CRP-C0010-01

Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	January 26, 2004 (ITC-4023)
Certification No.	C0010
Sponsor	Canon Inc.
Name of TOE	EOS-1D Mark II firmware
Version of TOE	Ver.1.0.1
PP Conformance	None
Conformed Claim	EAL2 + ALC_DVS.1
TOE 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.
July 21, 2004

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center
Information-Technology Promotion Agency, Japan

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "General Requirements for IT Security Evaluation Facility".

- Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations (as of 15 February 2002)

Evaluation Result: Pass

"EOS-1D Mark II firmware Ver.1.0.1" has been evaluated in accordance with the provision of the "General Rules for IT Product Security Certification" 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-1D Mark II firmware Ver.1.0.1” (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-1D Mark II
Developer:	Canon Inc.

1.2.2 Product Overview

The product is the EOS-1D Mark II (EOS digital camera) in which the digital camera firmware (TOE) was installed.

Unlike the conventional 35mm film photos, images taken by digital camera have various merits such as needlessness of development and printing / no secular degradation / easiness to store and search / transmission to a remote place using a communication channel. On the other hand, by digitization of images, there are some demerits such that processing and alteration can be easily performed using photo retouch tools. When the digital data of a digital camera are used, e.g. in the construction industry for checking of the progress or specification, the originality of the digital data is becoming a big issue.

The firmware that is the TOE provides the functionality that generates the verification data in order to verify the originality of the image file taken by the EOS digital camera.

The verification of the image data’s originality is realized by the Data Verification

System, which consists of EOS digital camera, the Data Verification Kit (the Verification Program, a Smart Card R/W, and a Smart Card), and PC. The overview of the operations of the Data Verification is described below.

1. The EOS digital camera generates a key for the verification, and generates the verification data using an image file and the generated key. (The firmware that is the TOE generates the verification data.)
2. Read the image file with the verification data into PC.
3. Select the image file that is verified from the list of the read image files by the Verification Program.
4. In the Smart Card, a key for the verification based on the image file selected by 3 is generated, and the verification data using both the generated key and the selected image file is generated.
5. Verify the originality of the image file by comparing the verification data generated by the EOS digital camera with the verification data generated by the Smart Card.

The brief description of the Data Verification System is shown in Figure 1.

