permit updating of Firmware from Communication Server	-RW-	-RW-	----	----	----	----	----	----	----	----	----	----
Security-Access Log												
Access Log	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	-R--	----	----	----

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1 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: the TSF]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[assignment: exporting and importing information listed in Table 5 between RC Gate and CS via HTTPS communication method]**.

Dependencies:

No dependencies

Table 5: Information passed between RC Gate and CS

Operation	Information
export from RC Gate to CS	alert of image I/O device alert of RC Gate

	status of image I/O device notice of image I/O device registration notice of RC Gate registration
import from CS to RC Gate	firmware of image I/O devices certificates of image I/O device request of setting modification of RC Gate

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform **[assignment: operations listed in Table 6]** in accordance with a specified cryptographic algorithm **[assignment: listed in Table 6]** and cryptographic key sizes **[assignment: listed in Table 6]** that meet the following: **[assignment: SSL V3.1 and S/MIME specification]**.

Dependencies (under consideration of final interpretation [FI220]):

[FDP_ITC.1 Import of user data without security attributes or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Table 6: Cryptographic operations, algorithms, and key sizes

Operation	Algorithm	Key size
Authentication and key exchange (HTTPS)	RSA	512 bits
	SHA-1	N/A
Encryption and decryption (HTTPS)	DES	56 bits
Encryption (S/MIME)	RSA	512 bits
	DES	56 bits
Signature (S/MIME)	RSA	512 bits
	SHA-1	N/A

Concerning Encryption and Signature for S/MIME, RFC2311 "S/MIME Version2 Message Specification" is supported.

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when **[selection: [assignment: three]]** unsuccessful authentication attempts occur related to **[assignment: consecutive presentations of a wrong password via RC Gate monitor]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: refuse to access via RC Gate monitor 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: operator identity (Administrator, Registrant and CE)]**.

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: the following: the password has to be at least 8 and at most 13 characters long]**.

Dependencies:

No dependencies

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow **[assignment: everybody to read the RC Gate version and Licenses and to select language and operator list via RC Gate monitor]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 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.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only **[assignment: asterisks]** to the user while the authentication is in progress.

Dependencies:

FIA_UAU.1 Timing of authentication

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow **[assignment: everybody to read the RC Gate version and Licenses and to select language and operator list via RC Gate monitor]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies:

No dependencies

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: modify]** the **[assignment: passwords]** to **[assignment: Administrator, Registrant and CE]**.

Dependencies:

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

Notes: Each operator has his/her 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: function to modify operator's password]**.

Dependencies:

No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: operator (Administrator, Registrant and CE), CS]**.

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

Dependencies:

FIA_UID.1 Timing of identification

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[selection: not specified]** level of audit; and

c) **[assignment: The events listed in Table 7]**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: no other audit relevant information]**

Dependencies:

FPT_STM.1 Reliable time stamps

Table 7: Events recorded to audit log

Type of audit log	Event
Access log	Login authentication
Communication log	Sending information to CS and image I/O device Receiving information from CS and image I/O device
System log	Start-up of the TOE Shutdown of the TOE Information of each function (e.g. PPP(Dial-up), CGI(Web) SMTP(E-Mail), DBMS(Database), …)

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event **[refinement: of access log]** with the identity of the user that caused the event.

Dependencies:

FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_SAR.1(a) Audit review

Hierarchical to: No other components.

FAU_SAR.1(a).1 The TSF shall provide **[assignment: Administrator, Registrant and CE]** with the capability to read **[assignment: communication and access log]** from the audit records.

FAU_SAR.1(a).2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies:

FAU_GEN.1 Audit data generation

FAU_SAR.1(b) Audit review

Hierarchical to: No other components.

FAU_SAR.1(b).1 The TSF shall provide **[assignment: CE, CS]** with the capability to read **[assignment: system log]** from the audit records.

FAU_SAR.1(b).2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies:

FAU_GEN.1 Audit data generation

FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to **[selection: prevent]** modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that **[assignment: 64k bytes latest]** audit records will be maintained when the following conditions occur: **[selection: audit storage exhaustion]**.

Dependencies:

FAU_GEN.1 Audit data generation

5.2 Minimum Strength of Function Claim

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

5.3 TOE Security Assurance Requirements

The assurance components for the TOE are shown Table 8. It is the set of components defined by the evaluation assurance level **EAL3** and no other requirements have been augmented.

