National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Ricoh Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B

Report Number: CCEVS-VR-07-0016

Dated: 16 May 2007

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Dr. Jerome F. Myers

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1 Identification ____ 5
1.1 Applicable Interpretations ____ 7
2 TOE Description ____ 7
2.1 Hard Disk Security Module (TOE) Description ____ 7
2.2 SF.RANDOMBUFFERS ____ 8
2.3 SF.SELFPROTECT ____ 8
3 Assumptions ____ 8
4 Threats ____ 9
5 Clarification of Scope ____ 9
6 Architecture Information ____ 10
6.1 Evaluated Configuration ____ 11
7 Product Delivery ____ 11
8 IT Product Testing ____ 12
8.1 Evaluator Functional Test Environment ____ 12
8.2 Functional Test Results ____ 13
8.3 Evaluator Independent Testing ____ 13
8.4 Evaluator Penetration Tests ____ 13
8.5 Test Results ____ 14
9 RESULTS OF THE EVALUATION ____ 14
10. VALIDATOR COMMENTS ____ 14
11. Security Target ____ 15
12. List of Acronyms ____ 15
13. Bibliography ____ 15

List of Figures

Figure 1 - TOE Boundary 11
Figure 2 - Test Bed Configuration 12

List of Tables

Table 1 - Evaluation Identifier 6

EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Ricoh Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B at EAL3. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 2 March 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 3 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B is a data overwrite tool.

The Hard Disk Security Module (HSM) is a software module executed on Multi-Function Printer (MFP) hardware and is contained on an SD memory card or DIMM-ROM providing adaptability to various MFP devices. Table 1 in the Security Target identifies and describes the HSM kit, the item, and the MFP devices suitable for each HSM kit type.

The HSM software provides the MFP with functionality that overwrites the Temporary Area of the Hard Disk Device (HDD). The HSM function is automatic. Once installed on the MFP device, the overwriting function becomes effective immediately. It cannot be turned off, unless the software is removed. There is, however, a priority scheme. For practical MFP usability, the HSM function will become suspended if another application job accesses the HDD for writing or reading data. Once that job is completed, the HSM resumes. If the MFP power is disrupted either during HSM execution or if HSM is idle, upon power restore HSM is executed before user functionality can begin. An icon on the printer control panel displays indicates when the HSM overwrite process has completed.

The evaluation covers the security functionality provided by the HSM; the other MFP hardware and the underlying MFP operating system and supporting applications are treated as part of the IT Environment and hence not included within the scope of the evaluation.

1 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifier

Evaluation Identifiers for Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B
Protection Profile	N/A
Security Target	Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B Security Target, dated May 8, 2007.
Evaluation Technical Report	Evaluation Technical Report for the Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B Document No. F3-0507-001, Dated 16 May 2007
Conformance Result	Part 2 conformant and EAL3 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on January 26, 2006.
Version of CEM	CEM Version 2.2 and all applicable NIAP and International Interpretations effective on January 26, 2006.
Sponsor	Ricoh Company, Ltd. 3-6, Nakamagome 1-chome, Ohta-ku Tokyo 143-8555, Japan
Developer	Ricoh Company, Ltd. 3-6, Nakamagome 1-chome, Ohta-ku Tokyo 143-8555, Japan
Evaluator(s)	**COACT Incorporated** Bob Roland Greg Beaver
Validator(s)	**NIAP CCEVS** Jerome F. Myers

1.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

2 TOE Description

The Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B is the software that once loaded is always resident in memory and constructs buffers containing two passes of random data and a single pass of nulls for use in overwriting copy and print residual data located in the Temporary Area of the MFP hard disk drive (HDD). During print and copy job processing, the MFP stores images as files in the Temporary Area of the hard disk drive. There is a risk that these images could be disclosed during subsequent jobs. When initialized, the TOE performs an inspection of a table resident in memory and if copy or print residual data is present on the HDD, the TOE begins the random data and null buffer generation which is used to overwrite those portions of the HDD. The MFP displays an icon indicating whether or not the HDD is “clean” (this functionality is provided by MFP firmware not included in the TOE boundary).

