Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2015-03-05 (ITC-5536)
Certification No.	C0498
Sponsor	RICOH COMPANY, LTD.
TOE Name	Security Card Type M19 (Japanese name) DataOverwriteSecurity Unit Type M19 (English name)
TOE Version	1.02
PP Conformance	None
Assurance Package	EAL2
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.
2016-03-09

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
"Security Card Type M19 (Japanese name), DataOverwriteSecurity Unit Type M19 (English name)" 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 "Security Card Type M19 (Japanese name), DataOverwriteSecurity Unit Type M19 (English name), Version 1.02" (hereinafter referred to as the "TOE") developed by RICOH COMPANY, LTD., and the evaluation of the TOE was finished on 2016-03 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 "procurement entities who purchase this TOE that is commercially available" 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.

1.1.2 TOE and Security Functionality

This TOE, an optional kit that ensures safe usage of the MFP, is the software that operates inside the MFP. This TOE is saved on an SD Memory Card to be distributed. By operating the MFP with the SD Memory Card installed, this TOE will be read into the MFP and operate.

This TOE overwrites an area on the HDD that is specified by the MFP.

The MFP, on which this TOE can be installed, has an overwrite function identical to that of the TOE. With this TOE installed, the MFP does not use its own overwrite function but uses the overwrite function of this TOE. This ensures that the overwrite function assured by the evaluation is operating.

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

No threats are assumed for this TOE. As a security function, this TOE has the function to overwrite an area on the HDD specified by the MFP. This function is to satisfy the demands of procurement entities when using the MFP.

1.1.2.2 Configuration and Assumptions

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

This TOE is operated while it is installed on the MFP. Refer to "4.2 Environmental Assumptions" for the target MFPs.

This TOE is assumed to be used under the environment where power supply to the MFP does not cease during the MFP operation.

1.1.3 Disclaimers

The assurance covers only the function to overwrite an area on the HDD as specified by the MFP. Whether the MFP instructs appropriately is not included in the 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 2016-03, 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 Report 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:	Security Card Type M19 (Japanese name) DataOverwriteSecurity Unit Type M19 (English name)
TOE Version:	1.02
Developer:	RICOH COMPANY, LTD.

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

Following the procedures described in the guidance documents, users operate the MFP and confirm that the name and version displayed on the screen are identical to those described in the guidance documents.

3. Security Policy

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

This TOE has the function to overwrite an area on the HDD specified by the MFP. This function prevents the leakage of data that exist in the area on the HDD specified by the MFP.

3.1 Security Function Policy

No threats are assumed for the TOE. The TOE possesses the security function to satisfy the organisational security policy shown in Section 3.1.2.

3.1.1 Threat and Security Function Policy

3.1.1.1 Threat

No threats are assumed for this TOE.

3.1.2 Organisational Security Policy and Security Function Policy

3.1.2.1 Organisational Security Policy

An organisational security policy required in use of the TOE is shown in Table 3-1.

Table 3-1 Organisational Security Policy

Identifier	Organisational Security Policy
P.UNREADABLE	The TOE shall prevent the data in the area on the HDD that the MFP specifies from being read. This policy is derived from the requirements considered to be required by procurement entities who operate the MFP.

3.1.2.2 Security Function Policy to Organisational Security Policy

The TOE provides the security function to satisfy the organisational security policy shown in Table 3-1.

(1) Means to support Organisational Security Policy, "P.UNREADABLE"

This TOE has the function to overwrite an area on the HDD specified by the MFP. P.UNREADABLE is achieved by this function.

The overwrite methods described below can be specified in this function. However, when using a function, which is out of the TOE, to encrypt data to be written on the HDD of the MFP, the TOE may not conform to the specified overwrite method. (Refer to "8.2 Recommendations.")