Table 8: TOE security assurance requirements (EAL3)

Assurance Class	Assurance Component	
Security Target	ASE_DES.1	TOE description
	ASE_ENV.1	Security environment
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives
	ASE_PPC.1	PP claims
	ASE_REQ.1	IT security requirements
	ASE_SRE.1	Explicitly stated IT security requirements
	ASE_TSS.1	TOE summary specification
Configuration Management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage

Assurance Class	Assurance Component	
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence 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
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.4 Security Requirements for the Environment

In this section, the functional requirements of the environment to achieve the security objectives identified in section 4.2 are described. The parts against which the assignment, selection, and refinement operations are performed are identified with **[bold letters and brackets]**.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The **[refinement: IT environment]** shall be able to provide reliable time stamps for its own use.

Dependencies:

No dependencies

6 TOE Summary Specification

6.1 TOE Security Functions

SF.OPE_I&A

TSF identifies and authenticates operator (Administrator, Registrant and CE) prior to the operation listed below. When authentication is succeeded, TSF assigns a role (Administrator, Registrant and CE) to the operator. If the authentication is failed, the operator cannot perform following operations:

- read audit logs
- read and modify setting information
- modify password

While the operator is entering password, the asterisks are shown instead of password characters.

If the wrong password is entered three consecutive times, TSF reject identification and authentication for one minutes.

The operator (Administrator, Registrant and CE) can change his own password. Furthermore, the customer engineer (CE) can change the administrator and registrant password if he knows their current password. The length of new password should be at least 8 and at most 13 characters. If the length new password is not in the range, the new password is rejected.

Prior to identification and authentication it is possible to read RC Gate version and Licenses and to select language and operator list via RC Gate monitor.

SF.OPE_AC

TSF controls operations performed by the operator based on the operator's identification information and method to communicate with CS. When direct HTTPS method, dialup HTTPS method, or SMTP method is used to communicate with CS, operators can access to the information based on Table 4.

SF.CS_I&A

TSF identifies and authenticates CS before communicates with CS by HTTPS. When the identification and authentication is succeeded, it is allowed to export or import information to/from CS. If the identification and authentication is failed, it is denied to export nor import information between CS.

For authentication of CS, TSF uses the HTTPS mutual authentication mechanism.

SF.CS_HTTPS

TSF can export and import information listed in Table 5 to/from CS by using HTTPS protocol.

TSF authenticates CS before export or import information. When CS is successfully authenticated, TSF encrypts the information to export, and decrypts the imported information. Furthermore, CS is able to perform the allowed operations as specified/stated in [ST], Table 4 after a successful authentication. If the authentication is failed, the information are not exported nor imported.

SF.CS_SMIME

TSF can export information listed in Table 4 and Table 5 to CS by E-Mail. When TSF export information to CS by using E-Mail, TSF encrypts E-Mail message by S/MIME. TSF encrypts the message by the public key of CS to prevent other than CS to read the message.

SF.AUDIT

TSF records 3 types of audit log, access log, communication log and system log. The events listed in Table 7 are recorded to each audit log, and the information listed in Table 9 are included in the records.

When size of each audit log exceeds 64 Kbytes, the oldest record is overwritten with new record.

The operator successfully authenticated by SF.OPE_I&A is allowed to read access log and communication log. Only CE successfully authenticated by SF.OPE_I&A is allowed to read system log. They cannot modify those audit logs.

Table 9: Information included in the audit records

Type of audit log	Content
Access log	date and time, terminal IP address, operator name, result of login
Communication log	date and time, IP address of CS or image I/O device, send or receive, content of sent/received information
System log	audit level, date and time, function name(PPP(Dial-up), CGI(Web) SMTP(E-Mail), DBMS(Database), …), error code, description

6.2 Strength of Function Claims

The security functions realised by probabilistic or permutational mechanisms are SF.OPE_I&A, SF.CS_I&A, SF.CS_HTTPS and SF.CS_SMIME. Three of those, SF.CS_I&A, SF.CS_HTTPS and SF.CS_SMIME, are realised only by cryptographic mechanisms. So, those three functions are excluded from the SOF-rating. Target of SOF-rating is only SF.OPE_I&A. The strength of function level for the function is **SOF-Basic**.

6.3 Assurance Measures

The following documents are provided as the assurance measures:

Security Target for

Remote Communication Gate Type BN1, Remote Communication Gate Type BM1

Version 1.0, 2005-08-15

Security Functional Specification for

Remote Communication Gate Type BN1, Remote Communication Gate Type BM1

Version 1.0, 2005-08-15

High-level Design for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Correspondence Analysis for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Setup Guide, Operating Instructions
Version 1.0, 2005-08-15

Security Test Documentation for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Strength of Function Analysis for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Vulnerability Analysis for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Configuration Management Plan for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Development Security Plan for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Delivery Procedure for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Production Procedure for
Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Service Manual for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Version 1.0, 2005-08-15

Remote Communication Gate Type BN1/BM1 (Machine Code: A768/A769) SERVICE MANUAL
Version 1.0 revised, 2005-05-24

Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Safety Information and Setup Guide
Version A768-8603A/ A768-8605A, 2005-06-22

Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Operating Instructions
Version A768-8604A/A768-8606A, 2005-07-01

Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
CS developer’s Guidance
Version 1.00, 2005-03-25

Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
Image I/O device developer’s Guidance
Version 1.00, 2005-03-25

7 PP Claims

There are no Protection Profiles claimed to which this ST is conformant.

