RICOH Remote Communication Gate A2

Security Target

Author : RICOH COMPANY, LTD.
Date : 2016-11-10
Version : 0.42

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

Revision History

Version	Date	Author	Description
0.10	2013-07-23	RICOH COMPANY, LTD.	First edition.
0.11	2014-02-19	RICOH COMPANY, LTD.	Deleted the term "general user" from the following sections and a figure. - 1.4.3 Definitions of the Related Roles - 1.4.5 Protected Assets - 3.1 Threats - Figure 3: Logical Scope of the TOE
0.12	2014-02-19	RICOH COMPANY, LTD.	Added Email Notice Function.
0.13	2014-10-27	RICOH COMPANY, LTD.	- Added Chapter 4 and later.
0.14	2014-11-12	RICOH COMPANY, LTD.	Modified the following chapters so that the written format is close to cPP. - Chapter 3 - Chapter 4
0.15	2014-11-17	RICOH COMPANY, LTD.	Modified the following chapters so that the written format is close to cPP. - Chapter 5 - Chapter 6 - Chapter 7
0.16	2014-11-20	RICOH COMPANY, LTD.	Added information regarding S/MIME when using Email Notice Function.
0.17	2014-11-27	RICOH COMPANY, LTD.	Fixed the distortion of Figure 2 occurred when printing it.
0.18	2015-02-09	RICOH COMPANY, LTD.	- Responded to the evaluator's comments RDZ-ASE_COM-0001-00 No.1 through 21. - Moved the Organisational Security Policies section under the Threats section.
0.19	2015-02-17	RICOH COMPANY, LTD.	- Responded to the evaluator's comments RDZ-ASE_COM-0001-01 No.12, No.22 through 27, 30, and 32 through 36.
0.20	2015-02-24	RICOH COMPANY, LTD.	Modified the description of FPT_FUD in Section 5.1 and related description. Corrected the TSS description of FAU_GEN.1 in Chapter 7.

0.21	2015-02-26	RICOH COMPANY, LTD.	- Responded to the evaluator's comments RDZ-ASE_ECOM-0001-02 No.37 through 40.
0.22	2015-03-09	RICOH COMPANY, LTD.	Corrected an erroneous description of FPT_FUD.2. Chapter 5.1, Section 6.1.5, and Chapter 7
0.23	2015-04-30	RICOH COMPANY, LTD.	- Responded to the evaluator's comments RDZ-ECOM-ASE-0001-03 No.34 through 42.
0.24	2015-05-14	RICOH COMPANY, LTD.	- Responded to the comment RDZ-ERE-0003-00.
0.25	2015-06-29	RICOH COMPANY, LTD.	- Deleted the Device Firmware Update History from the Protected Assets section because it is no longer used in TOE. - Changed from FTP_SSL.3 to FTP_SSL.1 because the system locks the screen and does not log out automatically when there is no operation from a computer. - Responded to the comment RDZ-ECOM_ASE-0001-04.
0.26	2015-07-24	RICOH COMPANY, LTD.	- Responded to the comment RDZ-ECOM_ASE-0001-07.
0.27	2015-07-30	RICOH COMPANY, LTD.	- Responded to the comment RDZ-ECOM_ASE-0001-08.
0.28	2015-08-07	RICOH COMPANY, LTD.	- Responded to the comment RDZ-ECOM_ASE-0001-09.
0.29	2015-08-07	RICOH COMPANY, LTD.	Deleted the Access Control Function from Figure 3.
0.30	2015-08-21	RICOH COMPANY, LTD.	Added a SMTP server to Figure 1.
0.31	2015-10-16	RICOH COMPANY, LTD.	- Responded to the comments RDZ-ECOM_ASE-0001-10 No.119 and 120.
0.32	2015-12-17	RICOH COMPANY, LTD.	Responded to the comment RDZ-ECOM_ASE-0001-10 No.121.
0.33	2016-01-08	RICOH COMPANY, LTD.	- Responded to the comments RDZ-ECOM_ASE-0001-12 No.122 through 130.
0.34	2016-01-13	RICOH COMPANY, LTD.	Added the name of guidance documents. Corrected erroneous descriptions.

0.35	2016-02-09	RICOH COMPANY, LTD.	- Responded to the comments RDZ-ECOM_ASE-0001-12 No.131 and 132. - Changed the version number of the TOE in accordance with the update of the TOE.
0.36	2016-03-16	RICOH COMPANY, LTD.	- Changed the revision number of guidance documents.
0.37	2016-05-19	RICOH COMPANY, LTD.	- Responded to the comments RDZ-ECOM_ASE-0001-14 No.133 through 137.
0.38	2016-05-23	RICOH COMPANY, LTD.	- Responded to the comments RDZ-ECOM_ASE-0001-15 No.138 through 143.
0.39	2016-07-05	RICOH COMPANY, LTD.	- Corrected typographical errors. - Corrected information related to audit.
0.40	2016-08-25	RICOH COMPANY, LTD.	- Corrected typographical errors. - Corrected information related to audit.
0.41	2016-09-15	RICOH COMPANY, LTD.	- Corrected the guidance documents list.
0.42	2016-11-10	RICOH COMPANY, LTD.	- Corrected the description of threats - Corrected typographical errors. 1.4.4.2 Security Functions 2.1 CC Conformance Claims - Corrected figure/table numbers

Table of Contents

1 ST Introduction 7
1.1 ST Reference 7
1.2 TOE Reference 7
1.3 TOE Overview 7
1.3.1 TOE Type 7
1.3.2 TOE Usage 7
1.3.3 Major Security Functions of TOE 9
1.4 TOE Description 10
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
1.5 Glossary 16
2 Conformance Claims 17
2.1 CC Conformance Claims 17
2.2 PP Claims 17
2.3 Package Claims 17
3 Security Problem Definition 18
3.1 Threats 18
3.2 Organisational Security Policies 19
3.3 Assumptions 19
4 Security Objectives 20
4.1 Security Objectives for the TOE 20
4.2 Security Objectives for Operational Environment 21
4.3 Security Objectives Rationale 21
4.3.1 Corresponding Relationship between Security Objectives and Security Problems 21
5 Extended Components Definition 25
5.1 Trusted Firmware Update (FPT_FUD) 25
6 Security Requirements 27
6.1 Security Functional Requirements 27
6.1.1 Class FAU: Security Audit 27
6.1.2 Class FIA: Identification and authentication 31
6.1.3 Class FMT: Security management 33
6.1.4 Class FPT: Protection of the TSF 34
6.1.5 Class FTA: TOE access 35
6.1.6 Class FTP: Trusted path/channels 35

6.2 Security Assurance Requirements 37
6.3 Security Requirements Rationale 38
6.3.1 Tracing 38
6.3.2 Justification of Traceability 40
6.3.3 Dependency Analysis 43
6.4 Security Assurance Requirements Rationale 44
7 TOE Summary Specification 45

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: List of auditable events....27
Table 4: Rules for the initial association of attributes....32
Table 5: List of TSF information management....33
Table 6: List of specification of management functions....34
Table 7: Functions requiring trusted channels for communication between the RC Gate A2 and CS (a)36
Table 8: Functions requiring trusted channels for communication between the RC Gate A2 and Registered HTTPS-compatible device (b)....36
Table 9: TOE security assurance requirements (EAL2+ALC_FLR.2)....37
Table 10: Relationship between security objectives and functional requirements....39
Table 11: Correspondence table of dependencies for the TOE security functional requirements....43

1 ST Introduction

This chapter describes the ST Reference, TOE Reference, TOE Overview, TOE Description and Glossary.

1.1 ST Reference

The ST identification information shows as follows:

ST Title:	RICOH Remote Communication Gate A2 Security Target
ST Version:	0.42
Date:	2016-11-10
Author:	RICOH COMPANY, LTD.

