CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9217**
Product / system:	Security SW Module for Ricoh's Multi-Functional-Printers **Software module, version 1.00 of** **imagio Security Module Type A,** **imagio Security Card Type A,** **DataOverwriteSecurity Unit Type A, and** **DataOverwriteSecurity Unit Type B** summarized as "Software Module V1.00 of the HSM Kit"
Product manufacturer:	Ricoh Company, Ltd. 1-3-6 Nakamagome, Ohta-ku Tokyo, 143-8555 Japan
Customer:	see above
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 1.1 as of 2004-01-21* Document-number: *20588724_TÜV_016.02* Author: Peter Herrmann
Result:	EAL3
Evaluation stipulations:	none
Certifier:	Joachim Faulhaber
Certification stipulations:	none

Essen, 2004-01-21

Dr. Christoph Sutter Joachim Faulhaber

Contents

Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate

Deutsches IT-Sicherheitszertifikat

anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

The Certification Body of TÜV Informationstechnik GmbH

hereby certifies that for Multi-Functional-Printers of Ricoh the

Software Module Version 1.00 of

imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,

of

Ricoh Company, Ltd., Tokyo, Japan

has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and *CEM Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.1* (ISO 15408) with the following results:

SECURITY FUNCTIONALITY
Product specific Security Target
Common Criteria part 2 conformant

ASSURANCE PACKAGE
Common Criteria part 3 conformant
EAL 3

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report. The recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TÜV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No.
TUVIT-DSZ-CC-9217-2004

Essen, 2004-01-21 **signed by Dr. Gruschwitz**
Certification Body

TÜV Informationstechnik GmbH - Subsidiary of the RWTÜV Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • 🖷 +49 201 8999-555 • tuvit@tuvit.de • www.certuvit.de
accredited for IT security certifications under DAR-registration no. DIT-ZE-006/99-00 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)

2 Certification Body – CERTÜViT

CERTÜViT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – a subsidiary of the RWTÜV Group - was established in 1998 and offers a variety of services in the context of security evaluation and validation.

CERTÜViT was accredited in September 1999 for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (Dekitz)* now *Deutsche Akkreditierungsstelle Technik e.V. (DATech), Frankfurt/Main* under DAR-registration no. DAT-ZE-014/99-00 and performs its projects under a quality management system certified against ISO 9001 by *Germanischer Lloyd, Hamburg*.

CERTÜViT is accredited by *Bundesamt für Sicherheit in der Informationstechnik*[2] to issue the “German IT Security Certificate” which is recognised by BSI as equivalent to the “German IT Security Certificate” of BSI.

3 Specifications of the Certification Procedure

The certification body conducts the certification procedure according to the criteria laid down in the following:

- DIN EN 45011
- TÜViT Certification Scheme
- TÜViT Certification Conditions
- Regulations on the “German IT Security Certificate” issued by the BSI and accepted in the contract of BSI and TÜViT as of December 2, 1997 (renewed on the 20th of November 2002).
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.1, August 1999.
- Common Methodology for Information Technology Security Evaluation (CEM) part 1, version 0.6, January 1997.

[1] in the following termed shortly TÜViT

[2] in the following termed shortly BSI

- Common Methodology for Information Technology Security Evaluation (CEM) part 2, version 1.0, August 1999.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

4 Recognition Agreements

In order to avoid multiple certification of the same product by different certification bodies a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC - under certain conditions was agreed. The CERTÜViT certificates are recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates.

4.1 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4 was signed between the national participants of Australia and New Zealand, Austria, Canada, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, The Netherlands, Norway, Spain, Sweden, Turkey, United Kingdom and the United States.

4.2 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The arrangement on the mutual recognition of IT security certificates based on the CC was extended by these participants up to and including the evaluation assurance level EAL7.

5 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The product Software Module V1.00 of the HSM Kit as undergone the certification procedure at TÜViT certification body. It was an initial certification.

The evaluation of the product Software Module V1.00 of the HSM Kit as conducted by the evaluation body for IT-security of TÜViT and concluded on January 21st, 2004. The TÜViT evaluation facility is recognised by BSI.

The sponsors as well as developers are Ricoh Company, Ltd. Distributors of the product are Ricoh Company, Ltd.

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on November 21st, 2004. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

This certification report applies only to the version of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

With regard to the meaning of the evaluation assurance levels (EAL) and the strength of function (SoF), please refer to part C of this report.

6 Publication

The following Certification Results consist of pages B-1 to B-18. The product Software Module V1.00 of the HSM Kit will be included in the BSI list of certified products which is published at regular intervals (e.g. in the Internet at http://www.bsi.bund.de) and the TÜViT certification lists (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the Certification Result

1 Executive Summary

1.1 Target of Evaluation and Evaluation Background

The product type is the software module of a Hard Disc Security Module (HSM) Kit for Ricoh's Multi-Functional Printer (MFP). MFP has not only basic copier function but also the several types of options, e.g. facsimile, printer or scanner in a body. MFP is used mostly in general office and input data or printed images are stored on the Hard Disc Drive (HDD) installed inside. For example copy image data will be printed out after temporary storage on the HDD.

HSM has a security function to clean up the temporary storage area of the Hard Disc Drive (HDD) in order to be unable to detect the traces of data. HSM adopts the overwriting method that is random digits are overwritten twice and null (0) data are overwritten once on the target area. HSM is delivered as an optional kit for Ricoh MFP, so that customer can add HSM Kit after setting MFP.

When HSM is in operation, two kinds of icons are displayed on the operation panel of MFP depending on the situation. The icons indicate the status of residual data on the HDD. One indicates existence of residual rata and another indicates no existence. Hereby customer can confirm easily whether residual data remains or not. The displaying of icons is the evidence that HSM Kit has installed correctly and the overwriting function is operating. Overwriting starts automatically if residual data exists without any user intervention.

To cover the different printers the Hard Disc Security Module Kits consist of different media. These are either a SD memory card (named *imagio Security Card Type A* in Japan or *DataOverwriteSecurity Unit Type B* in other countries respectively) or a DIMM-ROM (named *imagio Security Module Type A* in Japan or *DataOverwriteSecurity Unit Type A* in other countries respectively). Each type of media use the same software, which is considered here as the TOE, to execute the same security functionality.

The TOE[3] is defined as: *Software module version 1.00 of*
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B

[3] In the developer documents the TOE is for convenience also specified in a short form as "Software module of the Hard Disk Security Module Kit V1.00". In the evaluation reports this specification is also used.

The four listed product types of the Hard Disc Security Module Kit are dedicated to be an optional component of one of four types of Multi-Functional Printers. The assignment which product type is adaptable to which printer can be gathered from the table in chapter 2.5 of the security target (attached in part D).

The sponsor, vendor and distributor is “Ricoh Company, Ltd., 1-3-6 Nakamagome, Ohta-ku, Tokyo, 143-8555 Japan“

The TOE was evaluated against the claims of the Security Target[4] (attached in part D) by the “*evaluation body of TÜV Informationstechnik GmbH*” (TÜViT). The evaluation was completed on January 21st, 2004. TÜViT’s evaluation body is recognised by BSI.

1.2 Assurance Package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 3 (Evaluation Assurance Level 3).

1.3 Strength of Functions

The sponsor claimed no minimum strength of function level of the TOE security function.

