



# **Remote Communication Gate A**

## **Security Target**

Author: RICOH COMPANY, LTD.  
Date: 2010-09-27  
Version: 1.00.

This document is a translation of the evaluated and certified security target written in Japanese.

**Document Revision History**

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Description</b>
1.00	2010-09-27	RICOH COMPANY, LTD.	Released version

---

## Table of Contents

<b>1</b>	<b><i>ST Introduction</i></b> .....	<b>6</b>
<b>1.1</b>	<b>ST Reference</b> .....	<b>6</b>
<b>1.2</b>	<b>TOE Reference</b> .....	<b>6</b>
<b>1.3</b>	<b>TOE Overview</b> .....	<b>6</b>
1.3.1	TOE Type.....	6
1.3.2	TOE Usage.....	7
1.3.3	Major Security Functions of the TOE.....	7
1.3.4	Operational Environment for the TOE.....	7
<b>1.4</b>	<b>TOE Description</b> .....	<b>10</b>
1.4.1	Physical Scope of the TOE .....	10
1.4.2	Guidance Documents.....	11
1.4.3	Definitions of the Related Roles .....	12
1.4.4	Logical Scope of the TOE.....	13
1.4.4.1	Basic Functions .....	13
1.4.4.2	Security Functions.....	14
1.4.5	Protected Assets .....	15
<b>1.5</b>	<b>Terminology</b> .....	<b>16</b>
<b>2</b>	<b><i>Conformance Claims</i></b> .....	<b>17</b>
<b>2.1</b>	<b>CC Conformance Claims</b> .....	<b>17</b>
<b>2.2</b>	<b>PP Claims</b> .....	<b>17</b>
<b>2.3</b>	<b>Package Claims</b> .....	<b>17</b>
<b>3</b>	<b><i>Security Problem Definition</i></b> .....	<b>18</b>
<b>3.1</b>	<b>Threats</b> .....	<b>18</b>
<b>3.2</b>	<b>Organisational Security Policies</b> .....	<b>18</b>
<b>3.3</b>	<b>Assumptions</b> .....	<b>19</b>
<b>4</b>	<b><i>Security Objectives</i></b> .....	<b>20</b>
<b>4.1</b>	<b>Security Objectives for the TOE</b> .....	<b>20</b>
<b>4.2</b>	<b>Security Objectives for Operational Environment</b> .....	<b>21</b>
<b>4.3</b>	<b>Security Objectives Rationale</b> .....	<b>22</b>
4.3.1	Corresponding Relationship between Security Objectives and Security Problems .....	22
<b>5</b>	<b><i>Extended Components Definition</i></b> .....	<b>25</b>
<b>6</b>	<b><i>Security Requirements</i></b> .....	<b>26</b>
<b>6.1</b>	<b>Security Functional Requirements</b> .....	<b>26</b>
6.1.1	Class FDP: User data protection .....	26
6.1.2	Class FIA: Identification and authentication .....	28
6.1.3	Class FMT: Security management .....	29
6.1.4	Class FPT: Protection of the TSF.....	30
6.1.5	Class FTA: TOE access.....	31

---

6.1.6	Class FTP: Trusted path/channels.....	31
<b>6.2</b>	<b>Security Assurance Requirements.....</b>	<b>33</b>
<b>6.3</b>	<b>Security Requirements Rationale.....</b>	<b>33</b>
6.3.1	Tracing.....	34
6.3.2	Justification of Traceability.....	34
6.3.3	Dependency Analysis.....	37
<b>6.4</b>	<b>Security Assurance Requirements Rationale.....</b>	<b>38</b>
<b>7</b>	<b><i>TOE Summary Specification</i>.....</b>	<b>39</b>

## List of Figures

Figure 1: Connection figure of the TOE.....	8
Figure 2: Hardware configuration of the TOE.....	10
Figure 3: Logical scope of the TOE.....	13

## List of Tables

Table 1: Terms related to the TOE.....	16
Table 2: Corresponding relationship between security objectives and security problems.....	22
Table 3: Subjects, objects, and operations .....	26
Table 4: Subjects, objects, and security attributes .....	27
Table 5: Rules governing access.....	27
Table 6: Rules for the initial association of attributes.....	29
Table 7: List of TSF information management.....	30
Table 8: List of specification of management functions .....	30
Table 9: Functions to require trusted channels in the communication between the RC Gate and CS (a) .....	32
Table 10: Functions to require trusted channels in the communication between the RC Gate and the registered HTTPS-compatible device (b) .....	32
Table 11: TOE security assurance requirements (EAL3).....	33
Table 12: Relation between security objectives and functional requirements .....	34
Table 13: Corresponding table of dependencies for the TOE security functional requirements.....	37

## 1 ST Introduction

This chapter describes the Security Target (ST) reference, the Target of Evaluation (TOE) reference, TOE overview, TOE description and terminology.

### 1.1 ST Reference

The ST identification information shows as follows:

ST Title: Remote Communication Gate A Security Target  
ST Version: 1.00.  
Date: 2010-09-27  
Authors: RICOH COMPANY, LTD.

### 1.2 TOE Reference

Remote Communication Gate A, which is the TOE, is identified by the first four characters of the six-character Machine Code plus the firmware version. The firmware version combines versions of each firmware module: Application (A), Firmware Common Parts (C), Platform (P), and OS (K).

Manufacturer: RICOH COMPANY, LTD.  
Product Name: Remote Communication Gate A  
(Note) The above-mentioned product is hereinafter referred to as "RC Gate".  
Machine Code (First four characters): D459  
Firmware Version: A1.18-C1.14-P1.12-K1.04

### 1.3 TOE Overview

This section describes the TOE type, the TOE usage, major security functions, and operational environment for the TOE.

#### 1.3.1 TOE Type

The TOE is an IT device to be used for a service that remotely diagnoses and maintains digital MFPs and printers (hereinafter referred to as "devices") on a local area network (LAN). This remote diagnosis maintenance service, referred to as "@Remote" or "@Remote Service", provides the necessary maintenance functions for each device. The TOE sends information received from the targeted devices that use service to the maintenance centre, and the maintenance centre diagnoses the status of the devices based on the information.

### **1.3.2 TOE Usage**

To provide @Remote Service, the TOE intermediates the communication between the devices to receive the remote diagnosis maintenance service and the maintenance centre.

To use this service, users are required to connect the TOE to the office LAN where the device to receive the remote diagnosis maintenance service is installed.

Users can operate the TOE by using a Web browser from a computer that is connected to the LAN.

### **1.3.3 Major Security Functions of the TOE**

The major security functions of the TOE are the Communication Protection Function, the User Access Restriction Function, and the RC Gate Firmware Validation Confirmation Function.