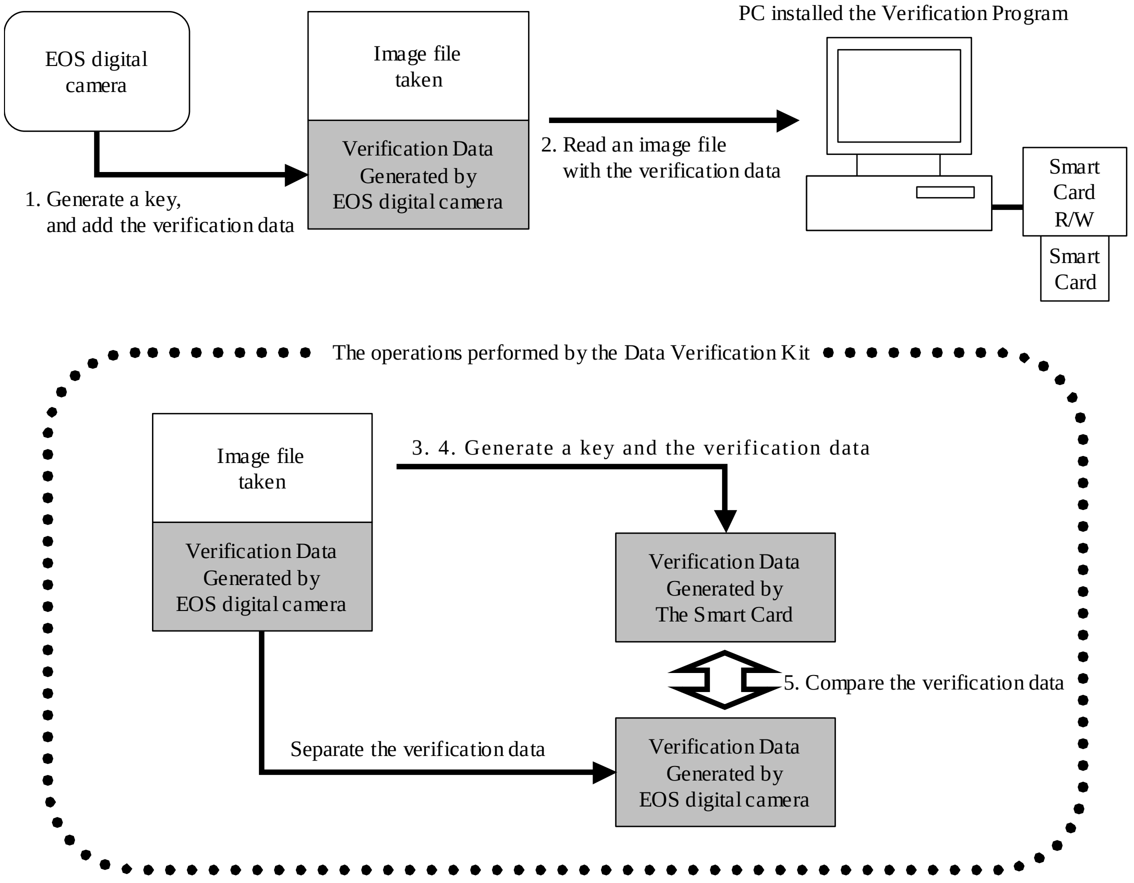
EOS digital camera
Image file taken
Verification Data Generated by EOS digital camera
1. Generate a key, and add the verification data
2. Read an image file with the verification data
PC installed the Verification Program
Smart Card R/W
Smart Card
The operations performed by the Data Verification Kit
Image file taken
Verification Data Generated by EOS digital camera
3. 4. Generate a key and the verification data
Verification Data Generated by The Smart Card
5. Compare the verification data
Separate the verification data
Verification Data Generated by EOS digital camera

Figure 1 The brief description of the Data Verification System

1.2.3 Scope of TOE and Overview of Operation

The brief description of the TOE components is shown in Figure 2.

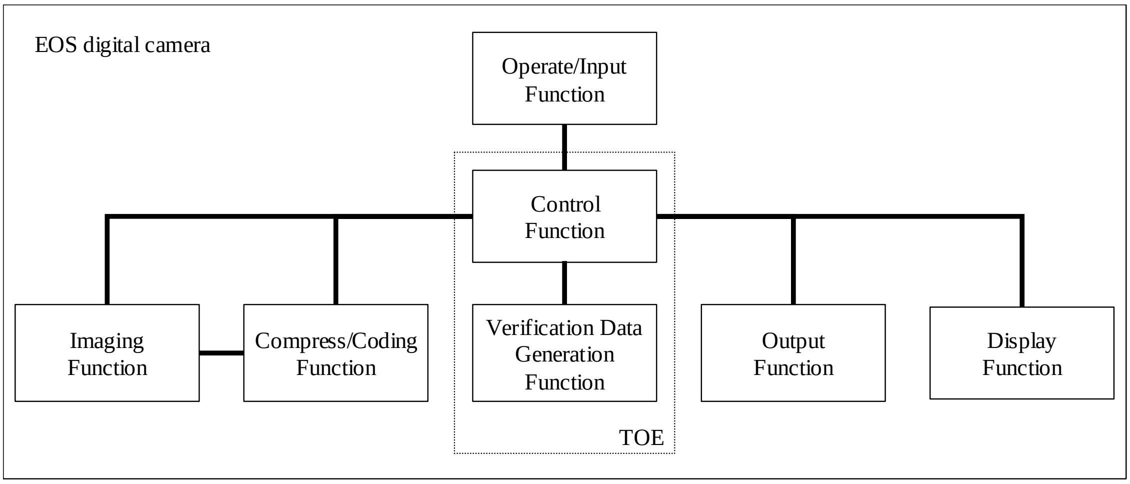

Figure 1 The brief description of the TOE components

The TOE is the "EOS-1D Mark II firmware Ver.1.0.1" that is installed in the EOS digital camera.