2.1 Hard Disk Security Module (TOE) Description

The Hard Disk Security Module (HSM) is a software module executed on MFP hardware and is contained on an SD memory card or DIMM-ROM providing adaptability to various MFP devices. The HSM is delivered in a kit and each kit is adaptable to a suitable MFP device. The kit contains the software either on a SD memory card or DIMM-ROM, an Operating Instruction Booklet or a CD-ROM containing the Operating Instruction Booklet and a Keytop version for each type of MFP device. Table 1 in the Security Target identifies and describes the HSM kit, the item, and the MFP devices suitable for each HSM kit type.

The HSM software executes exactly the same for each HSM kit type. The HSM creates buffers with two passes of random digits and a third pass of nulls. The HSM sends these buffers to the OS. The OS uses this data to overwrite the Temporary Area of MFP’s hard disk drive (HDD) upon completion of each copy or print job thereby removing residual data. Copy and print jobs use the Temporary Area of the MFP HDD as a temporary staging area, and upon completion of the copy or print function the HSM creates buffers which the OS uses to overwrite the clusters of the Temporary Area of the HDD used by the copy or print function, thereby removing residual data. The OS uses the HSM created buffers to overwrite the clusters of the Temporary Area of the HDD used by the copy or print function employing a three-pass method. HSM first creates a buffer of random digits and through system calls sends this pass of random digits to the OS.

The OS uses this pass of random digits to overwrite the targeted clusters in the Temporary Area of the HDD. This process is repeated a second time using a second buffer of random digits. Finally the HSM creates a buffer of nulls and sends this buffer to the OS. The OS then writes these nulls to the targeted clusters in the Temporary Area of the HDD.

The HSM function is automatic. Once installed on the MFP device, the overwriting function becomes effective immediately. It cannot be turned off, unless the software is removed. There is, however, a priority scheme. For practical MFP usability, the HSM function will become suspended if another application job accesses the HDD for writing or reading data. Once that job is completed HSM resumes. If the MFP power is disrupted either during HSM execution or if HSM is idle, upon power restore HSM is executed before user functionality can begin.

2.2 SF.RANDOMBUFFERS

The TOE Security Function SF.RANDOMBUFFERS generates buffers containing two passes of random data and one pass of nulls that are passed to the OS and used by the OS to overwrite copy and print data located in the Temporary Storage Area of the MFP HDD. SF.RANDOMBUFFERS inspects a table resident in memory (maintained by the IT Environment) for notification that residual data exists in the Temporary Storage Area of the MFP HDD. Upon discovery of the existence of residual data, SF.RANDOMBUFFERS seeks permission to begin the overwrite process. Once permission is given SF.RANDOMBUFFERS obtains random numbers from the IT Environment and generates buffers containing two passes of random data and one pass of nulls and sends these buffers to the OS to perform the overwrite. The TOE uses the standard rand() Unix function call for generating random numbers to populate the buffers with random data, but the TOE does not claim the use of a “random number generator” as specified by FIPS 140-2. The IT Environment is responsible for writing the supplied buffers to the designated locations on the HDD.

2.3 SF.SELFPROTECT

At each start-up, MFP firmware outside the TOE boundary checks to see if the TOE is physically installed (i.e., the DIMM or SD memory card is present). If the TOE is present, the IT Environment loads it into RAM for execution as a separate process. In order to remove the software from the MFP, the DIMM or SD memory card must be physically removed and the MFP device restarted. The TOE uses limited interfaces and cannot be directly accessed by a user. These interfaces use standard Unix socket-based communication channels where each communication path has a specified ID that ensures an exclusive connection and prevents access by other modules.

3 Assumptions

The assumptions listed below are assumed to be met by the environment and operating conditions of the system.

A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.INSTALL	The Ricoh Customer Engineer will install and configure the TOE according to the installation guidance.
A.NOEVIL	The personnel responsible for managing the MFP are non-hostile and follow the guidance when using the TOE.

A.PLATFORM The Ricoh Customer Engineer will ensure that the platforms used to host the TOE conform to the hardware and software outlined in the guidance.

A.LIMITS The personnel responsible for managing the MFP are knowledgeable about the limitations of the TOE and types of residual data that cannot be overwritten.

4 Threats

The following threats are addressed by the TOE and IT environment, respectively.