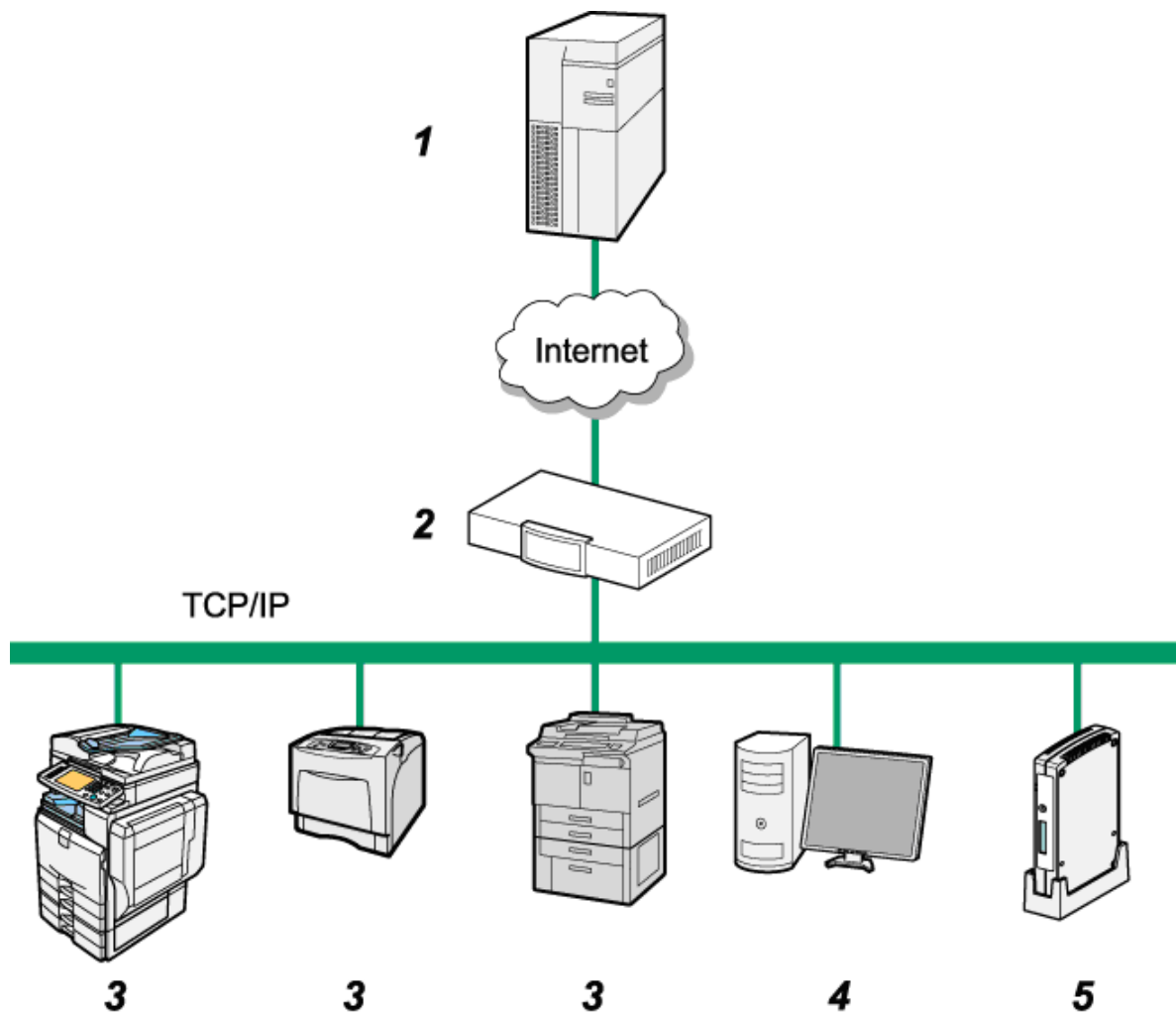
The Communication Protection Function is a function to protect the communication path between the TOE and the maintenance centre, computers, and devices that communicate using SSL.

The User Access Restriction Function is a function to identify and authenticate users who attempt to use the TOE from computers, and to provide only pre-authorised operations for authorised users who are successfully identified and authenticated.

The RC Gate Firmware Validation Confirmation Function is a function to confirm that the firmware of the TOE is manufacturer-genuine and to provide confirmation results for users.

### **1.3.4 Operational Environment for the TOE**

The connection image of the TOE is shown in Figure 1 and the TOE and non-TOE configuration items are described.



**Figure 1: Connection figure of the TOE**

1. CS (Communication Server)  
A server located in the maintenance centre. The TOE requests to start communications and sends or receives the information for the maintenance service between the TOE and the CS.
2. Firewalls  
A security system to protect the office LAN environment from external networks.
3. Devices  
In this Security Target (ST), the "device" means either a digital MFP or a printer, both of which are connected to the office LAN environment and can communicate with the TOE. It is categorised according to its communication method with the TOE as either an HTTPS-compatible device or an SNMP-compatible device. The HTTPS-compatible device is a device that can communicate with the TOE using the Communication Protection Function of the RC Gate, and the SNMP-compatible device is a device that is not an HTTPS-compatible device and that can communicate with the TOE by means of Management Information Base (MIB). The targeted devices of the remote diagnosis maintenance service are the HTTPS-compatible devices and SNMP-compatible devices that are registered in the TOE. They are called the registered HTTPS-compatible devices and the registered SNMP-compatible



devices, respectively. A registered device sends information related to the maintenance service to the TOE.

4. Computer

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

5. RC Gate

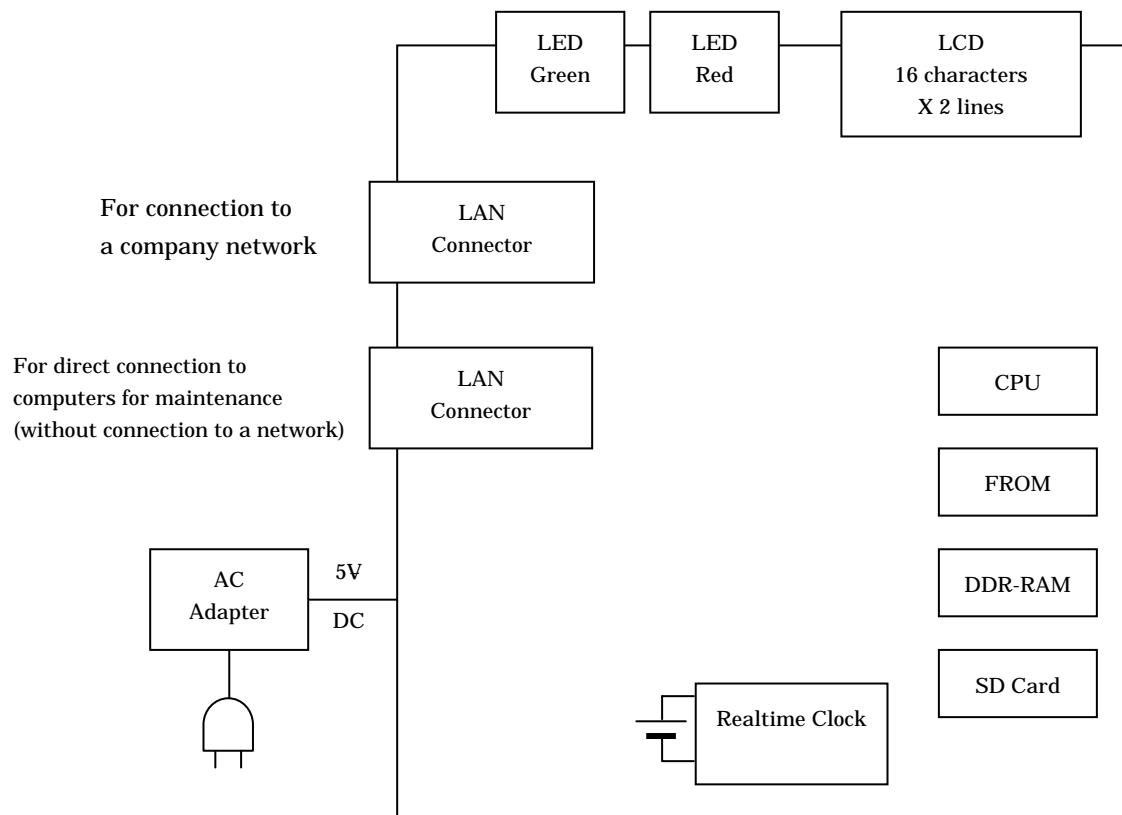
RC Gate is the TOE that is connected to the office LAN environment.