1.2 TOE Reference

The following describes the identification information for RICOH Remote Communication Gate A2 (hereinafter referred to as "RC Gate A2"), which is the TOE:

Manufacturer:	RICOH COMPANY, LTD.
Product Name:	RICOH Remote Communication Gate A2
Firmware Version:	V1.0.2

1.3 TOE Overview

This section describes the TOE Type, TOE Usage, Major Security Functions of TOE.

1.3.1 TOE Type

The TOE is an IT device to be used for @Remote Service that remotely maintains digital MFPs and printers (hereinafter referred to as "devices") from the communication server (herein after referred to as "CS") in the maintenance centre. The TOE is installed between the CS and the devices that use @Remote Service (hereinafter referred to as "@Remote-supported devices") to intermediate the information required to provide the @Remote Service.

1.3.2 TOE Usage

The TOE is used by connecting to the LAN that the @Remote-supported devices are connected. Users can access and operate the TOE by using a Web browser. The connection image of the TOE is shown in Figure 1 and the TOE and non-TOE configuration items are described below.

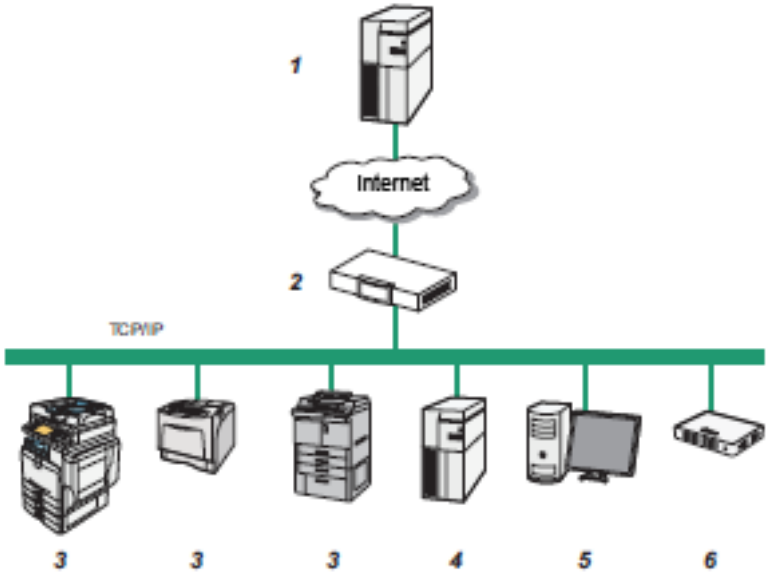


Figure 1: Connection figure of the TOE

1. CS (Communication Server)

   A server located in the maintenance centre. This server uses the TOE to send and receive information, which is required to provide @Remote Service, from @Remote-supported devices. The communication with the TOE is enabled only when the TOE requests it.

2. Firewalls

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

3. Devices[1]

   The devices here means digital MFPs and printers that can communicate with the TOE (hereinafter referred to as "@Remote-supported devices"), including the devices that are not manufactured by RICOH. The RICOH devices with the remote management function are referred to as HTTPS-compatible devices. The non-RICOH devices that do not have remote management function and that have the SNMP function are referred to as "SNMP-compatible devices". If a device is the HTTPS-compatible device, the RICOH Web site and the manual of the device describes that the device supports the remote management function.

   The devices that are registered as the target of @Remote Service on the TOE are referred to as "@Remote-supported devices".

   Moreover, the HTTPS-compatible devices and SNMP-compatible devices that use the @Remote Service are referred to as "Registered HTTPS-compatible devices" and "Registered SNMP-compatible devices" respectively. The communication between the TOE and Registered HTTPS-compatible devices are protected.

4. SMTP Server

   A server used for mail transfer when the TOE sends an email. The TOE sends the machine counter

[1] The following three devices (the HTTPS-compatible devices) are used for CC evaluation: RICOH MP C305, RICOH IPSiO SP 8300, and RICOH MP C40.

information, failure information, and supply information to the CS via email address specified on the TOE by the administrator.

5. Computer
   A personal 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 8 or later and Firefox 28.8 or later[2].
6. RC Gate A2
   RC Gate A2 is the TOE that is connected to the office LAN environment. Note that, as non-TOE configuration items, optional SD card (herein after referred to as "SD Card Option", whose product name is "RICOH Remote Communication Gate A2 Storage 1000") can be installed in the TOE. When the SD Card Option is installed in the TOE, this case is also included as the operational environment of the TOE.

1.3.3 Major Security Functions of TOE

The major security functions of the TOE are the Communication Data Protection Function, the User Access Restriction Function, the RC Gate A2 Firmware Verification Function, the Security Management Function, and the Audit Logging Function.
The Communication Data Protection Function is a function to protect the communication path between the TOE and the maintenance centre, computers, and the Registered HTTPS-compatible devices. The function also protects information in emails sent from the TOE.
The User Access Restriction Function is a function to perform user identification and authentication (hereinafter referred to as "User Identification") for users who attempt to use the TOE from computers, and to permit the TOE operation to the authorised users who are successfully identified and authenticated.
The RC Gate A2 Firmware Verification Function is a function to confirm that the firmware of the TOE received via network is manufacturer-genuine.
Security Management Function is a function to permit authorised users to set the TOE setting.
The Audit Logging Function is a function to record logs, and to provide the specified users with the logs.

[2] In the CC evaluation configuration, both Internet Explore and Firefox are assumed to be used as an available Web browser. The browsers used for the CC evaluation test are Internet Explorer 8/9/10/11 and FireFox 44.0.2.

1.4 TOE Description

This section describes 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.

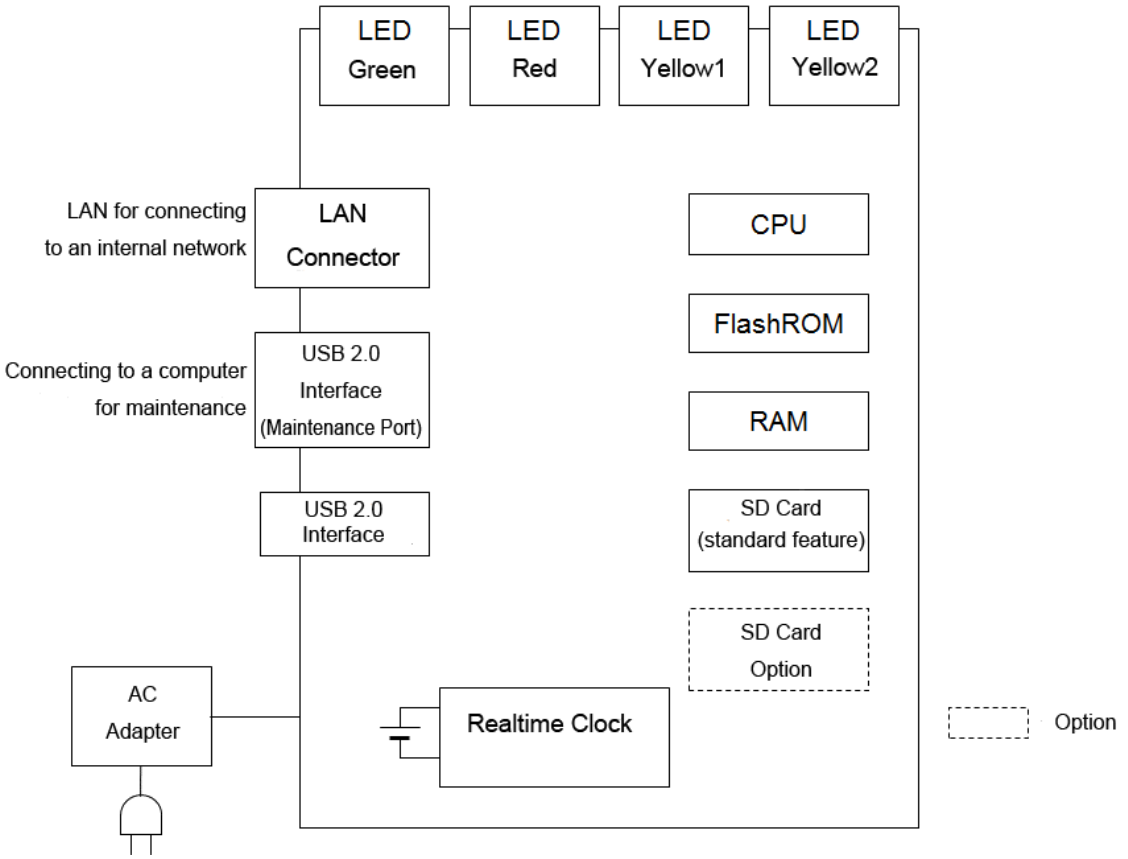


Figure 2: Hardware configuration of the TOE

CPU

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

FlashROM

A non-volatile semiconductor memory that stores boot loader data and certificate. No data will be lost even if the power is turned off.

