National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

EFI Fiery System 6 or 6e Secure Erase Option
And
EFI Fiery System 7 or 7e Secure Erase Option

Report Number: **CCEVS-VR-06-0041**
Dated: **October 10, 2006**
Version: **1.0**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE Evaluation was Sponsored by:

Electronics for Imaging, Inc.
303 Velocity Way
Foster City, CA 94404

Evaluation Personnel:

Science Applications International Corporation (SAIC)
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046-2554

Shukrat Abbas
Quang Trinh
Jean Petty

Validation Personnel:

Shaun Gilmore, National Security Agency
Daniel Faigin, Aerospace Corporation

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option software. 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 Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option software was performed by the SAIC Common Criteria Testing Laboratory in the United States and was completed during September 2006. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 3 augmented with ALC_FLR.1 have been met.

The EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option software provide the option to securely overwrite print job images. The Secure Erase Option contains the instructions to overwrite the images three (3) times when these print job images are no longer needed.

The Fiery System (the product) is installed on a machine running either Microsoft Windows XP embedded or Linux operating systems. The version of the Fiery System (the product), which includes the TOE that runs on Microsoft Windows XP embedded operating system, is referred to as the EFI Fiery System 6 and the EFI Fiery System 7. The version of the Fiery System (the product), which includes the TOE that runs on Linux operating system is referred as the EFI Fiery System 6e and the EFI Fiery System 7e.

During operation, images of print jobs submitted for printing are stored on the hard drive. The TOE will delete print job images left over from a completed print job by overwriting the sectors occupied by that image file with three (3) passes. The first pass overwrites the print job image with all zeros. The next pass overwrites the print job image with all ones. The final pass overwrites the print job image with random characters.

To activate or deactivate the secure erase option feature, the user must have administrator rights to the Fiery administrative screens. The IT Environment performs identification and authentication of all users to ensure they have the appropriate privileges (role) to access the TOE and its functions.

Print jobs are submitted through two methods: over a LAN or imported locally from the hard drive. Once the print job is imported, processed, and marked for deletion, the TOE will delete the file (print job image) using the three-pass overwrite method (described above). If the TOE is not enabled, then the file is deleted by the standard operating system deletion method. The Windows and Linux operation deletion scheme is the removal of the file pointer to the space on the hard drive without erasing the actual data on the occupied hard drives sectors.

The only user of the TOE is the authorized administrator. The authorized administrator may modify options in the product to include the activation or deactivation of the TOE. However, for the TOE to be in the evaluated configuration, the overwrite feature must be enabled.

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 CCTLs or candidate 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 and candidate 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 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 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	The TOE consists of the EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option software.
Security Target	EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option Security Target Version 1.0, 3 October 2006
Evaluation Technical Report	Evaluation Technical Report For EFI Fiery System 6.0 or 6.0e with Secure Erase and EFI Fiery System 7.0 or 7.0e with Secure Erase Version 0.1, September 11, 2006
Conformance Result	EAL 3 augmented with ALC_FLR.1
Sponsor	Electronics for Imaging, Inc. 303 Velocity Way Foster City, CA 94404
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046-2554

Item	Identifier
CCEVS Validator(s)	Shaun Gilmore National Security Agency Daniel Faigin Aerospace Corporation

3 TOE Security Services

The security services provided by the TOE are summarized below:

User Data Protection
The Secure Erase Option feature ensures that print job image files on the hard drive are overwritten before that disk space is reused. Before re-allocation of disk space, the sector level of the hard drive is overwritten 3 times, thereby ensuring no traces of print job image is left on the drive. The TOE ensures there is no residual information remaining on hard drive from the print jobs that have been queued, printed, and deleted.

Security Management
The TOE provides the authorized administrator with ability to configure the overwrite feature of the TOE. The only user of the TOE is the authorized administrator and the ability to manage the TOE is restricted to the authorized administrator. The authorized administrator is afforded the option to enable or disable the overwrite feature. However, in the evaluated configuration, the overwrite feature must always be enabled.

