Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2014-12-09 (ITC-4523)
Certification No.	C0535
Sponsor	RICOH COMPANY, LTD.
TOE Name	RICOH Remote Communication Gate A2
TOE Version	V1.0.2
PP Conformance	None
Assurance Package	EAL2 Augmented with ALC_FLR.2
Developer	RICOH COMPANY, LTD.
Evaluation Facility	ECSEC Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2016-12-27

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center
Technology Headquarters

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass

"RICOH Remote Communication Gate A2" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "RICOH Remote Communication Gate A2, Version V1.0.2" (hereinafter referred to as the "TOE") developed by RICOH COMPANY, LTD., and the evaluation of the TOE was finished on 2016-12-05 by ECSEC Laboratory Inc. Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, RICOH COMPANY, LTD., and provide security information to procurement entities and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is provided along with this report. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "the consumer who brings in the remote diagnosis maintenance service for digital MFP manufactured by RICOH COMPANY, LTD." to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL2 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

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 "device(s)") on a local area network (LAN) in general offices from the maintenance centre via the Internet.

This remote diagnosis maintenance service (hereafter, "@Remote Service") provides the necessary maintenance functions for each device. The TOE receives the maintenance information of the devices on the office LAN from the maintenance centre via the Internet, and the maintenance centre diagnoses the status of the devices based on the information. The devices which will be subject to @Remote Service shall be specified by the user. The specified devices are called "@Remote-supported devices." The TOE is connected to the office LAN. For providing @Remote Service, the TOE also intermediates the communication between the @Remote-supported devices and the maintenance centre. The TOE sends the maintenance information which is sent to the maintenance centre to the specified email address as well.

In order to ensure that the communication is performed with valid communication partners and to prevent leakage or tampering of communication content, the TOE uses the encryption mechanisms to protect the communication between the RICOH devices with the "Remote Management Function" which are subject to @Remote Service (hereafter,

"Registered HTTPS-compatible devices") and the TOE[1], and the communication between a server located in the maintenance centre (hereafter, "CS") and the TOE. In addition, in order to prevent tampering of emails sent from the TOE and to ensure only valid recipients are able to view the emails, the communication is protected by the encryption mechanisms.

Only pre-assigned operations are provided for successfully identified and authenticated users (administrator or CE) in order to prevent the Security Management Functions from being improperly operated.

For this security functionality, the evaluation for the validity of the design policy and the correctness of the implementation is conducted in the scope of the assurance package. The next clause describes the assumed threats and assumptions in this TOE.

1.1.2.1 Threats and Security Objectives

This TOE counters threats with the following Security Functions:

In order to protect the communication data, which includes the maintenance information as protected assets, from leakage or tampering by a third party on the Internet, the TLS protocol is used for the communication with the CS. This enables the communication data between the TOE and the CS to be secured and the data tampering to be detected.

Similarly, in order to protect the communication data from leakage or tampering by a third party on the LAN, the TLS protocol is used for the communication with the Registered HTTPS-compatible devices[1]. This enables the communication data between the TOE and the Registered HTTPS-compatible devices to be secured and the data tampering to be detected.

The TOE authenticates the CS and restricts communication with a pseudo CS in order to counter against sending malicious programs into the LAN if the attacker set up the pseudo CS on the Internet. This ensures that the TOE communicates with a genuine CS provided by RICOH COMPANY, LTD.

The TOE authenticates the Registered HTTPS-compatible devices and restricts communication with a pseudo Registered HTTPS-compatible device in order to counter against sending a pseudo maintenance information from a spoofed Registered HTTPS-compatible device by the attacker. This ensures that the TOE receives the information from a genuine Registered HTTPS-compatible device.

The TOE uses S/MIME for emails to be sent in order to counter against tampering of the contents of the emails sent by the TOE and prevent persons other than the valid recipients from viewing them. This enables that only the valid recipients view the emails, and the TOE detects tempering.

There is a threat that those who are not authorised TOE users (administrator or CE) access the TOE. As a countermeasure against this threat, for remote operation of the TOE from a client computer's web browser, the TOE identifies and authenticates users prior to the remote operation and allows the users to remotely operate the TOE. The TOE ensures users' use of the management functions according to the role (administrator or CE).

There is a threat that the firmware of the TOE is updated to an illegal firmware. As a

[1] Not all the communications between the TOE and the Registered HTTPS-compatible devices are protected by the encryption mechanisms. Refer to "Disclaimers."

countermeasure against this threat, the TOE verifies that the firmware is provided by a qualified provider.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

- This TOE is assumed to be used on the office LAN environment, and it is managed through Web browsers of client computers on the LAN.

- The TOE administrators, who have the necessary knowledge to securely manage and operate the TOE, physically protect the TOE. The LAN environment is protected from the external attackers through the Internet. The device administrator shall manage the maintenance of the @Remote-supported devices connected to the LAN. Genuine devices shall be acquired and used.

