National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1

Report Number: **CCEVS-VR-04-0063**
Dated: **28 June 2004**
Version: **1.0**

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

Jeffrey C. Gilliatt
Richard A. White
Mitretek Systems,
Falls Church, Virginia

Common Criteria Testing Laboratory

COACT, Inc.
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 was performed by COACT Common Criteria Testing Laboratory in the United States and was completed during June 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by COACT. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 3 have been met.

The TOE is the software that drives the imageRUNNER copier and contains the Complete Erase feature. During print, scan, fax, and copy job processing, the imageRUNNER stores images as files on the hard disk drive. As a result of the temporary storage of image files on magnetic media, there is a risk that these images could be disclosed during subsequent jobs. To mitigate this threat, the Complete Erase feature, when activated, completely overwrites files on the imageRUNNER hard disk drive once they are no longer needed.

The primary TOE security functions that enable this capability are:

- Complete Erase: Eliminates residual information by overwriting the data memory space with either: NULL data once, random data once, or random data three times.

- System Manager Logon: The System Manager Logon function ensures only authorized System Managers can access the interface used to activate and deactivate the Complete Erase function. The System Manager credentials, a seven digit password and a numeric user id, are set using the System Manager Settings user interface. Once set, the credentials can only be changed by an authorized System Manager.

  The System Manager Logon feature is invoked before access to the Complete Erase feature settings is allowed. Entering invalid credentials results in a failed logon attempt and a redisplay of the logon screen after a one second delay.

- Security Management: Once the System Manager successfully logs in to the administrative interface, the System Manager has the ability to activate or deactivate the Complete Erase functionality.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 3 evaluation. Therefore the validation team concludes that the COACT CCTL findings are accurate, and the conclusions justified.

2 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 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 desiring 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's 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 Protection Profile to which the product is conformant;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1
Protection Profile	Not applicable

Item	Identifier
Security Target	*Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 Security Target*, June 25, 2004, Document No. F3-0504-001(1).
Evaluation Technical Report	*Evaluation Technical Report for the Canon imageRUNNER 2200/2800/3300 Software Version 50.06 with Security Kit B1;* June 8, 2004 Document No. F3-0604-001.
Conformance Result	CC Part 2 conformant, CC Part 3 conformant, EAL 3
Sponsor	Canon U.S.A., Inc. One Canon Plaza Lake Success, New York 11042
Common Criteria Testing Lab (CCTL)	COACT, Inc., CAFÉ Lab Common Criteria Testing Laboratory 9140 Guilford Road, Suite G Columbia, Maryland 21046-2587
CCEVS Validator(s)	Jeffrey C. Gilliatt Richard A. White Mitretek Systems, Inc. 3150 Fairview Park South Falls Church, VA 22042-4519

3 Security Policy

The TOE implements a Residual Information Protection Security Policy which overwrites temporary data files, according to a pre-defined erase mode, when the print job has completed. Prior to installation of the Security Kit B1, it is the responsibility of the consumer to determine the appropriate erase mode: 1) write NULL data once, write random data once, or write random data three times. While the consumer cannot modify the erase mode without assistance from the developer, the consumer can enable or disable the enforcement of the overwrite function.

4 Assumptions

4.1 Personnel Assumptions

- System Managers are properly trained, follow all System Manager guidance, and do not attempt to attack or subvert the TOE and its policy.
- Attackers are assumed not to use sophisticated attack methods to attempt to compromise the TOE security functions.

4.2 Physical Assumptions

- The physical environment of the TOE is sufficient for secure operation of the hardware.

- The TOE cannot be physically accessed without disassembling the machine which embodies the TOE.

4.3 IT Environment Assumptions

.

- The operating system and device drivers are the only way to access the file system and will correctly execute functions to read, write, and delete files.

- The hardware and software required by the TOE are dedicated to the imageRUNNER and perform as documented for the TOE.

- A competent System Manager will be assigned to manage the TOE and its security functions.

- The hardware and software required by the TOE have been installed and configured according to the appropriate installation guides.

- The System Manager password is changed at least every sixty (60) days.