1.4 Functionality

For the TOE there has been defined one security requirement, which has exclusively been taken from CC part 2 (i.e. the set is CC part 2 conformant) [CC] and which belongs to the functional class “User Data Protection”. The security functional requirement is met by a suitable IT security function realized by the TOE:

SF.OVERWRITE TSF overwrites the area of Residual Data based on the permission from the MFP. TSF uses the overwriting method that is to write random data twice and null (0) data once.

TSF starts to overwrite after completion of a copy/print job. If the power supply is cut off while TSF is overwriting, TSF restarts to overwrite when the MFP is switched on after recovery of the power supply.

A copy/print job has priority to TSF. If another job is running at the start of TSF, TSF waits for the job to be over and starts to overwrite. If another job starts to run while TSF is overwriting, TSF gets into suspended and restarts after the job completion.

[4] hereinafter called ST

1.5 Summary of Threats and Organisational Security Policies (OSPs)

The assets that the TOE intends to protect are residual data in temporary area of the hard disk, installed in the MFP. This “protect” means getting the residual data unable to be analysed by means of overwriting erasing the disk areas by other values.

The threat countered by the TOE is the analysis of residual data in the HDD temporary area.

Organisational security policies have not been defined!

1.6 Special Configuration Requirements

The TOE is delivered as one fixed configuration of security functions and no further generation takes place after delivery to the customer. Depending on the MFP model, two different media, either SD Card or DIMM-ROM, will be installed by a “Customer Engineer” (CE), who is a employee of Ricoh or its affiliated company.

Details on secure TOE installation is provided for the Customer Engineer in the document “Service Manual" [SM] .

1.7 Assumptions about the Operating Environment

It is assumed that the MFP on which the TOE works is a genuine product of Ricoh without any conversions or illegal applications installed on it. The Customer Engineer (CE), who installs the TOE, is considered to be trusted.

The TOE is active all the while the MFP is running. The users can recognize that the TOE is active with the icon displayed on the operation panel.

The assumptions on secure usage are detailed in the ST which is attached as part D of this certification report.

1.8 Independence of the Certifier

Within the last two years, the certifier did not render any consulting- or other services for the company ordering the certification and there was no relationship between them which might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product which forms the basis of the certification.

1.9 Disclaimers

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept with regard to generation, configuration and operation as detailed in this certification report. This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or any other

organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The TOE is the "*Software module, version 1.00 of imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B".* The delivery to the user concerns the following components listed as items in the second column of the following table. The third column gives the target Multi-Functional Printers (MFP) adaptable with Hard Disc Security Module (HSM) including the TOE

Kit Name		Item	Target MFP (series)	
DIMM-ROM Media	(Japan) imagio Security Module Type A [Model No.: B694-00] (Other countries) DataOverwriteSecurity Unit Type A [Model No.: B694-01]	DIMM-ROM [P/N: B694-1500] Operating Instructions for users: (Japan) Booklet [P/N: B694-8600] (Other countries) CD-ROM [P/N: B692-8700] Keytop for model-1 [P/N: B027-1449] Keytop for model-2 [P/N: B077-1534]	Model-1	(Japan) Ricoh imagio Neo 221/271 (Other countries) Ricoh Aficio 2022/2027 infotec IS 2122/2127 Savin 4022/4027 Nashutec DSm622/627 RexRotary DSm622/627 Gestetner DSm622/627 Lanier LD122/127
			Model-2	(Japan) Ricoh imagio Neo 352/452 (Other countries) Ricoh Aficio 2035e/2045e/2035eG/2045eG infotec IS 2135/2145 Savin 4035e/4045e/4035eG/4045eG Nashutec DSm635/645 RexRotary DSm635/645 Gestetner DSm635/645/635G/645G Lanier LD135/145

Kit Name		Item	Target MFP (series)	
SD Memory Card Media	(Japan) imagio Security Card Type A [Model No.: B692-00] (Other countries) DataOverwriteSecurity Unit Type B [Model No.: B692-01]	SD memory card [P/N: B692-1200] Operating Instructions for users: (Japan) Booklet [P/N: B692-8501] (Other countries) CD-ROM [P/N: B692-8700] Keytop for Model-3 [P/N: G570-1963] Keytop for Model-4 [P/N: B027-1449]	Model-3	(Japan) Ricoh imagio Neo C325/C385 (Other countries) Ricoh Aficio 2232C/2238C infotec ISC 2432/2838 Savin C3224/3828 Nashutec DSc332/338 RexRotary DSc332/338 Gestetner DSc332/338 Lanier LD232c/238c
			Model-4	(Japan) Ricoh imagio Neo W400 (Other countries) None

Table 1: Delivery Items and Target MFP

3 Security Policy

The Copy/print function of the MFP uses Temporary Area of the HDD as temporary data storage during execution. In case of no installation of HSM, the temporary data is deleted logically after job completion but still remained physically on the HDD. After installing HSM Kit the overwriting function of HSM becomes effective immediately. When copy/print job was completed, HSM checks on Residual Data and overwrites random digits to prevent analyses remained data in Temporary Area. HSM adopts the overwriting method that is random digits are overwritten twice and null (0) data are overwritten once on the target area.

For the priority of MFP usability, HSM comes into suspended if other application job gets started to access the HDD for writing or reading temporary data during overwriting and HSM is trying to restart when the HDD is not accessed by the job. If succeeded, HSM restarts even though the job is not finished. If MFP is turned off during overwriting process, HSM will also restart overwriting after MFP is up and running.

Security policies are described more detailed in the ST which is attached as part D of this certification report.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

When HSM is in operation, two kinds of icons are displayed on the operation panel of MFP depending on the situation. The icons indicate the status of residual data on the HDD. One indicates existence of residual data and another indicates no existence. Hereby customer can confirm easily whether residual data remains or not. The displaying of icons is the evidence that HSM Kit has installed correctly and the overwriting function is operating automatically. Users are urged not to switch off the MFP before the icon switched to “clear” (no residual data present).

4.2 Environmental Assumptions

The specific conditions listed below are assumed to exist in the TOE environment. These assumptions include essential environmental constraints on the use of the TOE.

A.GENUINE It is assumed that the MFP on which the TOE works is trusted.

The MFP, that called various product names in [ST] table 1, is a genuine product of Ricoh without conversions. No illegal applications are installed on the MFP. Also each software or application on the MFP is not tampered.

A.PERFORM It is assumed that the TOE is always active.

The TOE is active all the while the MFP is running. The users can recognize that the TOE is active with the icon displayed on the operation panel.

A.CE It is assumed that Customer Engineer (CE) is trusted.

The CE is well trained and can be trusted. He/She belongs to Ricoh or a Ricoh’s affiliate company and reads the maintenance documentation thoroughly, takes the appropriate measures to MFP. He/She does not change the configuration of MFP, does not carry away the HDD inside MFP and does not install illegal programs into MFP without permission for the users.

4.3 Clarification of Scope

The overwriting function of HSM works on temporary data of the Copy- and Print-Function. These two functions use disk space in a Temporary Area of the HDD. Other functions use System Area of the HDD, e.g. Document Box, I-FAX and Paperless Fax. HSM has no influence on data, stored in the System Area. For more information refer to chapter 2.6 of the security target [ST] which is attached as part D of this certification report.

5 Architectural Information

HSM is one of Additional Equipment Modules expanding the functionality of the MFP. The MFP consists itself of various components, especially a Common Service Module (CSM), which provides the common functionality used by application modules like copier, printer, facsimile and scanner. HSM has interfaces to the CSM and the operating system (OS) (ref. Figure 1).