RAM

A volatile semiconductor memory that is used by the TOE to store data temporarily.

SD Card (standard feature)

A non-volatile semiconductor memory in which the RC Gate A2 Firmware (applications, software common components, platforms, and OSs) and initial information are recorded at the factory. When operating, it is used as temporary storage memory for audit log and @Remote-supported device data.

SD Card Option

An optional non-volatile semiconductor memory. It is used to expand the number of managed @Remote-supported devices. When operating, data in the expanded @Remote-supported devices is recorded.

Realtime Clock

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

LAN Connector

A LAN Connector for connecting to an internal network used for communicating with computers, the CS, and @Remote-supported devices.

USB 2.0 Interface (Maintenance Port)

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

USB 2.0 Interface

A USB Connector to connect an optional 3G module.

LED (green, red, yellow1, yellow2)

Lamps that lit, unlit, flash slowly, and flash rapidly to show the TOE status and error status.

AC Adapter

A power device to supply electric power.

1.4.2 Guidance Documents

The guidance documents consisting of this TOE are as follows:

Guidance documents for the TOE users in Japan

- Remote Communication Gate A2 Safety Information (D3AR-8500) (written in Japanese)
- Remote Communication Gate A2 Setup Guide (D3AR-8520) (written in Japanese)
- Remote Communication Gate A2 Operating Instructions (D3AR-8540C) (written in Japanese)

Guidance documents for the TOE users in North America

- Remote Communication Gate A2 Safety Information (D3AR-8610)

Guidance documents for the TOE users in Europe

- Remote Communication Gate A2 Safety Information (D3AR-8600)

Guidance documents for the TOE users in North America and Europe

- Remote Communication Gate A2 Setup Guide (D3AR-8620)
- Remote Communication Gate A2 Operating Instructions (D3AR-8640C)

1.4.3 Definitions of the Related Roles

The related roles to the TOE are defined as follows:

Administrator

Administrator means a users' administrator who manages the TOE. The administrator can change the settings, view the status of the TOE, and view the audit logs from a computer. When this ST simply refers to "administrator", it indicates an administrator of this TOE.

Device administrator

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

CE

Customer engineer (CE) is a person who is educated to handle the TOE and performs the maintenance of the TOE under the instruction of the administrator.

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.

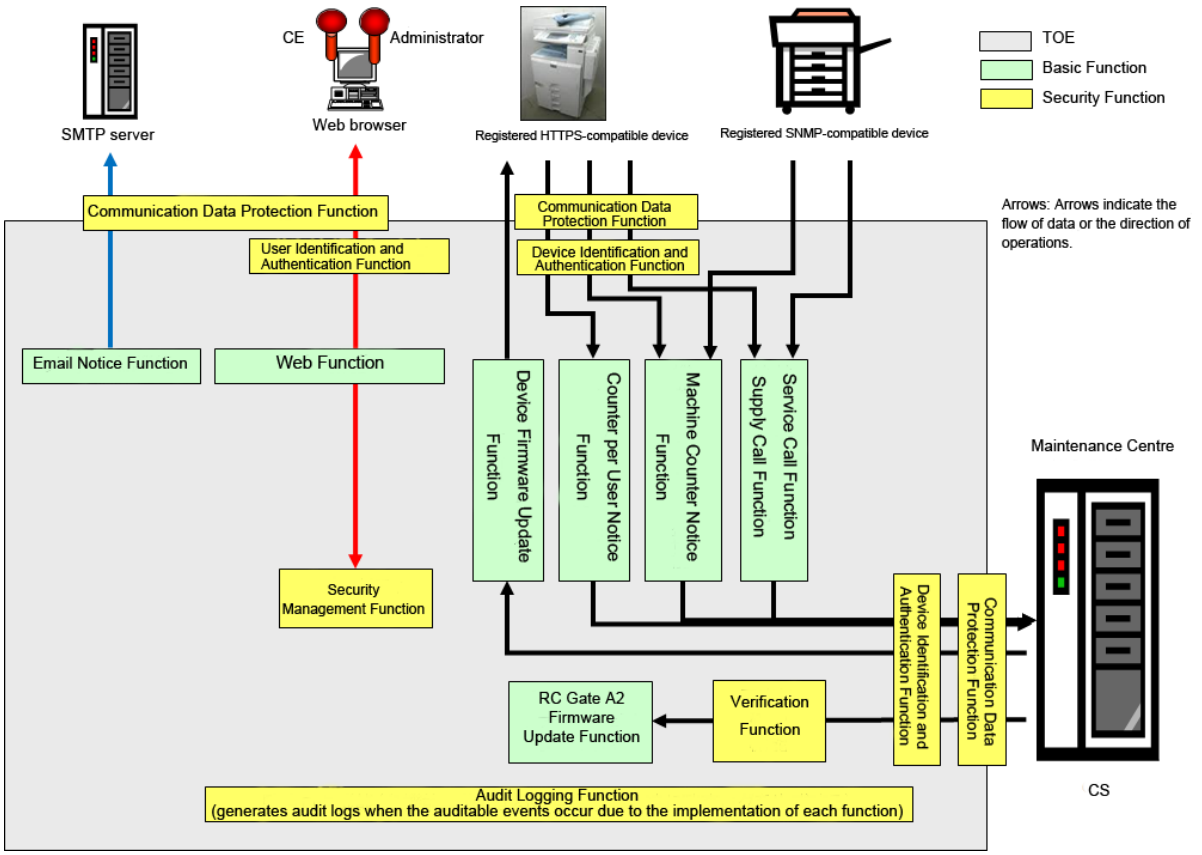


Figure 3: Logical scope of the TOE

1.4.4.1 Basic Functions

Service Call Function

A function that allows the TOE to report the device failure information received from the Registered HTTPS-compatible device and the Registered SNMP-compatible device to the CS.

Machine Counter Notice Function

A function that allows the TOE to periodically notify the CS of the number of print pages for each device (hereinafter referred to as "machine counter information"), which are received from the Registered HTTPS-compatible device and the Registered SNMP-compatible device.

Counter per User Retrieval Function

A function that regularly notifies the CS of counter information on a per-user basis (the number of print pages counted for each user) that the TOE retrieves from the Registered HTTPS-compatible device.

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 HTTPS-compatible device and the Registered SNMP-compatible 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 A2 Firmware Update Function

A function that allows the TOE to update its firmware with the firmware for update received from the CS.

Web Function

A user interface function that allows user to input and output information in the TOE. Users access the TOE via a computer's Web browser to use this function.

Email Notice Function

A function that allows the TOE to send information, which is to be sent from the TOE to the CS, to the email address specified by the administrator by using Service Call Function, Machine Counter Notice Function, Counter per User Notice Function, and Supply Call Function.

1.4.4.2 Security Functions

User Identification and Authentication Function

A function that allows the TOE to identify and authenticate users who attempt to access the TOE via Web browser on a computer. The TOE allows only the users who successfully identified and authenticated to operate the TOE.

Device Identification and Authentication Function

The TOE verifies whether the IT products that access the TOE through network is genuine CS or Registered HTTPS-compatible devices.

