Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-11-16 (ITC-9279)
Certification No.	C0253
Sponsor	RICOH COMPANY, LTD.
Name of TOE	imagio Security Card Type 9 Software (Japanese name) DataOverwriteSecurity Unit Type I Software (English name)
Version of TOE	1.01m
PP Conformance	None
Conformed Claim	EAL3
Developer	RICOH COMPANY, LTD.
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2010-03-29

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2

Evaluation Result: Pass

"imagio Security Card Type 9 Software (Japanese name), DataOverwriteSecurity Unit Type I Software (English name) Version 1.01m" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" 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

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "imagio Security Card Type 9 Software (Japanese name), DataOverwriteSecurity Unit Type I Software (English name) Version 1.01m" (hereinafter referred to as "the TOE") conducted by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, RICOH COMPANY, LTD. and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the corresponding ST. The operational conditions, details of usage assumptions, corresponding security objectives, security functional and assurance requirements needed for its enforcement, their summary of security specifications and rationale of sufficiency are specifically described in ST.

This certification report assumes "consumer who purchase the TOE or person who are responsible for management of MFP in which the TOE is installed" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

1.1.1 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

1.1.2 PP Conformance

There is no PP to be conformed.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows;

Name of Product:	imagio Security Card Type 9 (Japanese name) DataOverwriteSecurity Unit Type I (English name)
Version:	1.01m
Developer:	RICOH COMPANY, LTD.

1.2.2 Product Overview

The target product of this certification is the software that is installed on the MFP and saved on the SD Memory Card.
Because of this, "Software" is added to the TOE name to clarify that the target of evaluation is not the SD Memory Card but the software that is saved on the SD Memory Card.
This product is an optional kit that ensures safe usage of MFP and overwrites the area on the HDD that is specified by the MFP.

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Scope of TOE and Operational Environment

The scope of the TOE is the same as the product described in "1.2.1 Name of Product". Fig.1-1 shows the relation between the TOE and MFP as TOE's operational environment. The TOE is saved on the SD Memory Card, and the SD Memory Card is inserted into the SD CARD slot of MFP. The TOE is loaded on the Controller Board inside the MFP, and operates on the Controller Board.

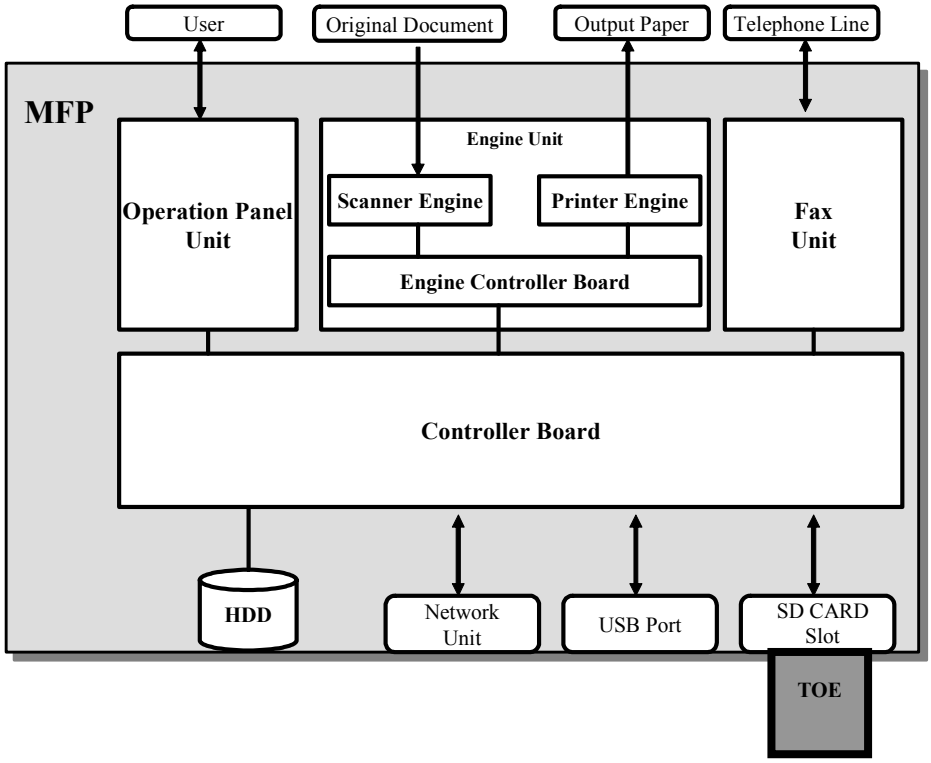

Fig.1-1 TOE and its Operational Environment "MFP"

1.2.3.2 TOE Security Functions

The TOE has the function to overwrite the area on the HDD that is specified by the MFP.