4 Assumptions

4.1 Physical Security Assumptions

- The product will be located within an environment that is sufficient for secure operation.

4.2 Personnel Security Assumptions

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized Administrators are not willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.3 System Assumptions

- The hardware and software with the TOE have been delivered, installed, and setup in accordance with documented delivery and installation procedures.

5 Architectural Information

Figure 1 depicts the Fiery System product, including the TOE, the EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option. Within the Fiery System product, the major components are administrative management options, operator options, user options, secure erase option (the TOE), job management, color management, networking, and image rasterization.

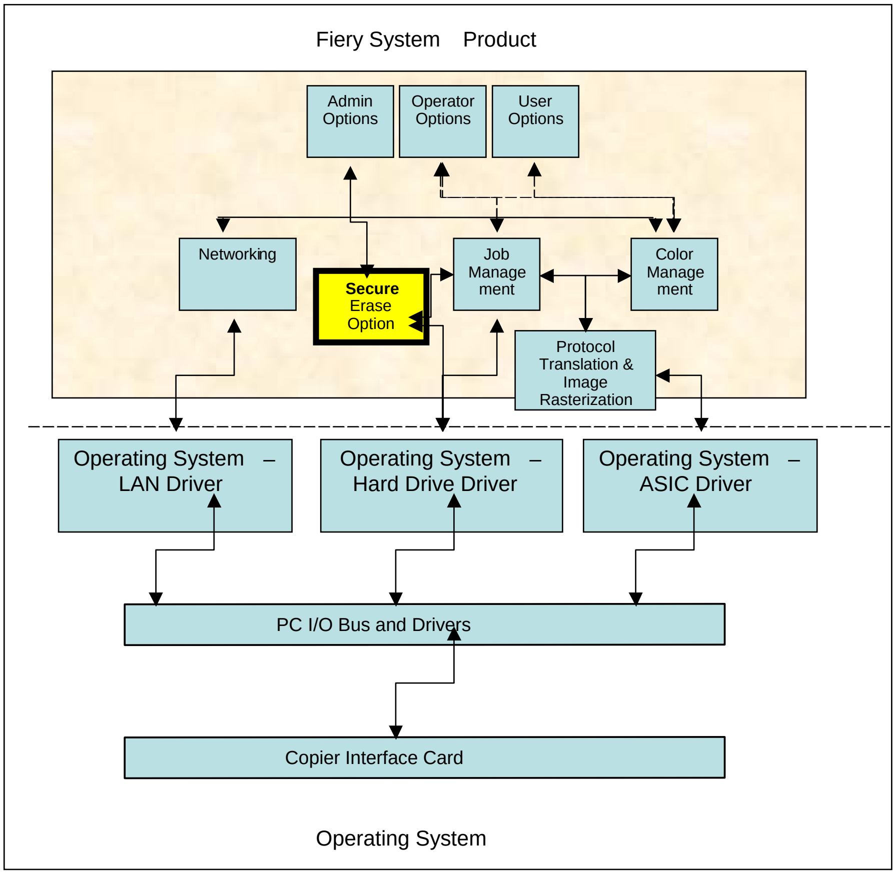


Figure 1 Fiery System Product Architecture

The following table provides a description of the major components of a print server.

Print Server Components	
EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option (TOE)	TOE - Software providing algorithm to overwrite deleted image files with random data.
EFI Fiery System Product	IT Environment – Software to manage the print server, which includes the following major components; administrative management options, operator options, user options, secure erase option (the TOE), job management, color management, networking, and image rasterization
Operating System	IT Environment - Software to control the computer hardware, drivers, and user interfaces
CPU	IT Environment - Intel brand Central Processing Unit
RAM	IT Environment - Random access memory providing temporary memory storage for computing functions
Motherboard, I/O Bus and Devices	IT Environment - Motherboard and common communications channel for hardware devices. I/O devices includes DVD/CD-ROM, Monitor/Keyboard

Print Server Components	
Hard drive (disk)	IT Environment - Physical storage holding operating system, Fiery software, TOE software, and user data
ASIC	IT Environment - ASIC containing compression algorithms
Copier Interface Card	IT Environment - Interface card containing physical port that will be connecting to the copier cable