Communication Data Protection Function

A function that allows the TOE to prevent leaking of information communicated through the Registered HTTPS-compatible devices, CS, computers, and SMTP server, as well as to detect tampering. The communication between the TOE and the SNMP-compatible devices is not protected by this function.

Verification Function

A function that allows the TOE to confirm that the firmware for update received from the CS via network is the firmware officially provided by the manufacturers.

Security Management Function

A function that allows the TOE to limit the usage range of management function based on the user's role.

Audit Function

A function that allows the TOE to record the required information for audit as an audit log in the TOE when the events that require the User Identification and Authentication Function, Security Management Function, Verification Function, and the CS's Identification and Authentication Function occur. It is not allowed to change or delete the audit logs in the TOE, and only the administrator can view the audit logs.

1.4.5 Protected Assets

This subsection explains machine counter information, failure information, supply information, device firmware, RC Gate A2 firmware, and TSF data that the TOE protects.

Machine Counter Information

Machine counter information means the number of print pages counted for each @Remote-supported device.
Machine counter information is sent from each @Remote-supported device to the TOE, temporarily stored in the machine counter information area of the TOE, and periodically sent to the CS. If the machine counter information sent from the @Remote-supported devices to the CS is tampered with, no appropriate @Remote services will be provided for the @Remote-supported devices.
Confidentiality and integrity of this information must be assured in the Internet communication between the CS and TOE. In the LAN environment, confidentiality and integrity of this information must be assured in the communication between the HTTPS-compatible devices and TOE.

Failure Information and Supply Information

Failure and supply information is sent from each @Remote-supported device to the TOE, and then sent from the TOE to the CS as needed. If the failure information and supply information sent from the @Remote-supported devices to the CS is tampered with, no appropriate @Remote service will be provided for the @Remote-supported devices.
Confidentiality and integrity of this information must be assured in the Internet communication between the CS and TOE. In the LAN environment, confidentiality and integrity of this information must be assured in the communication between the HTTPS-compatible devices and TOE.

Device Firmware

Device firmware is the firmware for a Registered HTTPS-compatible device. Device firmware is installed in a Registered HTTPS-compatible device via the TOE from the CS.

Confidentiality of this information must be assured in the Internet communication between the CS and TOE. Integrity of the device firmware is assured separately from this TOE function. It is assured by the mechanism that the CS provide signature on the firmware and then the HTTPS-compatible devices verify the signature. Thus, this TOE only provides the mechanism protecting the device firmware on the communication path between the CS and the TOE in addition to the signature and verification mechanism. This TOE does not provide the mechanism protecting the communication path between the HTTPS-compatible devices and the TOE.

RC Gate A2 Firmware

RC Gate A2 Firmware is the TOE firmware. RC Gate A2 Firmware is installed in the TOE at the manufacturing facilities and delivered to users. It can be updated with the RC Gate A2 Firmware Update Function when the TOE administrator give permission to do it. The RC Gate A2 Firmware must be a genuine product of the manufacturer.
Confidentiality and integrity of this information must be assured in the Internet communication between the CS and TOE.

TSF Data

TSF data is recorded in the TOE. It includes the administrator's password, CE password, date and time, CE Access Permission Settings, Device Firmware Update Permission Settings, RC Gate A2 Firmware Update Permission Settings, screen lock period, destination address for Email Notice, device certificate information, and SSL/TLS settings.
In the LAN environment, confidentiality and integrity of this information must be assured in the communication between Web browsers and the TOE.

1.5 Glossary

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 @Remote-supported devices.
Boot Loader	Loads the operating system immediately after turning on the power of the TOE.
Screen Lock Function	While accessing RC Gate from a computer, the screen will be locked if a user has not accessed the screen for a certain period of time exceeding the screen lock period set by the administrator. The user cannot operate the screen until the authentication succeeds.

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 Version 3.1 Revision 4 (Japanese translation Ver.1.0)
  CCMB-2012-09-001

  Part 2:

  Security functional components Version 3.1 Revision 4 (Japanese translation Ver.1.0)
  CCMB-2012-09-002

  Part 3:

  Security assurance components Version 3.1 Revision 4 (Japanese translation Ver.1.0)
  CCMB-2012-09-003

- Functional requirements: Part 2 expansion
- 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 EAL2+ALC_FLR.2.

3 Security Problem Definition

This chapter defines Threats, Organisational Security Policies, and Assumptions.

3.1 Threats

This section identifies and defines the assumed threats for the TOE and the working environments where the TOE is installed.

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Attackers may use the TOE as an administrator or a CE.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Attackers may sniff or tamper the communication information on the communication path sent and received between the TOE and CS, and emails sent to users from the TOE using the Email Notice Function.

T.FAKE_NOTICE_POINT

Attackers may spoof the CS or the destination address of Email Notice Function to obtain information from the TOE.

T.UPDATE_COMPROMISE

Attackers may install malicious software to the TOE through the network.

T.HTTPS_DEV

When the TOE communicates with Registered HTTPS-compatible devices for the Counter per User Notice Function, the Machine Counter Notice Function, the Supply Call Function, and the Service Call Function, attackers may spoof the Registered HTTPS-compatible devices, or may sniff or tamper the communication data.

T.PC_WEB

When the TOE communicates with a computer, attackers may sniff or tamper the communication data.

3.2 Organisational Security Policies

This TOE does not provide the organisational security policies.

3.3 Assumptions

This section describes the assumptions of the TOE operations.

A.PHYSICAL_PROTECTION

The operation of the TOE shall be performed using physical protective measures.

A.NO_THRU_TRAFFIC_PROTECTION

The TOE shall use other network devices such as firewall to connect the network that is protected from external networks.

A.TRUSTED_ADMINISTRATOR

The administrator and device administrator shall have knowledge necessary to manage and operate TOE securely, and perform their work roles respectively.

A.DEVICE

The device administrator shall perform maintenance management of the devices that are connected to LAN. The genuine devices, which are not modified, shall be purchased and operated.

A.CE

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 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

The TOE ensures that users who attempt to use the TOE are identified and authenticated.

O.ACCESS

The TOE ensures that only the identified and authenticated users access to TSF data.

O.TRUSTED_NOTICE_POINT

The TOE ensures that communication data on the communication path is secured and sent to genuine destination when communicating with the CS and the destination address of Email Notice Function. It also ensures detection of data tampering.

O.GENUINE

The TOE ensures that only the TOE's genuine firmware received from the CS is installed.

O.AUDIT_LOGGED

The TOE ensures that the audit logs are recorded when the events related to user identification and authentication, the TSF data modification, communication failure with the CS, and the TOE firmware update occur, and provided only to the administrator for the detection of security intrusion. It also ensures that the audit logs are not modified or deleted.

O. TRUSTED _HTTPS_DEVICE

The TOE ensures that it communicates with the Registered HTTPS-compatible devices and the communication data on the communication path is secured for Machine Counter Notice Function, Service Call Function, Supply Call Function, and Counter per User Notice Function. It also ensures detection of data tampering.

O. TRUSTED _OPERATOR

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.

4.2 Security Objectives for Operational Environment

This section describes security objectives for the operational environment.

OE.PHYSICAL

The TOE shall be protected by physical security.

OE.NO_THRU_TRAFFIC_PROTECT

The network environment to which to connect the TOE shall be protected from attacks from external networks.

OE.TRUSTED_ADMIN

The administrator and device administrator shall understand the TOE guidance documents, and manage and operate the TOE and devices according to the description of the guidance documents.

OE.DEVICE

The device administrator shall purchase and install the devices through the official channels, and then perform maintenance management to prevent the devices from being modified.

OE.CE

For the maintenance of the TOE, only a qualified CE shall be allowed to maintain it.