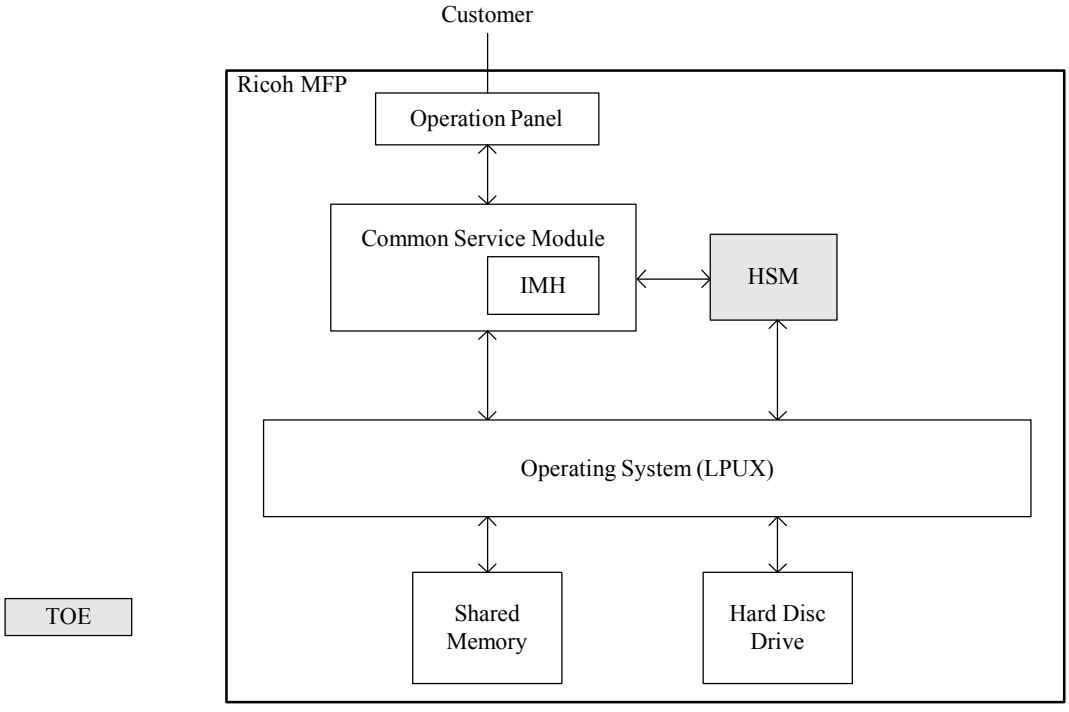

Figure 1: TOE and components of MFP

The TOE consists of the following subsystems as defined in the high level design:

SS.HSM	Searching and overwriting Residual Data
SS.DISPATCHER	Event handling
SS.MAIN	Starting SS.DISPATCHER and SS.HSM

6 Documentation

The following documentation is provided with the product by the developer to the consumer:

In the case of the DIMM-ROM

- Operating Instructions for users:
  (Japan) Booklet [P/N: B694-8600]
  (Other countries) CD-ROM [P/N: B692-8700]

In the case of the SD Memory Card

- Operating Instructions for users:
  (Japan) Booklet [P/N: B694-8501]
  (Other countries) CD-ROM [P/N: B692-8700]

Furthermore for the Customer Engineer there exists the manual

- DataOverwriteSecurity Unit Type A/Type B (Machine Code: B692-01/B694-01); Service Manual, V1.0, 2003-12-12.

7 IT Product Testing

The developer's tests were conducted with the goal to confirm that the TOE meets the security functional requirement. The developer's strategy was to test the TOE against the specification of the security enforcing function detailed in the functional specification and in the high-level design.

The tests reported in the test documentation completely covers the security function of the TOE and corresponds to the three subsystems of the TOE defined in the high-level design.

The developer performed the following tests:

- 36 tests in all (e.g. 9 times 4 tests) with regard to the security function SF.OVERWRITE
- 4 tests in all with regard to the subsystems
- 42 tests in all with regard to the platforms on which the TOE will be reside.

The tests performed by the developer comprise the defined security functionality of the TOE including tests in relation to the two external TOE interfaces, tests for checking the subsystems as well as tests in relation to the platforms used by the TOE.

The evaluator's independent testing as well as penetration tests were performed in the developer's testing environment. The same platforms and tools as for the developer tests were used.

The evaluator's objective was to test the functionality of the TOE as described in the functional specification and the high-level design, and to verify the developer's test results. The devised test subset includes repeated developer tests, independent functionality tests, test concerning vulnerability search and confirmation of non-exploitability of vulnerabilities. The evaluators repeated all 9 tests of the security function (at least with one MFP model), 1 subsystem test and 6 independent tests (with different MFP models).

The tests of the TOE had been performed on the following platforms:

Test target containing the TOE as software is the

- imagio Security Module Type A; Version: V1.00 (equivalent to DataOverwriteSecurity Unit Type A)

and the

- imagio Security Card Type A; Version: V1.00 (equivalent to DataOverwriteSecurity Unit Type B)

These products were tested on the following multi-functional printers (MFPs):

Type of MFP	Item	Version / Spec.
imagio Neo 352	Kernel	NetBSD 1.3.3 (FUJIEDA_RAM) #19: Thu Dec 13 08:58:51 JST 2001
	CPU system bus clock	100.0 MHz
	CPU pipeline clock	200.0 MHz
	Board type	20
	ASIC version	1397306168
	RTC	Equipped
imagio Neo 221	Kernel	NetBSD 1.3.3 (HARA_RAM) #2: Wed Sep 10 14:10:57 JST 2003
	CPU system bus clock	124.0 MHz
	CPU pipeline clock	310.0 MHz
	Board type	21
	ASIC version	1296118832
	RTC	existence
imagio Neo C325	Kernel	NetBSD 1.5.3 (LPUXMIPS) #4: Mon Oct 6 19:25:43 JST 2003

Type of MFP	Item	Version / Spec.
	CPU system bus clock	124.0 MHz
	CPU pipeline clock	496.0 MHz
	Board type	24
	ASIC version	1129067312
	RTC	existence
imagio Neo W400	Kernel	NetBSD 1.5.3 (LPUXMIPS) #8: Mon Sep 8 19:28:55 JST 2003
	CPU system bus clock	124.0 MHz
	CPU pipeline clock	496.0 MHz
	Board type	24
	ASIC version	1129067568
	RTC	existence

Table 2: System configuration of the MFP

Type of MFP	Software	Version
imagio Neo 352	System/copy	2.37.1
	Operation panel	3.01
imagio Neo 221	System/copy	1.02.1
	Operation panel	1.01
imagio Neo C325	System/copy	1.10.1
	Operation panel	1.01
imagio Neo W400	System/copy	1.05
	Operation panel	1.01

Table 3: Software version of the MFP

Test environment and tools used for testing are described in the Evaluation Technical Report (ETR).

The test results obtained for all of the performed tests turned out to be as expected. No errors or other flaws occurred with regard to the specified security functionality and mechanisms.

The penetration testing conducted confirms that all the obvious vulnerabilities were considered and that the vulnerabilities identified are non-exploitable in the intended operational environment of the TOE, if taking into consideration all the measures the user is informed about.