- NSA method
  NSA method overwrites data as follows:
  > overwrites twice by random numbers, and
  > once by Null(0).
- DoD method
  DoD method overwrites data as follows:
  > overwrites once by a fixed value,
  > once by the complements of the fixed value,
  > once by random numbers, and
  > verifies that the data is properly overwritten by reading the HDD.
- Random number method
  Random number method overwrites data the specified number of times (1–9 times) using random numbers.
- BSI/VSITR method
  BSI/VSITR method overwrites data seven times by 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA in this order.

  Note: This method can be specified only when using the batch overwrite function. (Refer to "5.1 TOE Boundary and Components.")

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 performance of the TOE security function is not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.MODE.AUTOMATIC	The TOE operations shall not be interrupted by MFP power-off before the TOE completes overwrite operations by the sequential overwrite method. In sequential overwriting, the MFP instructs the TOE to overwrite the area on the HDD of the MFP when any unnecessary data is generated.
A.MODE.MANUAL	Against user's will, the implementation of the Batch Overwrite Function of the TOE shall not be unintentionally suspended by the operation of temporary suspension button or the MFP power-off, before the TOE completes overwrite operations by the Batch Overwrite Function. In batch overwriting, the MFP instructs the TOE to overwrite all area on the HDD.
A.MFP	The MFP with the TOE installed shall be properly set up and operated without any failure.

4.2 Environmental Assumptions

This TOE is installed and operated on any of the MFPs of "RICOH MP CW2201/CW1201 Series."

The reliability of hardware and software of the MFP is outside the scope of this evaluation (it is assumed to be trustworthy).

4.3 Clarification of Scope

This TOE overwrites an area on the HDD as specified by the MFP (which is outside the scope of the TOE). The instruction by the MFP (which is outside the scope of the TOE) also specifies the area on the HDD.

5. Architectural Information

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

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE.