- The devices are categorised as an HTTPS-compatible device and an SNMP-compatible device depending on the compatible communication methods. Both compatible devices are the scope of @Remote Service.

- The TOE administrator and device administrator shall not use their privileges maliciously.

- For the maintenance of the TOE, the TOE administrator shall allow only the qualified Customer Engineer (hereafter, "CE") who is qualified by RICOH COMPANY, LTD., to maintain it.

1.1.3 Disclaimers

(1) This TOE does not provide the following functions:

- The TOE does not provide the Communication Data Protection Function to use the TLS protocol in the Device Firmware Update Function on the communications between the TOE and Registered HTTPS-compatible devices.

- The TOE does not provide the Communication Data Protection Function to use the TLS protocol on the communications between the TOE and Registered SNMP-compatible devices, because SNMP-compatible devices rarely support TLS-protected SNMP.

(2) In this TOE, the following is not the scope of this evaluation:

- If updated with the RC Gate A2 Firmware Update Function to the version except for V1.0.2, the updated version is out of the scope of this evaluation assurance.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2016-12, based on functional requirements and assurance requirements of the TOE according to the publicised documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and the Observation Reports prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure.

The certification oversight reviews were also prepared for those concerns found in the certification process.

Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]).

The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name: RICOH Remote Communication Gate A2

TOE Version: V1.0.2

Developer: RICOH COMPANY, LTD.

Users can verify that a product is the evaluated and certified TOE by the following means.

The administrator can display the name and version of the TOE by operating the TOE via the Web browser, according to the guidance document. By comparing them with the above listed name and version of the TOE, the user can verify that the installed product is the TOE, which is evaluated and certified.

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organisational security policies.

The TOE sends the information received from the @Remote-supported devices installed on the office LAN to the maintenance centre on the Internet, and the maintenance centre diagnoses the status of the @Remote-supported devices based on the information. It is used for the service to execute the maintenance required for each @Remote-supported device. The TOE provides the following functions to securely use the service:

The TOE provides the functions to protect the communication data, including the maintenance information flown via the Internet, and the communication data flown over the LAN, from leakage or tampering.

In order to prevent unauthorised persons from exploiting the TOE, the TOE provides the User Identification and Authentication Function and the function that allows the successfully authenticated users to configure and change the management function settings according to their roles.

The TOE provides a function for users to confirm that the firmware of the TOE is manufacturer-genuine and provided by RICOH COMPANY, LTD.

The TOE records the necessary information as an audit log in the TOE at the occurrence of events required to be recorded for the security audit and allows administrators only to operate the viewing. The TOE does not provide the function to delete/change the audit log.

The following roles are assumed as the users of the TOE.

- Administrator (TOE administrator)

  An administrator who introduces and manages this TOE.
  The administrator can change the settings, view the status of the TOE, and view the audit logs from a computer.

- CE

  A person who is educated to handle the TOE and performs the maintenance of the TOE.

The following role is not assumed to use the TOE. However, this is assumed as a role related to the operational environment.

- Device administrator

  A person who manages the maintenance of the devices that are connected to the LAN where the TOE is installed.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Section 3.1.1 and to satisfy the organisational security policies shown in Section 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functions to counter them.

Table 3-1 Assumed Threats

Identifier	Threat
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.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. (Note) The communication between the TOE and the Registered HTTPS-compatible devices for the Device Firmware Update Function is excluded from the scope of threats.
T.PC_WEB	When the TOE communicates with a computer, attackers may sniff or tamper the communication data.
T.UPDATE_ COMPROMISE	Attackers may install malicious software to the TOE through the network.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1) Countermeasures against Threat, T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

The TOE identifies and authenticates the user who is attempting to use the TOE as an administrator or a CE. Only the users who have succeeded in identification and authentication are allowed to use the TOE as an administrator or a CE.

This enables the TOE to counter against the threat.

(2) Countermeasures against Threats, T.UNTRUSTED_COMMUNICATION_CHANNELS, T.FAKE_NOTICE_POINT, and T.HTTPS_DEV

The TOE uses TLS for the communication with the CS and the Registered HTTPS-compatible devices. The TOE prevents spoofing of the CS and the Registered HTTPS-compatible devices by the TLS Authentication Function, and prevents disclosure and tampering of communication content by the functions to encrypt communication content and to authenticate the message.

The TOE uses S/MIME for the emails sent by the Email Notice Function. The encryption and electronic signature functions of S/MIME prevent disclosure and tampering of the contents of the emails. Since the TOE acts as the sender of the emails, it also prevents spoofing of the sender by the encryption function.

This enables the TOE to counter against the threats.

(3) Countermeasures against Threat, T.PC_WEB

The TOE uses TLS for the communication with the computer. The TOE prevents disclosure and tampering of communication content by the functions to encrypt communication content and to authenticate the message using TLS.