8 Evaluated Configuration

The TOE is delivered in one fixed configuration and no further generation takes place. Therefore the evaluated configuration is identified by the version number:

Software module version 1.00 of

imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by TÜViT's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS].

The verdicts for the CC, part 3 assurance classes and components (according to EAL3 and the class ASE for the Security Target Evaluation) are summarised in the following table:

EAL3 assurance classes and components		**Verdict**
Security Target evaluation	**CC Class ASE**	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	n.a.[5]
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration Management	**CC Class ACM**	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and operation	**CC Class ADO**	PASS
Delivery procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	**CC Class ADV**	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	**CC Class AGD**	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS

[5] n.a. = not applicable

Life cycle support	**CC Class ALC**	PASS
Identification of security measures	ALC_DVS.1	PASS
Tests	**CC Class ATE**	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	**CC Class AVA**	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

No Protection Profile (PP) compliance claims were made in the ST. Thus, the component ASE_PPC.1 is not applicable. All other assurance components were assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the security target is considered to be Part 3 conformant.

The security target, chapter 5 claims, that the TOE will fulfil one TOE security functional requirement, which is exclusively taken from [CC] part 2:

Component ID	Component title
FDP_RIP.1	Subset residual information protection

The evaluation performed in accordance to EAL3 has shown that the TOE security functional requirement is correctly realised by the TOE security function. Thus, in realising this functional requirement, it is assured that the TOE will meet the security objective claimed in the ST.

A strength of function (SOF) has not been claimed, because no probabilistic and permutational mechanisms (account name/password based authentication and cryptographic operations) have been used. This has been verified by the evaluator.

The sponsor must advise the certification authority about any modification of the TOE or its guidance documentation. The certification authority will then check whether the certification results are still valid and, if necessary, initiate all further steps concerning a re-evaluation. The results of the evaluation are only applicable to "*Software Module V1.00 of the HSM Kit*". The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

10 Evaluation stipulations, comments and recommendations

There are no evaluation stipulations, comments, or recommendations.

11 Certification stipulations and notes

There are no stipulations or notes.

12 Security Target

The security target for "*imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B*", as of 2004-01-21, version 1.5 from Ricoh Company, Ltd. is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ADM	Administrator Guidance
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CE	Customer engineer (performing installation and maintenance procedures)
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
CSM	Common Service Module
EAL	Evaluation Assurance Level
FAX	Facsimile
FCU	FAX Control Unit
FSP	Functional Specification
HDD	Hard Disk Drive
HLD	High-level Design
HSM	Hard Disk Security Module Kit

MFP	Multi-functional Printer
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TD	Test Documentation
TOE	Target Of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from Part3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[GD] DataOverwriteSecurity Unit Type A, DataOverwriteSecurity Unit Type B Operating Instructions, B6928600A, Author: Ricoh Company, LTD.

[AIS] Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[CC] ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security,
ISO/IEC 15408-1:1999 (E), Part 1: Introduction and general model
ISO/IEC 15408-2:1999 (E), Part 2: Security functional requirements
ISO/IEC 15408-3:1999 (E), Part 3: Security assurance requirements

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 1: Introduction and general model, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, version 1.0, revision August 1999

[ETR] Evaluation Technical Report, version 1.1, 2004-01-21, TÜV Informationstechnik GmbH

[SM] DataOverwriteSecurity Unit Type A/Type B (Machine Code: B692-01/B694-01); Service Manual, version 1.0, 2003-12-12, Ricoh

[ST] Security Target for *imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B*, version 1.5, 2004-01-21, Ricoh

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- caveats on evaluation results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance results (section 5.4 of CC part 1 with final interpretation 008)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2.

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3.

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

a) ***Package name* Augmented** - A PP or TOE is an augmentation of a predefined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.“

CC Part 3:

Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in *Table 1*.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 1: Assurance family breakdown and mapping

Evaluation assurance levels (chapter 6)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances.

Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview

„Table 2 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration Management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and Operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_IMT					**1**	**2**	***3***
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance Documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life Cycle Support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability Assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Table 2: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested

“EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay. An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested

“EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked

“EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed

“EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested

“EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested

"EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL7) - formally verified design and tested

"EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Strength of TOE security functions (AVA_SOF)

AVA_SOF Strength of TOE security functions

"Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large."

Three levels exist: SOF-basic, SOF-medium, and SOF-high.

Vulnerability analysis (AVA_VLA)

AVA_VLA Vulnerability analysis

“Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE.”

Application notes

“A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.

The intent of the developer analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment for the TOE and that the TOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that requires a minimum of understanding of the TOE, skill, technical sophistication, and resources. These might be suggested by the TSF interface description. Obvious vulnerabilities include those in the public domain, details of which should be known to a developer or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer identify those vulnerabilities in a structured and repeatable way, as opposed to identifying them in an ad-hoc fashion. The associated evidence that the search for vulnerabilities was systematic should include identification of all TOE documentation upon which the search for flaws was based.

Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential. To accomplish this intent, the evaluator first assesses the exploitability of all identified

vulnerabilities. This is accomplished by conducting penetration testing. The evaluator should assume the role of an attacker with a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential when attempting to penetrate the TOE. Any exploitation of vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to the AVA_VLA.*.2C elements) in the context of the components AVA_VLA.2 through AVA_VLA.4.”

Part D

Security Target

Attached is the Security Target for *imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B*,

Author: Masahiro ITOH, Hiroshi KIMURA, Atsushi SATOH, Keiichi YOKOYAMA, Haruyuki HIRABAYASHI & Yusuke OHTA, Ricoh Company, Ltd.

Date: 2004-01-21

Version: 1.5

Security Target for

imagio Security Module Type A,

imagio Security Card Type A,

DataOverwriteSecurity Unit Type A, and

DataOverwriteSecurity Unit Type B

Author: Masahiro ITOH, Hiroshi KIMURA, Atsushi SATOH, Keiichi YOKOYAMA,
Haruyuki HIRABAYASHI & Yusuke OHTA,
Ricoh Company, Ltd.
Date: 2004-01-21
Version: 1.5

Document Revision History

Version	Date	Author	Description
1.0	2003-09-26	Masahiro ITOH, Hiroshi KIMURA, Atsushi SATOH, Keiichi YOKOYAMA, Haruyuki HIRABAYASHI, and Yusuke OHTA	Revised - determined TBD items - added Table 1 and related explanations
1.1	2003-10-31	Masahiro ITOH	Revised - revised Table 1 - corrected product name - updated references
1.2	2003-11-14	Masahiro ITOH	Revised - fixed chapter 2.5 - fixed chapter 2.6 - fixed chapter 2.7 - fixed chapter 4.2.2 - fixed [GD] in chapter 6.3 and Table 8
1.3	2003-11-21	Masahiro ITOH	Revised - deleted versions and dates in Table 8 - corrected versions and dates in chapter 6.3
1.4	2004-01-19	Masahiro ITOH	Revised. - revised Table 1
1.5	2004-01-21	Masahiro ITOH	Revised. - revised Assurance Measures - revised Table 8

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 ST Identification

Title:	Security Target for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B
Version:	1.5
Date:	2004-01-21
Author:	Masahiro ITOH, Hiroshi KIMURA, Atsushi SATOH, Keiichi YOKOYAMA, Haruyuki HIRABAYASHI & Yusuke OHTA, Ricoh Company, Ltd.
Product:	imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B

Note: Hereafter these products are called with a generic name "Hard Disc Security Module Kit".