The MFP specifies the area on the HDD where the residual data exists. Assuming that the MFP correctly specifies the area where the residual data exist, the TOE overwriting prevents the residual data from being leaked.

The residual data includes the following:

- The MFP provides the functions of copier, printer, scanner, fax, and document server. The MFP creates temporary working data on the HDD including some or all of the document information when these functions are implemented. When these functions are terminated, temporary working data become unnecessary data, that is residual data.
- The MFP can store documents on the HDD using the Document Server Function. When a user sends instructions to the MFP to delete the stored document, the target document to be deleted will become residual data.

It is assumed that the MFP specifies the area on HDD in the following method:

- If the MFP is normally used, the MFP specifies the area where the residual data exists whenever it is generated for the TOE. (Sequential Overwrite)
- If the HDD is replaced or disposed of, or the MFP is returned, users can send instructions to the MFP to overwrite the whole area on the HDD. The MFP specifies the whole area on the HDD for the TOE. (Batch Overwrite)

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow;

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "imagio Security Card Type 9, DataOverwriteSecurity Unit Type I Security Target" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "imagio Security Card Type 9 Software (Japanese name), DataOverwriteSecurity Unit Type I Software (English name) Version 1.01m Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2010-03 submitted by the evaluation facility and those concerns pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

2. Summary of TOE

2.1 Security Problem and assumptions

The problems that the TOE should solve and the assumptions that are required for the TOE usage are as follows:

2.1.1 Threat

No threats are assumed for this TOE.

2.1.2 Organisational Security Policy

Table 2-1 shows the organisational security policy required for the TOE usage.

Table 2-1 Organisational Security Policy

Identifier	Organisational Security Policy
P.UNREADABLE	The TOE shall protect the data area on the HDD that the MFP specifies and prevent the data in the area from being read.

2.1.3 Assumptions for Operational Environment

Table 2-2 shows the environmental assumptions for the TOE usage.
Unless these assumptions are not satisfied, effective performance of the security functions of this TOE cannot be assured.

Table 2-2 Assumptions in Use of the TOE

Identifier	Assumptions
A.MODE.AUTOMATIC	The TOE operations shall not be interrupted by MFP power-off while the TOE completes overwrite operations by the sequential overwriting method.
A.MODE.MANUAL	The implementation of the Batch Overwrite Function of the TOE shall not be unintentionally suspended while the TOE completes overwrite operations by the Auto Erase Memory Function. The unintentional suspension means the operation of temporary suspension button or the MFP power-off.

2.1.4 Documents Attached to Product

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

Document for Japanese products

- imagio Security Card Type7
  imagio Security Card Type9
  Operating Instructions

Version D377-7902

Documents for overseas products

- DataOverwriteSecurity Unit Type H
  DataOverwriteSecurity Unit Type I
  Operating Instructions
  Version D377-7940

- Notes for Users D377-7250

2.1.5 Configuration Requirements

This TOE can be installed on the MFPs shown in Table 2-3. However, evaluation on the reliability of the hardware and software of the MFPs that this TOE is installed on is not covered by this evaluation.

Table 2-3 TOE Installable MFP

Japanese Product Name	Overseas Product Names
Ricoh imagio MP 4000/5000 series	Ricoh Aficio MP 4000/5000 series Savin 9040/9050 series Lanier LD 040/050 series Lanier MP 4000/5000 series Gestetner MP 4000/5000 series infotec MP 4000/5000 series nashuatec MP 4000/5000 series Rex-Rotary MP 4000/5000 series

2.2 Security Objectives

The TOE satisfies the organisational security policy in 2.1.2 with its security functions as described below.