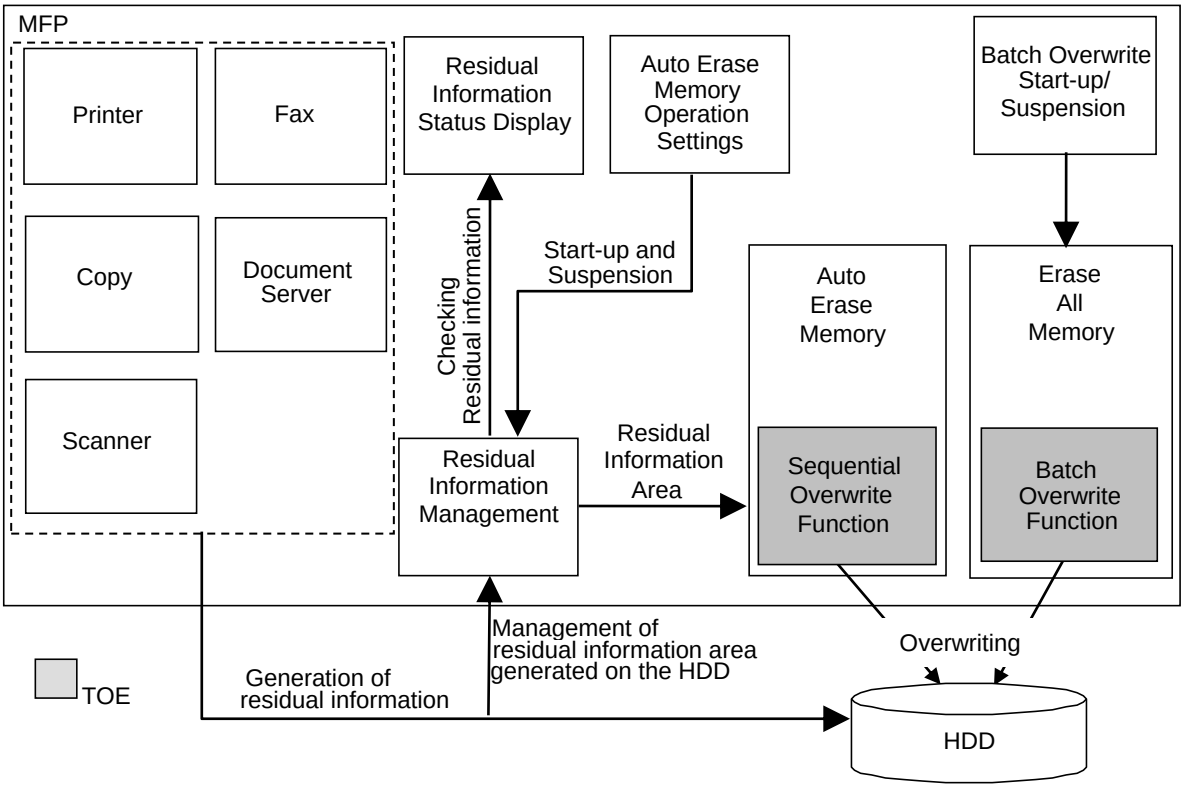

Figure 5.1 Configuration and Operation Environment of the TOE

Shown below are the explanations of Sequential Overwrite Function and Batch Overwrite Function, which are the components that configure the TOE.

- Sequential Overwrite Function
  As the TOE receives an instruction from "Residual Information Management" of the MFP to overwrite the area on the HDD where residual information exists, the TOE executes overwrite operation on the area.

- Batch Overwrite Function
  As the TOE receives an instruction from "Batch Overwrite Start-up/Suspension" to start batch overwriting, the TOE overwrites all areas on the HDD. The overwrite operation can be suspended by the instruction from the MFP as well.

5.2 IT Environment

This TOE operates inside the MFP. Software that controls the MFP also operates inside the MFP, besides this TOE. This TOE is operated by the instructions from the software that control the MFP.

- Residual Information Management

  This is a function to manage the area on the HDD where residual information exists. Any residual information, generated when using the MFP functions, is notified to the "Residual Information Management." The "Residual Information Management" instructs the "Sequential Overwrite Function" of the TOE to overwrite.

  "Residual information" is the data as described below:

  > The MFP provides the functions of Copy, Printer, Scanner, Fax, and Document Server. When performing these functions, the MFP creates on the HDD the temporary working data, including a part of or all data of documents. The temporary working data that become unnecessary when those functions terminate become the "residual information."

  > The MFP can store documents on the HDD using Document Server Function. When users instruct the MFP to delete the stored documents, the target documents to be deleted become the "residual information."

- Auto Erase Memory Operation Settings

  This is a function to set whether "Residual Information Management" gives an instruction to overwrite.

- Batch Overwrite Start-up/Suspension

  This is a function to instruct "Batch Overwrite Function" of the TOE to start or suspend batch overwriting.

- Residual Information Status Display

  This is a function to display an icon representing the residual information status on the MFP's Operation Panel. The icon indicates three states: residual information available, no residual information available, and data being overwritten.

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.

Documents for Japan

- Security Card Type M19 Operating Instructions D3BS-7000

Documents for overseas

- DataOverwriteSecurity Unit Type M19 Operating Instructions D3BS-7002

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 is agreed on mutual recognition with 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 2015-03 and concluded upon completion of the Evaluation Technical Report dated 2016-03. 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 2015-10 and 2016-01, and examined the procedural status conducted in relation to each work unit for configuration management and 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 2015-10.

Concerns found in evaluation activities for each work unit were all issued as the Observation Report, and it was 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 verifying the evidence shown in the process of the evaluation and the testing performed by the developer, the evaluator performed the reproducibility testing and additional testing judged to be necessary. As a result of vulnerability assessments, the evaluator determined that the penetration testing was not 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

The developer testing was performed with the TOE installed on the following MFP.

- RICOH MP CW2201 (System version: 0.20)

The following testing tools were also used for operating tests and observing results.

- Computers for testing
  Computers on which terminal software connected to the MFP via RS232C or Ethernet were used.
- SATA protocol analyser
  ST2-31-4-A (DE), manufactured by Catalyst Enterprises, Inc.
- Other devices
  A boot server to start the MFP in boot mode
  A mail server when using e-mail sending function

Specific versions of the specific MFP models identified in the ST were used as the TOE operation environment. Since the parts related to the TOE on the MFP identified in the ST have common behavior regardless of models or versions, the evaluator determined that the testing was conducted on the environment equivalent to the MFP identified in the ST.