TOE:	Software module of the Hard Disc Security Module Kit V1.00
CC used:	ISO/IEC 15408:1999(E)
Keywords:	document, copier, printer, facsimile, FAX, scanner, network, office, hard disc, security, overwrite

1.2 ST Overview

This Security Target (ST) describes the security specification of software module of the Hard Disc Security Module (HSM) Kit for Ricoh's Multi-Functional Printer (MFP). MFP has not only basic copier function but also the several types of options, e.g. facsimile, printer or scanner in a body. MFP is used mostly in general office and input data or printed images are stored on the Hard Disc Drive (HDD) installed inside. For example copy image data will be printed out after temporary storage on the HDD.

HSM has a function to clean up the temporary storage area of the HDD in order to be unable to detect the traces of data. HSM adopts the overwriting method that is random digits are overwritten twice and null (0) data are overwritten once on the target area. HSM is delivered as an optional kit for Ricoh MFP, so that customer can add HSM Kit after setting MFP.

The TOE is the Software module of the Hard Disc Security Module Kit. Attached the HSM Kit, the TOE works following security feature:

- Prevention of analyses the residual temporary image data on the HDD inside Ricoh MFP.

1.3 ISO/IEC 15408 Conformance Claim

The TOE is **conformant** to ISO/IEC 15408-2:1999(E).

The TOE is **conformant** to ISO/IEC 15408-3:1999(E), assurance level **EAL3**.

There are no PPs claimed to which this ST is conformant.

2 TOE Description

2.1 Product Type

The product type of HSM Kit is the optional kit for Multi-functional Printers manufactured by Ricoh. All of those product names are listed in Table 1and detailed explanation about the products is described later. This optional kit can be installed in a factory or customer's site.

2.2 Multi-Functional Printer (MFP)

Ricoh's Multi-functional Printer (MFP) has not only basic copier function but also the several types of options, e.g. facsimile, printer or scanner in a body. It is used mostly in general office, and also used in public space such as copy service shops. MFP has an HDD inside. The HDD is available for the MFP system area or temporary storing image data of copier and printer.

2.3 Importance of security for Residual Data

It becomes important to protect all information at the office. Digital equipments like copier, facsimile or printer almost have huge memories or large capacity HDD for data storages. The data storages are available for basic and also expanded applications of MFP. MFP receives and stores various data by scanner, through telephone lines or data connection cables like LAN or Centronics parallel interface. In general the digital equipment makes electronic images on the memories or HDD before printing. Those data and images have the potential to become residual temporary image data.

The residual temporary image data is generated by deletion of those data and images. Usually 'delete' process deletes the recorded data logically, but the trails of the data remain physically on the HDD. Hereafter the residual temporary image data is labelled as Residual Data.

Up to now, not so much attention has been given to the protection of Residual Data in digital equipments. But it is needed to guarantee clearing up Residual Data in order to protect customer's secrets from now on.

2.4 HDD Area and related operations

The HDD inside Ricoh MFP is divided into two kinds of areas, Temporary Area and System Area.

In Temporary Area, working data is created temporarily by copy or print jobs. Customer could not notice that such working data is created on the HDD. System Area is available to keep job data of applications or to spool data received from external devices.

The functions using Temporary Area of the HDD are as follows:

- General Copy; Copy function in commonly used. Makes temporary image data in Temporary Area,
- General Print; Print function in commonly used. Makes temporary image data in Temporary Area,
- Sample Print; Stores temporary image data in Temporary Area, and

- Locked Print; Keeps up image data until the owner operates to print.

Notice that General Facsimile function does not need the HDD, because the dedicated SRAM are available for General Facsimile function. Other functions also use System Area of the HDD, e.g. Document Box, I-FAX and Paperless Fax.

2.5 Hard disc Security Module (HSM)

HSM is a software module executed on MFP hardware and is written into suitable media as SD memory card or DIMM-ROM for adaptable to MFP and delivered to customers.

2 types of HSM Kits according to the software provided media will be differently adaptable to 2 models of target MFP, therefore there are 4 models of target MFP in which HSM Kit will be attached. All combinations of HSM Kit and MFP are listed in Table 1. Copy/print function uses Temporary Area of the HDD as temporary data storage during execution. In case of no installation of HSM, the temporary data is deleted logically after job completion but still remained physically on the HDD. After installing HSM Kit the overwriting function of HSM becomes effective immediately. When copy/print job was completed, HSM checks on Residual Data and overwrites random digits to prevent analyses remained data in Temporary Area. HSM adopts the overwriting method that is random digits are overwritten twice and null (0) data are overwritten once on the target area.

For the priority of MFP usability, HSM comes into suspended if other application job gets started to access the HDD for writing or reading temporary data during overwriting and HSM is trying to restart when the HDD is not accessed by the job. If succeeded, HSM restarts even though the job is not finished. If MFP is turned off during overwriting process, HSM will also restart overwriting after MFP is up and running.

When HSM is in operation, two kinds of icons are displayed on the operation panel of MFP depending on the situation. The icons indicate the status of Residual Data on the HDD. One indicates existence of Residual Data and another indicates no existence. Hereby customer can confirm easily whether Residual Data remains or not. The displaying of icons is the evidence that HSM Kit has installed correctly and the overwriting function is operating automatically.

Table 1: HSM Kit and Target MFP

Kit Name		Item	Target MFP (series)	
DIMM-ROM Media	(Japan) imagio Security Module Type A [Model No.: B694-00] (Other countries) DataOverwriteSecurity Unit Type A [Model No.: B694-01]	DIMM-ROM [P/N: B694-1500] Operating Instructions for users: Booklet (Japan) [P/N: B694-8600] CD-ROM (Other countries) [P/N: B692-8700] Keytop for model-1 [P/N: B027-1449] Keytop for model-2 [P/N: B077-1534]	**Model-1**	(Japan) Ricoh imagio Neo 221/271 (Other countries) Ricoh Aficio 2022/2027 infotec IS 2122/2127 Savin 4022/4027 Nashutec DSm622/627 RexRotary DSm622/627 Gestetner DSm622/627 Lanier LD122/127
			Model-2	(Japan) Ricoh imagio Neo 352/452 (Other countries) Ricoh Aficio 2035e/2045e/2035eG/ 2045eG infotec IS 2135/2145 Savin 4035e/4045e/4035eG/4045eG Nashutec DSm635/645 RexRotary DSm635/645 Gestetner DSm635/645/635G/645G Lanier LD135/145
SD Memory Card Media	(Japan) imagio Security Card Type A [Model No.: B692-00] (Other countries) DataOverwriteSecurity Unit Type B [Model No.: B692-01]	SD memory card [P/N: B692-1200] Operating Instructions for users: Booklet (Japan) [P/N: B692-8501] CD-ROM (Other countries) [P/N: B692-8700] Keytop for Model-3 [P/N: G570-1963] Keytop for Model-4 [P/N: B027-1449]	**Model-3**	(Japan) Ricoh imagio Neo C325/C385 (Other countries) Ricoh Aficio 2232C/2238C infotec ISC 2432/2838 Savin C3224/3828 Nashutec DSc332/338 RexRotary DSc332/338 Gestetner DSc332/338 Lanier LD232c/238c
			Model-4	(Japan) Ricoh imagio Neo W400 (Other countries) None

2.6 Evaluated Configuration

HSM has no effects on the following applications, functions and data. They are classified into two categories.