2.2.1 Realisation of P.UNREADABLE

In order to satisfy P.UNREADABLE, the TOE has the function to overwrite the area on the HDD that the MFP specifies using specific methods.

The MFP specifies the area on the HDD for the TOE using the following two methods.

- Sequential Overwrite Function
  The MFP's Residual Data Management Function constantly monitors the residual data area on the HDD. If an area of generated residual data is detected, the TOE applies data overwrite operations to the residual data area.

- Batch Overwrite Function
  When receiving batch overwrite instructions from the MFP, the TOE applies batch overwrite operations to the data that is stored on the HDD. For the batch overwrite instructions, the TOE applies the operation on the whole area on the HDD.

Optional overwrite methods are as follows:

- NSA Method
  NSA Method overwrites the data as follows:
  > Overwrites twice with random numbers.

> Overwrites once with Null (0).

- DoD Method
  DoD Method overwrites the data as follows:
  > Overwrites once with a fixed value.
  > Overwrites once with the complement of the fixed value.
  > Overwrites once with random numbers.
  > Lastly, executes the verification.

- Random Number Overwrite Method
  Overwrites the specified number of times (1 to 9 times) with random numbers.

It is not the TOE that manages the area on the HDD but the MFP, which is the TOE's operational environment. The TOE provides protections for the area managed by the MFP. To facilitate TOE users' understanding of this behaviour, P.UNREADABLE is defined as the organisational security policy, NOT as a threat.

3. Conduct and Results of Evaluation by Evaluation Facility

3.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

3.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows;

Evaluation has started on 2009-11 and concluded by completion the Evaluation Technical Report dated 2010-03. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2009-12 and 2010-03 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-12.

About some portions of procedural status conducted in relation to work unit for development security, the evaluation facility determined that the result that was examined on 2007-12, 2009-08 and 2009-09 as evaluation of another TOE (that assurance level is same as the TOE) was now also acceptable, and accepted the result as evaluation of the TOE.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

3.3 Product Testing

The evaluator confirmed the validity of the test that the developer had executed. The evaluator executed reappearance tests, additional tests and penetration tests based on vulnerability assessment judged to be necessary from the evidence shown by the process of the evaluation and results by the verification of the developer testing.

3.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing conducted by the developer and the deliverables of actual test results. The overview of evaluated developer testing is shown as the following:

1) Developer Test Environment

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

- Ricoh imagio MP 4000 / Ricoh Aficio MP 4000

(System version: 2.00)

The following devices were also used for the test and result observation.

- Computers for testing
  Terminal software connected to MFP via RS232C or Ethernet.

- IDE bus analyser
  IDE-Pocket Ultra DMA/100 supported, manufactured by TOYO Corporation

- Other devices:
  A boot server to start the MFP in boot mode
  A mail server to enable e-mail sending function

Some of MFP models identified in the ST were used as the TOE operational environment. The differences between the MFPs identified in the ST were examined. Accordingly, the evaluators also verified those MFP models used for the test bridge the gaps between the MFP models identified in the ST.
Therefore, it can be concluded that the developer testing was performed in the TOE testing environment, which was identical with the TOE configurations specified in the ST.

2) Overview of Developer Testing

Outlining of the testing performed by the developers is as follows:

a. Test Overview

The following methods were used to stimulate the TSFI and observe the behaviour of the TSFI.

- Operate using the Operation Panel, and check the display of the Operation Panel.

- Check the log details that were sent to the testing computer connected to the MFP.

- Monitor the interface to the HDD using IDE bus analyser.

b. Test Scope

The developer testing included 51 items.
It is verified that a coverage analysis was conducted, and all of the security functions and external interfaces described in the functional specifications were fully tested. Also, it was verified that a depth analysis was conducted, and all of the subsystems and subsystem interfaces described in the TOE design were fully tested.

c. Results

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

3.3.2 Evaluator Independent Testing

To revalidate that the security functions of the product were accurately implemented, the evaluators performed an independent testing with reference to the evidence, which was provided during the evaluation process. The following is an overview of the independent testing performed by the evaluators.

1) Evaluator Independent Testing Environment

The configuration of the tests conducted by the evaluators was the same as the configuration of the developer testing.