Therefore, it can be concluded that the developer testing was performed in the TOE testing environment, which was identical to the TOE configurations specified in the ST.

2) Summary of the Developer Testing

A summary of the developer testing is described as follows.

a. Developer Testing Outline

An outline of the developer testing is described as follows.

<Developer Testing Approach>

The following methods were used to stimulate the TSFI and observe the behaviour of the TSFI. The evaluator had confirmed that the "TOE for testing" and the "MFP with a mode in which the behaviour of the OS can be observed" are appropriate for operation check of the TOE.

- Operating from the Operation Panel of the MFP, and checking the display of the Operation Panel.
- Using the TOE for testing with the additional function to output logs as well as the MFP with a mode in which the behaviour of the OS can be observed, and checking the behaviour of the OS in the TOE and the MFP from the computers for testing connected to the MFP.
- Monitoring the interface to the HDD using SATA protocol analyser.

(Note) Regarding a boot server and a mail server in the developer testing environment:
A boot server was used to set the MFP mode in which the behaviour of the OS can be observed.
A mail server was prepared for the testing in which a mail is sent from the MFP by the MFP operation.

<Content of the Performed Developer Testing>

The TSFI was stimulated by the MFP operation. The MFP operation was performed covering parameters of each TSFI.

By checking the behaviour of the OS in the TOE and the MFP from the computers for testing, it was confirmed that the TOE operated as parameters intended. In addition, whether overwriting was properly performed was checked by monitoring, using SATA protocol analyser.

b. Scope of the Performed Developer Testing

The developer testing was performed on 57 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested. As a result, it was found that some parameters related to the behaviour of security functions might have not been sufficiently tested. Therefore, the independent testing was conducted by the evaluator to cover this insufficiency.

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 configuration of the testing performed by the evaluator was the same as the configuration of the developer testing except that the MFPs shown below were used. The evaluator judged that the MFP configuration, which differs from that of the developer testing, has no influence on the TOE testing.

- RICOH MP CW1201 (System version: 0.22)
- RICOH MP CW2201 (System version: 0.22)

The testing tools used for the independent testing were identical to those used in the developer testing. Operation check of the testing tools was performed by the evaluator.

2) Summary of the Independent Testing

A summary of the independent testing is described as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluator designed from the developer testing and the provided evaluation documentation are shown below.

<Viewpoints of the Independent Testing>

1. For the sampling of the developer testing, sufficient tests should be selected so that all security functions and interfaces are subject to be sampled.
2. If there is a concern in sufficiency of the developer testing in terms of the completeness of the parameters or the timing of interface usage, additional proprietary testing to cover the developer testing will be devised.

b. Independent Testing Outline

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

<Independent Testing Approach>

The same methods with the developer testing were used.

<Independent Testing Tools>

The same testing tools with the developer testing were used.

<Content of the Performed Independent Testing>

Table 7-1 shows viewpoints of the independent testing and the content of the testing corresponding to them.

Table 7-1 Content of the Performed Independent Testing

Viewpoint	Outline of the Independent Testing
1	By performing the same testing with the developer testing, from which the test items were extracted based on the viewpoints of testing, it is confirmed that the results were identical to those of the developer testing. The testing was performed on 19 items.
2	When overwrite method is changed during sequential overwriting, it is confirmed that overwriting is performed by the expected overwrite method.
2	When performing more than one sequential overwriting simultaneously, it is confirmed that more than one object is overwritten.
2	For sequential overwriting function and batch overwrite function, there is a concern that the parameter of the number of overwriting might not have been sufficiently tested during the developer testing. Therefore, by changing the number of overwriting to another number that is not used in the developer testing, it is confirmed that the expected number of overwriting is performed.

c. Result

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

7.4.3 Evaluator Penetration Testing

From the evidence shown in the process of the evaluation, the evaluator analysed if the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level exist.