5 Architectural Information

The TOE Security Functions are architecturally divided into three separate subsystems, the Adm., the File System (FS), and the Initialize Control. These subsystems are depicted in Figure 1 and are summarized in the text below.

a) Adm.: A logical component that handles the role of the administrator, including the implementation of the system manager identified and authentication mechanism and the ability to control the enabling or disabling of the hard disk data complete erase function.
b) File System: A logical component that lies under the network application and the local application. It provides common functions for the purpose of create/write/read/delete files for the components that sit above it. Together these operations implement basic functionality required for the complete erase functionality.
c) Initialize Control: The Initialize Control handles system initialization and is the first code executed after the Bootable is loaded. The Initialize Control is responsible for over writing any partially deleted files remaining on the hard drive after a power loss..

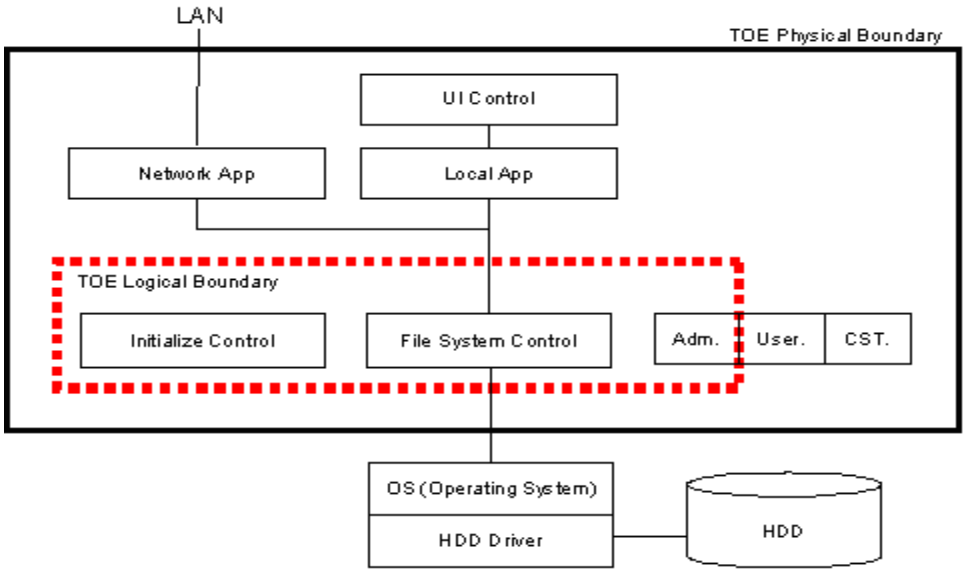

Figure 2: Canon imageRUNNER / iR Software Architecture

6 Documentation

The following is provided to the consumer:

- Installation Check List.

- Canon iR Security Kit-B1 Reference Guide.
- Canon imageRUNNER 3300/2800/2200 Reference Guide.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and the high level design and mapped each test to the security function tested. The scope of the developer tests included all three TOE Security Functions: Complete Erase, System Manager Logon, and Security Management.

The developer tested the Bootable Version iR2200N-USen50.06 with Security Kit B1 on the imageRUNNER 3300.

Test depth is addressed by analyzing the functions addressed in the high level design and associating test cases that cover the addressed functionalities. The high level design addressed the general functions of the TOE components. Each security function maps to the appropriate test suite, and the test rational demonstrates why the test suits provide adequate test coverage of a given security function.

The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification and high level design. The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests. Although the evaluation team performed a sample of the developer's test suite, the selected test were representative of the TOE Security Functions.

The following hardware and software comprised the test configuration:

<u>System Hardware</u>

A) Multifunction Printer: imageRUNNER 3300 Series Software Version iR2200N-USen50.06 with Security Kit B1.

B) PC: Computer that allows serial and network connections. Any model is acceptable.

C) 232cBOARD: Serial communication board to be connected to the iR3300 controller.

D) HUB: 100Mbs Switching HUB.

Installed System Software

A) OS: Windows XP

B) Communication Software (for serial communication)

C) Application software that can produce multiple pages of documents and that can invoke a printer driver.