8 Rationale

8.1 Security Objectives Rationale

In this section, it is demonstrated that the security objectives identified in section 4 are suitable and covering all aspects of the security environment described in section 3.

Table 10 shows that each security objective covers at least one threat, OSP or assumption, and that each threat and assumption is covered by at least one security objective.

Table 10: Correspondence between security needs and security objectives

	O.OPE_I&A	O.CS_ID	O.A_RIGHTS	O.TRUST_NET	O.CIPHER	O.AC_AUDIT	O.COM_AUDIT	O.SYS_AUDIT	OE.TIME	OE.PHYSIAL	OE.DEVICE	OE.NETWORK	OE.CE	OE.ADMIN	OE.CS
T.WEB	X		X		X										
T.CS_COMM				X	X										
T.CS_MAIL					X										
T.FAKE_CS		X													
OSP.AUDIT						X	X	X	X						
A.PHYSICAL										X					
A.DEVICE											X				
A.NETWORK												X			
A.CE													X		
A.ADMIN														X	
A.CS															X

T.WEB is countered by O.OPE_I&A, O.CIPHER and O.A_RIGHTS, because it is ensured user access is/user access rights are limited via web interface. O.OPE_I&A is performed for operators by login ID and password process. Access rights, as defined in Table 4 are ensured by O.A_RIGHTS. Furthermore, data transmission is encoded by O.CIPHER. O.CIPHER serves as prevention against network monitoring and therefore no one can analyse the password respectively no one can analyse the authentication data to get unauthorized access rights.

T.CS_COMM is countered by O.TRUST_NET, O.CIPHER, because it is ensured that TOE communicates CS using O.TRUST_NET. Communication data between TOE and CS is encrypted by O.CIPHER.

T.CS_MAIL is countered by O.CIPHER, because it is ensured that Mail information toward CS is encrypted by O.CIPHER. Encrypted mail information is decrypted by the private key of CS.

T.FAKE_CS is countered by O.CS_ID, because it is ensured that TOE identifies and authenticates CS using a unique ID by O.CS_ID.

OSP.AUDIT is countered by O.AC_AUDIT, O.COM_AUDIT, O.SYS_AUDIT and OE.TIME, because it is ensured that access evidence is logged with occurred time by O.AC_AUDIT, O.COM_AUDIT, O.SYS_AUDIT and OE.TIME.

A.PHYSICAL is covered by OE.PHYSICAL, because it is ensured that storage media and the information stored in are protected from an attacker (outer evil person).

A.DEVICE is covered by OE.DEVICE, because it is ensured that image I/O devices are set up in an orderly manner, and illegal applications could not be installed without being noticed by those responsible, therefore the image I/O device is held genuine status.

A.NETWORK is covered by OE.NETWORK, because it is ensured that the office network is working well and LAN circumstance is protected by firewall.

A.CE is covered by OE.CE, because it is ensure that reliable CE comes to carry out the maintenance of RC Gate since the user commissions the proper dealer to repair. They are responsible for the TOE confirms that CE is an authentic person of Ricoh or a proper distributor and make efforts to keep up it correctly.

A.ADMIN is covered by OE.ADMIN, because it is ensure that user administrator carries out the settings of RC Gate since he/she reads user’s documentations properly.

A.CS is covered by OE.CS, because it is ensured that CS is unique and trusted. CS is protected from outer evil person.

8.2 Security Requirements Rationale

8.2.1 Rationale for functional requirements

In this section, it is demonstrated that the security functional requirements specified in section 5 achieve the security objectives identified n section 4.

Table 11 shows that TOE security functional requirement covers security objective for the TOE, and security functional requirement for the IT environment covers security objective for the IT environment.

Table 11: Correspondence between security objectives and functional requirements

	FDP_ACC.1	FDP_ACF.1	FTP_ITC.1	FCS_COP.1	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.7	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1(a)	FAU_SAR.1(b)	FAU_STG.2	FPT_SMT.1
O.OPE_I&A					X	X	X	X	X	X			X						
O.CS_ID			X																
O.A_RIGHTS	X	X									X	X							
O.TRUST_NET			X	X															
O.CIPHER				X															
O.AC_AUDIT														X	X	X		X	
O.COM_AUDIT														X		X		X	
O.SYS_AUDIT														X			X	X	
OE.TIME																			X

O.OPE_I&A is achieved by FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1 and FMT_SMR.1, because those requirements ensure that only authorized operator can access TOE data, i.e. unauthorized person cannot access TOE.