2) Overview of Evaluator Independent Testing

Outlining of the independent testing performed by the evaluators is as follows:

a. Viewpoints of Independent Testing

15 items were tested, of which 4 items were originally devised by the evaluators and 11 items were borrowed from the sampling of the developer testing. The testing items were devised according to the selection criteria based on CEM: ATE_IND.2-4 and ATE_IND.2-6. The major viewpoint is as follows:

(1) If the sufficiency of the developer testing can be doubted in terms of the completeness of the parameters or the timing of interface usage, additional proprietary testing for the developer testing will be devised.

(2) For the sampling of the developer testing, sufficient tests should be sampled so that all security functions and interfaces are subject to sampling.

b. Test Overview

The testing tools and approaches used for the independent testing by the evaluators were identical with those used in the developer testing.

c. Results

All of the evaluator independent testing were completed correctly, and the behaviour of the TOE could be confirmed. The evaluator confirmed that all the test results were in conformity with the expected behaviour.

3.3.3 Evaluator Penetration Testing

The evaluator devised and conducted the necessary penetration testing about the possibility of exploitable concern at assumed environment of use and attack level, with reference to the evidence, which was provided during the evaluation process. Outlining of the evaluator penetration testing is as follows:

1) Evaluator Penetration Testing Overview

Outlining of penetration testing performed by the evaluator is as follows:

a. Vulnerability of concern

The evaluator searched a deliverables and the public domain information for the potential vulnerabilities and then identified the following vulnerabilities which require the penetration testing.

- If the SD Memory Card that contains the TOE is removed, users may continue to use the TOE if they do not recognise the removal of the Card.
- Unexpected TOE behaviour may result if unexpected values are entered into the TOE interfaces.
- The contents of the SD Memory Card that contains the TOE may change. Users may continue to use the TOE if they do not recognise this.

- The data that the TOE overwrites may remain undeleted if the MFP is turned off while the TOE is overwriting the data, or other accidents occur.

b. Scope of Test Performed

The evaluator conducted the following penetration testing to determine the exploitable potential vulnerability:

- Remove the SD Memory Card that contains the TOE from the MFP, and check if users can recognise that the Card has been removed from the MFP.
- Operate the MFP in the TOE operational environment, and check if unexpected values can be entered into the TOE interfaces.
- Insert into the MFP the SD Memory Card whose contents have been modified, and check if users can recognise that the contents have been modified.
- Turn off the power of the MFP while the TOE is overwriting data, and turn on the power again. Check if the TOE overwriting processes can be resumed and completely ended.

c. Results

In the conducted evaluator penetration testing, the vulnerability that attackers who have the assumed attack potentials could exploit was not found.

3.4 Evaluation Result

3.4.1 Evaluation Result

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

3.4.2 Evaluator comments/Recommendations

There is no evaluator's recommendation to be reported to consumers.

4. Conduct of Certification

The certification body conducted the following certification based on each materials submitted by evaluation facility during evaluation process.

1. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
2. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
3. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification review and were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in certification review were solved in the ST and the Evaluation Technical Report and issued this certification report.

5. Conclusion

5.1 Certification Result

The Certification Body verified the Evaluation Technical Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body determined the TOE is satisfied the assurance requirements of EAL3 components prescribed in CC Part 3.

5.2 Recommendations

None.

6. Glossary

The abbreviations relating to 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 Functions

The definition of terms used in this report is 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, and Document Server Functions, users can print and delete the document that is stored on the HDD of the MFP.

MFP:
A digital multi function product.
A printer with multiple functions (copy, print, etc.)

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.

7. Bibliography

[1] imagio Security Card Type 9, DataOverwriteSecurity Unit Type I Security Target Version 1.00 (March 25, 2010) RICOH COMPANY, LTD.

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 2, September 2007, CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 2, September 2007, CCMB-2007-09-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001 (Japanese Version 1.2, March 2007)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 2, September 2007, CCMB-2007-09-002 (Japanese Version 2.0, March 2008)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 2, September 2007, CCMB-2007-09-003 (Japanese Version 2.0, March 2008)

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004

[12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004 (Japanese Version 2.0, March 2008)

[13] imagio Security Card Type 9 Software (Japanese name), DataOverwriteSecurity Unit Type I Software (English name) Version 1.01m Evaluation Technical Report Version 4.0, March 25, 2010, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center