Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2006-10-20 (ITC-6108)
Certification No.	C0115
Sponsor	Canon, Inc
Name of TOE	EOS Original Data Security System
Version of TOE	1.0
PP Conformance	None
Conformed Claim	EAL2
Developer	Canon, Inc
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2007-08-30

Hideji Suzuki, Deputy Technical Manager
Information Security Certification Office
IT Security Center

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

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

Evaluation Result: Pass

"EOS Original Data Security System" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “EOS Original Data Security System” (hereinafter referred to as “the TOE”) conducted by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, Canon, Inc.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	EOS Original Data Security System
Version:	1.0
Developer:	Canon, Inc

1.2.2 Product Overview

This TOE is a system that is comprised of a digital camera called the EOS-1D Mark III (referred to as the “EOS digital camera” below), the Original Data Security Administrator (referred to as the “administrator tool” below), the Original Data Security Utility (referred to as “the browser tool” below), and the Original Data Security Card (referred to as “the OS card” below).

This TOE makes it possible to verify the originality of image files shot by the EOS digital camera, and offers the following security functions as a system for keeping image files confidential.

- The EOS digital camera has functions to generate “original image determination data” (referred to as “verification data” below) for verifying the originality of an image file that is a shot image, to encrypt or decrypt an image file, to encrypt or decrypt a key used in the image file encryption process (referred to as the “image key” below), to verify and connect the OS card, and others.
- The browser tool has a function for decrypting image files. The administrator tool and the browser tool have functions that support the registration of authentication information related to the function of authenticating the identity of users.

- The OS card has a function for verifying the originality of image files based on "verification data," a function that decrypts encrypted image keys, a function that both encrypts and decrypts card keys etc., functions for administering and controlling the access of card keys etc., a function for verifying and connecting the EOS digital camera, and functions for authenticating the identity of the users of the administrator tool and the browser tool.

1.2.3 Scope of TOE and Overview of Operation

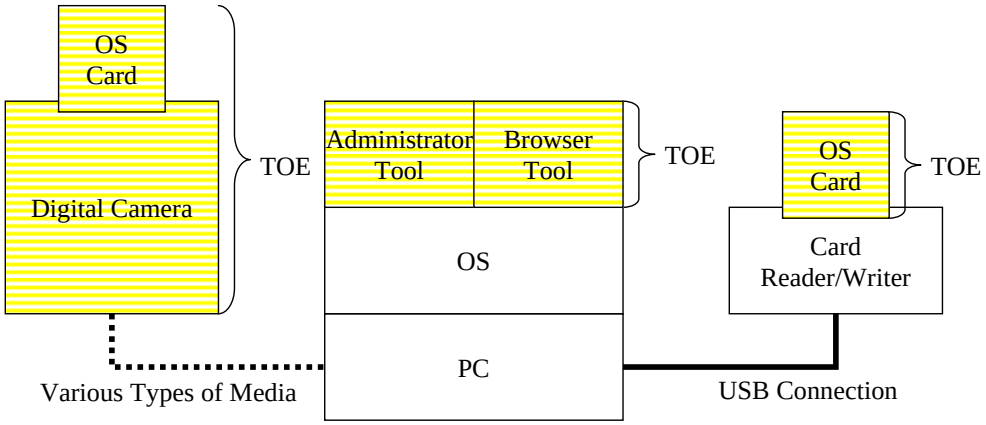

Figure 1-1 Configuration of TOE

As shown in Figure 1-1, this entire system is comprised of the EOS digital camera, the administrator tool, the browser tool, the OS (Operating System), the PC, the OS card, and the card reader/writer, and the TOE is comprised of the EOS digital camera, the administrator tool, the browser tool, and the OS card.

The system is designed to protect image files shot with the EOS digital camera from the perspectives of originality and confidentiality. In other words, this system makes it possible to use image files while maintaining their originality and confidentiality, with its "functions for verifying the originality of image files" and "functions for maintaining the confidentiality of image files." The "functions for verifying the originality of image files" use MAC (Message Authentication Code), and the "functions for maintaining the confidentiality of image files" are implemented with encryption. The MAC functionality is comprised of a function that uses a MAC processing key (referred to as the "MAC key" below) to generate verification data, and a function that verifies the originality of image files based on the MAC key and verification data. Encryption is comprised of a function for encrypting image files using image keys, and a function for decrypting encrypted image files using image keys. Furthermore, this system offers functions to support this functionality, including functions to generate image keys, functions to control access to image keys etc., functions to encrypt and decrypt image keys, functions to encrypt and decrypt card keys etc., functions to connect devices between the EOS digital camera and OS card, functions to authenticate the identity of administrators and browsers, and so on.