This enables the TOE to counter against the threat.

(4) Countermeasures against Threat, T.UPDATE_COMPROMISE

Before installing the firmware, the TOE confirms whether the firmware to be installed is genuine by verifying an electronic signature. The TOE installs the firmware only when it is confirmed as genuine.

This enables the TOE to counter against the threat.

3.1.2 Organisational Security Policies and Security Function Policies

This TOE does not provide the organisational security policies that are required for this TOE usage.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
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 the device administrator shall have the necessary knowledge and perform their respective roles for the secure management and operation of the TOE in their respective works.
A.DEVICE	The device administrator shall manage the maintenance of the devices that are connected to the LAN. The genuine and unmodified devices shall be acquired and used.
A.CE	Only a qualified CE shall be able to maintain the TOE. [Additional remarks] To satisfy this assumption, the TOE administrator shall allow only a qualified CE to maintain the TOE.

4.2 Environmental Assumptions

This TOE is installed in general offices and connected to the internal networks, and it is used by computers connected to the internal networks in the same way. Figure 4-1 shows the general operational environment of this TOE.

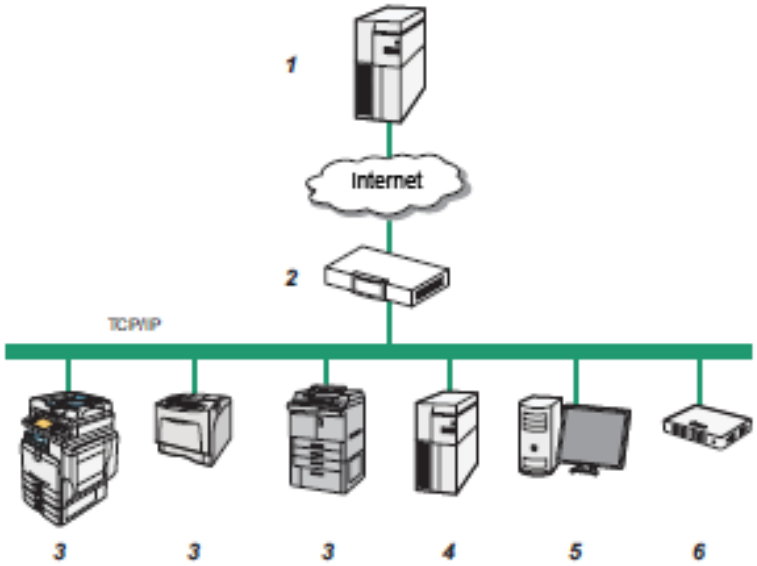

Figure 4-1 Operational Environment and Configuration

According to the number of Figure 4-1, the roles of each machine are explained as follows:

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. @Remote-supported devices

   The following two types are assumed:

   - Registered HTTPS-compatible devices

     The RICOH devices with the Remote Management Function. In this evaluation, the following devices were used:

     > RICOH MP C305
     > RICOH IPSiO SP 8300
     > RICOH MP C401

   - Registered SNMP-compatible devices

     The devices with the SNMP agent function (not necessary to be the RICOH devices)

4. SMTP server

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

5. Client computer

   A personal computer connected to the office LAN environment. Users can remotely operate the TOE from a client computer's Web browser.

In this evaluation, the following Web browsers were used: Both (a) and (b) are required for the evaluation.

(a) Any of Internet Explorer 8, 9, 10, or 11
(b) FireFox 44.0.2

6. RC Gate A2

RC Gate A2 is the TOE that is connected to the office LAN environment. Note that the optional SD card (RICOH Remote Communication Gate A2 Storage 1000), which is non-TOE configuration item, can be installed in the TOE. When this option is installed in the TOE, this case is also included as the operational environment of the TOE.

4.3 Clarification of Scope

It is not assumed that the Device Firmware Update Function protects the communication data on the communication path between the TOE and the Registered HTTPS-compatible devices. The integrity of the device firmware in this communication is assumed to be ensured by verifying an electronic signature, which is added by a CS, by the Registered HTTPS-compatible devices. Therefore, the Device Firmware Update Function does not provide the Communication Data Protection Function by the TLS protocol.

In addition, the TOE provides no Communication Data Protection Functions using the TLS protocol on the communication between the TOE and the Registered SNMP-compatible devices, because SNMP-compatible devices rarely support TLS-protected SNMP.

5. Architectural Information

This chapter explains the scope and the main components (subsystems) of the TOE.

5.1 TOE Boundary and Components

The TOE consists of the entire hardware of RC Gate A2 and the equipped firmware, and it consists of configuration items shown in Figure 5-1.