O.CS_ID is achieved by FTP_ITC.1, because that requirement ensures that RC Gate identifies and authenticates CS, i.e. RC Gate never connects pseudo CS.

O.A_RIGHTS is achieved first by FDP_ACC.1 and FDP_ACF.1, because these two requirements ensure that RC Gate gives the defined/specified access rights (as stated in Table 4) to the operator or CS, as correctly identified and

authenticated before. Additionally, O.A_RIGHTS is achieved by FMT_MTD.1 (restriction to modify the password) and by FMT_SMF.1 (capability to modify operator's password).

O.TRUST_NET is achieved by FTP_ITC.1 and FCS_COP.1, because those requirements ensure that CS is identified and authenticated (when establishing a trusted channel) and the information (as stated in Table 5 respectively the relevant defined assets in chapter 3.1) between RC Gate and CS is protected, i.e. it is hard to analyse the information.

O.CIPHER is achieved by FCS_COP.1, because this requirement ensures that communication data are encrypted by HTTPS or S/MIME.

O.AC_AUDIT is achieved by FAU_GEN.1, FAU_GEN.2, FAU_SAR.1(a) and FAU_STG.2 because those requirements ensure that the access log is recorded, is associated with operator identity, is reviewed by operators, and is guaranteed in term of availability.

O.COM_AUDIT is achieved by FAU_GEN.1, FAU_SAR.1(a) and FAU_STG.2 because those requirements ensure that the communication log is recorded, is reviewed by operators, and is guaranteed in term of availability.

O.SYS_AUDIT is achieved by FAU_GEN.1, FAU_SAR.1(b) and FAU_STG.2 because those requirements ensure that the system log is recorded, is reviewed by CE, and is guaranteed in term of availability.

OE.TIME is achieved by FPT_STM.1 because this requirement ensures that correct time stamp is provided for TOE.

8.2.2 Rationale for minimum strength of function level

To achieve O.OPE_I&A, identification and authentication (I&A) is needed for operators to access the TOE. Since the RC Gate is used in the relatively secure environment as described in OE.PHYSICAL, the TOE is just intended to protect the assets and to be protected itself against low potential attackers. Additionally RC Gate manages only data from the image devices, which are assets of only low financial value. Therefore, SOF-Basic can be considered appropriate for the minimum strength of function level for the TOE.

8.2.3 Rationale for assurance requirements

An attacker may disclose the information data, which is sent/received between RC Gate and CS via Internet or telephone line directly. The attacker may be an evil person wandering around Internet or monitoring line in secret. For providing this countermeasure, the TOE identifies and authenticates operator (SF.OPE_I&A) and communication apparatus (SF.CS_I&A). In addition, user data is encrypted by HTTPS (SF.CS_HTTPS) and SMIME (SF.CS_SMIME).
Summarized the following security functions are realised by probabilistic or permutational mechanisms:

- SF.OPE_I&A,

- SF.CS_I&A,
- SF.CS_HTTPS and
- SF.CS_SMIME,

Three of those,

- SF.CS_I&A,
- SF.CS_HTTPS and
- SF.CS_SMIME,

are realised only by cryptographic mechanisms whereas the strength of function of SF.OPE_I&A will be “SOF-Basic”. Furthermore, the higher attack potential is required for such attacks as bypassing or tampering the TSF itself, and it is out of scope of this evaluation, RC Gate manages only data from the image devices, no direct financial assets, i.e. analysis of obvious vulnerabilities (AVA_VLA.1) is enough for general needs.

On the other hand, it is needed to keep the secret concerning the relevant information in an effort to make an attack harder, and Ricoh considers that it is meaningful to get confidence of security also from the development environment, i.e. development security (ALC_DVS.1).

For the reason stated above, EAL3 is selected as the proper estimation assurance level for this TOE.

8.2.4 Mutual support of security requirements

The set of security functional requirements that are selected in this ST covers all the TOE security objectives as demonstrated in section 8.2.1.

In this ST, the component FMT_MSA.3 is required as the dependencies of FDP_ACF.1, but FMT_MSA.3 is not included in the TOE security functional requirements. The access right to the setting information is fixed, and the security attributes are not changed. So, it is not necessary to change initial values of security attribute, and the requirement FMT_MSA.3 is not required.