1.2.4 TOE Functionality

The components comprising the TOE offer the following security functions:

(1) The EOS digital camera component

This component is comprised of the digital camera hardware and digital camera firmware, and offers the following security functions:

- Verification and connection function: A function for verifying that the OS card supports the digital camera, and for connecting.
- Image key generation function: A function for generating image keys.
- Encryption function: A function for encrypting image files and image keys.
- Decryption function: A function for decrypting encrypted image files and encrypted image keys.
- Verification data generation function: A function for generating verification data for verifying the originality of image files using MAC keys.

(2) The OS card component

This component is comprised of the Original Data Security Card hardware and the Original Data Security Card applet, and provides the following security functions:

- I&A function: A function that uses PIN authentication to identify and authenticate the administrators and browsers.
- Verification and connection function: Functions that verify that the EOS digital camera is registered, and then connect.
- Information management functions: Functions that enable only administrators to initialize the administrator ID/PIN, browser ID/PIN, the EOS digital camera ID, and card keys. These functions can also initialize card keys, and maintain and manage EOS digital camera IDs and browser IDs. When a PIN modification request is received from a browser, if the requester is a correct browser, then a function will allow that PIN modification (these functions control access to the OS card).
- Encryption function: A function for encrypting the card key or OS card data, and for generating encrypted OS card data.
- Decryption function: A function for decrypting encrypted OS card data and encrypted image keys.
- Verification data verification function: A function for verifying the originality of image files based on the MAC key and verification data.

(3) The administrator tool

This tool is an application that runs on compatible PCs running one of the following operating systems: “Microsoft Windows 2000 Professional with Service Pack 4,” “Microsoft Windows XP Professional with Service Pack 2 (32-bit system),” “Microsoft Windows XP Home Edition with Service Pack 2 (32-bit system),” or “Microsoft Windows Vista (32-bit system).” The following security functions are included:

- PIN length inspection function: This function inspects the length of the PIN to be registered during the registration of OS card user information, and ensures that it contains between 8 and 15 characters.

(4) The browser tool

This tool is an application that runs under operating systems installed on compatible PCs, and which includes the following security functions:

- PIN length inspection function: This function inspects the length of one’s own PIN when it is to be changed, ensuring before registration that the new PIN contains between 8 and 15 characters.
- Decryption function: A function for decrypting encrypted image files.

.

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the

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

Scope of the evaluation is as follow.

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

More specific, the evaluation facility examined “EOS Original Data Security System” as the basis design of security functions for the TOE (hereinafter referred to as “the ST”)[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex B of CC Part 1 (either of [5]or [8]]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in “EOS Original Data Security System Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”) [13]. Further, evaluation methodology should comply with the CEM (either of [11] or [12]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated March 2007 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL2 conformance.

1.5.3 Security Functions

Security functions of the TOE are as follow.

- Image file verification functions

  This TOE includes functions to generate verification data and to verify the originality of image files based on this verification data.

  The “function for generating verification data” complies with FIPS PUB 198, and configures the Keyed-Hash Message Authentication Code with a key based on a fixed value with a 128-bit or longer bit length. The “function for verifying the originality of image files based on verification data” also generates verification data just like the “verification data generation function,” and verifies by comparing verification data affixed to an image file with generated verification data (with FCS_COP.1a support). Also, since the originality of an image is a condition that is independent from any administrator or browser, this function can be used even if administrator or browser identity authentication is not carried out.

- Image file encryption functions

  This TOE includes an image file encryption functions. These image file encryption functions include the image file encryption/decryption and image key encryption/decryption function shown in Figure 1-2.