4.3 Security Objectives Rationale

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

4.3.1 Corresponding Relationship between Security Objectives and Security Problems

Table 2 shows the corresponding relationship between security objectives and security problems that includes assumptions, threats, and organisational security policies.
As shown in Table 2, one of the security objectives satisfies the assumptions, counters the threats, and

fulfils the organisational security policies. 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

	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	T.UNTRUSTED_COMMUNICATION_CHANNELS	T.FAKE_NOTICE_POINT	T.UPDATE_COMPROMISE	T.HTTPS_DEV	T.PC_WEB	A.PHYSICAL_PROTECTION	A.NO_THRU_TRAFFIC_PROTECTION	A.TRUSTED_ADMINISTRATOR	A.DEVICE	A.CE
O.I&A	✓										
O.ACCESS	✓										
O.TRUSTED_NOTICE_POINT		✓	✓								
O.GENUINE				✓							
O.AUDIT_LOGGED	✓	✓	✓	✓							
O.TRUSTED_ HTTPS_DEVICE					✓						
O.TRUSTED_ OPERATER						✓					
OE.PHYSICAL							✓				
OE.NO_THRU_TRAFFIC_PROTECT								✓			
OE.TRUSTED_ADMIN									✓		
OE.DEVICE										✓	
OE.CE											✓

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS is countered by O.I&A, O.ACCESS, and O.AUDIT_LOGGED. O.I&A performs identification and authentication for the users who attempt to use the TOE. Only the users who are successfully identified and authenticated within three attempts are allowed to use the TOE. In addition, O.ACCESS allows only the users who have succeeded in O.I&A authentication to access TSF data. O.AUDIT_LOGGED reduces threats by recording and tracing the events related to the user identification and authentication, and the changes of TSF data.

T.UNTRUSTED_COMMUNICATION_CHANNELS is countered by O. TRUSTED_NOTICE_POINT and O.AUDIT_LOGGED. O.TRUSTED_NOTICE_POINT secures the communication data on the communication path and sends it to genuine destination when communicating with the TOE, CS and SMTP server, as well as detects data tampering. O.AUDIT_LOGGED reduces threats by tracing the communication failure events between the TOE and CS.

T.FAKE_NOTICE_POINT is countered by O.TRUSTED_NOTICE_POINT and O.AUDIT_LOGGED. O.TRUSTED_NOTICE_POINT allows the TOE to send the communication data to the genuine destination when communicating with the CS, SMTP server, and Registered HTTPS-compatible devices. O.AUDIT_LOGGED reduces threats by tracing the communication failure events between the TOE and CS.

T.UPDATE_COMPROMISE is enforced by O.GENUINE and O.AUDIT_LOGGED. O.GENUINE installs only the genuine RC Gate A2 Firmware received from the CS. O.AUDIT_LOGGED reduces threats by tracing the events related to the TOE firmware updates.

T.HTTPS_DEV is enforced by O.TRUSTED_ HTTPS_DEVICE. O.TRUSTED_ HTTPS_DEVICE allows only the Registered HTTPS-compatible devices to communicate with the TOE in the Machine Counter Notice Function, the Service Call Function, the Supply Call Function, and Counter per User Notice Function. It also secures the protected assets on the communication path between the TOE and the Registered HTTPS-compatible devices, and detects data tampering.

T.PC_WEB is countered by O.TRUSTED_ OPERATER. O.TRUSTED_ OPERATER detects the tampering of TSF data on the LAN and enables passwords to be secured when the Web function is used.

A.PHYSICAL_PROTECTION is upheld by OE.PHYSICAL. OE.PHYSICAL installs the TOE in the environment where it can be protected from physical attacks.

A.NO_THRU_TRAFFIC_PROTECTION is upheld by OE.NO_THRU_TRAFFIC_PROTECTION. OE.NO_THRU_TRAFFIC_PROTECTION protects the network environment to which to connect the TOE from attacks from external networks.

A.TRUSTED_ADMINISTRATOR is upheld by OE.TRUSTED_ADMIN. The administrator and device administrator understand the TOE guidance documents, and manage and operate the TOE and devices according to the description of the guidance documents.

A.DEVICE is upheld by OE.DEVICE. OE.DEVICE requires the device administrator to purchase the devices through the official channels so that only genuine devices communicate with TOE, and also requires the device administrator to manage the devices to prevent them from being modified.

A.CE is upheld by OE.CE. The administrator allows only a qualified CE to maintain the TOE for the maintenance.

5 Extended Components Definition

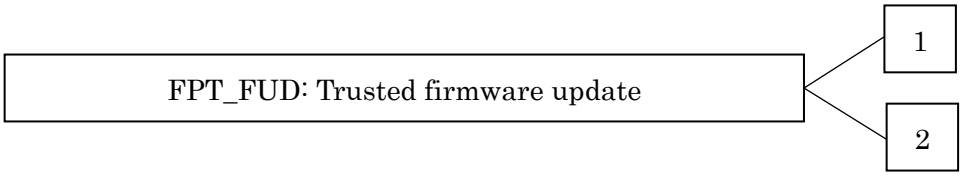
This chapter defines the extended security functional requirements.

5.1 Trusted Firmware Update (FPT_FUD)

What the Family Does

This family defines the update requirements for the TOE firmware and software.

Level Placement of Components



FPT_FUD.1 Trusted firmware update requests a management tool to verify the TOE firmware and software updates before installing them.

FPT_FUD.2 Trusted firmware update requests a management tool not to install the firmware and software updates when the verification fails, as a part of the trusted firmware update process.

Management: FPT_FUD.1 and FPT_FUD.2

No management activity foreseen exists.

Audit: FPT_FUD.1 and FPT_FUD.2

If the security audit data generation (FAU_GEN) is included in PP/ST, the following action shall be the auditable.

a) Start-up of update

Reason:

When updating the TOE firmware, the administrator allows the firmware update and the TOE verifies the validity of it before updating. The TOE updates the firmware only if it is valid. The administrator can view the version of the firmware installed in TOE. This function is a security function that prevents the attacks installing malicious firmware to the TOE, and maintains integrity of the TSF. In the FPT class where integrity of the TSF is maintained, however, there is no component verifying the firmware before installing it to the TOE, though there are components that detect the tampering of the TSF data and the TOE. Therefore, this extended components need to be registered on the FPT class.

FPT_FUD.1 Trusted Firmware Update

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FUD.1.1 The TSF shall provide the administrator with the capability to inquire the current version of the TOE firmware and software.

FPT_FUD.1.2 The TSF shall provide the administrator with the capability to start the update process of the TOE firmware and software.

FPT_FUD.1.3 The TSF shall provide the capability to verify the TOE firmware and software updates before installing them.

FPT_FUD.2 Handling of when Trusted Firmware Update is failed

Hierarchical to: No other components.

Dependencies: FPT_FUD.1

FPT_FUD.2.1 The TSF does not install the TOE firmware and software updates if the verification is failed.

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. (Refinement:) is used for identification of refinement. Also, alphabet suffixes with brackets such as "(a)" and "(b)" are used for identification of "iterations".

6.1.1 Class FAU: Security Audit

FAU_GEN.1	**Audit data generation**
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamp
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: auditable events shown in Table 3]**.

Table 3 shows the actions of the basic level or below that are recommended by the CC as auditable for each functional requirement (CC rules), and the corresponding auditable events of the TOE.