D) Printer Driver (PCL) that is provided with the iR3300.

E) Network Scan Gear (Twain Driver) that is provided with the iR3300.

Test Equipment

A) Serial Cable: One with a DSUB 9-pin connector (cross cable).

B) UTP cable (Category 5) x 2.

8 Evaluated Configuration

The evaluated configuration consisted of the components identified in the table below.

Component	Description
Bootable Version iR2200N-USen50.06	Software that controls all the functions of the imageRUNNER.
Security Kit B1	Tools and processes to replace the Bootable. The image in the kit has the Complete Erase functionality enabled.
imageRUNNER 2200/2800/3300 Series	Multifunction peripheral hardware device with scan, fax, print, and copy capabilities.

Table 2 - Hardware and Software Components

9 Validator Comments

The validation team would like to note that the imageRUNNER 2200/2800/3300 series devices are not delivered with the "Complete Erase" functionality enabled. Rather, it is the responsibility of the consumer to ensure an authorized Canon Service Technician (CST) applies Security Kit B1 and sets the erase mode to either 1) write NULL data once, 2) write random data once, or 3) write random data three times.

Furthermore, the consumer must ensure that the Complete Erase function is enabled using the System Manager interface after installation of Security Kit B1. If these steps are not taken by the consumer, the residual information protection offered by this TOE will not be employed.

10 Security Target

Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 Security Target June 25, 2004, Document Number F3-0504-001(1).

The document identifies the security functional requirements necessary to implement Residual Information Protection security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 3.

11 Glossary

CC	Common Criteria
CST	Canon Service Technician
HDD	Hard Disk Drive
iR	imageRUNNER
IT	Information Technology
NIAP	National Information Assurance Partnership
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

12 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, version 2.1, August 1999, Parts 1, 2, and 3

- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, version 0.6, 11 January 1997.

- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, version 1.0, August 1999.

- *Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 Security Target* June 23, 2003, Document Number F3-0504-001.

- Evaluation Technical Report for the Canon imageRUNNER 2200/2800/3300 Software Version 50.06 with Security Kit B1, June 8, 2004, Document Number F3-0604-001.

13 National and International Interpretations

The Evaluation Team determined that the following CCIMB Interpretations were applicable to this evaluation:

1. *RI # 3 - Unique identification of configuration items in the configuration list, 2002-02-11*
2. *RI # 4 - ACM_SCP.*.1C requirements unclear, 2001-11-12*
3. *RI #19 – Assurance Iterations, 2002-02-11*
4. *RI #49 – Threats met by the Environment, 2001-02-16*
5. *RI #64 – Apparent higher standard for explicitly stated requirements, 2001-02-16*
6. *RI # 65 - No component to call out security function management, 2001-07-31*
7. *RI #84 – Aspects of objectives in TOE and environment, 2001-02-16*
8. *RI #85 – SOF Claims additional to the overall claim, 2002-02-11*
9. *RI #138 – Iteration and narrowing of scope, 2002-06-05*

The Evaluation Team determined that the following NIAP interpretations were applicable to this evaluation:

1. *I-0405 – American English Is An Acceptable Refinement, 2000-12-20*
2. *I-0406 – Automated Or Manual Recovery Is Acceptable*, *2001-03-15*
3. *I-0407 – Empty Selections Or Assignments, 2002-01-04*
4. *I-0409 - Other Properties In FMT_MSA.3 Should Be Specified By Assignment, 2002-01-04*
5. *I-0410 – Auditing Of Subject Identity For Unsuccessful Logins, 2002-01-04*
6. *I-0414 – Site-Configurable Prevention Of Audit Loss, 2002-01-04*
7. *I-0421 – Application Notes In Protection Profiles Are Informative Only, 2001-06-22*
8. *I-0423 – Some Modifications To The Audit Trail Are Authorized, 2000-12-11*
9. *I-0425 – Settable Failure Limits Are Permitted, 2000-12-05*
10. *I-0427 – Identification of Standards, 2001-06-22*
11. *I-0429 – Selecting One Or More, 2002-01-04*

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.