In this ST, the components FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2 are required as the dependencies of FCS_COP.1, but those requirements are not included in the TOE security functional requirements. The cryptographic key is installed during production of RC Gate and is not replaced until the end of the life cycle. Therefore, the requirements FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2 are not required.

In this ST, the component FPT_STM.1 is required as the dependencies of FAU_GEN.1, but FPT_SMT.1 is not included in the TOE security functional requirements. FPT_SMT.1 is included in security functional requirements for the environment.

8.3 TOE Summary Specification Rationale

8.3.1 Rationale for TOE security functions

In this section, it is demonstrated that the security functions defined in section 6.1 realize the security functional requirements specified in section 5.1.

Table 12 shows that each security function for the TOE covers at least one TOE security functional requirement, and that each TOE security functional requirement is covered by at least one security function for the TOE.

Table 12: Correspondence between functional requirements and security functions

	SF.OPE_I&A	SF.CS_I&A	SF.OPE_AC	SF.CS_HTTPS	SF.CS_SMIME	SF.AUDIT
FDP_ACC.1			X			
FDP_ACF.1			X			
FTP_ITC.1		X		X		
FCS_COP.1		X		X	X	
FIA_AFL.1	X					
FIA_ATD.1	X					
FIA_SOS.1	X					
FIA_UAU.1	X					
FIA_UAU.7	X					
FIA_UID.1	X					
FMT_MTD.1	X					
FMT_SMF.1	X					
FMT_SMR.1	X	X				
FAU_GEN.1						X
FAU_GEN.2						X
FAU_SAR.1(a)						X
FAU_SAR.1(b)						X
FAU_STG.2						X

The following Table 13 shows the corresponding part of description of the security function, which derives from section 6.1.

Table 13: Corresponding description of security functions

Requirement	Description of security functions
FDP_ACC.1 FDP_ACF.1	**SF.OPE_AC:** TSF controls operations performed by the operator based on the operator's identification information and method to communicate with CS. When direct HTTPS method, dialup HTTPS method, or SMTP method is used to communicate with CS, operators can access to the information based on Table 4.

FTP_ITC.1	**SF.CS_I&A:** TSF identifies and authenticates CS before communicates with CS by HTTPS. When the identification and authentication is succeeded, it is allowed to export or import information to/from CS. If the identification and authentication is failed, it is denied to export nor import information between CS. **SF.CS_HTTPS:** TSF can export and import information listed in Table 5 to/from CS by using HTTPS protocol. TSF authenticates CS before export or import information. When CS is successfully authenticated, TSF encrypts the information to export, and decrypts the imported information.
FCS_COP.1	**SF.CS_HTTPS:** TSF can export and import information listed in Table 5 to/from CS by using HTTPS protocol. When CS is successfully authenticated, TSF encrypts the information to export, and decrypts the imported information.. **SF.CS_SMIME:** TSF can export information listed in Table 4 and Table 5 to CS by E-Mail. When TSF export information to CS by using E-Mail, TSF encrypts E-Mail message by S/MIME. TSF encrypts the message by the public key of CS to prevent other than CS to read the message. **SF.CS_I&A:** TSF identifies and authenticates CS before communicates with CS by HTTPS. When the identification and authentication is succeeded, it is allowed to export or import information to/from CS. If the identification and authentication is failed, it is denied to export nor import information between CS. For authentication of CS, TSF uses the HTTPS mutual authentication mechanism.
FIA_AFL.1	**SF.OPE_I&A:** If the wrong password is entered three consecutive times, TSF reject identification and authentication for one minutes.
FIA_ATD.1	**SF.OPE_I&A:** TSF identifies and authenticates operator (Administrator, Registrant and CE) prior to the operation listed below. When authentication is succeeded, TSF assigns a role (Administrator, Registrant and CE) to the operator. If the authentication is failed, the operator cannot perform following operations: - read audit logs - read and modify setting information - modify password
FIA_SOS.1	**SF.OPE_I&A:** The operator can change his own password. The length of new password should be at least 8 and at most 13 characters. If the length new password is not in the range, the new password is rejected.