## 1.4 TOE Description

This section describes the physical scope of the TOE, guidance documents, definitions of the related roles, logical scope of the TOE, and protected assets.

### 1.4.1 Physical Scope of the TOE

The physical scope of the TOE consists of the hardware/firmware shown in Figure 2.



**Figure 2: Hardware configuration of the TOE**

#### CPU

A semiconductor chip that performs basic computational processing for the TOE operations.

#### FROM

A non-volatile semiconductor memory medium that stores boot loader data, etc. No data will be lost even if the power is turned off. FROM is also called flash memory.

**DDR-RAM**

A volatile semiconductor memory that programs and data are loaded into at the TOE start-up.

**SD Card**

A non-volatile semiconductor memory in which the RC Gate Firmware and initial information are recorded at the factory. When operational, it is used as the storage memory.

**Realtime Clock**

A clock that keeps current time and is equipped with a battery to work during power-off.

**LAN Connector for Connecting to an Internal Network**

A LAN Connector used for communicating with computers, the CS, and devices.

**LAN Connector for Connecting Computers**

A LAN Connector to connect a computer for initial setting of IP addresses and for maintenance in the event of the TOE failure.

**LCD**

A display device that shows the IP address, status, and error messages of the TOE.

**LED Green**

A lamp that shows the power is ON/OFF, and is lit when the power is on.

**LED Red**

A lamp that shows the status of the RC Gate, which can be indicated by either of the following: the LED Red is lit or unlit, the LED Red flashes on and off at normal speed or rapidly.

**AC Adapter**

A power device to supply electric power.

**RC Gate Firmware**

A built-in system in the TOE that consists of modules for Application, Software Common Parts, Platform, and OS.

**1.4.2 Guidance Documents**

The guidance documents consisting of this TOE are as follows:

Guidance documents for Japan

- Remote Communication Gate A Safety Information (written in Japanese)
- Remote Communication Gate A Setup Guide (written in Japanese)
- Remote Communication Gate A Operating Instructions (written in Japanese)

Guidance documents for overseas countries

- Remote Communication Gate A Safety Information
- Remote Communication Gate A Setup Guide
- Remote Communication Gate A Operating Instructions

### 1.4.3 Definitions of the Related Roles

The related roles to RC Gate are defined as follows:

#### **User**

User means, collectively, the administrator and the general user of the RC Gate as described below. When this ST simply refers to 'user', it refers to the administrator and the general user of the RC Gate.

#### **Administrator**

Administrator means an administrator of users who manage the RC Gate. The administrator can change the settings and view the status of the RC Gate from the computer. When this ST simply refers to "administrator", it indicates administrator of this RC Gate.

#### **General user**

General user is the authorised user whose TOE user account is given by administrator. The general user can view the device status from the computer.

#### **Network administrator**

Network administrator is an IT manager for users' LAN where the TOE is installed.

#### **Device administrator**

Device administrator is a person who manages the maintenance of the device that is connected to the users' LAN where the TOE is installed.

#### **Organisational responsible manager**

Organisational responsible manager is the responsible manager of users who belong to the organisation where the TOE is installed and operated. The organisational responsible manager has the authority to appoint each administrator.

#### **CE**

Customer engineer (CE) is a person who is educated to handle the TOE and performs the maintenance of the TOE. For maintenance, the CE can operate the TOE via the interface for the CE from a computer's Web browser. However, after the installation/setup of the TOE, the interface for the CE is disabled by the administrator.

#### **Network user**

Network user means the generic name of users who access the users' LAN environment where the TOE is installed. It also includes users who have no TOE user accounts.

### 1.4.4 Logical Scope of the TOE

An operational diagram of the TOE and the logical scope in the operational diagram are shown in Figure 3. The Basic Functions (non-Security Functions) that the TOE provides and the Security Functions of the TOE are described.

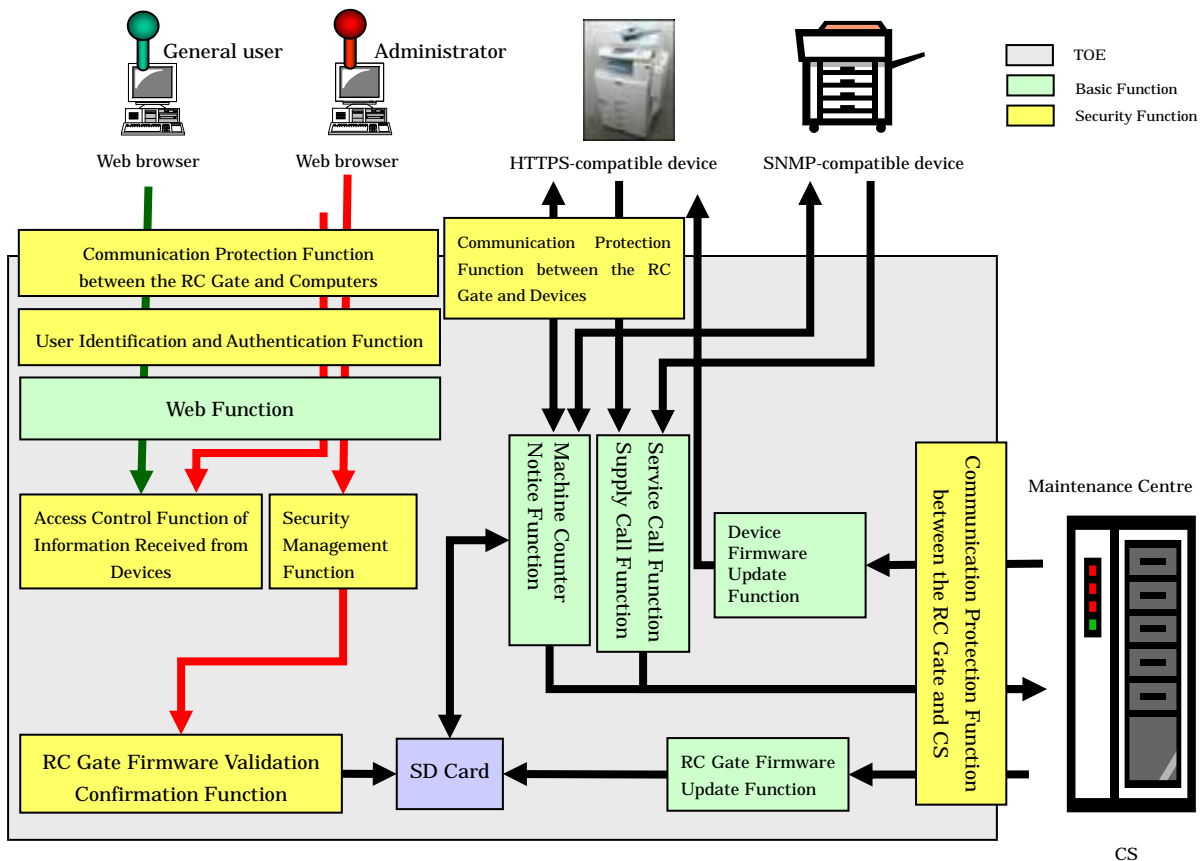


Figure 3: Logical scope of the TOE

#### 1.4.4.1 Basic Functions

##### Service Call Function

A function that allows the TOE to report to the CS the device failure information received from the registered device. Based on the report, the maintenance centre analyses and handles the cause of the failure.

**Machine Counter Notice Function**

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

**Supply Call Function**

A function that allows the TOE to notify the CS about the supply information (remaining toner and paper) received from the registered device. Based on the report, the maintenance centre supplies toner and paper.

**Device Firmware Update Function**

A function that allows the TOE to update the firmware of the registered HTTPS-compatible device with the device firmware received from the CS.

**RC Gate Firmware Update Function**

A function that allows the TOE to update the RC Gate's firmware with the RC Gate Firmware received from the CS.