Table 3: List of auditable events

Functional requirements	Actions which should be auditable	Auditable events of TOE
FAU_GEN.1	None	-
FAU_GEN.2	None	-
FAU_SAR.1	a) Basic: Reading of information from the audit records.	a) Basic Reading of audit logs
FAU_SAR.2	a) Basic: Unsuccessful attempts to read information from the audit records.	None (Auditable events are not recorded because the unsuccessful attempts to read information from the audit records do not exist.)
FAU_STG.1	None	-

Functional requirements	Actions which should be auditable	Auditable events of TOE
FAU_STG.4	a) Basic: Actions taken due to the audit storage failure.	None (Auditable events are not recorded because the actions taken due to the audit storage failure do not exist.)
FIA_AFL.1	a) Minimal: The reaching of the threshold for the unsuccessful authentication attempts, the actions (e.g. disabling of a terminal) taken after reaching the threshold, and, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	a) Minimal Lockout start
FIA_ATD.1	None	-
FIA_SOS.1	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.	Changing the administrator's password (Outcome: Success/Failure) Changing the CE's password (Outcome: Success/Failure)
FIA_UAU.2	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	b) Basic Login (Outcome: Success/Failure)
FIA_UAU.6	a) Minimal: Failure of re-authentication; b) Basic: All re-authentication attempts.	a) Minimal Failure of re-authentication
FIA_UID.2	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	b) Basic Login (Outcome: Success/Failure)
FIA_USB.1	a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject); b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	b) Basic Login (Outcome: Success/Failure)

Functional requirements	Actions which should be auditable	Auditable events of TOE
FMT_MTD.1	a) Basic: All modifications to the values of TSF data.	a) Basic: All modifications to the values of TSF data.
FMT_SMF.1	a) Minimal: Use of the management functions.	a) Minimal: Use of the management functions.
FMT_SMR.1	a) Minimal: Modifications to the group of users that are part of a role; b) Detailed: Every use of the rights of a role.	None (Auditable events does not occur because the function to modify a role is not provided.)
FPT_STM.1	a) Minimal: Changes to the time; b) Detailed: Providing a timestamp.	a) Minimal:: Changing time and date
FPT_FUD.1	a) Start-up of update.	Start-up of update Update results (Success/Failure)
FPT_FUD.2	None	-
FTA_SSL.1	a) Minimal: Locking of an interactive session by the session locking mechanism; b) Minimal: Successful unlocking of the interactive session; c) Basic: All attempted successful unlocking of the interactive session.	c) Basic: Unlocking locked screen (Result: Success/Failure)
FTP_ITC.1(a)	a) Minimal: Failure of the trusted channel functions; b) Minimal: Identification of the initiator and target of failed trusted channel functions; c) Basic: All attempted uses of the trusted channel functions; d) Basic: Identification of the initiator and target of all trusted channel functions.	a) Minimal: Communication failure between the TOE and CS

FAU_GEN.1.2 The TSF shall record the following information at minimum at every audit record:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, **[assignment: no other audit relevant information]**, based on the auditable event definitions of the functional components included in the PP/ST.

FAU_GEN.2	**User identity association**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the user identification information that caused the event.

FAU_SAR.1	**Audit review**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide **[assignment: the administrator]** with the capability to read **[assignment: audit data generated with FAU_GEN.1]** from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the users to interpret the information.

FAU_SAR.2	**Restricted audit review**
Hierarchical to:	No other components.
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those who have been granted explicit read-access.

FAU_STG.1	**Protected audit trail storage**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to **[selection: prevent]** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4	**Prevention of audit data loss**
Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage

FAU_STG.4.1	If the audit trail is full, the TSF shall **[selection: overwrite the oldest stored audit records]** and **[assignment: no other actions to be taken in case of audit storage failure]**.

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 the authentication attempts fail **[selection: [assignment: in consecutive three (positive integer number)]]** times, regarding **[assignment: the user identification and authentication for each user name within five 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 one minute to identify and authenticate the user from the computer used by the unsuccessful user]**.

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].**

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 are **[assignment: a password with 8 or more characters that composed of numbers, lower case alphabetic characters, upper case alphabetic characters, and symbols ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")")]**.

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 and before the CE is allowed to change the CE'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].**

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 4]**

Table 4: 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. Set a name of a user who is successfully identified and authenticated to the User name.
CE	User process	Set CE to the User type. Set a name of a user who is successfully identified and authenticated 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 abilities to **[selection: change default values, modify, delete [assignment: newly create, reset]] [assignment: TSF data in Table 5]** to **[assignment: the roles permitted and identified in Table 5]**.

Table 5: List of TSF information management

TSF Data	Operation	Permitted and Identified Role
Administrator's password	Change default values Modify	Administrator
Administrator's password	Reset	CE
CE's password	Modify	CE
Date and time	Modify	Administrator CE
CE Access Permission Settings	Modify	Administrator
Device Firmware Update Permission Settings	Modify	Administrator
RC Gate A2 Firmware Update Permission Settings	Modify	Administrator
Screen Lock Period	Modify	Administrator CE
Destination Address for Email Notice	Newly registered Modify Delete	Administrator
Device Certificate Information	Newly registered Modify Delete	Administrator CE
SSL/TLS Settings	Modify	Administrator CE

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 6]**.

Table 6: List of specification of management functions

Management Function
Change a default value of the administrator's password and modify it by administrator
Reset the administrator's password by CE
Modify the CE's password by CE
Modify date and time by administrator and CE
Modify CE Access Permission Settings by administrator
Modify Device Firmware Update Permission Settings by administrator
Modify RC Gate A2 Firmware Update Permission Settings by administrator
Modify Screen Lock Period by administrator and CE
Newly register, modify, and delete the Destination Address for Email Notice by administrator
Newly register, modify, and delete Device Certificate Information
Modify SSL/TLS Settings

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 and CE]**.

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_FUD.1 Trusted Firmware Update

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FUD.1.1	The TSF shall provide the administrator with the capability to inquire the current version of the TOE firmware and software.
FPT_FUD.1.2	The TSF shall provide the administrator with the capability to start the update process of the TOE firmware and software.
FPT_FUD.1.3	The TSF shall provide the capability to verify the TOE firmware and software updates before installing them.

FPT_FUD.2 Handling of when Trusted Firmware Update Verification is failed

Hierarchical to:	No other components.
Dependencies:	FPT_FUD.1
FPT_FUD.2.1	The TSF does not install the TOE firmware and software updates if the verification is failed.

6.1.5 Class FTA: TOE access

FTA_SSL.1 TSF-initiated session lock

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FTA_SSL.1.1	When **[assignment: the screen lock period (one minute to 60 minutes) specified by the administrator or CE elapses after the last operation by a user who login from the Web browser]**, the TSF shall lock interactive session by using the following methods: a) Delete or overwrite the display device to prevent the current contents from being read; b) Prohibit any operation relating to user data access or display device except for releasing session lock.
FTA_SSL.1.2	The TSF shall require **[assignment: successful user authentication]** before releasing session lock.

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 **(refinement: 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 7]**.

Table 7: Functions requiring trusted channels for communication between the RC Gate A2 and CS (a)

Function
Machine Counter Notice Function
Service Call Function
Supply Call Function
Device Firmware Update Function
RC Gate A2 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 **(refinement: 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 8]**.

Table 8: Functions requiring trusted channels for communication between the RC Gate A2 and Registered HTTPS-compatible device (b)

Function
Machine Counter Notice Function
Service Call Function
Supply Call Function
Counter per User Notice Function

FTP_ITC.1(c)	**Inter-TSF trusted channel**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1(c)	The TSF shall provide a communication channel between itself and another trusted IT product **(refinement: the destination address for email notice registered by the administrator)** 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(c)	The TSF shall permit **[selection: the TSF]** to initiate communication via the trusted channel.
FTP_ITC.1.3(c)	The TSF shall initiate communication via the trusted channel for **[assignment: Email Notice 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 EAL2+ALC_FLR.2. Table 9 lists the TOE assurance components. This list shows a set of components defined by EAL2 of the Evaluation Assurance Level with the addition of ALC_FLR.2.

Table 9: TOE security assurance requirements (EAL2+ALC_FLR.2)

Assurance Class	Assurance Component	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures

Assurance Class	Assurance Component	
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
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.1	Analysis of coverage
	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 10 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 "✓" marks in the table indicate the corresponding relation.