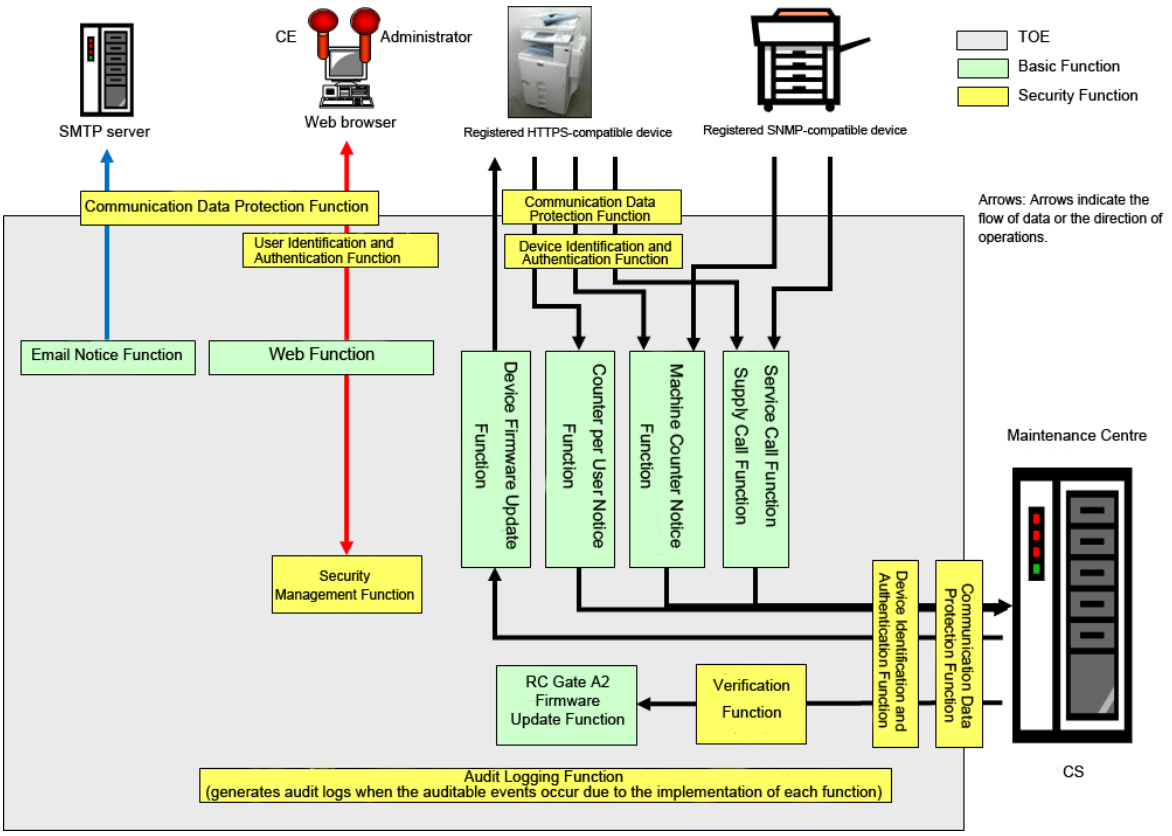

Figure 5.1 TOE boundary

The TOE consists of the Basic Functions and the Security Functions as functional components. The following shows the overview of the Basic Functions provided by @Remote Service.

- Service Call Function

  A function that allows the TOE to report to the CS on the device failure information received from the @Remote-supported 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 @Remote-supported device.

- Machine Counter Notice Function

  A function that allows the TOE to periodically notify the CS about the machine counter information (the number of print pages counted for each device) received from the @Remote-supported device.

- Counter per User Retrieval Function

  A function that allows the TOE to periodically notify the CS about the counter information on a per-user basis (the number of print pages counted for each user) received from the @Remote-supported device.

- 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 function, provided by the TOE, which allows users to remotely operate the TOE. Users access the TOE via a computer's Web browser.

- 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, Supply Call Function, Machine Counter Notice Function, and Counter per User Notice Function.

The following explains the security functions of the TOE.

- Device Identification and Authentication Function, Communication Data Protection Function

  The functions that confirm validity of the communication destination using the TLS protocol and prevent disclosure and tampering of communication content for the following communication. (The function which verifies the communication destination corresponds to the Device Identification and Authentication Function, and the function which prevents disclosure and tampering of communication content corresponds to the Communication Data Protection Function.)

  > Communication between the TOE and the Registered HTTPS-compatible devices due to the following functions:

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

  > Communication between the TOE and the CS

    The function prevents disclosure and tampering of communication content by using the TLS protocol for the use of Web Function. (It corresponds to the Communication Data Protection Function.)

    The function prevents disclosure and tampering of communication content by using S/MIME for the use of Email Notice Function. (It corresponds to the Communication Data Protection Function.)

- User Identification and Authentication Function

  The 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 use the Web Function.

- Verification Function

  The function that allows the TOE to verify an electronic signature of the firmware received by the RC Gate A2 Firmware Update Function and confirms that the firmware is officially provided by the manufacturers.