FIA_UAU.1 FIA_UID.1	**SF.OPE_I&A:** TSF identifies and authenticates operator (Administrator, Registrant and CE) prior to the operation listed below. When authentication is succeeded, TSF assigns a role (Administrator, Registrant and CE) to the operator. If the authentication is failed, the operator cannot perform following operations: - read audit logs - read and modify setting information - modify password
FIA_UAU.7	**SF.OPE_I&A:** While the operator is entering password, the asterisks are shown instead of password characters.
FMT_MTD.1	**SF.OPE_I&A:** The operator can change his own password. The length of new password should be at least 8 and at most 13 characters. If the length new password is not in the range, the new password is rejected.
FMT_SMF.1	**SF.OPE_I&A:** The operator can change his own password. The length of new password should be at least 8 and at most 13 characters. If the length new password is not in the range, the new password is rejected.
FMT_SMR.1	**SF.OPE_I&A:** TSF identifies and authenticates operator (Administrator, Registrant and CE) prior to the operation listed below. When authentication is succeeded, TSF assigns a role (Administrator, Registrant and CE) to the operator. If the authentication is failed, the operator cannot perform following operations: - read audit logs - read and modify setting information - modify password **SF.CS_I&A:** TSF identifies and authenticates CS before communicates with CS by HTTPS. When the identification and authentication is succeeded, it is allowed to export or import information to/from CS. If the identification and authentication is failed, it is denied to export nor import information between CS. For authentication of CS, TSF uses the HTTPS mutual authentication mechanism.
FAU_GEN.1	**SF.AUDIT:** TSF records 3 types of audit log, access log, communication log and system log. The events listed in Table 7 are recorded to each audit log, and the information listed in Table 9 are included in the records.
FAU_GEN.2	**SF.AUDIT:** TSF records 3 types of audit log, access log, communication log and system log. The events listed in Table 7 are recorded to each audit log, and the information listed in Table 9 are included in the records.

FAU_SAR.1(a)	**SF.AUDIT:** The operator successfully authenticated by SF.OPE_I&A is allowed to read access log and communication log. Only CE successfully authenticated by SF.OPE_I&A is allowed to read system log. They cannot modify those audit logs.
FAU_SAR.1(b)	**SF.AUDIT:** The operator successfully authenticated by SF.OPE_I&A is allowed to read access log and communication log. Only CE successfully authenticated by SF.OPE_I&A is allowed to read system log. They cannot modify those audit logs.
FAU_STG.2	**SF.AUDIT:** TSF records 3 types of audit log, access log, communication log and system log. The events listed in Table 7 are recorded to each audit log, and the information listed in Table 9 are included in the records. When size of each audit log exceeds 64 Kbytes, the oldest record is overwritten with new record.

8.3.2 Rationale for strength of function claims

As shown in section 6.2, there are four security functions (SF.OPE_I&A, SF.CS_I&A, SF.CS_HTTPS and SF.CS_SMIME) that have the probabilistic or permutational mechanism. Only the function SF.OPE_I&A has the strength SOF-Basic. Other functions, SF.CS_I&A, SF.CS_HTTPS, and SF.CS_SMIME, are excluded from the SOF-rating. On the other hand, as claimed in section 5.2, the minimum strength of TOE security functions is SOF-Basic. RC Gate manages data which are assets of only low financial value. Therefore, SOF-Basic can be considered appropriate for the assets. It is obvious that those claims are consistent.

8.3.3 Rationale for combination of security functions

As shown in section 8.3.1, the 6 security functions defined in section 6.1 cover all the security functional requirements. And as shown in section 8.2.4, those requirements mutually support each other. In addition, there is no security weakness due to the combination of security functions, since those functions are independent each other (because it is obvious that there are no overlapping parts of them). That is, all the security functions work together so as to satisfy the security functional requirements.

8.3.4 Rationale for assurance measures

Table 14 shows that the corresponding assurance measures are provided for each assurance requirement due to class ASE and EAL 3. The actual fulfilment of the requirements by these assurance measures is inspected during the evaluation.

Table 14: 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	Security Target for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15
ACM: Configuration management	ACM_CAP.3 ACM_SCP.1	Configuration Management Plan for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15
ADO: Delivery and operation	ADO_DEL.1 ADO_IGS.1	Delivery Procedure for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15 Production Procedure for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15 Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Setup Guide, Operating Instructions Version 1.0, 2005-08-15
ADV: Development	ADV_FSP.1	Security Functional Specification for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15
	ADV_HLD.2	High-level Design for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15
	ADV_RCR.1	Correspondence Analysis for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15
AGD: Guidance documents	AGD_ADM.1 AGD_USR.1	Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Setup Guide, Operating Instructions Version 1.0, 2005-08-15 Service Manual for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1

Assurance Class	Assurance Component	Assurance Measure
		Version 1.0, 2005-08-15 Remote Communication Gate Type BN1/BM1 (Machine Code: A768/A769) SERVICE MANUAL Version 1.0 revised, 2005-05-24 Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Safety Information and Setup Guide Version A768-8603A/ A768-8605A, 2005-06-22 Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Operating Instructions Version A768-8604A/A768-8606A, 2005-07-01 Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 CS developer's Guidance Version 1.00, 2005-03-25 Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Image I/O device developer's Guidance Version 1.00, 2005-03-25 Remote Communication Gate Type BN1/BM1 (Machine Code: A768/A769) SERVICE MANUAL Version 1.0 revised, 2005-05-24 Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Safety Information and Setup Guide Version A768-8603A/ A768-8605A, 2005-06-22 Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Operating Instructions Version A768-8604A/A768-8606A, 2005-07-01 Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 CS developer's Guidance Version 1.00, 2005-03-25 Remote Communication Gate Type BN1, Remote