Threats Addressed by the TOE

The TOE addresses the following threats:

T.ANALYSE Copy and print data resident on the MFP hard disk drive may be inadvertently accessed or maliciously accessed and analyzed by agents who gain physical access to the HDD

T.INTERFERE The TOE could be by-passed or interfered with during operation by malicious users.

5 Clarification of Scope

The evaluation only covers a small portion of the functionality that is provided by the MFPs in which the TOE is installed. The TOE is a hardware module that coordinates activities that are performed within other part of the MFP that are part of the IT Environment. The combined activities of the TOE and the cooperating environment have the effect of overwriting the specified portions of the HDD and displaying an indicator on MFP when the operation has completed.

The evaluation of the Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B consists of the software that once loaded is always resident in memory and constructs buffers containing two passes of random data and a single pass of nulls for use in overwriting copy and print residual data located in the Temporary Area of the MFP hard disk drive (HDD). During print and copy job processing, the MFP stores images as files in the Temporary Area of the hard disk drive. There is a risk that these images could be disclosed during subsequent jobs. When initialized, the TOE performs an inspection of a table resident in memory and if copy or print residual data is present on the HDD, the TOE begins the random data and null buffer generation which is used to overwrite those portions of the HDD.

The MFP displays an icon indicating whether or not the HDD is “clean” (this functionality is provided by MFP firmware not included in the TOE boundary).

The following capabilities of the MFP platforms that support the TOE must be disabled for the TOE to initialize and hence are excluded from the MFP platform in its evaluated configuration:

- Scanner Application (except Network TWAIN scanning)
- I-Fax
- Printer data spooling function
- Document Box Application
- Paperless Fax, and
- eCabinet.

The following data cannot be stopped or turned off; personnel responsible for managing the MFP must be aware that the hard disk drive will remain "dirty" while any of these types of data are present on the MFP.

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

The TOE is intended for use in environments where the normal overwriting of disk sectors three times is considered to be adequate erasure of residual data. When the TOE has completed its operation and the status icon on the display indicates that the HDD is clean, those sectors of the HDD Temporary Area that were used, will have been overwritten at least three times since any sensitive information was placed on them.

The functionality provided by the TOE is intended to reduce the risk of accidental disclosure of information previously processed by the MFP. Due to the prioritization process, residual data may be present while some subsequent jobs are printed, or if the system is abruptly shut down. Procedures need to be followed to ensure that the TOE completes its operation prior to removal of the HDD from the MFP facility or its reuse in another device within the same facility.

6 Architecture Information

The Hard Disk Security Module (HSM) is a software module executed on MFP hardware and is contained on an SD memory card or DIMM-ROM providing adaptability to various MFP devices. The HSM is delivered in a kit and each kit is adaptable to a suitable MFP device. The kit contains the software either on a SD memory card or DIMM-ROM, an Operating Instruction Booklet or a CD-ROM containing the Operating Instruction Booklet and a Keytop version for each type of MFP device. Table 1 in the ST identifies and describes the HSM kit, the item, and the MFP devices suitable for each HSM kit type.