- Security Management Function

  The function that allows the TOE to limit the usage of management function based on the user's role (administrator or CE).

- Audit Logging Function

  The function that allows the TOE to record the necessary information as an audit log in the TOE at the occurrence of events required to be recorded for the security audit. Only the administrators are allowed to view the audit logs with Web browser.

5.2 IT Environment

The Web browser, Registered HTTPS-compatible devices, and a CS shall comply with the TLS protocol for the Device Identification and Authentication Function and Communication Data Protection Function of the TOE.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

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 and Europe

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

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)

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

ECSEC Laboratory Inc. Evaluation Center that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2014-12 and concluded upon completion of the Evaluation Technical Report dated 2016-12. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2015-11, 2016-01 and 2016-03 and examined procedural status conducted in relation to the work unit for delivery by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2016-07.

Concerns found in evaluation activities for each work unit were all issued as the Observation Reports, and those were reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility.

After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As a result of the evidence shown in the process of the evaluation and those confirmed validity, the evaluator performed the reproducibility testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration performed by the developer.

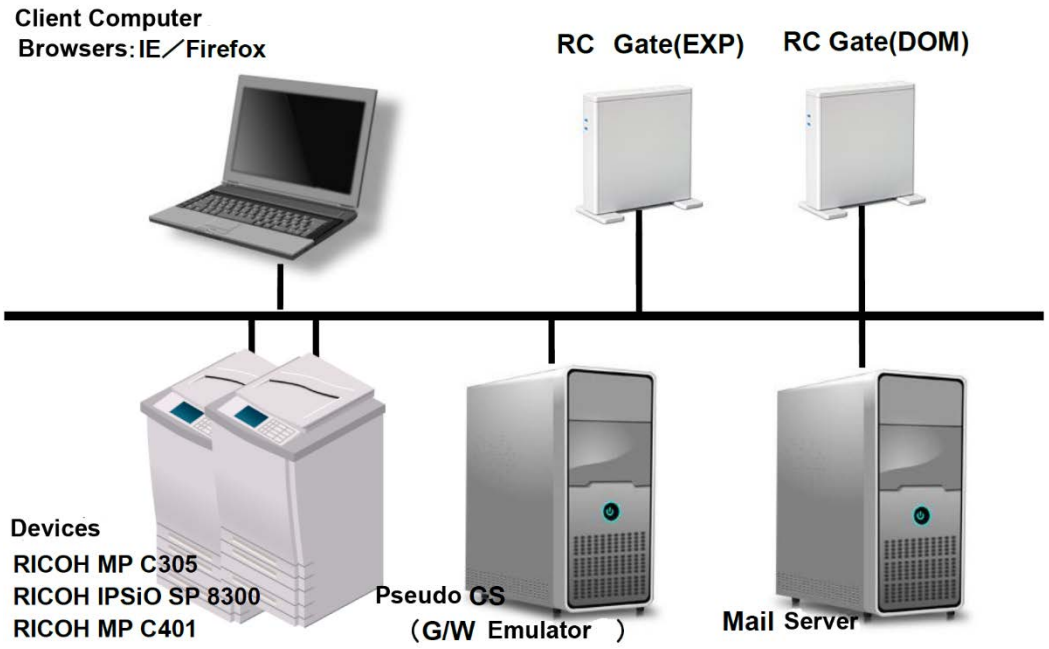

Figure 7-1 Configuration of the Developer Testing

The developer testing was conducted with the following devices connected to the network environment. As the network environment, both IPv4 and IPv6 environments were used.

- CS (Pseudo CS in Figure 7-1)

  A device to emulate the communication of the CS was used.

- Devices (@Remote-supported devices)

  The following devices (all are HTTPS-compatible devices) were used.

  > RICOH MP C305
  > RICOH IPSiO SP 8300
  > RICOH MP C401

- SMTP server (Mail server in Figure 7-1)

  A computer on which the following software run was used.

  > BlackJumboDog 6.2.0

- Client computer

  The computer with Windows 7 Professional SP1 on which the following Web browsers run was used.

  > Internet Explorer 8 / 9 / 10 / 11
  > FireFox 44.0.2

- RC Gate A2 (RC Gate in Figure 7-1)

  This is the TOE and shall correspond with the identification described in the ST.

  > Remote Communication Gate A2 V1.0.2

  The two units, one with settings for Japan (indicated as DOM in Figure 7-1) and the other one with settings for Overseas (indicated as EXP in Figure 7-1), were used.

The configuration of the developer testing differs from the configuration identified in the ST in the following points. However, the evaluator evaluated that the configuration is equivalent to the one in the ST, and that there is no problem with the functional check for the TOE as described below.