The "EOS-1D Mark II firmware Ver.1.0.1" that is the TOE provides "Verification Data Generation Function" as the security function. "Control Function" is not the security function.

The example of the operations to take the image with the verification data~~,~~ is shown below.

- The user perform the settings to generate the verification data on the EOS digital camera, and press down the shutter button (Display Function, Operate/Input Function, Control Function)
- The camera inputs the light as image data, compresses the image data, encodes the image data, generates an image file (Imaging Function, Compress/Coding Function, Control Function)
- The camera generates the verification data based on the generated image file, and outputs the image data with the verification data to a storage media.

1.2.4 TOE Functionality

The TOE consists of "Verification Data Generation Function" and "Control Function".

(1) Verification Data Generation Function
The Verification Data Generation Function generates the verification data of an image file using a key. This function inputs the data to be verified (the image file without the verification data), and output the verification data. And the Verification Data Generation Function generates a key from the seed of the key, which is used in generating the verification data.

(2) Control Function (Non-security function)
The Control Function controls Imaging Function, Compress/Coding Function, Operate/Input Function, Display Function, Output Function, and Verification Data Generation Function. This function makes it possible to take images, and to generate the verification data by controlling other functions.

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 "Guidance for IT Security Certification Application, etc."[2], "General Requirements for IT Security Evaluation Facility"[3] and "General Requirements for Sponsors and Registrants of IT Security Certification"[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-1D Mark II firmware Security Target Version 1.8" 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 C of CC Part 1 (either of [5], [8], [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9], [12] or [15]) 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], [10], [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in "EOS-1D Mark II firmware ver.1.0.1 Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report")[22]. Further, evaluation methodology should comply with the CEM Part 2 (either of [17], [18] or [19]). In addition, the each part of CC and CEM shall include contents of interpretations （either of [20] and [21]）.

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 June, 2004 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 augmented with ALC_DVS.1.

1.5.3 SOF

This ST claims “SOF-basic” as its minimum strength of function for the verification data, which is generated by the verification data generation mechanism.

It assumes that the verification function of an image file, which the Data Verification System contains, is used by the commercial system, and it is not assumed that it handles certain information that is economically highly evaluated. From the above background, the TOE assumes the attacker who is not an expert. Therefore it is appropriate that the minimum strength of function is SOF-basic.

1.5.4 Security Functions

Security functions of the TOE are as follow.

(1) SF.GEN_DV
The SF generates the verification data as an evidence of the image file’s originality by using a key. The algorithm for generating the verification data is "The Keyed-Hash Message Authentication Code" that meets the FIPS PUB 198. The key size of "The Keyed-Hash Message Authentication Code" is fixed value beyond 128 bits.

The key used by generating the verification data is generated from the seed of the key using the Camera Development Center original key generation algorithm (the de-obfuscation algorithm). The key length is fixed value beyond 128 bits. And the key that is generated by the SF is stored on a volatile RAM.

1.5.5 Threat

There is no threat for the TOE.

1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1.

Table 1 Organisational Security Policy

Identifier	Organisational Security Policy
P.GEN_VD	The TOE must generate verification data for verifying integrity of image file, in order to make integrity of the image file verifiable in the Data Verification System which consists of the EOS digital camera, and the Data Verification Kit, etc. Especially the TOE must generate the verification data using the key only to the image file that is taken by the EOS digital camera. Additionally the verification data must be the data that a malicious user without advanced special knowledge cannot generate illegally.
P.SECURE_KEY	The key must be protected securely.

1.5.7 Configuration Requirements

The TOE is the firmware that is installed in the EOS digital camera.

The verification data added to image data by the TOE security function is used by the Data Verification System, which consists of the Data Verification Kit (DVK-E2) and PC that executes the verification operations.