**Web Function**

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

**1.4.4.2 Security Functions****Communication Protection Function between the RC Gate and Devices**

A function to detect communication data tampering. This function can be mutually used by the TOE and the registered HTTPS-compatible devices for communication between them if the Service Call Function, the Machine Counter Notice Function, and the Supply Call Function are enabled.

**Communication Protection Function between the RC Gate and CS**

A function that allows the TOE to specify only the CS as a communication destination via the Internet, and furthermore, communication data between the TOE and the CS is secured. Also, this function detects data tampering.

**Communication Protection Function between the RC Gate and Computers**

A function that enables communication data between the TOE and computers to be secured if the Web Function is enabled.

**User Identification and Authentication Function**

A function that allows the TOE to provide only the authorised users for the TOE (administrator, general user) with the Web Function. The TOE requires entering the information (hereinafter referred to as

"account information") to identify and authenticate users who attempt to use the Web Function. When users enter the account information, only successfully identified and authenticated users can operate the TOE.

#### **Access Control Function of Information Received from Devices**

A function that allows the TOE to restrict access to the information received from devices to only authorised users. The TOE allows successfully identified and authenticated users to access the information received from devices according to the users' roles.

#### **RC Gate Firmware Validation Confirmation Function**

A function that allows the TOE to confirm that Application, Software Common Parts, Platform, and OS are officially provided by the manufacturers at the request of the user.

#### **Security Management Function**

A Web-based TOE Function that allows the administrator to exercise management authorities for the TOE.

### **1.4.5 Protected Assets**

This subsection explains machine counter information, failure information, supply information, call notice history, device firmware, device firmware update history, RC Gate Firmware, and TSF data that the TOE protects.

#### **Machine Counter Information**

Machine counter information means the number of print pages counted for each device.

The machine counter information is sent to the TOE from each device, temporarily stored in the machine counter information area of the TOE, and periodically sent to the CS. Immediately after the TOE sends it to the CS, the machine counter information is overwritten in the machine counter information area. While the TOE stores the machine counter information, the administrator and the general user are allowed to view the information and perform no other operations related to the machine counter information. If the machine counter information sent from the device to the CS is tampered with, no appropriate @Remote services will be provided for the registered device.

#### **Failure Information, Supply Information, and Call Notice History**

Failure and supply information is sent from each device to the TOE, from the TOE to the CS as needed. If the failure information and supply information sent from the device to the CS is tampered with, no appropriate @Remote services will be provided for the registered device.

If the TOE receives the failure information or supply information, the TOE records service calls and supply calls (hereinafter referred to as "call notice history") in the call notice history area. The administrator and the general user are allowed only to view the call notice history; they cannot perform any other operations related to the call notice history.

**Device Firmware and Device Firmware Update History**

Device firmware and device firmware update history is part of the Device Firmware Update Functions, and device firmware will be sent from the CS to each device. Device firmware is installed in a device via the TOE from the CS. Integrity of the device firmware sent from the CS to the TOE must be assured.

The TOE records the history (hereinafter referred to as "device firmware update history") in the device firmware update history area for the execution of updating the device firmware. Only the administrator is allowed to view the device firmware update history; the administrator cannot perform other operations related to the device firmware update history.

**RC Gate Firmware**

RC Gate Firmware is installed in the TOE at the manufacturing facilities of the TOE and delivered to the user's site. It is authorised by the TOE administrator and sometimes can be updated with the RC Firmware Update Function. The RC Gate Firmware must be a genuine product of the manufacturer.

**TSF Data**

TSF data is recorded in the TOE. The authorised users for the TOE can newly create, alter, and delete the TSF data. Operations on TSF data are restricted by roles of the authorised users.

**1.5 Terminology**

For clear understanding of this ST, the meanings of the specific terms are defined in Table 1.

**Table 1: Terms related to the TOE**

Term	Definition
@Remote	A commercial name of this remote service
Information Received from Devices	A generic name of machine counter information, failure information, and supply information that the TOE receives from the registered device
Boot Loader	Loads the operating system immediately after turning on the power of the TOE.
MIB	An abbreviation of Management Information Base, a type of information of SNMP-controlled network devices. This information is used for disclosure of the current status of the devices.



## 2 Conformance Claims

This chapter describes conformance claims.

### 2.1 CC Conformance Claims

CC conformance claims in this ST and TOE are described as follows:

- CC versions to which this ST claims conformance

Part 1:

Introduction and general model July 2009, Version 3.1 Revision 3 (Japanese translation Ver.1.0)  
CCMB-2009-07-001

Part 2:

Security functional components July 2009, Version 3.1 Revision 3 (Japanese translation Ver.1.0)  
CCMB-2009-07-002

Part 3:

Security assurance components July 2009, Version 3.1 Revision 3 (Japanese translation Ver.1.0)  
CCMB-2009-07-003

- Functional requirements: Part 2 conformant
- Assurance requirements: Part 3 conformant

### 2.2 PP Claims

This ST and TOE do not conform to any PPs.

### 2.3 Package Claims

The package that this ST and TOE conform to is Evaluation Assurance Level EAL3.

### 3 Security Problem Definition

This chapter defines threats, organisational security policies, and assumptions.

#### 3.1 Threats

Identified and defined below are the assumed threats for the TOE and the working environments where the TOE is installed.

**T. FAKE\_CS      Impersonation on the Internet**

Attackers may launch a pseudo CS on the Internet, install device firmware in the registered device, or send malicious programs such as a virus into the LAN.

**T. INTERNET      Tampering of Communication Information on the Internet**

Attackers may disclose or tamper communication data that flows over the Internet when the TOE communicates with the CS.

**T. ACCESS      Unauthorised Access**

Unauthorised persons may perform a TOE operation that is authorised only for the general user or administrator. The general user may accidentally use the Security Management Function that is authorised only for the administrator.

#### 3.2 Organisational Security Policies

This section describes the organisational security policies.

**P.ATR\_DEVICE      Communication with HTTPS-Compatible Devices**

When the TOE communicates with the registered HTTPS-compatible devices for the Machine Counter Notice Function, the Service Call Function, and the Supply Call Function, measures shall be provided at communication start-up to confirm that the HTTPS-compatible devices are valid, and the communication information between the TOE and the registered HTTPS-compatible devices shall be protected.

**P.SOFTWARE      Confirmation of the RC Gate Firmware Integrity**

Procedures shall be provided to confirm that the RC Gate Firmware built into the TOE is a genuine RC Gate Firmware (that is, a manufacturer-genuine RC Gate Firmware).

**P.PC\_WEB      Communication with Computers**

For the Web Function, tampering of the information between computers and the TOE shall be detected and disclosure of passwords shall be prevented.

### **3.3 Assumptions**

This section describes the assumptions of the TOE operations.

**A.ADMINSHIP      Conditions of Administrator**

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

**A.TOE\_ADMIN      Administration of the TOE**

The administrator shall have the necessary knowledge and perform the administrative roles for the secure management and operation of the TOE in the administrators' work. The administrator shall also provide physical protection for the TOE.

**A.NETWORK      Network Management**

The network administrator shall maintain the LAN and instruct network users not to change the communication information between the TOE and registered devices that are not the HTTPS-compatible devices. The network administrator shall also provide protection for the LAN environment from external attackers via the Internet.

**A.DEVICE      Device Management**

The device administrator shall maintain the device connected to the LAN. The genuine and unmodified device shall be acquired and used.

**A.CE      TOE Maintenance**

Only a qualified CE shall be able to maintain the TOE.

## 4 Security Objectives

This chapter describes security objectives for the TOE, security objectives for the operational environment, and security objectives rationale.