- A device to emulate the communication on behalf of the CS was used. Since this device appears to behave in the same manner as the CS to the TOE, it is suitable as a substitute device for the CS.
- This network configuration does not have a firewall. Since the presence of a firewall does not affect the communication between the TOE and the CS, the network configuration in which the firewall is not installed is appropriate as a test configuration.
- SMTP server (Mail server in Figure 7-1) was used only in the IPv6 environment. Since the function of the TOE which sends emails does not depend on the implementation of the IP protocol stack, there is no insufficiency of the testing.

Regarding the following points, some parts of the environment configuration identified in the ST are not included in the configuration of the developer testing. These points are considered not to affect security-related operations. However, the evaluator independent testing is conducted to confirm that these points actually do not affect the operations.

- Registered SNMP-compatible device is not included in the configuration.
- Optional SD card (RICOH Remote Communication Gate A2 Storage 1000) is not included in the configuration.

2) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

For the User Identification and Authentication Function and the Audit Function, the behaviour was confirmed by stimulating the TOE from the external interfaces of the TOE (Web browser, and interfaces for the communication with the Registered HTTPS-compatible devices and the CS), and then by observing the screen display on the Web browser and the output results of the audit log, and the information output or recorded to the device other than the TOE, such as the communication log output to the CS and the status of the Registered HTTPS-compatible devices.

For the Firmware Verification Function, the behaviour of the TOE (output results of the audit log) was confirmed by preparing valid TOE firmware and invalid TOE firmware (such as the firmware with different firmware certificates), and then by downloading them from the CS.

For the Communication Data Protection Function using the TLS, it was confirmed whether the communication between the TOE and the "CS, Registered HTTPS-compatible devices, and Web browser, for which the TLS was confirmed to function properly" was performed properly. In addition, Wireshark was used to capture and observe the communication packets in order to confirm that the communication was performed with a designated protocol.

For the protection of email contents using S/MIME, it was confirmed whether emails sent from the TOE could be properly received by "a mail client for Windows 7 Professional SP1, for which S/MIME was confirmed to function properly."

<Developer Testing Tools>

Table 7-1 shows the tool used for the developer testing. This tool was also used for the evaluator independent testing, and the specification check and performance test were conducted by the evaluator at the time.

Table 7-1 Developer Testing Tool

Tool Name (Version)	Overview / Usage
Wireshark (Ver.1.12.4)	Tool for monitoring and analysing the communication data on the LAN

<Content of the Performed Developer Testing>

By means of the above-described test approaches, applicable security functions were confirmed to function as specified for each interface.

b. Scope of the Performed Developer Testing

The developer testing was performed on 108 items by the developer. The coverage analysis verified the coverage of the testing for Security Functions and external interfaces described in the functional specifications. For some of the external interfaces, the coverage was considered to be insufficient and complemented in the evaluator independent testing.

c. Result

The evaluator confirmed the approach of the performed developer testing and the legitimacy of tested items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach. The evaluator confirmed consistencies between the testing results expected by the developer and the actual testing results performed by the developer.

7.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further assurance that security functions are certainly implemented, based on the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The testing environment for the independent testing was the same as the environment for the developer testing.

The components of the testing environment and programs for the testing were identical to those for the developer testing. The specification check, performance test, and correction were performed by the evaluators.

2) Summary of the Independent Testing

The independent testing includes sampling the results of the developer testing and conducting the evaluator independent testing that the evaluators devised.

Details of the independent testing performed by the evaluators are as follows:

a. Viewpoints of the Independent Testing

<Sampling testing viewpoints>

The evaluators sampled 39 out of 108 items of the developer testing regarding the following viewpoints:

(1) At least one test was sampled from the various categories including interfaces, similar testing, testing environment, and TOE configuration.

(2) In this TOE, the test case for Web interface was selected to enforce the test more than other interfaces, because the greater part of the Security Functions is related to this interface and is complex.

(3) In case of implementing the two types of the normal and abnormal testing for one testing, the abnormal testing was sampled because the normal testing was implicitly conducted in other testing.

<Evaluator independent testing viewpoints>

The evaluators devised the independent testing from the following viewpoints:

(1) For the Web interfaces, etc., the testing items that changed the parameters were added to the items that have insufficient types of the parameters (e.g. values entered as the password, etc.).

(2) No tests to simultaneously check the security functionalities were included in the developer testing, so the test was added to the independent testing.

(3) Since there are verification approaches for the interfaces or functionalities other than those which developers implemented in the developer testing, other approaches were

added to the independent testing due to insufficient verification for the operations in such methods.

(4) There are various types of exception handling for each interface, so that if an exception handling was not tested in the developer testing, it was added to the independent testing.

(5) The functional specifications state the permutational and probabilistic mechanisms of passwords. To check that this function can meet the expectations and assumptions, the test was added to the independent testing.

(6) The test was added for the behaviour of the TOE which was not confirmed in the developer testing.

(7) In case of the operating environment configuration whose operation has not been confirmed in the developer testing, the evaluators confirmed that it would not affect the behaviour of the security for the TOE.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

The independent testing was conducted using the following approaches along with the same approaches used for the developer testing.