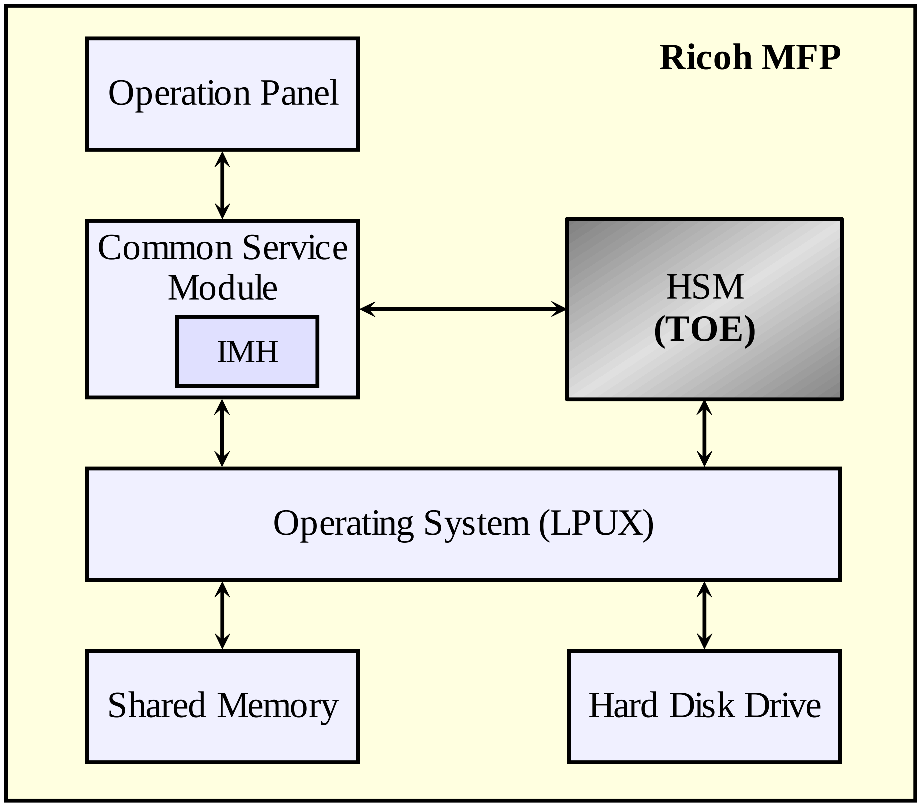


Figure 1 - TOE Boundary

6.1 Evaluated Configuration

The TOE is dependent on its environment to function properly. An authorized customer engineer must turn off the following applications and functions of the MFP device:
Scanner Application (except Network TWAIN scanning)
I-Fax
Printer data spooling function
Document Box Application
Paperless Fax, and
eCabinet.

The TOE will not initialize unless the above functions are turned off.

7 Product Delivery

The TOE must be installed by a vendor representative to comply with the constraints of the evaluation. Properly trained customer engineers from a service company deliver the HSM Kit to the customer's site and perform the installation. Hence, there are no end-user procedures for the installation of the HSM Kit, the installation procedures are part of the purchase and delivery of the TOE. The HSM is delivered in a kit and each kit is adaptable to a suitable MFP device. The kit contains the software either on a SD memory card or DIMM-ROM, an Operating

Instruction Booklet or a CD-ROM containing the Operating Instruction Booklet and a Keytop version (covers the operation panel key describing the specific function of that key) for each type of MFP device. No other documents are delivered with the product.