### 4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE.

- O.I&A Identification and Authentication**
- For remote operation of the TOE by users (general user and administrator) from a computer's Web browser, the TOE ensures that users are identified and authenticated prior to the remote operation and it ensures that the users are authorised to perform the remote operation of the TOE.
- O.ACCESS Access Restriction**
- The TOE ensures that the protected assets can be accessed by users only according to their roles (general user, administrator).
- O.COM\_CS Protection of Communication Channels with CS**
- The TOE ensures that communication data on the communication path is secured when communicating with a genuine CS. It also ensures detection of data tampering.
- O.COM\_ATR\_DEVICE Protection of Communication Channels with Devices**
- For the Machine Counter Notice Function, the Service Call Function, and the Supply Call Function, the TOE ensures that it communicates with the registered HTTPS-compatible device and secures the communication data on the communication path. It also ensures detection of data tampering.
- O.COM\_OPERATOR Data Protection of Remote Operation by User**
- For remote operation of the TOE by a user from a computer's Web browser, the TOE ensures that communication data on the communication path is secured. It also ensures detection of data tampering.
- O. GENUINE Confirmation of the RC Gate Firmware Integrity**
- The TOE ensures that users can check the RC Gate Firmware built into the TOE is the genuine RC Gate Firmware.

---

## 4.2 Security Objectives for Operational Environment

This section describes security objectives for the operational environment.

### **OE.SUPER Appointment of Administrator Related to the TOE**

Prior to the delivery of the TOE, the organisational responsible manager shall appoint the TOE administrator, the network administrator, and the device administrator. These candidates must be reliable persons in the organisation.

### **OE.ADMIN TOE Management**

Administrators shall understand the TOE guidance, physically protect the TOE, and perform TOE management.

### **OE.NETWORK Network Management**

The network administrator shall instruct network users not to change the communication information between the TOE and registered devices that are not the HTTPS-compatible devices.

The network administrator shall install security systems such as firewalls between the external network and the LAN to protect the LAN environment from external attackers via the Internet.

### **OE.DEVICE Device Management**

The device administrator shall acquire a device from a qualified channel and install it, and manage it, so it cannot be modified.

### **OE.CE CE Confirmation**

For the maintenance of the TOE, administrators shall allow only the qualified CE to maintain it.

### 4.3 Security Objectives Rationale

This section describes the corresponding relationship between security objectives and security problems, which constitute security objectives rationale.

#### 4.3.1 Corresponding Relationship between Security Objectives and Security Problems

Table 2 shows the corresponding relationship for security objectives and security problem definition that includes threats, organisational security policies, and assumptions.

As shown in Table 2, one of the security objectives satisfies the assumption, counters the threat, and fulfils the organisational security policy. Each of the security objectives corresponds to at least one of the assumptions, threats, or organisational security policies.

**Table 2: Corresponding relationship between security objectives and security problems**

	O.I&A	O.ACCESS	O.COM_CS	O.COM_ATR_DEVICE	O.COM_OPERATOR	O.GENUINE	OE.SUPER	OE.ADMIN	OE.NETWORK	OE.DEVICE	OE.CE
T.FAKE_CS			X								
T.INTERNET			X								
T.ACCESS	X	X									
P.ATR_DEVICE				X							
P.SOFTWARE						X					
P.PC_WEB					X						
A.ADMINSHIP							X				
A.TOE_ADMIN								X			
A.NETWORK									X		
A.DEVICE										X	
A.CE											X

---

**T.FAKE\_CS** is countered by O.COM\_CS because the TOE ensures communication with the CS only if the CS is genuine.

**T.INTERNET** is countered by O.COM\_CS because O.COM\_CS enables communication data on the communication path including the Internet between the TOE and the CS to be secured, and it detects data tampering.

**T.ACCESS** is countered by O.I&A and O.ACCESS. Confronted with threats posed by anyone other than the TOE users who access the TOE and other threats posed by the general user who mistakenly performs the TOE operations that are authorised only for the administrator, O.I&A identifies and authenticates users prior to the TOE operation from a computer's Web browser, which is the only way to access TOE management information and to operate the Management Functions. O.I&A allows users to operate the TOE only if such users are successfully authenticated within the preset number of authentication attempts, and O.ACCESS allows the users to manage the TOE management information, according to the user roles.

**P.ATR\_DEVICE** is enforced by O.COM\_ATR\_DEVICE because O.COM\_ATR\_DEVICE allows only the pre-registered device to communicate with the TOE in the Counter Information Notice Function, the Service Call Function, and the Supply Call Function. O.COM\_ATR\_DEVICE also ensures that the protected assets are secured on the communication path between the TOE and the device, and detects data tampering.

**P.SOFTWARE** is enforced by O.GENUINE because users can check that the RC Gate Firmware is the genuine RC Gate Firmware.

**P.PC\_WEB** is enforced by O.COM\_OPERATOR because O.COM\_OPERATOR detects the tampering of TSF data on the LAN and enables passwords to be secured when the Web Function is used.

**A.ADMINSHIP** is upheld by OE.SUPER because according to OE.SUPER, the organisational responsible manager appoints the TOE administrator, the network administrator, and the device administrator from reliable persons in the organisation prior to the delivery of the TOE. For this reason, the appointed person does not use the privileges maliciously.

**A.TOE\_ADMIN** is upheld by OE.ADMIN because according to OE.ADMIN, administrators understand and perform the operational procedures for the management in accordance with the guidance.

**A.NETWORK** is upheld by OE.NETWORK because OE.NETWORK requires the network administrator to instruct network users not to change the communication information between the TOE and registered devices that are not the HTTPS-compatible devices, and to install security systems such as firewalls, and to allow only appropriate communication from the Internet to the LAN, so the LAN can be protected from the Internet.

**A.DEVICE** is upheld by OE.DEVICE because OE.DEVICE requires the device administrator to acquire the device from a qualified channel, so only a genuine device communicates with the TOE, and manage the device, so it cannot be modified.

**A.CE** is upheld by OE.CE because administrators allow a qualified CE only to maintain the TOE for the maintenance.



## **5 Extended Components Definition**

This ST and TOE do not define any extended security requirements, i.e. any new security requirements and security assurance requirements that are not described in the CC conforming claims in "2.1 CC Conformance Claims".

## 6 Security Requirements

This chapter describes security functional requirements, security assurance requirements, and security requirements rationale.

### 6.1 Security Functional Requirements

This section defines the security functional requirements of the TOE. The security functional requirements are cited from the requirements specified in the CC Part 2.

**[Bold typeface and Brackets]** is used for identifying the operations of assignments and selections defined in CC Part 2. Also, brackets and alphabet suffixes such as "(a)" and "(b)" are used for identification of "iterations".

#### 6.1.1 Class FDP: User data protection

##### FDP\_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP\_ACF.1 Security attribute based access control

FDP\_ACC.1.1 The TSF shall enforce the **[assignment: access control policy of TOE management information]** on **[assignment: list of subjects, objects, and operations among subjects and objects shown in Table 3]**.

**Table 3: Subjects, objects, and operations**

Subject	Object	Operations among subjects and objects
User process (The user type is administrator)	Machine counter information area	Viewing
	Call notice history area	Viewing
	Device firmware update history area	Viewing
User process (The user type is general user)	Machine counter information area	Viewing
	Call notice history area	Viewing

##### FDP\_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP\_ACC.1 Subset access control  
FMT\_MSA.3 Static attribute initialisation

FDP\_ACF.1.1 The TSF shall enforce the [assignment: access control policy of TOE management information] to objects based on the following: [assignment: list of subjects and objects shown in Table 4, and for each, security attributes].