As a result of the analysis, the evaluator concluded that such vulnerabilities did not exist in the scope of the TOE for the reasons described below. Therefore, the penetration testing was unnecessary.

- This TOE is the software inside the MFP. In its usage environment, this TOE operates indirectly with the use of MFP functions.
- Considering such usage environment, as for the potential access to this TOE in the scope of the assumed attack level, the behaviour of this TOE is sufficiently verified in the developer testing and the independent testing.

a. Result

Based on the analysis 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

This TOE is assumed to be installed on the MFP models indicated in "4.2 Environmental Assumptions." The TOE was installed on some of those MFP models in the evaluated configuration.

For the reasons shown in "7.4.1 Developer Testing," the evaluator determined that the evaluation could be assured when any of the MFPs indicated in "4.2 Environmental Assumptions" is used as the configuration of the evaluation.

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 Extended
- 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

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

There is no evaluator recommendation to be addressed to procurement entities.

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 Report shall be adequate.

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

3. The submitted documentation was sampled, the contents were 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 Report and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL2 in the CC Part 3.

8.2 Recommendations

- The evaluation only assures that the overwriting by this TOE is performed "as specified by the MFP."
- Whether the MFP instructs appropriately is not included in the scope of the assurance. Concerning an overwrite instruction to this TOE by the MFP, for instance, the following points are not included in the scope of the assurance.
  - > Whether the area with residual information generated by the MFP use is correctly specified.
  - > Whether an overwrite instruction is given at appropriate timing.
- To effectively operate security functions of this TOE, the following MFP functions of the TOE operation environment must be operated correctly:
  - > To allow only the MFP administrator to enable or disable the sequential overwriting function.
  - > To display the TOE status to determine whether the TOE is operating or not.
  - > To properly notify the MFP administrator of the situations where the TOE does not operate correctly due to MFP failures.

> To enable the input of values within the assumed scope as the value specified in the overwrite method or as the number of overwriting.
> Note that the TOE interface accepts the input of values even outside the assumed scope in specification (for example, more than 9 can be input as the number of overwriting).

This evaluation does not assure the behaviour of the MFP functions of the TOE operation environment. Therefore, procurement entities have responsibility for proper operation of the MFP functions. The evaluator determined that the appropriate guidance documents were to be provided.

- When using and operating a function, which is out of the TOE, to encrypt data to be written on the HDD of the MFP, the data to be overwritten is encrypted by Sequential Overwrite Function (Auto Erase Memory). Therefore, if NSA and DoD methods are specified when using Sequential Overwrite Function, the TOE does not conform to these methods. (When writing the fixed data, such as constants and complements, the data that is actually overwritten is changed by the encryption function.)

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.

Security Card Type M19, DataOverwriteSecurity Unit Type M19 Security Target
Version 3.03 (February 24, 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
TSFI	TSF Interface

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

DoD	Department of Defense
HDD	Hard Disk Drive
MFP	Multi Function Product
NSA	National Security Agency
OS	Operating System
SATA	Serial Advanced Technology Attachment (One of the HDD interfaces)

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

Document Server Function	One of the MFP functions. This function allows users to store scanned paper document data on the HDD of the MFP. In addition, by using its Copy, Print, Fax, and Document Server Functions, users can print and delete the document that is stored on the HDD of the MFP.
SD Memory Card	A secure digital memory card. A highly functional memory card that is the size of a postage stamp and can be used to install the TOE and other applications on the MFP.

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] Security Card Type M19, DataOverwriteSecurity Unit Type M19 Security Target Version 3.03 (February 24, 2016) RICOH COMPANY, LTD.

[13] Security Card Type M19 (Japanese name), DataOverwriteSecurity Unit Type M19 (English name) Ver.1.02 Evaluation Technical Report, Version 2.1 (VST-ETR-0002-01) March 1, 2016, ECSEC Laboratory Inc. Evaluation Center