Table 10: Relationship between security objectives and functional requirements

	O.I&A	O.ACCESS	O.TRUSTED_NOTICE_POINT	O.GENUINE	O.AUDIT_LOGGED	O.TRUSTED _HTTPS_DEVICE	O. TRUSTED _OPERATOR
FAU_GEN.1					✓		
FAU_GEN.2					✓		
FAU_SAR.1					✓		
FAU_SAR.2					✓		
FAU_STG.1					✓		
FAU_STG.4					✓		
FIA_AFL.1	✓						
FIA_ATD.1	✓						
FIA_SOS.1	✓						
FIA_UAU.2	✓						
FIA_UAU.6	✓						
FIA_UID.2	✓						
FIA_USB.1	✓						
FMT_MTD.1		✓					
FMT_SMF.1		✓					
FMT_SMR.1		✓					
FPT_STM.1					✓		
FPT_FUD.1				✓			
FPT_FUD.2				✓			
FTA_SSL.1	✓						
FTP_ITC.1(a)			✓				
FTP_ITC.1(b)						✓	
FTP_ITC.1(c)			✓				
FTP_TRP.1							✓

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

O.I&A is a security objective that allows only administrator 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 administrator or CE is associated with the user process which is associated with the user type and security attributes of the user name. According to FIA_ATD.1, the administrator or CE is allowed to remotely operate the TOE by maintaining these security attributes.

(3) The TOE terminates the TOE remote operation automatically.
According to FTA_SSL.1, if the successfully authenticated user does not operate the computer for a certain period of time, the computer locks the operation screen. Because of this functionality, even if the successfully authenticated user is away from the computer 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 the administrator and CE.
According to FIA_SOS.1, passwords are secured by specifying the number of characters and using a combination of character types so that passwords are not decoded easily. According to FIA_AFL.1, no sufficient time to decode passwords shall be given.

(5) The TOE re-authenticates the user before changing the administrator's password or CE's password.
To prevent persons other than the user from changing the password, according to FIA_UAU.6, users shall be re-authenticated before changing passwords.

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.1 considered as the necessary security functional requirements for these countermeasures.

O.ACCESS

O.ACCESS is a security objective for the authenticated users to control the access to TSF data. To fulfil this security objective, the following countermeasures must be satisfied:

(1) The TOE allows only the administrator and CE to perform the security management.
According to FMT_MTD.1 and FMT_SMF.1, only the administrator and CE are allowed to manage TSF data.

(2) The TOE maintains the user type.
According to FMT_SMR.1, the roles of the administrator and CE are maintained.

The necessary countermeasures to fulfil O.ACCESS are (1) and (2). Therefore, O.ACCESS is fulfilled by accomplishing FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1 considered as the necessary security functional requirements for these countermeasures.

O.TRUSTED_NOTICE_POINT

O.TRUSTED_NOTICE_POINT is a security objective that ensures the information retrieved from the @Remote-supported device is sent to correct destination (the destination address for Email Notice Function specified in the TOE by the CS and administrator) and that ensures security of the communication data and detection of 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), the communication channels that provide the function to identify the CS in the communication between the TOE and the CS are established and the correctness of the CS is verified.

(2) The TOE protects the communication data with the CS.
According to FTP_ITC.1(a), the reliable communication channels in the communication between the TOE and the CS are established to prevent disclosure of protected assets on the communication path and detect data tampering.

(3) The TOE sends the communication data to the destination address for Email Notice Function.
According to FTP_ITC.1(c), the TOE sends the communication data only to the destination address specified by the administrator. Even if the data is sent to incorrect destination, the received person cannot read the received email.

(4) The TOE protects the data until it arrives at the destination address.
According to FTP_ITC.1(c), the TOE prevents disclosure of sent email on the communication path and detects tampering.

The necessary countermeasures to fulfil O.TRUSTED_NOTICE_POINT are (1), (2), (3), and (4). Therefore, O.TRUSTED_NOTICE_POINT is fulfilled by accomplishing FTP_ITC.1(a) and FTP_ITC.1(c) considered as the necessary security functional requirements for these countermeasures.

O.GENUINE

O.GENUINE is a security objective to ensure that RC Gate A2 Firmware built in the TOE is the genuine RC Gate A2 Firmware. To fulfil this security objective, the following countermeasure must be satisfied:

(1) The TOE verifies the correctness of firmware and software before updating.
According to FPT_FUD.1, the administrator can check the versions of software and hardware installed on the TOE so that the administrator is able to decide if the firmware and software should be updated. The start-up of update is allowed in accordance with the administrator's decision. When updating firmware and software, the TOE verifies the correctness of updates before installing them. According to FPT_FUD.2, updates are not installed if the correctness is not confirmed.

The necessary countermeasures to fulfil O.GENUINE is (1) and (2). Therefore, O.GENUINE is fulfilled by accomplishing FPT_FUD.1 and FPT_FUD.2 considered as the necessary security functional requirements for these countermeasures.

O.AUDIT_LOGGED

O.AUDIT_LOGGED is a security objective to record the audit logs when the event related to user identification and authentication, the TSF data modification, communication failure with the CS, and the TOE firmware update occur. It also allows the administrator with the management permission of RC Gate A2 to view the audit logs. To fulfil this security objective, the following countermeasures must be satisfied:

(1) Record audit logs.
According to FAU_GEN.1 and FAU_GEN.2, the TOE records information for security audit when the auditable events shown in Table 3 occur, including the user identification information that caused the events. Auditable events shown in Table 3 includes the events required for all SFR that prescribes the events related to user identification and verification, the TSF data modification, communication failure with the CS, and the TOE firmware updates.

(2) Provide Audit Function.
According to FAU_SAR.1, the administrator with management permission of RC Gate A2 can read the audit logs in a format that can be verified. According to FAU_SAR.2, reading audit logs by persons other than the administrator with management permission of RC Gate A2 is prohibited.

(3) Protect audit logs.
According to FAU_STG.1, audit logs are protected from being modified. According to FAU_STG.4, the audit logs that have the oldest time stamp are overwritten with the newer audit logs, when auditable events occur but the audit log file is full.

(4) Provide reliable time of event occurrence.
According to FPT_STM.1, trusted time stamps are provided, and the reliable times are recorded in the audit logs when events occurred.

The necessary countermeasures to fulfil O.AUDIT_LOGGED are (1), (2), (3) and (4). Therefore, O.AUDIT_LOGGED is fulfilled by accomplishing FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.4, FAU_SAR.1, FAU_SAR.2, and FPT_STM.1 considered as the necessary security functional requirements for these countermeasures.

O.TRUSTED _HTTPS_DEVICE

O. TRUSTED _HTTPS_DEVICE is a security objective to ensure that, for the Machine Counter Notice Function, the Service Call Function, the Supply Call Function, and the Counter per User Notice Function, the TOE communicates only with the @Remote-supported devices, secures the communication data between the Registered HTTPS-compatible devices and the TOE in the LAN, and detects data tampering. To fulfil this security objective, the following countermeasure must be satisfied:

(1) The TOE communicates with the genuine Registered HTTPS-compatible devices.
According to FTP_ITC.1(b), the communication channels that provide the function to identify HTTPS in the communication between the TOE and the Registered HTTPS-compatible devices are established, and the correctness of the Registered HTTPS-compatible devices is verified.

(2) The TOE protects the communication data with the Registered HTTPS-compatible devices.
According to FTP_ITC.1(b), the reliable communication channels in the communication between the TOE and the Registered HTTPS-compatible devices are established to secure the communication data on the communication path and detect data tampering.

The necessary countermeasures to fulfil O. TRUSTED _HTTPS_DEVICE is (1) and (2). Therefore, O. TRUSTED _HTTPS_DEVICE is fulfilled by accomplishing FTP_ITC.1(b) considered as the necessary security functional requirement for these countermeasures.

O. TRUSTED _OPERATOR

O. TRUSTED _OPERATOR is a security objective to secure communication data on the communication path in the communication when the users operate the TOE remotely by using their computer's Web browsers. It also ensures detection of data tampering. To fulfil this security objective, the following countermeasures must be satisfied:

(1) The TOE protects communication data for remote operation of the TOE by a user.
According to FTP_TRP.1, the trusted path is used for communication between the TOE and computers that are used for the remote operation to secure communication data on the communication path. It also detects data tampering.