**Table 4: Subjects, objects, and security attributes**

Category	Subject or Object	Security Attributes
Subject	User process	User type
Object	Machine counter information area	List of user types
Object	Call notice history area	List of user types
Object	Device firmware update history area	List of user types

FDP\_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access on operations on objects shown in Table 5].

**Table 5: Rules governing access**

Operations on Object	Rules governing access
Viewing of machine counter information area	If one of the user types listed in the list of user types (administrator, general user) that is associated with the machine counter information area is identical to the user type associated with the user process, the user is allowed to view the machine counter information area.
Viewing of call notice history area	If one of the user types listed in the list of user types (administrator, general user) that is associated with the call notice history area is identical to the user type associated with the user process, the user is allowed to view the call notice history area.
Viewing of device firmware update history area	If one of the user types (administrator) listed in the list of user types that is associated with the device firmware update history area is identical to the user type associated with the user process, the user is allowed to view the device firmware update history area.

FDP\_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: no rules, based on security attributes that explicitly authorise access of subjects to objects].

FDP\_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: no rules, based on security attributes that explicitly deny access of subjects to objects].

---

## 6.1.2 Class FIA: Identification and authentication

### FIA\_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA\_UAU.1 Timing of authentication

FIA\_AFL.1.1 The TSF shall detect when [selection: [assignment: 3 (positive integer number)]] unsuccessful authentication attempts occur related to [assignment: identification and authentication within 5 minutes from a computer's Web browser].

FIA\_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met], the TSF shall [assignment: deny for 1 minute to identify and authenticate from computers by user name for administration or user name of general user which have been unsuccessful].

### FIA\_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA\_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: user type, user name of general user].

### FIA\_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA\_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: password composed of 8 to 13 ASCII characters from the following set, enclosed in parentheses  
(SP(space)!"#\$%&'()\*,-./0123456789;<=>?@ABCDEFGHIJKLMNPOQRSTUVWXYZ[¥]^\_`abcdefghijklmnopqrstuvwxyz{|}~)].

### FIA\_UAU.2 User authentication before any action

Hierarchical to: FIA\_UAU.1 Timing of authentication

Dependencies: FIA\_UID.1 Timing of identification

FIA\_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

### FIA\_UAU.6 Re-authenticating

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA\_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: before the administrator is allowed to change the administrator's password].

**FIA\_UID.2 User identification before any action**

Hierarchical to: FIA\_UID.1 Timing of identification

Dependencies: No dependencies.

FIA\_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

**FIA\_USB.1 User-subject binding**

Hierarchical to: No other components.

Dependencies: FIA\_ATD.1 User attribute definition

FIA\_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[assignment: user type, user name of general user]**.

FIA\_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: rules for the initial association of attributes listed in Table 6]**.

**Table 6: Rules for the initial association of attributes**

User	Subject on behalf of users	Rules for the initial association of security attributes
Administrator	User process	Set administrator to the user type. Clear user name.
General user	User process	Set general user to the user type. Set user name of general user to the user name.

FIA\_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: no rules for the changing of attributes]**.

**6.1.3 Class FMT: Security management**

**FMT\_MTD.1 Management of TSF data**

Hierarchical to: No other components.

Dependencies: FMT\_SMR.1 Security roles

FMT\_SMF.1 Specification of Management Functions

FMT\_MTD.1.1 The TSF shall restrict the ability to **[selection: modify, delete [assignment: newly create]]** the **[assignment: TSF data in Table 7]** to **[assignment: user type in Table 7]**.

**Table 7: List of TSF information management**

<b>TSF Data</b>	<b>Operation</b>	<b>User Type</b>
Administrator's password	Modify	Administrator
General user's user name	Newly create, delete	Administrator
General user's password	Newly create, modify, delete	Administrator
CE Access Permission Settings	Modify	Administrator
Device Firmware Update Permission Settings	Modify	Administrator
RC Gate Firmware Update Permission Settings	Modify	Administrator

**FMT\_SMF.1 Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT\_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: management functions listed in Table 8].

**Table 8: List of specification of management functions**

<b>Management Function</b>
Modify administrator's password by administrator
Newly create and delete the general user's user name by administrator
Newly create, modify, and delete the general user's password by administrator
Modify CE Access Permission Settings by administrator
Modify Device Firmware Update Permission Settings by administrator
Modify RC Gate Firmware Update Permission Settings by administrator

**FMT\_SMR.1 Security roles**

Hierarchical to: No other components.

Dependencies: FIA\_UID.1 Timing of identification

FMT\_SMR.1.1 The TSF shall maintain the roles of [assignment: administrator].

FMT\_SMR.1.2 The TSF shall be able to associate users with roles.

**6.1.4 Class FPT: Protection of the TSF**

**FPT\_STM.1 Reliable time stamps**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT\_STM.1.1 The TSF shall be able to provide reliable time stamps.

**FPT\_TST.1 TSF testing**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT\_TST.1.1 The TSF shall run a suite of self tests [**selection: at the request of the authorised user**] to demonstrate the correct operation of [**selection: [assignment: Communication Protection Function between the TOE and CS]**].

FPT\_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [**selection: TSF data**].

FPT\_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [**selection: TSF**].

**6.1.5 Class FTA: TOE access****FTA\_SSL.3 TSF-initiated termination**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA\_SSL.3.1 The TSF shall terminate an interactive session after [**assignment: the fixed auto logout time (5 minutes) from the last operation of the administrator and the general user after login from a Web browser**].

**6.1.6 Class FTP: Trusted path/channels****FTP\_ITC.1 (a) Inter-TSF trusted channel**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP\_ITC.1.1 (a) The TSF shall provide a communication channel between itself and another trusted IT product (**detailed: CS**) 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 (a) The TSF shall permit [**selection: the TSF**] to initiate communication via the trusted channel.

FTP\_ITC.1.3 (a) The TSF shall initiate communication via the trusted channel for [**assignment: list of functions described in Table 9**]

**Table 9: Functions requiring trusted channels for communication between the RC Gate and CS (a)**

Function
Machine Counter Notice Function
Service Call Function
Supply Call Function
Device Firmware Update Function
RC Gate Firmware Update Function

**FTP\_ITC.1 (b) Inter-TSF trusted channel**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP\_ITC.1.1 (b) The TSF shall provide a communication channel between itself and another trusted IT product (**detailed: the registered HTTPS-compatible device**) 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 (b) The TSF shall permit [**selection: the TSF, another trusted IT product**] to initiate communication via the trusted channel.

FTP\_ITC.1.3 (b) The TSF shall initiate communication via the trusted channel for [**assignment: list of functions described in Table 10**].

**Table10: Functions requiring trusted channels for communication between the RC Gate and the registered HTTPS-compatible device (b)**

Function
Machine Counter Notice Function
Service Call Function
Supply Call Function

**FTP\_TRP.1 Trusted path**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP\_TRP.1.1 The TSF shall provide a communication path between itself and [**selection: remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**selection: modification, disclosure**].

FTP\_TRP.1.2 The TSF shall permit [**selection: remote users**] to initiate communication via the trusted path.

FTP\_TRP.1.3 The TSF shall require the use of the trusted path for [**selection: [assignment: remote operation of the TOE by a user using a computer's Web browser]**].



## 6.2 Security Assurance Requirements

The Evaluation Assurance Level of this TOE is EAL3. Table 11 lists the TOE assurance components. This list demonstrates a set of components defined by EAL3 of the Evaluation Assurance Level. No additional requirements were added to this list.

**Table11: TOE security assurance requirements (EAL3)**

Assurance Class	Assurance Component	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing-sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

## 6.3 Security Requirements Rationale

This section shows that the security functional requirements in "6.1 Security Functional Requirements" are valid because tracing, justification of traceability, and dependency are satisfied.