Table 1 Print Server Hardware and Software Component Descriptions

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

Design documentation:

Functional Specification:

- *Fiery System 6 Color Server Specification, EFI, 11/4/04*
- *Fiery System 6e (Color-Disk) Specification, EFI, 11/4/04*
- *Fiery Sys 7 Color Server Specification, EFI, 09/16/05*
- *Fiery System 7e (Color-Disk) Specification, EFI, 09/16/05*
- *Fiery System 6 Color Server Specification, Section 4, v1.3 05/04/05*
- *Secure Erase Product Addendum for Fiery System 6/6e/7/7e OEM Specs(v1.6, August 23, 2006), DRAFT*

High-Level:

- *Fiery System 6 & 7 (Server) Secure Erase High Level Design Document, Version 1.07, August 17, 2006*
- *Fiery System 6e and 7e (Embedded) Secure Erase High Level Design Document, Version 1.06, August 17, 2006*

Guidance documentation:

- *Secure Erase Administrator Guide, version 1.2 March 22, 2006*

Configuration Management:

- *Electronics for Imaging Software Configuration Management Plan (SCMP), Version 3.3, March 23, 2006 (referred to as CM document)*
- *EFI TOE Configuration Management Item Supplement, Version 2.3, 22 August, 2006 (refer to as CI document)*

Lifecycle Support:

- *Electronics for Imaging Supplement Security Information, Version 1.0, May 2, 2005*
- *EFI Password Policy*

- *Electronics for Imaging Information Security Policy, Version 11.1, April 26, 2005*
- *Electronics for Imaging Corporate Headquarters Campus Security Protection*
- *Electronics for Imaging Security Procedures, Version 2005.1.0, February 28, 2005*
- *Information Technology Acceptable Use Policy for EFI Employees, Agents and Contractors*
- *Siebel Defect Process*
- *Defect resolution workflow*
- *EFI OEM Siebel Handbook, February 7, 2005*

Delivery and Operation documentation:

- *Electronics for Imaging, Delivery Process Manual, version 1.1, 05 July 2005*
- *Release TO Manufacturing For Fiery Products, Guidelines to Define responsibilities and Milestone 45027243, Rev C*
- *Secure Erase Administrator Guide, version 1.2 March 22, 2006*

Test documentation:

- *Network & Operating System Master Test Plan For Secure Erase Option, Version: 2.14, May 8, 2006*
- *Network & Operating System Master Test Matrix Instructions For "Secure Erase Option (Embedded)", Version: .69, August 25, 2006*
- *Network & Operating System Master Test Matrix Instructions For "Secure Erase Option (Server)", Version: .73, August 25, 2006*
- *SecureEraseCertificationServerMatrix.xls for each Server product*
- *SecureEraseCertificationEmbeddedMatrix.xls for each Embedded product*

Vulnerability Assessment documentation:

- *Secure Erase Administrator Guide, version 1.2 March 22, 2006*
- *Secure Erase Product Addendum for Fiery System 6/6e/7/7e OEM Specs (v1.2)*
- *Fiery System* 6/6e and 7/7e *Secure Erase Vulnerability Assessment Document, Version 1.02, 03/09/06*

Security Target:

- *EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option Security Target, Version 0.85, September 11, 2006.*

7 IT Product Testing

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

7.1 Developer Testing

EFI's approach to test the TOE security functions consists of a series of manual tests. The test suite runs through a series of tests classified as basic, functional test, configuration access can be restricted, role differentiation and data overwritten which runs through general functions of the Fiery product as well as specific tests that demonstrate the security functions described in the functional specification, the high-level design, and Security Target.

Note that for completeness, the vendor has performed tests to verify role differentiation and configuration access restriction. However, the IT environment (Fiery System) enforces these security features, not the TOE. Therefore, the evaluator team may choose not to run these specific set of tests.

7.2 Evaluation Team Independent Testing

This section summarizes the team's test coverage analysis approach. The correspondence between security functions and interfaces is clearly defined in the functional specification and need not be repeated here.