In order to enable the TOE security function, it is necessary to set the personal function of EOS digital camera “P.Fn-31” to “ON”.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 2.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 2 Assumptions in Use of the TOE

Identifier	Assumptions
A.TAMPER	The user of the TOE must use the EOS digital camera, which is protected from the direct-hardware-attack during working, and only the dedicated software can be installed.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- EOS-1D Mark II DIGITAL Instruction Manual, CT1-5158-000, February, 2004. (This manual is Japanese version. The English version is CT1-1260-000)
- EOS-1D Mark II DIGITAL EOS DIGITAL Solution Disk, Software Instruction Manual, CT1-5159-001, February, 2004. (This manual is Japanese version. The English version is CT1-1261-000)

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM Part 2 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 Part 2.

2.2 Overview of Evaluation Conducted

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

Evaluation has started on January, 2004 and concluded by completion the Evaluation Technical Report dated June, 2004. 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.

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

Test configuration performed by the developer is showed in Figure 3.

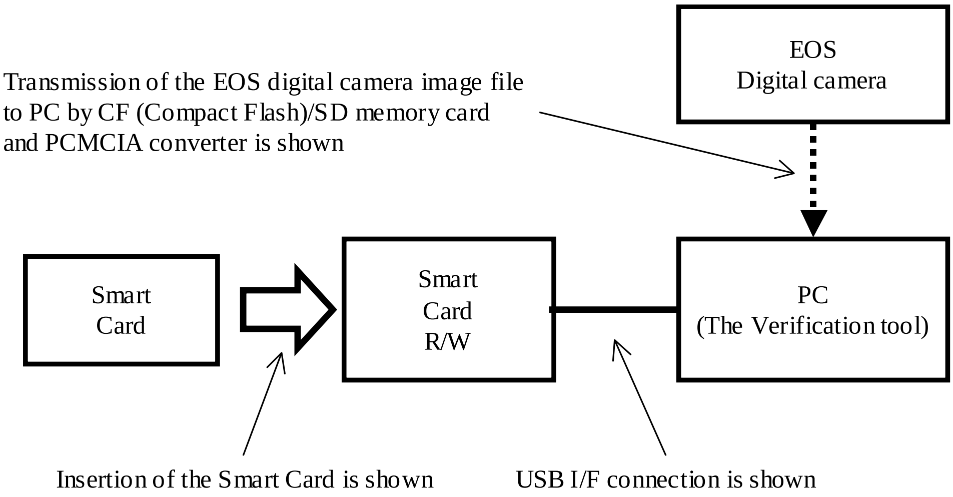
EOS
Digital camera
Transmission of the EOS digital camera image file to PC by CF (Compact Flash)/SD memory card and PCMCIA converter is shown
Smart Card
Smart Card R/W
PC
(The Verification tool)
Insertion of the Smart Card is shown
USB I/F connection is shown

Figure 3 Configuration of Developer Testing

2) Outlining of Developer Testing

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

a. Test configuration

The test configuration of the developer testing is shown in Figure 3.

- EOS Digital Camera (Product code: EOS-1DMK2)
- Firmware version 1.0.1 (To be installed in EOS digital camera)
- A Smart Card (Secure Mobile Card, Enclosed with the Data Verification Kit DVK-E2)
- A Smart Card (Secure Mobile Card, The inaccurate key is installed for testing)
- Smart Card R/W (Enclosed with the Data Verification Kit DVK-E2)
- The Data Verification Tool (The same as the Verification Program enclosed with the Data Verification Kit DVK-E2)
- CF (Compact Flash), SD memory card, PCMCIA converter (To import image file from EOS digital camera to PC)

b. Testing Approach

For the testing, following approach was used.

1. Press down the shutter button of the EOS digital camera, and confirm the security function, which generates an image file with the verification data.
2. Compare the actual test results with the expected test results, and determine whether test is achieved.

c. Scope of Testing Performed

The developer's testing sets test items, so as to confirm that all security functions (the key generation, the verification data generation) that are described in the functional specification, work correctly by pressing ~~a~~ the shutter button and generating an image file with the verification data.
The tests conducted by the developer are as follows.

- Generate an image file with the verification data by the EOS digital camera, and confirm the originality of the image file by using the Data Verification

Tool and the Smart Card (enclosed with the Data Verification Kit DVK-E2) with the correct key installed. Confirm that the image file is determined to be original by using the Data Verification Tool.