  The image file encryption and decryption functions are comprised of the following elements:

  - An AES encryption/decryption function with a key length of 128 bits and FIPS PUB 197 compliance
  - A key generation function compliant with FIPS PUB 186-2, with a PRNG based on SHA-1 for general purposes in FIPS186-2 (+ change notice 1) Appendix 3.1
  - A key nullification function that zeroes out keys

  The image key encryption and decryption functions are comprised of the following elements:

  - Triple DES encryption and decryption functions with a 168-bit key length and compliance with NIST SP800-67
  - A key generation function compliant with ANSI X9.31, with a PRNG based on ANSI X9.31
  - A key zeroization function that zeroes out keys

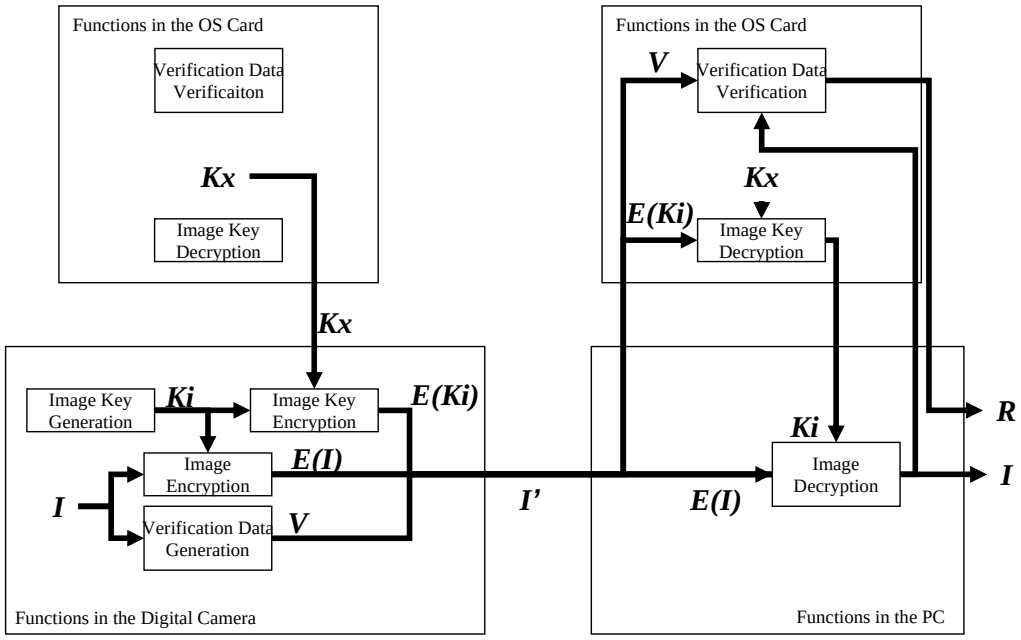

Figure 1-2 Image File Processing Procedure

- I&A function

  This TOE has a function that allows the OS card to identify and authenticate the user. The identification information and PIN are used to identify and authenticate an administrator or browser. This TOE can also perform the following processes without authenticating a user's identity:
  - Obtain the OS card's OSCID.
  - Obtain the OS card's version information.
  - Generate verification data for an image file.
  - Verify an image file based on the verification data.

  If the I&A function fails to authenticate the administrator or any browser three times, then it will return the authentication result after waiting five seconds from the next authentication attempt. If the identification & authentication is a success, then the I&A function will bind the user to the subject and define user attributes. Also, when identification & authentication succeeds, the number of authentication failures of the corresponding user will be cleared.
- PIN length inspection function

  This TOE verifies that a registered PIN is between 8 and 15 characters long.
- Verification and connection function

  The EOS digital camera, which is this TOE, verifies and connects to the OS card. The OS card, which is also a TOE, verifies that this is the designated EOS digital camera, and then connects. The camera and OS card verify each other, and after they have connected, the card key maintained in the OS card is transferred to the EOS digital camera with its confidentiality maintained by this function.
- Access control function

  This TOE includes a function whereby the OS card controls user access. This access control function applies the following access rules to the seed information for image files, OS card data, and OS card data encryption keys:

Table 1-1 Access Rules for Image Files

Security Attribute	Condition	Possible Operations (only when conditions are met)
Browser	With the browser security attribute	Decryption is possible
Administrator	With the administrator security attribute	Decryption is possible

Table 1-2 Access Rules for OS Card Data

Security Attribute	Condition	Possible Operations (only when conditions are met)
Administrator	With the administrator security attribute	Exporting is possible Importing is possible

Table 1-3 Access Rules for the Seed Information of Encryption Keys for OS Card Data

Security Attribute	Condition	Possible Operations (only when conditions are met)
Administrator	With the administrator security attribute	Importing is possible

Also note that when there is an OS card, the application process will always be able to verify image files based on verification data. Regardless of the security attribute held, the application process will not be able to encrypt image files or generate image file verification data.