The team test cases are categorized according to the security function. The evaluation team tests were derived based on perceived gaps or areas of weakness in the developer's test suite based on the preceding coverage and depth analyses.

Although the developer's testing was considered adequate, the evaluators also tested each of the security functions as defined in the Security Target. Specifically:

- User Data Protection
- Security management

The evaluators also executed a number of tests to determine whether the TOE is vulnerable to attacks aimed at bypassing the security functions or subverting the basic protection mechanisms.

User Data Protection

Through code inspection the tester determined what type of data is used to overwrite the identified file, when the overwrite feature is enable and determine that the TOE can determine what sectors of the HDD the file was stored. The review of the code resulted in the determination that the high-level design was accurate (which indicates that the data will be overwritten with 0s, 1s, and random data), that there is a marker that indicates that overwrite function should be executed, and that there is clear identification of the file to be deleted.

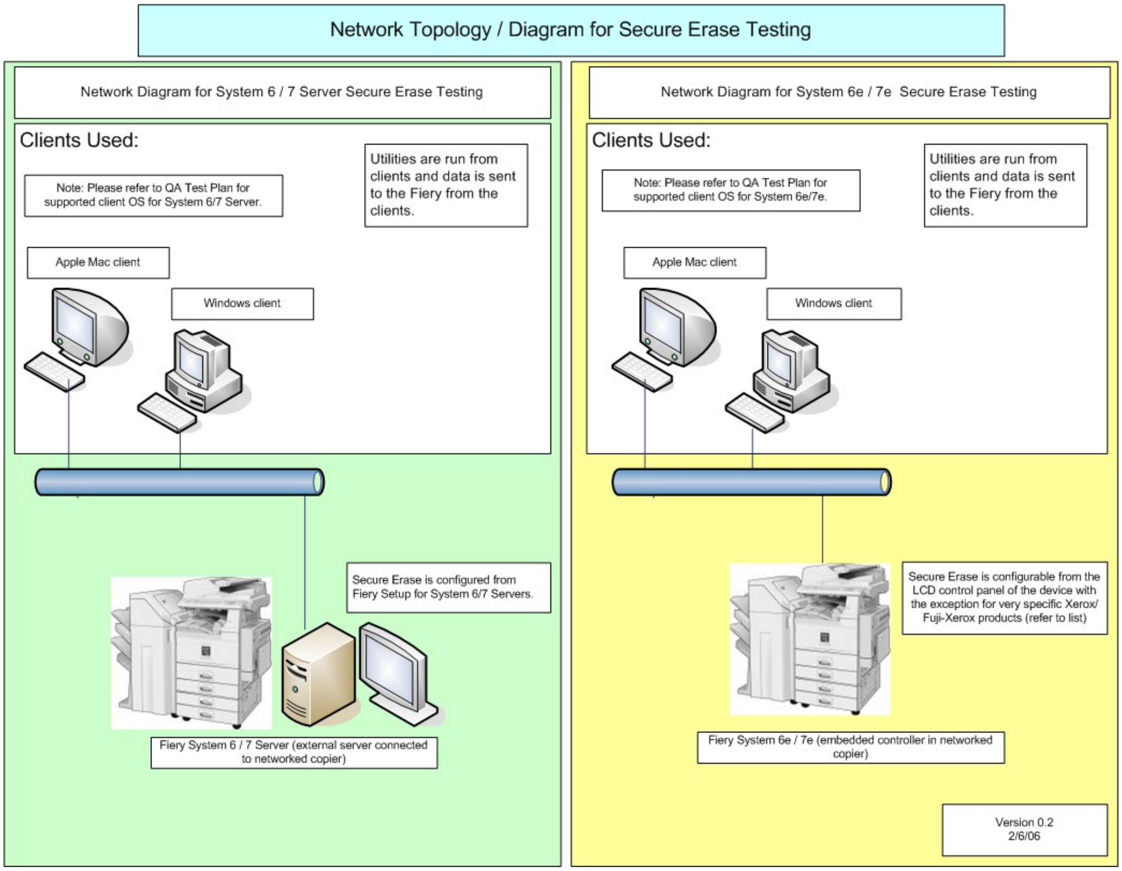
Security Management

The tester confirmed that only the correct administrator password can be used to access and change configuration of Secure Erase via Fiery Setup or the LCD. The administrator password is assumed to be set during "Step: Configure Fiery with Administrator password" test. The evaluator is free to choose a different password. The evaluation team utilized the vendor test instructions for Configuration Access Can Be Restricted and Role Differentiation to perform testing. The tests resulted with all passwords failing except for the correct password and only the administrator role is able to access the interface. Specific interfaces tested included:

- Command Workstation
- LCD
- Fiery Setup

8 Evaluated Configuration

The evaluation team exercised developer and independent tests against the evaluated configuration of the TOE. The following diagram depicts the test configuration and the hardware and software components are summarized in the subsequent sections.


Network Topology / Diagram for Secure Erase Testing
Network Diagram for System 6 / 7 Server Secure Erase Testing
Clients Used:
Note: Please refer to QA Test Plan for supported client OS for System 6/7 Server.
Utilities are run from clients and data is sent to the Fiery from the clients.
Apple Mac client
Windows client
Secure Erase is configured from Fiery Setup for System 6/7 Servers.
Fiery System 6 / 7 Server (external server connected to networked copier)
Network Diagram for System 6e / 7e Secure Erase Testing
Clients Used:
Note: Please refer to QA Test Plan for supported client OS for System 6e/7e.