- Generate an image file with the verification data by the EOS digital camera, and confirm the originality of the image file by using the Data Verification Tool and the Smart Card with the inaccurate key installed for testing. Confirm that the image file is determined to be not original by using the Data Verification Tool.

The evaluator confirmed that the developer's testing considers all security functions. However the evaluator determined that test items only operate the security function indirectly, and test items are insufficient in order to guarantee the operations of the security function. So the evaluator tested the additional test items for the evaluator's testing.

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 testing is shown in Figure 3.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Test configuration performed by the evaluator shall be the same configuration with developer testing. 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. Press down the shutter button of the EOS digital camera, and confirm the security function, which generates an image file with the verification data.
2. Confirm the developer's test results by re-conducting the developer's testing.
3. Guarantee the security function by confirming the test results of the module testing conducted by the developer, regarding the security function, that cannot be confirmed only by pressing ~~a~~ the shutter button and generating the image file with the verification data.

c. Scope of Testing Performed

The evaluator conducted following tests. With these tests, the evaluator confirmed all security functions (generating the key and the verification data).

1. The additional Testing conducted by the Evaluator

- Confirm the security function accompanied with the change of the parameter “P.Fn-31” for the verification data generation. Generate an image file with the parameter “P.Fn-31” set to “OFF” (Not to add the verification data), and confirm whether the image file is original by using the Data Verification Tool.
- Confirm the security function accompanied with the change of the parameters “Output Image Format, Image quality”. Generate an image file with some different parameters of “Output Image Format, Image quality”, and confirm whether the image file is original by using the Data Verification Tool.
- Confirm the security function accompanied with the change of the parameter “Output Media (CF, SD memory card)”. Generate an image file, output the image file to both CF and SF memory cards, and confirm whether the image file is original by using the Data Verification Tool.

2. Verification of the tests conducted by the developer

- Confirm the security function by using the Smart Card with correct key.
- Confirm the security function by using the Smart Card with inaccurate key.

3. Confirm the test results of the module testing conducted by the developer

- Confirm the implementation of the verification generation algorithm “The Keyed-Hash Message Authentication Code” with fixed value beyond 128 bits key length.
- Confirm that the verification data generated by the verification generation algorithm is correctly added to the image file.
- Confirm that the key is correctly generated from the seed of the key by the de-obfuscation algorithm.

d. Result

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

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM Part 2 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 augmented with ALC_DVS.1 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

6. Bibliography

[1] EOS-1D Mark II firmware Security Target Version 1.8, June 30, 2004, Camera Developer Center, Canon Inc.

[2] Guidance for IT Security Certification Application, etc. April 2004, Information-Technology Promotion Agency, ITQM-23 (Revised on November 5, 2004)

[3] General Requirements for IT Security Evaluation Facility, April 2004, Information-Technology Promotion Agency, ITQM-07

[4] General Requirements for Sponsors and Registrants of IT Security Certification, April 2004, Information-Technology Promotion Agency, ITQM-08 (Revised on November 5, 2004)

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-00-031

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031 (Translation Version 1.2 January 2001)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (Translation Version 1.2 January 2001)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (Translation Version 1.2 January 2001)

[11] ISO/IEC15408-1: 1999 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model JIS

[12] ISO/IEC 15408-2: 1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:1999 - Information technology - Security techniques – Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 - Security techniques - Evaluation criteria for IT security - Part 1: General Rules and general model

[15] JIS X 5070-2: 2000 - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[16] JIS X 5070-3: 2000 - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999

[18] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999
(Translation Version 1.0 February 2001)

[19] JIS TR X 0049: 2001 – Common Methodology for Information Technology Security Evaluation

[20] CCIMB Interpretations (as of 15 February 2002)

[21] CCIMB Interpretations (as of 15 February 2002)
(Translation Version 2.0 August 2004)

[22] EOS-1D Mark II firmware ver.1.0.1 Evaluation Technical Report Version 2.2, June 30, 2004, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center