**6.3.1 Tracing**

Table 12 demonstrates the corresponding relationship between security objectives and functional requirements for the TOE respectively. The TOE security functional requirements trace back to one or more security objectives of the TOE (tracing). The "X" marks in the table indicate the corresponding relation.

**Table12: Relationship between security objectives and functional requirements**

	O. I&A	O.ACCESS	O.COM_CS	O.COM_ATR_DEVICE	O.COM_OPERATOR	O.GENUINE
FDP_ACC.1		X				
FDP_ACF.1		X				
FIA_AFL.1	X					
FIA_ATD.1	X					
FIA_SOS.1	X					
FIA_UAU.2	X					
FIA_UAU.6	X					
FIA_UID.2	X					
FIA_USB.1	X					
FMT_MTD.1		X				
FMT_SMF.1		X				
FMT_SMR.1		X				
FPT_TST.1						X
FTA_SSL.3	X					
FTP_ITC.1(a)			X			
FTP_ITC.1(b)				X		
FTP_TRP.1					X	

**6.3.2 Justification of Traceability**

This subsection shows that the security functional requirements of the TOE satisfy the security objectives for the TOE.

**O.I&A Identification and Authentication**

O.I&A is a security objective that allows only general users or administrators to operate the TOE remotely. To fulfil this security objective, the following countermeasures must be satisfied:

- (1) A user who remotely operates the TOE shall be successfully identified and authenticated.  
According to FIA\_UID.2, the person who tries to remotely operate the TOE is identified as a user. According to FIA\_UAU.2, it is required that the identified user be successfully authenticated.
- (2) The successfully authenticated user can remotely operate the TOE during the session.  
According to FIA\_USB.1, the general user and administrator must be associated with the user process, with which the user type and security attributes of the user name are associated. According to FIA\_ATD.1, the general user or the administrator is allowed to remotely operate the TOE by maintaining these security attributes.
- (3) The TOE terminates the session of the TOE remote operation automatically.  
According to FTA\_SSL.3, if the successfully authenticated user does not operate the computer for a certain period of time, the computer automatically logs off. Because of this functionality, if the successfully authenticated user is not available for operations during the session, unauthorised users are less likely to remotely operate the TOE from the computer.
- (4) The TOE makes it difficult to decode login passwords of general users and administrators.  
According to FIA\_SOS.1, passwords must be secure by using a number of characters and a combination of character types that are not guessable. According to FIA\_AFL.1, no sufficient time to decode passwords shall be given.
- (5) The TOE re-authenticates users before changing the administrator's password.  
To prevent users other than the administrator from changing the administrator's password, according to FIA\_UAU.6, users shall be re-authenticated before changing administrator's password.

The necessary countermeasures to fulfil O.I&A are (1), (2), (3), (4), and (5). Therefore, O.I&A is fulfilled by accomplishing FIA\_AFL.1, FIA\_ATD1, FIA\_SOS.1, FIA\_UAU.2, FIA\_UAU.6, FIA\_UID.2, FIA\_USB.1, and FTA\_SSL.3 considered as the necessary security functional requirements for these countermeasures.

**O.ACCESS Access Restriction**

O.ACCESS is a security objective to control the access to protected assets in accordance with user types of users. To fulfil this security objective, the following countermeasures must be satisfied:

- (1) The TOE specifies and performs the access control for the machine counter information area, the call notice history area and the device firmware update history area.  
By FDP\_ACC.1 and FDP\_ACF.1, according to the access control policy of the TOE management information, if the user type associated with user process is administrator, the user is allowed to view machine counter information area, the call notice history area, and the device firmware update history area. If the user type is general user, the user is allowed to view the machine counter information area and call notice history area.
- (2) The TOE allows only the administrator to perform the security management.  
According to FMT\_MTD.1 and FMT\_SMF.1, only the administrator is allowed to manage the TSF data.

- (3) The TOE maintains user type.

According to FMT\_SMR.1, the identified and authenticated administrator is allowed to maintain its administrator role during the session and perform the Security Management Function.

The necessary countermeasures to fulfil O.ACCESS are (1), (2), and (3). Therefore, O.ACCESS is fulfilled by accomplishing FDP\_ACC.1, FDP\_ACF.1, FMT\_MTD.1, FMT\_SMF.1, and FMT\_SMR.1 considered as the necessary security functional requirements for these countermeasures.

#### **O.COM\_CS      Protection of Communication Channels with CS**

O.COM\_CS is a security objective to assure communications with the genuine CS, secure communication data when communicating with the CS, and to detect data tampering. To fulfil this security objective, the following countermeasures must be satisfied:

- (1) The TOE communicates with the genuine CS.

According to FTP\_ITC.1 (a), establish the communication channels to provide the function to identify the CS in the communication between the TOE and the CS, and verify the correctness of the CS.

- (2) The TOE protects the communication data with the CS.

According to FTP\_ITC.1 (a), establish the reliable communication channels in the communication between the TOE and the CS, and prevent disclosure of protected assets on the communication path and detect the tampering of data.

The necessary countermeasures to fulfil O.COM\_CS are (1) and (2). Therefore, O.COM\_CS is fulfilled by accomplishing FTP\_ITC.1 (a) considered as the necessary security functional requirements for these countermeasures.

#### **O.COM\_ATR\_DEVICE                      Protection of Communication Channels with Devices**

O.COM\_ATR\_DEVICE is a security objective to ensure that for the Counter Information Notice Function, the Service Call Function, and the Supply Call Function, the TOE communicates with the registered devices and it secures the communication data between the registered HTTPS-compatible devices and the TOE in the LAN to detect data tampering. To fulfil this security objective, the following countermeasures must be satisfied:

- (1) The TOE communicates with the genuine and registered HTTPS-compatible device.

According to FTP\_ITC.1 (b), establish the communication channels to provide the function to identify HTTPS in the communication between the TOE and the registered HTTPS-compatible device, and verify the correctness of the registered HTTPS-compatible device.

- (2) The TOE protects the communication data with the registered HTTPS-compatible devices.

According to FTP\_ITC.1 (b), establish the reliable communication channels in the communication between the TOE and the registered HTTPS-compatible devices, secure the communication data on the communication path, and detect data tampering.

The necessary countermeasures to fulfil O.COM\_ATR\_DEVICE are (1) and (2). Therefore, O.COM\_ATR\_DEVICE is fulfilled by accomplishing FTP\_ITC.1 (b) considered as the necessary security functional requirements for these countermeasures.

**O.COM\_OPERATOR Data Protection of Remote Operation by User**

O.COM\_OPERATOR is a security objective to enable communication data on the communication path in the communication of the TOE remote operation by using a computer's Web browser by users to be secured. It also ensures detection of data tampering. To fulfil this security objective, the following countermeasure must be satisfied:

- (1) The TOE protects data for the bilateral communication between the TOE and users operating the Web Function.

According to FTP\_TRP.1, communicate with a trusted path between the TOE and computers that are used for the remote operation and secure the communication data on the communication path. It also detects data tampering.

The necessary countermeasure to fulfil O.COM\_OPERATOR is (1). Therefore, O.COM\_OPERATOR is fulfilled by accomplishing FTP\_TRP.1 considered as the necessary security functional requirements for this countermeasure.

**O.GENUINE Confirming the Integrity of RC Gate Firmware**

O.GENUINE is a security objective to ensure that RC Gate Firmware built in the TOE is the genuine RC Gate Firmware. To fulfil this security objective, the following countermeasure must be satisfied:

- (1) The TOE checks the integrity of the RC Gate Firmware.

According to FPT\_TST.1, verify the integrity of executable codes of the RC Gate Firmware at the request of the authorised user and verify that it is the genuine RC Gate Firmware.