(A) Applications and functions should be stopped to make HSM become active. Customer engineer (CE) sets up each configuration disable for following features:

- Scanner Application (except Network TWAIN scanning),
- I-FAX (Internet Faxing),
- Printer data spooling function,
- Document Box (electronic filing) Application,
- Paperless FAX, and
- eCabinet (the intelligent electronic file cabinet).

(B) Data could not be stopped to use. Customers should pay attention to the following data for using:

- Printer font set,
- Printer form data, and
- RTIFF emulation print data.

The TOE is evaluated on the presupposition that whole of above functions and data are unused.

2.7 Physical boundary of the TOE

Ricoh MFP consists of hardware and software parts. The software part consists of Operation System (OS), Common Service Module, Application Modules and Additional Equipment Module.

The OS is Ricoh's original operation system based on NetBSD. Common Service Module (CSM) provides the common functionality used by Application Modules. Also image data management function is included in CSM. Application Modules realize various functions of basic use for customers, like copier, printer, facsimile and scanner. And Additional Equipment Modules also realize optional functions for customers.

HSM is one of Additional Equipment Modules and expands the function of CSM. After installing HSM, the following behaviour will be executed:

- CSM stores image data temporarily on the HDD through OS,
- After using that data, CSM deletes the data logically,
- HSM asks CSM whether HSM may overwrite the used data area or not,
- After receiving permission from CSM, HSM overwrites digits on the used data area to clean up, and
- CSM checks on the existence of HSM and indicates the icon on the operation panel.

The TOE is a software module called HSM.

The Operating Environments for the TOE are presented in Table 1.

There are 4 models of target MFP in which HSM Kit will be attached. Each model of target MFP has several brand names for oversea sales and OEM other than Ricoh brand for Japan, but each model of target

MFP has the same hardware and software except brand names. The combination of HSM Kit and models of target MFP is shown in Table 1.

And the applicable TOE version is HSM V1.00.

Figure 1 shows physical boundary of the TOE.

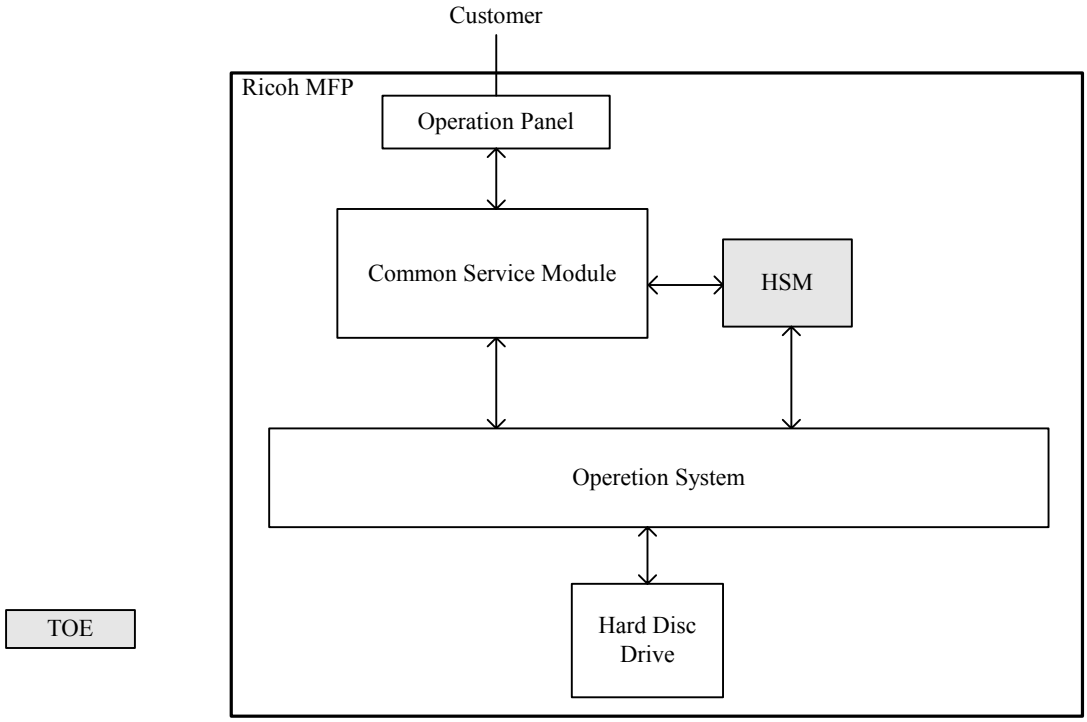

Figure 1: Physical boundary of the TOE

2.8 Logical boundary of the TOE

The TOE undertakes a role as follows:

- Checking on Residual Data on the HDD through Common Service Module, and
- Overwriting random digits and null over Residual Data on the HDD.

Common Service Module manages and operates other functions around the TOE as follows:

- Management of Residual Data area on the HDD,
- Indication of icons on the operation panel,
- Control of HSM working all the time in resident, and
- Identification & Authentication of the CE and Administrator for changing the configuration of MFP.

2.9 Definition of Specific Terms

For clear understanding of this ST, the meanings of specific terms are defined as shown in Table 2.

Table 2: Specific terms related to the Hard Disc Security Module Kit

Term	Definition
MFP	Multi-Functional Printer, which includes two or more functions, i.e. copier, printer and so on, in a body. The TOE in this ST is available for MFP manufactured by Ricoh. See Table 1.
HSM	HSM, Hard Disc Security Module, has a function to clean up the temporary storage area of the HDD in order to be unable to detect the traces of data. HSM adopts the overwriting method that is random digits are overwritten twice and null (0) data are overwritten once on the target area.
CSM	CSM, Common Service Module, provides the common functionality used by Application Modules, e.g. Copy or Printer function. Also image data management function is included in CSM.
Residual Data	Residual Data means the residual temporary image data generated by deletion of those data and images. Usually 'delete' process deletes the recorded data logically, but the trails of the data remain physically on the HDD. Those trails are the residual temporary image data.
Temporary Area	Temporary Area, in which working data is created temporarily by copy or print jobs. Customer could not notice that such working data is created on the HDD.
System Area	System Area, which is available to keep job data of applications or to spool data received from external devices.
Access Code	Access Code is the identification number that is used to authenticate Administrator. Administrator is assumed to use 8 digits for it.
Administrator	Administrator is the trusted person who is authorised to perform the administrative operations of the MFP with Access Code.
CE	CE, Customer Engineer, is the person who performs maintenance operations against the MFP. The Customer Engineers are employees of Ricoh or its affiliated company.
Document Box	Document Box is the logical box in the MFP, in which electronic files of documents are stored. It is available when Document Box option is included.
eCabinet	eCabinet is the intelligent electronic file cabinet. It automatically archives any file type from networked peripherals like scanners, copiers, printers, fax machines, and PCs (including Web and email), retrieving them to users desktop in seconds through a convenient Web browser.
I-FAX	Internet Fax, which communicates through internet instead of telephone line.