Utilities are run from clients and data is sent to the Fiery from the clients.
Apple Mac client
Windows client
Secure Erase is configurable from the LCD control panel of the device with the exception for very specific Xerox/ Fuji-Xerox products (refer to list)
Fiery System 6e / 7e (embedded controller in networked copier)
Version 0.2
2/6/06

The testing environment included four printers with the Fiery products with the embedded TOE. The tester will run the test instructions from the desktop attached to each printer and one computer, Apple Macintosh, will be able to access each printer from the test network.

System	**System 7e**	**System 6e**
OEM	Canon imagePASS-C2 (USA)	Ricoh E7000
IP Address	10.10.95.66	10.10.95.72
DNS Name	SERVER99534	E-7000_00DB

System	**System 6**	**System 7**
OEM	Konica-Minolta 8050 / C500	Xerox EXP 4110
IP Address	10.10.95.68	10.11.96.135
DNS Name	OEM-NX197YDDXD1	EXP4110_11

Hardware

The following hardware is necessary to create the test configurations as depicted in the diagram above:

- TOE Hardware
    - None
- IT Environment Hardware
    - 4 - IBM PC
    - 1 MAC
- Test Hardware (printers)
    - Konica Minolta 8050 / C500 -
    - Ricoh E7000
    - Xerox EXP 4110
    - Canon imagePASS-C2 (USA)
    -

Software

The following software is required to be installed on the IT environment hardware used for the test:

- TOE Software
    - None
- IT Environment Software
    - None
- Test software
    - Windows XP Professional (with latest Service Pack)
    - OS 9.2.2 or lower
    - WinHex for Windows

9 Validator Comments

The TOE developer and sponsor, and the Evaluation Team are commended for their effort in developing tests for the System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option software. All test plans were clear, complete, and comprehensible.

It is important to note that there are multiple patches that are required for secure installation of the Fiery product, however these updates do not affect the TOE and are clearly outlined in the Security Target.

10 Security Target

EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option, Version 1.0, 3 October 2006

11 List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
MFD	Multifunction Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

.

12 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.2, Revision 256, January 2004.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, Version 2.2, Revision 256, January 2004.

[7] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, dated February 2002, version 1.1

[8] Evaluation Technical Report For EFI Fiery System 6.0 or 6.0e with Secure Erase and EFI Fiery System 7.0 or 7.0e with Secure Erase Part 2 (Proprietary).

[9] EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option Security Target, Version 1.0, October 03, 2006.

[10] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001