Encryption and decryption of OS card data complies with NIST SP800-67, and is comprised of Triple DES, using a 168-bit key length. Also, this encryption key is generated with information inputted from outside as the seed.

- Administration functions

  Administrators can execute the following operations as administration functions:
  - Add and delete a browser's ID and PIN as a set.
  - Change administrator and browser PINs.
  - Initialize administrator IDs, PINs, and card keys.
  - Initialize an administrator's ID and PIN, or a browser's ID and PIN and card key as a set.
  - Add, delete, change, and initialize the EOS digital camera ID so that the OS card can identify it.

1.5.4 Threat

This TOE assumes such threats presented in Table 1-4 and provides functions for countermeasure to them.

Table 1-4 Assumed Threats

Identifier	Threat
T.MODIFY_IMAGE	A third party with malicious intent and no advanced technical knowledge might use an IT device to falsify image files shot by the EOS digital camera on a medium between the EOS digital camera and the browser tool.
T.DISCLOSE_IMAGE	A third party with malicious intent and no advanced technical knowledge might use an IT device to expose image files shot by the EOS digital camera on a medium between the EOS digital camera and the browser tool.
T. DISCLOSE_OSC	A third party with malicious intent and no advanced technical knowledge might use a PC to access the OS card and obtain card keys maintained by that OS card. They might then be able to use these keys to decrypt any encrypted image files.
T.ILLEGAL_ACCESS	A browser with malicious intent and no advanced technical knowledge might use the browser tool, the administrator tool, or a combination of the two to access the OS card and alter the OS card data.

	This might allow any user to decrypt encrypted image files.
T.BACKUP	A browser with malicious intent and no advanced technical knowledge might obtain OS card data from the OS card backup data to expose or falsify image files.

1.5.5 Organisational Security Policy

No organisational security policy exists that has been requested based on the use of this TOE.

1.5.6 Configuration Requirements

This TOE consists of the digital camera called EOS-1D Mark III. Original Data Security Administrator、Original Data Security Utility and Original Data Security Card.

1.5.7 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-5. The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-5 Assumptions in Use of the TOE

Identifier	Assumptions
A.PHOTOGRAPHER	The photographer must manage the OS card he is using in such a way that it is not switched for another OS card by a third party.
A.VIEWER	The browser (viewer) must manage the PIN for the OS card he is using in such a way that it is not leaked to another person. Also, the browser must select and set a PIN that is difficult for third parties to guess.
A.MANAGER	The administrator (manager) is given the role of correctly registering the EOS digital camera and browsers that can access the OS card. Also, the administrator must select and set a PIN that is difficult for third parties to guess.
A.PLATFORM	The PC and OS in which the administrator installs the administrator tool for use must be managed in such a way that undependable third parties cannot fraudulently use it. The PC and OS in which the browser installs the browser tool for use must be managed in such a way that undependable third parties cannot fraudulently use it. Also, these operating systems must be managed correctly so that no malicious applications are installed that might monitor or interfere with the operation of the administrator tool or the browser tool.
A.PERIPHERAL	A card reader/writer connected to a PC on which

	the browser has installed the browser tool for use must be managed in such a way that undependable third parties cannot use it for falsification. Also, this card reader/writer must be connected to the PC in such a way that eavesdropping does not occur between the two.

1.5.8 Documents Attached to Product

Documents attached to the TOE are listed below.