Term	Definition
Paperless FAX	Paperless FAX is a fax function that stores receiving fax data into the HDD and can print out the stored fax data if needed.
RTIFF emulation	RTIFF emulation is an extended emulation, which can print out TIFF (Tagged Image File Format) formed bit map image data from UNIX workstation or PC.
NetBSD	UNIX compatible OS; freeware and high portability
DIMM-ROM	DIMM-ROM is Dual In-line Memory Modules formed ROM (Read Only Memory), which is used for providing the TOE or other applications for the MFP.
SD memory card	SD memory card is Secure Digital memory card, which is a highly-sophisticated memory device about the size of a postage stamp and it is used for providing the TOE or other applications for the MFP
TWAIN	TWAIN is API and Protocol for image processing devices, which is used as the interface for scanner in the MFP.

3 TOE Security Environment

3.1 Assets

The assets that the TOE intends to protect are Residual Data in Temporary Area of the HDD. This "protect" means getting the Residual Data unable to be analysed by means of destruction (erasing by other values).

3.2 Assumptions

In this section, the assumptions concerning the environment of the TOE are identified and described.

A.GENUINE **It is assumed that the MFP on which the TOE works is trusted.**

The MFP that called various product names in Table 1 is a genuine product of Ricoh without conversions. No illegal applications are installed on the MFP. Also each software or application on the MFP is not tampered.

A.PERFORM **It is assumed that the TOE is always active.**

The TOE is active all the while the MFP is running. The users can recognize that the TOE is active with the icon displayed on the operation panel.

A.CE **It is assumed that Customer Engineer (CE) is trusted.**

The CE is well trained and can be trusted. He/She belongs to Ricoh or a Ricoh's affiliate company and reads the maintenance documentation thoroughly, takes the appropriate measures to MFP. He/She does not change the configuration of MFP, does not carry away the HDD inside MFP and does not install illegal programs into MFP without permission for the users.

3.3 Threats

In this section, the threats that will be countered by the TOE or its environment are identified and described.

T.ANALYSE **Residual Data in the HDD Temporary Area may be analysed.**

The HDD inside the MFP could be carried away by an attacker and the attacker may analyse Residual Data on Temporary Area of the HDD. The attacker may be an inside user with evil intent or an evil person from the outside.

3.4 Organisational Security Policies

There are no organisational security policies with which the TOE must comply.

4 Security Objectives

4.1 Security Objectives for the TOE

In this section, the security objectives of the TOE that cover the aspects of the threats in section 3.3 are described.

O.RESIDUAL **The TOE will ensure that Residual Data cannot be analysed after completion of copy/print operation.**

After completion of copy/print operation, the TOE overwrites Residual Data with other data to prevent anyone from analysing Residual Data on the HDD.

4.2 Security Objectives for the Environment

4.2.1 Security objectives for the IT environment

There are no security objectives for the IT environment.

4.2.2 Security objectives for the non-IT environment

In this section, the security objectives of the non-IT environment that cover the aspects of the assumptions or threats described in section 3.

OE.GENUINE **Responsible persons who should watch the TOE working correctly will ensure that the MFP on which the TOE is installed is trusted.**

Responsible persons who should watch the TOE confirm that the identification of CE who set up the MFP is correct. Responsible persons who should watch the TOE keep up the MFP from installing illegal applications or changing modules in the MFP

OE.ICON **Users will be sure to confirm that the TOE works correctly before operations.**

When the TOE is installed and booted up, the icon is always displayed on the operation panel. There are two icons in different shapes. One is called ‘dirty’ shown existence of residual data in the HDD and the other is called ‘clean’ shown no residual data. While the TOE works to overwrite, the ‘dirty’ icon is displayed. When the TOE is waiting to work, the ‘clean’ icon is displayed. Users can find whether the TOE is active or not by display of either icon before copy/print operations.

OE.CE **The maintenance of the MFP will be sure to carry out by Customer Engineer (CE) who is an employee of Ricoh or a Ricoh's affiliate company.**

CE is well trained and well informed about MFP, therefore he/she can take the appropriate measures to MFP.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

In this section, the functional requirements of the TOE to achieve the security objectives identified in section 4.1 are described. The parts against which the assignment and selection operations defined in [CC] are performed are identified with **[bold letters and brackets]**.

5.1.1 User data protection (FDP)

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[deallocation of the resource from]** the following objects: **[image data of copy/print operations]**.

Dependencies: No dependencies

5.2 Minimum Strength of Function Claim

The minimum strength level claimed for the TOE does not exist, because the security function of the TOE does not include probabilistic or permutational mechanism.

5.3 TOE Security Assurance Requirements

The assurance components for the TOE are shown Table 3. It is the set of components defined by the evaluation assurance level **EAL3** and no other requirements have been augmented.

Table 3: TOE security assurance requirements (EAL3)

Assurance Class	Assurance Component	
Security Target	ASE_DES.1	TOE description
	ASE_ENV.1	Security environment
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives
	ASE_PPC.1	PP claims
	ASE_REQ.1	IT security requirements
	ASE_SRE.1	Explicitly stated IT security requirements
	ASE_TSS.1	TOE summary specification
Configuration Management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.4 Security Requirements for the Environment

There are no security requirements for the environment in which the TOE works.

6 TOE Summary Specification

6.1 TOE Security Functions

SF.OVERWRITE

TSF overwrites the area of Residual Data based on the permission from the MFP. TSF uses the overwriting method that is to write random data twice and null (0) data once.

TSF starts to overwrite after completion of a copy/print job. If the power supply is cut off while TSF is overwriting, TSF restarts to overwrite when the MFP is switched on after recovery of the power supply.

A copy/print job has priority to TSF. If another job is running at the start of TSF, TSF waits for the job to be over and starts to overwrite. If another job starts to run while TSF is overwriting, TSF gets into suspended and restarts after the job completion.

6.2 Strength of Function Claims

No security function realised by probabilistic or permutational mechanism exists.

6.3 Assurance Measures

The following documents are provided as the assurance measures:

Security Target for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.5, 2004-01-21

Security Functional Specification for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.4, 2004-01-21,

High-level Design for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.2, 2004-01-21,

Correspondence Analysis for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.2, 2004-01-21,

Guidance document;
DataOverwriteSecurity Unit Type A,
DataOverwriteSecurity Unit Type B,
Operating Instructions,
Version B692-8600A, 2003-11-07

Security Test Documentation for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.1, 2004-01-21,

Vulnerability Analysis for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.2, 2004-01-21-

Configuration Management Plan for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.4, 2004-01-21,

Development Security Plan for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.2, 2004-01-21,

Delivery and Setup Procedure for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.4, 2004-01-21,

Production Procedure for
imagio Security Module Type A,
imagio Security Card Type A,
DataOverwriteSecurity Unit Type A, and
DataOverwriteSecurity Unit Type B,
Version 1.3, 2004-01-21,

DataOverwriteSecurity Unit Type A/Type B (Machine Code: B692-01/B694-01) Service Manual,
Version 1.0, 2003-12-12

7 PP Claims

There are no Protection Profiles claimed to which this ST is conformant.

8 Rationale

8.1 Security Objectives Rationale

In this section, it is demonstrated that the security objectives identified in section 4 are suitable and covering all aspects of the security environment described in section 3.

Table 4 shows that each security objective covers at least one threat or assumption, and that each threat and assumption is covered by at least one security objective.

Table 4: Correspondence between security needs and security objectives

	O.RESIDUAL	OE.GENUINE	OE.ICON		OE.CE
T.ANALYSE	X				
A.GENUINE		X			
A.PERFORM			X		
A.CE					X

T.ANALYSE is countered by O.RESIDUAL, because it is ensured that TOE overwrites used part of Temporary Area of the HDD with different values from stored image data, therefore no one can analyse the original image data.