- In order to enter parameters which are difficult to enter to the TOE via the Web browser, and to observe output of the TOE which are difficult to observe via the Web browser, the inspection tool of Web vulnerabilities with Proxy traffic was installed.

<Independent Testing Tools>

The independent testing was conducted using the tools specified in Table 7-2, along with the tools used in the developer testing. The specification check and performance test for these tools were conducted by the evaluators.

Table 7-2 Tools Used in Independent Testing

Tool Name (Version)	Overview / Usage
Burp Suite (Ver.1.7.03)	Inspection tool of Web vulnerabilities with Proxy traffic.
Wireshark (Ver.2.0.4)	Tool for monitoring and analysing the communication data on the LAN. (Note) Ver.1.12.4, which is the same as for the developer testing, was used in the sampling testing, and Ver.2.0.4, which is shown on the left, was used in the evaluator independent testing.
AATOOL2 (version 1.10.2)	This tool was used to decode and observe the ASN.1 data.
openssl-1.0.1k-13.fc22	This tool was used to create a public key certificate.
RICOH Remote Communication Gate A2 Storage 1000	The optional SD card for the TOE.
Ricoh MP C306Z	This device was used as an SNMP-compatible device.

<Content of the Performed Independent Testing>

The outlines of the evaluator independent testing are described in Table 7-3.

Table 7-3 Outlines of the Evaluator Independent Testing

Viewpoints of the independent testing	Outlines of the evaluator independent testing
(1) (5)	Checked the operation of the TOE in the variations of character configurations for password, for example, in case of the unavailable characters, etc.
(1) (2) (4)	Checked the operation of the TOE in the variations of character configurations for entering the user name and password to release the screen lock.
(6)	Checked that the information from the Registered SNMP-compatible devices is properly handled in the environment where the Registered SNMP-compatible devices are connected.
(1) (3) (4)	For the User Identification and Authentication Function, checked that the session between the Web browser and the TOE is properly maintained by observing and modifying communication content with Burp Suite.
(6)	Checked that the modification of the firmware can be detected by the Firmware Verification Function when the firmware is modified. Checked that the TLS is properly applied when acquiring the firmware from the CS with Wireshark.
(1)	Checked that operations which are not assumed in the specifications are not available when using the TOE via the various assumed Web browsers.
(7)	Conducted a part of the testing equivalent to the developer testing with the configuration in which the SD card (RICOH Remote Communication Gate A2 Storage 1000) is installed to the TOE, and confirmed that it does not affect the behaviour of the security.
(6)	Checked that the TLS is properly applied to the communications between the TOE and the @Remote-supported devices, as well as between the TOE and the CS, that occur for the Counter per User Retrieval Function, with Wireshark.
(6)	In order to confirm the protection of the email contents using S/MIME, decoded the email contents with AATOOL2 to confirm that appropriate encryption algorithms are configured.
(3)	Checked that there is no sending and receiving of the information that is not assumed in the specifications when using the TOE via the Web browser by observing communication content with Burp Suite.
(1)	For the TLS Certificate Verification Function, checked that certificates with a signature of illegal CA or a self-signed certificate are not accepted.

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation. The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

Table 7-4 Vulnerability of Concern

Vulnerability identifier	Contents
(1)	Security functions may be bypassed to leak or tamper the protected assets of the TOE by initiating network services that are not described in the design materials.
(2)	Security functions may be bypassed to access to the protected assets because operations other than the intended operations are executable for the running network services due to the known vulnerabilities.
(3)	Although this TOE can be remotely accessed by specifying the URL, the identification and authentication and the access control may be bypassed if the URL, for which the session information is not confirmed, exists.
(4)	Due to the functional specifications related to the Audit Logging Function, an arbitrary character code may be entered into the audit log. The TOE may cause unexpected operation, resulting in affecting the secure use of the TOE.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The testing environment for the penetration testing was identical with that of the

independent testing, and also the tools in Table 7-5 were added. The specification check and performance test for the tools have been conducted by the evaluators.

Table 7-5 Penetration Testing Tools

Tool Name (Version)	Overview / Usage
NMAP (Ver. 7.12)	Port Scan Tool
Nessus (Ver. 6.7.0)	Vulnerability scanner
Netcat (v1.11)	General-purpose TCP/UDP operation tool

<Content of the Performed Penetration Testing>

Table 7-6 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-6 Outlines of the Penetration Testing

Vulnerability identifier	Outlines of the penetration testing
(1)	Performed the testing to confirm that ports other than the ones that the TOE provides cannot be accessed by using Port Scan Tool (NMAP).
(2)	Confirmed that there is no exploitable known vulnerability in the network services provided by the TOE by scanning them with the vulnerability scanner (Nessus). Attempted to access to the Web interface, one of the network services provided by the TOE, with Netcat. Attempted to access to the Web interface, which is not assumed to be accessed via the browser, using the browser. At this time, checked the packets captured by Wireshark and confirmed that there is no suspicious packet.
(3)	Examined the URLs, which are accessible after authentication, by using Burp Suite. Accessed to those URLs without authentication and confirmed that the target screens cannot be accessed unless authentication is completed. (Confirmed that the check function for the session information is functioning.)
(4)	Gave inputs including various character codes for the input items which may be reflected to the audit log by using Burp Suite. Confirmed that these inputs do not cause problems for Audit Logging Function.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

The setting values recommended in the guidance document are specified for the initialisation of the TOE at the beginning of the evaluation.