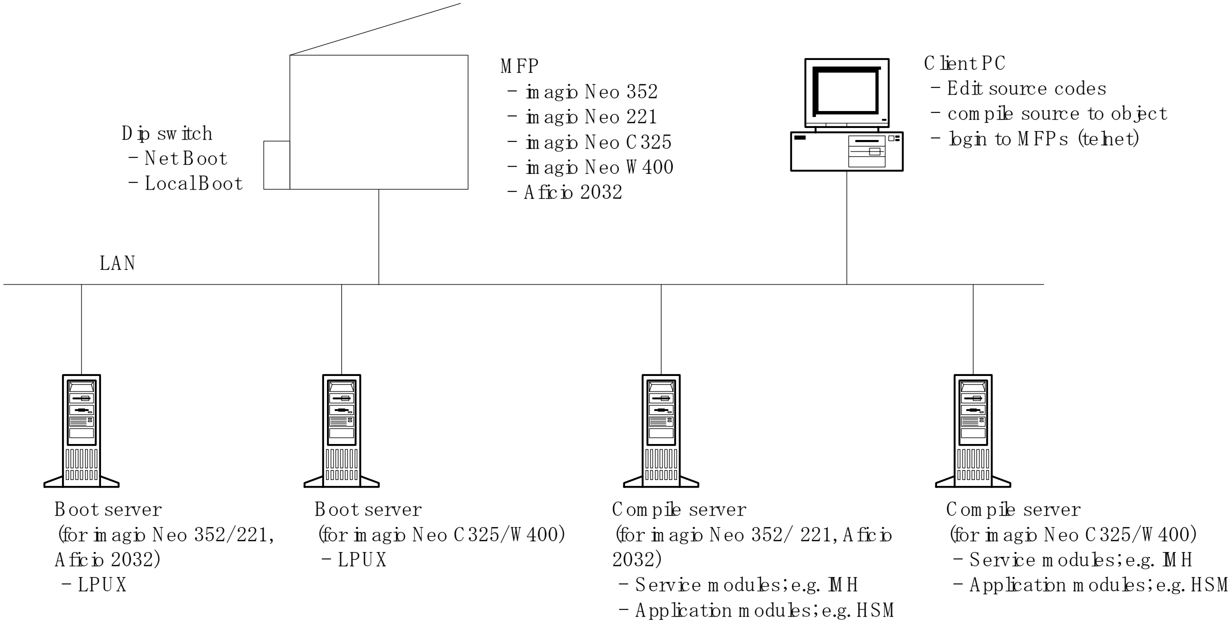
8 IT Product Testing

Testing was performed between February 20 through February 22 2007 at the Ricoh facilities in Tokyo, Japan. A COACT employee performed the tests.

8.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of the following test bed configuration. The test configuration has been modified from below in that only one MFP family class is to be tested and verified. The MFP used in the test configuration was the Neo C325. The TOE software was modified to permit telnet login and the recording of data to log files.

Figure 2 - Test Bed Configuration



8.2 Functional Test Results

The evaluation team executed the entire developer test suite. All security functions and interfaces were tested. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the developer and CCTL proprietary report, Ricoh Functional Test Report F3-0307-002, dated 16 May 2007.

8.3 Evaluator Independent Testing

The evaluation team selected a sample of the vendor tests to be reproduced. The tests selected validated the security functions and the TOE operational status. The purpose of this testing was to provide evidence which indicates that the TSF behaves as expected. Furthermore, this testing provides evidence that indicates that the MFP functionalities related to the TSF behave as expected. This is because the TSF is premised that the MFP, which is the platform of the TOE, correctly performs.

The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests.

8.4 Evaluator Penetration Tests

The evaluator examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

A) https://cirdb.cerias.purdue.edu/coopvdb/public/

B) http://xforce.iss.net/

C) http://cve.mitre.org

D) http://www.securityfocus.com

The vendor used the third listed source (as well as the vendors documentation) for identifying known obvious vulnerabilities for the technology under consideration. The evaluators agreed that it was sufficient since most of the MFP vendors as well as the underlying OS developers actively participate in the cve effort to identify vulnerabilities. However, the validators checked the other three sources to confirm that no additional obvious vulnerabilities were documented at those sites. After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicting that the vulnerability is non-exploitable in the intended environment of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

As a result of the evaluator's examination of the developer's vulnerability analysis and the independent search of for obvious TOE vulnerabilities, the evaluator did not identify any additional possible vulnerabilities. However, the evaluator noted that several of the developer identified vulnerabilities were mitigated by relying upon the developer supplied user guidance.

8.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

9 RESULTS OF THE EVALUATION

The evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the identified vulnerabilities by testing the MFP for selected developer identified vulnerabilities.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, COACT document F3-0507-003 Penetration Test Report for the Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B,dated 16 May 2007.

The evaluation determined that the product meets the requirements for EAL 3. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. VALIDATOR COMMENTS

This product coordinates activities that are primarily performed in the IT Environment. The TOE relies heavily upon the correct functioning of unevaluated aspects of the IT Environment. In particular, it relies upon the IT Environment to correctly identify the disk sectors that need to be cleansed, to generate the random patterns that are eventually used to overwrite the disk sectors, to perform the actual writing to the disk sectors, and to provide the visible notification to the end users when the disk has been cleansed. These supporting functions are performed by the operating system and associated applications that are installed on the MFP separately from the chip that contains the TOE. Although tests demonstrated that the TOE performed correctly and the supporting hardware and software appears to provide the correct support in the test configuration, the supporting components of the MFP platforms were not evaluated to ensure that they cannot be compromised in a manner that would nullify the TOE. The vendor controls the supporting components that are installed on the MFP platforms, but the vendor chose not to include those additional components of the supporting MFP platforms in the evaluation. Hence, a separate analysis of those components will be necessary for the TOE to be used in some of the environments that expect the disk sector cleansing features that the TOE supports.

11. Security Target

The Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B Security Target, dated March 8, 2007 is incorporated here by reference.

12. List of Acronyms

CC	Common Criteria
EAL3	Evaluation Assurance Level 3
HDD	Hard Disk Drive
HSM	Hard Drive Security Module
IT	Information Technology
MFP	Multi-Function Printer
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

13. Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.2, dated January 2004
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000