The necessary countermeasure to fulfil O.GENUINE is (1). Therefore, O.GENUINE is fulfilled by accomplishing FPT\_TST.1 considered as the necessary security functional requirements for this countermeasure.

**6.3.3 Dependency Analysis**

Table 13 demonstrates the corresponding status of dependencies for security functional requirements of the TOE. For security functional requirements of the TOE that do not satisfy any dependencies, the verifiable rationale of the dependencies is specified.

**Table13: Corresponding table of dependencies for the TOE security functional requirements**

TOE Security Functional Requirement	Dependency required by the CC	Dependency satisfied in the ST	Dependency not satisfied in the ST
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	N/A
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1	FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	N/A
FIA_ATD.1	N/A	N/A	N/A
FIA_SOS.1	N/A	N/A	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2	N/A

TOE Security Functional Requirement	Dependency required by the CC	Dependency satisfied in the ST	Dependency not satisfied in the ST
FIA_UAU.6	N/A	N/A	N/A
FIA_UID.2	N/A	N/A	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	N/A
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	N/A
FMT_SMF.1	N/A	N/A	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2	N/A
FPT_TST.1	N/A	N/A	N/A
FTA_SSL.3	N/A	N/A	N/A
FTP_ITC.1 (a)	N/A	N/A	N/A
FTP_ITC.1 (b)	N/A	N/A	N/A
FTP_TRP.1	N/A	N/A	N/A

Described below is the rationale for dependencies whose functional requirements are not necessarily satisfied:

**The reason for removing the dependencies from FDP\_ACF.1 to FMT\_MSA.3.**

The security attributes of objects (the machine counter information area, the call notice history area, and the device firmware update history area) are fixed, so they are not initialised. The security attributes of subject (user process) are fixed, so they are not initialised. Therefore, FMT\_MSA.3 is not required.

**6.4 Security Assurance Requirements Rationale**

This TOE is a commercial product used in general office environments. It is assumed to attack from the Internet by attackers who have a basic capability, and it is assumed that protected assets are disclosed and modified by misuse of the TOE in the office.

To respond to such attacks, the TOE security assurance requirements include the evaluation of the TOE design, the evaluation of securely using the TOE as described in the guidance, and since the confidentiality of the relevant information are protected to make such attacks more difficult, it also includes that the secure development environment is evaluated. All dependencies of assurance requirements are met because these assurance requirements conform to EAL3. Therefore, EAL3 is appropriate.

## 7 TOE Summary Specification

This chapter describes each security functional requirement for the methods and mechanisms of the TOE that satisfy the security functional requirements described in 6.1.

### **FDP\_ACC.1 Subset access control**

The TOE enforces the access control policy of the TOE management information. The access control policy of the TOE management information is an access control policy that allows the administrator and the general user to view the machine counter information area and the call notice history area. It also allows the administrator to view the device firmware update history area.

### **FDP\_ACF.1 Security attribute based access control**

The TOE provides the successfully identified and authenticated user with the screen to view the machine counter information area and the call notice history area. If the user type of the successfully identified and authenticated user is administrator, it also provides the user with the screen to view the device firmware update history area. The TOE does not implement any interfaces to modify or delete the machine counter information area, the call notice history area, and the device firmware update history area.

### **FIA\_AFL.1 Authentication failure handling**

The TOE counts the number of the authentication failure attempts within five minutes for each user from a computer's Web browser. A user who fails to login three times will not be authenticated for the next one minute even if the user enters the correct password that satisfies the requirements of the Identification and Authentication Function. If the user is successfully authenticated, the TOE resets to 'ZERO' the number of the failure attempts of the user.

### **FIA\_ATD.1 User attribute definition**

The TOE maintains the user type that the user selects for identification and authentication until session termination. If the user is general user, the TOE associates and maintains the user type with the user name of the general user for identification and authentication.

### **FIA\_SOS.1 Verification of secrets**

When the administrator intends to change passwords of the administrator and general user, the TOE checks if a new password satisfies the conditions specified in (1) and (2). If both of these conditions are met, the TOE registers the new password. Otherwise, an error message will appear without registering the login password.

(1) Characters that can be used: the following ASCII characters

```
SP(space)!"#$%&'()*+,-./0123456789:;<=>?@`{|}~  
ABCDEFGHIJKLMNPOQRSTUVWXYZ[¥]^_  
abcdefghijklmnopqrstuvwxyz
```

(2) Required number of characters: 8-13 characters.

**FIA\_UAU.2 User authentication before any action**

The TOE displays the login screen for the user who attempts to use it from a computer's Web browser. In the login screen, there is the entering area for their user type, user name, and password. The administrator enters their user type and password and the general user enters their user type, user name, and password. The TOE does not display other screens until the user is successfully authenticated.

**FIA\_UAU.6 Re-authenticating**

The TOE displays the administrator screen for password change and requires the administrator to enter the current password if the administrator chooses to change it, and the TOE re-authenticates the administrator using the entered password.

**FIA\_UID.2 User identification before any action**

The TOE displays the login screen to enter the user type, the user name, and the password if the user attempts to use it from a computer's Web browser. The TOE does not display other screens until the user is successfully authenticated.

**FIA\_USB.1 User-subject binding**

The TOE associates the user process with the user who is successfully identified and authenticated. The user process associates the user type and the user name as security attributes.

**FMT\_MTD.1 Management of TSF data**

The TOE provides the screen to perform the following operations on TSF data, only if the user type of the successfully identified and authenticated user is administrator:

- Change administrator's password
- Newly create and delete general user's user name
- Newly create, change, and delete general user's password
- Change the CE Access Permission Settings
- Change the Device Firmware Update Permission Settings
- Change the RC Gate Firmware Update Permission Settings

**FMT\_SMF.1 Specification of Management Functions**

The TOE provides the screen to perform the following operations, only if the user type of the successfully identified and authenticated user is administrator:

- Change administrator's password by administrator
- Newly create and delete general user's user name by administrator
- Newly create, change, and delete general user's password by administrator
- Change CE Access Permission Settings by administrator
- Change Device Firmware Update Permission Settings by administrator
- Change RC Gate Firmware Update Permission Settings by administrator



**FMT\_SMR.1 Security roles**

The TOE maintains the user type (administrator) associated with the user process that is associated with administrator who is successfully identified and authenticated until session termination from the Web browser after being successfully identified and authenticated.

**FPT\_TST.1 TSF testing**

The TOE runs a suite of self tests at the request of the administrator to demonstrate the correct operation of the Communication Protection Function between the TOE and CS. The TOE also runs a suite of self tests to verify the integrity of executable codes in TSF data and the RC Gate Firmware.

**FTA\_SSL.3 TSF-initiated termination**

The TOE provides functions that force the user to log off automatically when the fixed auto logout time (five minutes) elapses after the last user operation from the Web browser.

**FTP\_ITC.1 (a) Inter-TSF trusted channel**

The TOE communicates with the CS using SSL and verifies that the CS is certified, and provides SSL cryptographic communications for communications via the LAN between the TOE and the CS. The encrypted communication can be used for the Machine Counter Notice Function, the Service Call Function, the Supply Call Function, the Device Firmware Update Function, and the RC Gate Firmware Update Function.

**FTP\_ITC.1 (b) Inter-TSF trusted channel**

The TOE communicates with HTTPS-compatible devices using SSL and verifies that the HTTPS-compatible devices are certified, and provides SSL cryptographic communications between the TOE and the registered HTTPS-compatible devices. The encrypted communication can be used for the Machine Counter Notice Function, the Service Call Function, and the Supply Call Function.

**FTP\_TRP.1 Trusted path**

The TOE provides SSL cryptographic communications between the TOE and computers by SSL communication for remote access from a computer's Web browser.