Assurance Class	Assurance Component	Assurance Measure
		Communication Gate Type BM1 Image I/O device developer's Guidance Version 1.00, 2005-03-25
ALC: Life cycle support	ALC_DVS.1	Development Security Plan for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15
ATE: Tests	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_INT.2	Security Test Documentation for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15
AVA: Vulnerability assessment	AVA_MSU.1	Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Setup Guide, Operating Instructions Version 1.0, 2005-08-15
	AVA_SOF.1	Strength of Function Analysis for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15
	AVA_VLA.1	Vulnerability Analysis for Remote Communication Gate Type BN1, Remote Communication Gate Type BM1 Version 1.0, 2005-08-15

8.4 PP Claims Rationale

There are no Protection Profiles claimed to which this ST is conformant.

9 Annex

9.1 Source

ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security,

ISO/IEC 15408-1:1999(E), Part 1: Introduction and general model,

ISO/IEC 15408-2:1999(E), Part 2: Security functional requirements,

ISO/IEC 15408-3:1999(E), Part 3: Security assurance requirements.

9.2 Abbreviation

CC	Common Criteria
CE	Customer Engineer
CS	Communication Server
DBMS	Data Base Management System
Image I/O device	Copier, Printer, Facsimile, and Multi-functional Printer
LAN	Local Area Network
MIB	Management Information Base
OS	Operating System
PP	Protection Profile
SC	Service Call
SD memory card	Secure Digital memory card
SF	Security Function
ST	Security Target
TIA/EIA	The US Telecommunications Industries Association and Electronics Industries Association
TOE	Target of Evaluation
TSF	TOE Security Function

9.3 Grouping Setting Items

RC Gate has many setting items and the setting items contain items not related to security functions. The setting items shown in Table 4 are summarized for simplification. Each setting items shown in Table 4 are grouped from several corresponding detailed items. Table 15 shows the relations between grouped items and corresponding detailed items.

Table 15: Relations between grouped items and detailed item

Category	Grouped item	Detailed item
RC Gate Settings-Basic	RC Gate Setting-Basic parameters 1	RC Gate ID, Model name, Application version, OS version
	RC Gate Setting-Basic parameters 2	RC Gate location, Application last updated, OS last updated, Service depot, Service depot contact
	Language	Language
	Time zone	Time zone
	RC Gate Setting-Basic parameters 3	Log max capacity, Log collection level
	Auth key version	Auth key version
RC Gate Settings-Date/Time	Date / Time	Date, Time
RC Gate Settings-Network	Maintenance Port IP address	IP address
	Other Maintenance Port parameters	MAC address, Subnet Mask
	LAN Port MAC address	MAC address
	Other LAN Port parameters	DHCP, IP address, Subnet mask, Default gateway address, Ethernet speed
	DNS server parameters	Main DNS server, Sub DNS server
RC Gate Settings-E-mail	Send Test E-mail	Send Test E-mail (function)
	E-mail parameters 1	RC Gate E-mail address (for sender), RC Gate E-mail address (for receiver)
	Communication Server E-mail address	Communication Server E-mail address
	RC Gate admin's E-mail address	RC Gate admin's E-mail address
	E-mail parameters 2	Number of times to resend E-mail, Resend E-mail interval time

	SMTP server parameters 1	SMTP server address, SMTP server port, SMTP user name
	SMTP server parameters 2	SMTP_AUTH flag, SMTP_AUTH authentication method
	SMTP password	SMTP password
	POP server parameters 1	POP server address, POP server port, POP user name
	POP server parameters 2	POP before SMTP flag, Wait time after authentication
	POP password	POP password
RC Gate Settings-Communication Method	Communication method	Communication method
	Internet connection method	Internet connection method
	Other communication method parameters	Communication server address, Interval time to Sleep shift, Interval time to Sleep return detection, Interval time to retry HTTP connection, Number of times to retry HTTP connection, HTTP connection demand transmitting delay, HTTP connection timeout, HTTP transmitting timeout, HTTP receiving timeout, Interval time to retry HTTP GET/POST, Number of times to retry HTTP GET/POST
RC Gate Settings-Net Connection Settings-Connection Details	Internet connection method	Internet connection method
	Proxy password	Proxy password
	Proxy server parameters	Proxy server, Proxy address Proxy port Proxy user name
RC Gate Settings-Net Connection Settings-Dial-up	Dial-up internet connection method	Internet connection method
	Access point parameters 1	Access point (select), RC Gate phone No., Line connection