- EOS-1D Mark III User's Guide J, CT1-5228-000 (Japanese version)
- Original Data Security Kit OSK-E3 User's Guide J, CT1-7775J-000 (Japanese version)
- Preparing to Use the OSK-E3, CT1-7779-000 (Japanese version)

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

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

2.2 Overview of Evaluation Conducted

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

Evaluation has started on October 2006 and concluded by completion the Evaluation Technical Report dated August 2007. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by rental of developers' environments on May 2007.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

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

2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1) Developer Test Environment

Table 2-1 shows the configuration of tests implemented by the developer.

Table 2-1 Configuration of Developer Tests

Resource Name	Name	Description of Resource Used by Developers
Hardware	Digital Camera	EOS-1D Mark III hardware EOS-1D Mark III EOS-1D Mark III firmware 1.0.8
	OS Card	Original Data Security Card hardware OSC-128M Original Data Security Card applet 00000003 (applet name: FF34123456100101)
	Card Reader/Writer	Included with the Original Data Security Kit OSK-E3 and connected to the PC to allow for accessing, reading, and writing to the OS card
	PC	A PC/AT-compatible machine
	Lens	A lens that can be attached to and removed from the digital camera
Software	The Administrator Tool	Original Data Security Administrator 1.0
	The Browser Tool	Original Data Security Utility 1.0
	Windows 2000	Microsoft Windows 2000 Professional Service Pack 4
	Windows XP	Microsoft Windows XP Professional Service Pack 2 (32-bit system)
		Microsoft Windows XP Home Edition Service Pack 2 (32-bit system)
	Windows Vista	Microsoft Windows Vista (32-bit system)

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a. Test configuration

Test configuration performed by the developer is showed in the Table 2-1. Developer testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

The following method was used for the testing:
i) Confirmation of all security function operations from TSFI

c. Scope of Testing Performed

Testing is performed about 37 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

d. Result

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

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Test configuration performed by the evaluator is showed in the Table 2-1. Evaluator testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

For the testing, following approach was used.
1. All developer tests were implemented in order to confirm the reproducibility

of the test results.
2. The developer tests are inspected in order to check whether or not TSFI parameters exist that have not been implemented with the developer tests.
3. Additional tests which have been determined as necessary based on the examination results are implemented

c. Scope of Testing Performed

Total of 48 items of testing; namely 11 items from testing devised by the evaluator and 37 items from testing from sampling of developer testing was conducted. As for selection of the test subset, the following factors are considered.

1. Security functions whose operation according to the specifications is called into question based on developer tests.
2. Security functions that are more important than other security functions.
3. Security functions that are the subject of function enhancement
4. Function used by different interface.

d. Result

All evaluator testing conducted is completes correctly and could confirm the behavior of the TOE. The evaluator also confirmed that all the test results are consistent with the behavior.

2.4 Evaluation Result

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

3. Conduct of Certification

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

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

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

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

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL2 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC:	Common Criteria for Information Technology Security Evaluation
CEM:	Common Methodology for Information Technology Security Evaluation
EAL:	Evaluation Assurance Level
PP:	Protection Profile
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

The glossaries used in this report are listed below.

AES:	Encryption algorithm
ANS:	American National Standards Institute
CF:	A type of memory card referred to as “Compact Flash”
DES:	Decryption algorithm
FIPS:	The Commerce Department‘s Federal Information Processing Standards
MAC:	Message Authentication Code
NIST:	The U.S. National Institute of Standards and Technology
PIN:	Personal Identification Number (password/code number)
PRNG:	Pseudorandom number generator
SD:	A type of memory card referred to as “Secure Digital”
USB:	An interface standard for connecting peripheral devices to a PC

6. Bibliography

[1] EOS Original Data Security System Security Target Version 1.7 (May 17th, 2007) Canon Inc.

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

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

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

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 September 2005 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 3.1 September 2005 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 September 2005 CCMB-2006-09-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 September 2005 CCMB-2006-09-001 (Japanese Version 1.2 March 2007)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 3.1 September 2005 CCMB-2006-09-002 (Japanese Version 1.2 March 2007)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 September 2005 CCMB-2006-09-003 (Japanese Version 1.2 March 2007)

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 September 2005 CCMB-2006-09-004

[12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology V Version 3.1 September 2005 CCMB-2006-09-004 (Japanese Version 1.2 March 2007)

[13] EOS Original Data Security System Evaluation Technical Report Version 2.2, August 22nd, 2007, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center