As for the devices used in the testing, there were some differences between the CS/network configuration and the components identified in the ST. In addition, the configuration not covered in the developer testing (configuration including the Registered SNMP-compatible devices and the optional SD card) were covered in the evaluator testing. Therefore, the evaluators determined that the performance of the TOE in the configuration identified in the ST had been assured.

7.6 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance: None

- Security functional requirements: Common Criteria Part 2 Conformant

- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL2 package

- Additional assurance component ALC_FLR.2

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.7 Evaluator Comments/Recommendations

- A function to display the audit log on the Web browser has been assured as a function for performing an audit. Although this TOE has a function to export the audit logs in the CSV format, this function is out of the scope of assurance.

  It should be noted that a secure operation is not assured when using the function which exports the audit logs in the CSV format for performing an audit.

- Both CS and Registered HTTPS-compatible devices should have proper Security Functions in order to protect the contents of the communication with the TOE. Although the CS and the Registered HTTPS-compatible devices are provided by the same developers as the TOE, their Security Functions are out of the scope of assurance.

  That is, the reliability of Security Functions for the CS and the Registered HTTPS-compatible devices needs to be determined separately from assurance by this evaluation, like other operating environments.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Reports shall be adequate.

2. Contents pointed out in the Observation Reports shall properly be solved.

3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL2 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

Procurement entities who are interested in this TOE shall pay attention whether the restrictions and the scope of the evaluation for this TOE match their expected operation conditions by referring to the descriptions in "1.1.3 Disclaimers," "4.3 Clarification of Scope," "7.5 Evaluated Configuration" and "7.7 Evaluator Comments/Recommendations."

The points to note regarding the operational environment for which the performance of the TOE is assured are as follows:

- For the Registered HTTPS-compatible devices, specific three models were assured. The safety when other models are used as the Registered HTTPS-compatible devices needs to be determined separately from assurance by this evaluation.

  > RICOH MP C305
  > RICOH IPSiO SP 8300
  > RICOH MP C401

- For the client computer, both of the following Web browsers (a) and (b) should be available to view the audit logs.

  (a) Any of Internet Explorer 8, 9, 10, or 11
  (b) FireFox 44.0.2

9. Annexes

There is no annex.

10. Security Target

The Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

RICOH Remote Communication Gate A2 Security Target Version 0.42 (November 10, 2016)
RICOH COMPANY, LTD.

11. Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

CS	Communication Server
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
LAN	Local Area Network
OS	Operating System
RC Gate A2	Remote Communication Gate A2
SNMP	Simple Network Management Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator

The definitions of terms used in this report are listed below.

@Remote	A commercial name of this remote service using this TOE.
@Remote-supported device	A device which is specified by the user as a target of @Remote Service.
Administrator (TOE administrator)	An administrator who introduces and manages this TOE. The administrator can change the settings, view the status of the TOE, and view the audit logs from a computer.
CE (Customer Engineer)	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.
Device administrator	A person who manages the maintenance of the devices that are connected to the LAN where the TOE is installed.
HTTPS-compatible device	The RICOH device with the "Remote Management Function." (The availability of the "Remote Management Function" will be publicly announced by RICOH COMPANY, LTD.)

Maintenance centre	A facility where the maintenance of the @Remote-supported devices is managed.
Maintenance information	Information sent from the @Remote-supported devices to the maintenance centre via the TOE. This includes the machine counter information, counter per user information, failure information, and supply information.
Registered HTTPS-compatible device	An HTTPS-compatible device which is specified by the user as a target of @Remote Service.
Registered SNMP-compatible device	An SNMP-compatible device which is specified by the user as a target of @Remote Service.
SNMP-compatible device	A device with the SNMP agent function (not necessary to be the RICOH device).
User	A generic name of "administrator" and "CE."

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001 (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002 (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003 (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004 (Japanese Version 1.0, November 2012)

[12] RICOH Remote Communication Gate A2 Security Target Version 0.42 (November 10, 2016) RICOH COMPANY, LTD.

[13] RICOH Remote Communication Gate A2 Evaluation Technical Report, Version 2.0, December 5, 2016, ECSEC Laboratory Inc. Evaluation Center