	Access point text	Access point (text)
Dialing Line Settings	Dialing Line parameters	Pulse/Tone dialing line, Outside access No.
Modem Settings	Modem parameters	Dial-up authentication method, Dial-up User name, Dial-up Password, Connection timeout, Number of times to re-dial, Interval time to re-dial, Number of times to retry callback, AT command, Ring count, Timers T1 to T7, IT Pattern, Timer for a fax on-hook at call-back
Auto Discovery-Auto Discovery Settings	Auto Discovery	Auto Discovery
	Auto Discovery permit	Permit setting of Auto Discovery from Communication Server
Auto Discovery Settings	Auto Discovery server address	Auto Discovery server address
	Max. E-mail size	Max. E-mail size
	Auto Discovery Range parameters	Range, Subnet Mask, Discovery, Range Name, Comment
Device Management-Common management	Information Retrieval settings	Interval time to retrieve device information, Interval time to re-retrieve device information, Number of times to re-retrieve device information, Interval time to retrieve device counter information, Interval time to re- retrieve device counter information, Number of times to re-retrieve device counter information
	Devices to repeat search (HTTP and SNMP)	Devices to repeat search (HTTP and SNMP)

	Other Network Connection settings	Interval time to refresh device connection (HTTP), Interval time to refresh device connection (SNMP), Interval time to detect device warning (SNMP), Interval time to start repeat search function for devices (HTTP and SNMP), Interval time to start repeat search devices (HTTP and SNMP), Time lapse before devices are considered temporarily suspended (HTTP and SNMP), Time lapse before devices are considered suspended (HTTP and SNMP)
	RS-485 Connection parameters	Interval time to refresh device connection (RS-485), Time lapse before devices are considered temporarily suspended (RS-485), Time lapse before devices are considered suspended (RS-485), Time lapse before devices are considered disconnected (RS-485)
Device Management-Connection Details	Device retry parameters	Interval times to retry HTTP/ SNMP/RS-485 connections, Numbers of times to retry HTTP/ SNMP/RS-485 connections
Device Management-Registered Device List	M-R Device List parameters 1	IP address, Device location, Supply ordering person's E-mail address
	Device name	Device name
	SNMP community name	SNMP community name
	M-R Device List parameters 2	Machine ID, Model name, MAC address, Connection Type, Meter Reading Date (Time), Device ID (RS-485), Status
	Method to assign IP address	Method to assign IP address

	Machine administrator's E-mail address	Machine administrator's E-mail address
	M-R Device List parameters 3	Service depot, Service depot contact, Supply order from, Supply order phone No.
Device Management-Notify	Device Management-Notify parameters	SC/CC, MC, Alarm, Supply
Device Management-Update Device Firmware	Device Firmware parameters 1	Schedule, Period, URL for firmware download, Message
	Device Firmware functions	Update button, Previous Update Details button
	Object devices list	Object devices list
	Device Firmware parameters 2	Device ID, Update Status, Update date/time, Update Result
Maintenance-Restart RC Gate	Maintenance-Restart function	Restart (function)
Maintenance-Communication Server Calls-Service Test Call	Service Test Call function	Service Test Call (function)
	CS Test Call Log	Log
Maintenance-Communication Server Calls-Device Check Req.Call	Device Check Req.Call functions	Device Check Req.Call functions
	CS Check Req.Call Message	Message
Maintenance-Restore	Restore parameters	Last backup date/time, Last restoration date/time, Restoration result, Error code
	Restore function	Restore (function)
Maintenance-Restore(Notify)	Maintenance-Restore Notify function	Notify (function)
Maintenance-Log-Log setup	Maintenance Log parameters	Communication log max capacity, Log max capacity
	Maintenance Log collection level	Log collection level
Maintenance-Log-System Log	Maintenance System Log	System Log
	Maintenance Communication Log	Communication Log

Maintenance-Memory	Maintenance-Memory parameters	Used RAM area, Free RAM area, Used storage area, Free storage area
Maintenance-Service Call	Maintenance-Service Call parameters 1	“Current SC status”, SC code, Detail code, Date/time, Center communication
	Maintenance-Service Call parameters 2	Service depot, Service depot connection
Maintenance-System Status	Maintenance-System Status parameters	“Current system status”, Date/time, Reason
Security-Password	CurrentUser	CurrentUser
	Password	password
Security-Permissions	Permit access by service	Permit access by service
	Permit updating of Firmware from Communication Server	Permit updating of Firmware from Communication Server
Security-Access Log	Access Log	Log
Security-Format RC Gate	Format function	Format (function)