The necessary countermeasure to fulfil O. TRUSTED _OPERATOR is (1). Therefore, O. TRUSTED _OPERATOR is fulfilled by accomplishing FTP_TRP.1 considered as the necessary security functional requirement for this countermeasure.

6.3.3 Dependency Analysis

Table 11 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.

Table 11: Correspondence 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
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2	N/A
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	N/A
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	N/A
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	N/A
FAU_STG.4	FAU_STG.1	FAU_STG.1	N/A
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

TOE security functional requirement	Dependency required by the CC	Dependency satisfied in the ST	Dependency not satisfied in the ST
FIA_UAU.2	FIA_UID.1	FIA_UID.2	N/A
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_STM.1	N/A	N/A	N/A
FPT_FUD.1	N/A	N/A	N/A
FPT_FUD.2	FPT_FUD.1	FPT_FUD.1	N/A
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2	N/A
FTP_ITC.1(a)	N/A	N/A	N/A
FTP_ITC.1(b)	N/A	N/A	N/A
FTP_ITC.1(c)	N/A	N/A	N/A
FTP_TRP.1	N/A	N/A	N/A

6.4 Security Assurance Requirements Rationale

This TOE is a commercial product used in general office environments. It is assumed to attack using Web browser and network by attackers who have a basic attack capability.

To respond to such attacks, the following security assurance requirements must be evaluated: the attacks can be countered by the security functions implemented to the TOE; the security functions are correctly implemented; the TOE with the security functions is distributed to users without being tampered; and the guidance for the proper use of the TOE security functions are provided to users. These requirements conform to EAL2.

In addition, using the Flaw reporting procedures (ALC_FLR.2) to properly report and fix defects found after starting operation is important for continued and secure operation of the TOE.

Therefore, the Evaluation Assurance Level EAL2+ALC_FLR.2 is appropriate for this TOE.

7 TOE Summary Specification

This chapter describes the methods and mechanisms for each security functional requirement, which are used by the TOE to satisfy the security functional requirements described in 6.1.

FAU_GEN.1 Audit data generation

The TOE generates the audit logs when the following auditable events occur, and adds them to the audit log files.

- Start-up of audit function
- Shutdown of audit function
- Reading audit logs
- Success/failure of login
- Failure of re-authentication
- Lockout
- Success of administrator's password change
- Success of CE's password change
- Set up of date and time
- Changing the CE Access Permission Settings
- Changing the Device Firmware Update Permission Settings
- Changing the RC Gate A2 Firmware Update Permission Settings
- Changing the Screen Lock Period
- Newly registering, changing, deleting the Destination Address for Email Notice
- Newly registering, changing, deleting Device Certificate Information
- Modifying SSL/TLS Settings
- SSL/TLS communication failure with CS
- Starting firmware update, success/failure of update
- Success/failure of screen lock release

The security audit log consists of the following information:

- Date and time of events
- Type of events
- User name
- Results

FAU_GEN.2 User identity association

The TOE records the name of the user that caused the auditable event in the audit logs.

FAU_SAR.1 Audit review

The TOE has a function that allows viewing the audit logs from Web browser of a computer and provides the administrator with this function.

FAU_SAR.2 Restricted audit review

The TOE has a function that allows viewing the audit logs from Web browser of a computer and provides only the administrator with this function.

FAU_STG.1 Protected audit trail storage

The TOE does not provide the function that deletes and changes the audit logs and audit log files.

FAU_STG.4 Prevention of audit data loss

The TOE writes the newer audit logs over the oldest audit logs if the audit log file is full and has no space to add the new audit logs.

FIA_AFL.1 Authentication failure handling

The TOE counts the number of the authentication attempts failure 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 User Identification and Authentication Function. If the user is successfully authenticated, the TOE resets the number of the failure attempts of the user to 'ZERO'.

FIA_ATD.1 User attribute definition

The TOE maintains the user type and user name that are specified when performing user identification and authentication until session termination.

FIA_SOS.1 Verification of secrets

When the administrator intends to change the administrator's password or when the CE intends to change the CE's password, 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: numbers, lower case alphabetic characters, upper case alphabetic characters, and symbols ("!", "@", "#", "$", "%", "^","&", "*", "(", ")")
(2) Required number of characters: 8 or more 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. The TOE does not display other screens until the user is successfully authenticated.

FIA_UAU.6 Re-authenticating

The TOE provides the capability to change passwords from the screen for the administrator or the CE. When the TOE displays the administrator or CE screen for password change, it requires the administrator or the CE to enter the current password. Then the TOE re-authenticate them using the entered password.

FIA_UID.2 User identification before any action

The TOE displays the login screen to enter 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 administrator or the CE who is successfully identified and authenticated with the screen to perform the following operations on TSF data:

- Change default values of, change, and reset the administrator's password
- Change the CE's password
- Change date and time
- Change the CE Access Permission Settings
- Change the Device Firmware Update Permission Settings
- Change the RC Gate A2 Firmware Update Permission Settings
- Change the Screen Lock Period
- Newly register, change, delete the Destination Address for Email Notice
- Newly register, modify delete Device Certificate Information
- Modify SSL/TLS Settings

FMT_SMF.1 Specification of Management Functions

The TOE provides the administrator or the CE who is successfully identified and authenticated with the screen to perform the following operations:

- Change the default value of the administrator's password and change the administrator's password by administrator
- Reset the administrator's password by CE
- Change the CE's password by CE
- Change date and time by administrator
- Change date and time by CE
- Change CE Access Permission Settings by administrator
- Change Device Firmware Update Permission Settings by administrator

- Change RC Gate A2 Firmware Update Permission Settings by administrator
- Change Screen Lock Period by administrator
- Change Screen Lock Period by CE
- Newly register, change, delete the Destination Address for Email Notice by administrator
- Newly register, modify delete Device Certificate Information by administrator or CE
- Modify SSL/TLS Settings by administrator or CE

FMT_SMR.1 Security roles

The TOE maintains the administrator and CE as the user type.

FPT_STM.1 Reliable time stamps

The TOE provides its system clock for the date (year/month/day) and time (hour/minute/second) of the audit log records.

FPT_FUD.1 Trusted Firmware Update

The TOE provides the administrator with the function to check the firmware version from the Web function.
The TOE allows only the administrator to set acceptance or rejection of the firmware received from CS with Firmware Update Function.
When the TOE receives the firmware from CS, it installs the firmware only if the correctness is confirmed. RC Gate A2 firmware verifies the signature of the file that composes the firmware.

FPT_FUD.2 Handling of when Trusted Firmware Update Verification is failed

When the TOE receives RC Gate A2 firmware from CS, it verifies the firmware. It installs the firmware only if the correctness is confirmed. RC Gate A2 firmware verifies the signature of the file that composes the firmware.

FTA_SSL.1 TSF-initiated session Lock

The TOE provides functions that forces the user to log off automatically when the screen lock period (one minute to 60 minutes) specified by the administrator or CE elapses after the last operation by the user who login from the Web browser.

FTP_ITC.1(a) Inter-TSF trusted channel

The TOE communicates with the CS using SSL/TLS, verifies that the CS is certified as genuine CS, and provides SSL/TLS communications for communications via the LAN between the TOE and the CS. The SSL/TLS 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 A2 Firmware Update Function.

FTP_ITC.1(b) Inter-TSF trusted channel

The TOE communicates with Registered HTTPS-compatible devices using SSL/TLS, verifies that the Registered HTTPS-compatible devices are certified as genuine Registered HTTPS-compatible devices, and provides SSL/TLS communications between the TOE and the Registered HTTPS-compatible devices. The SSL/TLS communication can be used for the Machine Counter Notice Function, the Service Call Function, the Supply Call Function, and the Counter per User Notice Function.

FTP_ITC.1(c) Inter-TSF trusted channel

The TOE protects the emails sent by the Email Notice Function using S/MIME.

FTP_TRP.1 Trusted path

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