A.GENUINE is covered by OE.GENUINE, because it is ensured that those responsible for the TOE confirm that CE is an authentic person of Ricoh or a proper distributor and make efforts to keep up the MFP correctly. User's MFP is set up in an orderly manner by well-trained CE of Ricoh or a proper distributor, and illegal applications could not be installed without being noticed by those responsible, therefore the MFP is held genuine status.

A.PERFORM is covered by OE.ICON, because it is ensured that the icon is not displayed if the TOE does not work and the user confirms the configuration of the MFP after CE's maintenance work, therefore the MFP has the correct configuration and the TOE also works correctly.

A.CE is covered by OE.CE, because it is ensure that reliable CE comes to carry out the maintenance of MFP since the user commissions the proper dealer to repair.

8.2 Security Requirements Rationale

8.2.1 Rationale for functional requirements

In this section, it is demonstrated that the security functional requirements specified in section 5 achieve the security objectives identified n section 4.

Table 5 shows that TOE security functional requirement covers security objective for the TOE.

Table 5: Correspondence between security objectives and functional requirements

	FDP_RIP.1
O.RESIDUAL	X

O.RESIDUAL is achieved by FDP_RIP.1, because this requirement ensures that the temporary stored image data at the previous operation is turned into unavailable, i.e. nobody can analyse the data any longer.

8.2.2 Rationale for minimum strength of function level

The minimum strength of function level is not defined, because the security function realized by probabilistic or permutational mechanism does not exist as shown in section 6.2.

8.2.3 Rationale for assurance requirements

In order to get the originals from image data that is deleted logically but remains physically on the HDD, it is needed to disassemble the HDD out of the MFP, to read out Residual Data from the HDD and to analyze the data with referring to the specified format of the image data.

As the HDD-analyzing tools are getting common, there is a possibility that even low-level attackers can read out the Residual Data from the HDD. Even though it is necessary and difficult to get the specific information concerning the MFP for effective attack, customers who take count of security need more practical countermeasures.

For providing this countermeasure, the TOE overwrites the Residual Data (SF.OVERWRITE). If the function works correctly, it becomes impossible to perform the above-mentioned attacks. The high-level design evaluation (ADV_HLD.2) is enough to show such correctness, because this function includes no probabilistic or permutational mechanisms.

Furthermore, the higher attack potential is required for such attacks as bypassing or tampering the TSF itself, and it is out of scope of this evaluation, i.e. analysis of obvious vulnerabilities (AVA_VLA.1) is enough for general needs.

On the other hand it is needed to keep the secret concerning the relevant information in an effort to make an attack harder, and Ricoh considers that it is meaningful to get confidence of security also from the development environment, i.e. development security. (ALC_DVS.1)

For the reason stated above, EAL3 is selected as the proper estimation assurance level for this TOE.

8.2.4 Mutual support of security requirements

This ST includes only one security functional requirement. Therefore the security functional requirement has no mutual support.

8.3 TOE Summary Specification Rationale

8.3.1 Rationale for TOE security functions

In this section, it is demonstrated that the security functions defined in section 6.1 realize the security functional requirements specified in section 5.1.

Table 6 shows that TOE security functional requirement covers security function for the TOE, and that security function for the TOE is covered by TOE security functional requirement.

Table 6: Correspondence between functional requirements and security functions

	SF.OVERWRITE
FDP_RIP.1	X

The following Table 7 shows the corresponding part of description of the security function, which derives from section 6.1.

Table 7: Corresponding description of security functions

Requirement	Description of security functions
FDP_RIP.1	**SF.OVERWRITE:** TSF overwrites the area of Residual Data based on the permission from the MFP. TSF uses the overwriting method that is to write random data twice and null (0) data once. TSF starts to overwrite after completion of a copy/print job.

8.3.2 Rationale for strength of function claims

Any security function including probabilistic or permutational mechanism does not exist as shown in section 6.2. Therefore no strength of function claims are needed in this ST.

8.3.3 Rationale for combination of security functions

As shown in section 8.3.1, one (1) security function covers one (1) security functional requirement. That is, there is no mutual support in this ST. Therefore the security function works so as to satisfy the security functional requirement.

8.3.4 Rationale for assurance measures

Table 8 shows that the corresponding assurance measures are provided for each assurance requirement due to class ASE and EAL 3. The actual fulfilment of the requirements by these assurance measures is inspected during the evaluation.

Table 8: Correspondence between assurance requirements and assurance measures

Assurance Class	Assurance Component	Assurance Measure
ASE: Security Target evaluation	ASE_DES.1 ASE_ENV.1 ASE_INT.1 ASE_OBJ.1 ASE_PPC.1 ASE_REQ.1 ASE_SRE.1 ASE_TSS.1	Security Target for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.5, 2004-01-21
ACM: Configuration management	ACM_CAP.3 ACM_SCP.1	Configuration Management Plan for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.4, 2004-01-21,
ADO: Delivery and operation	ADO_DEL.1 ADO_IGS.1	Delivery and Setup Procedure for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.4, 2004-01-21, Production Procedure for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.3, 2004-01-21,
ADV: Development	ADV_FSP.1	Security Functional Specification for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.4, 2004-01-21,

Assurance Class	Assurance Component	Assurance Measure
	ADV_HLD.2	High-level Design for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.2, 2004-01-21,
	ADV_RCR.1	Correspondence Analysis for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.2, 2004-01-21,
AGD: Guidance documents	AGD_ADM.1 AGD_USR.1	Guidance document; DataOverwriteSecurity Unit Type A, DataOverwriteSecurity Unit Type B, Operating Instructions, Version B692-8600A, 2003-11-07 DataOverwriteSecurity Unit Type A/Type B (Machine Code: B692-01/B694-01) Service Manual, Version 1.0, 2003-12-12
ALC: Life cycle support	ALC_DVS.1	Development Security Plan for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.2, 2004-01-21,
ATE: Tests	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_INT.2	Security Test Documentation for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.1, 2004-01-21,
AVA: Vulnerability assessment	AVA_MSU.1	Guidance document; DataOverwriteSecurity Unit Type A, DataOverwriteSecurity Unit Type B, Operating Instructions, Version B692-8600A, 2003-11-07
	AVA_SOF.1	None
	AVA_VLA.1	Vulnerability Analysis for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B, Version 1.2, 2004-01-21-

No Assurance Measure exists corresponding to AVA_SOF.1, because of no probabilistic or permutational mechanism in this ST.

8.4 PP Claims Rationale

There are no Protection Profiles claimed to which this ST is conformant.

9 Annex

9.1 Source

ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security,

ISO/IEC 15408-1:1999(E), Part 1: Introduction and general model,

ISO/IEC 15408-2:1999(E), Part 2: Security functional requirements,

ISO/IEC 15408-3:1999(E), Part 3: Security assurance requirements.

9.2 Abbreviation

CC	Common Criteria
CE	Customer Engineer
DIMM-ROM	Dual In-line Memory Modules formed ROM (Read Only Memory)
FAX	Facsimile
HDD	Hard Disc Drive
LAN	Local Area Network
MFP	Multi-functional Printer
OS	Operation System
PP	Protection Profile
SD memory card	Secure Digital memory card
SF	Security Function
SRAM	Static Random Access Memory
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function