This document is a translation of the security target written in Japanese, which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

EOS-1D Mark II firmware Security Target

Version 1.8

Date June 30, 2004

Author Camera Development Center, Canon Inc.

Revision History

Version	Date	The contents of change
1.0	2004/01/26	Initial release
1.1	2004/02/25	Revised to add the Display function Revised by ORs issued on 2004/02/20
1.2	2004/03/10	Revised for typo
1.3	2004/04/01	Revised for typo
1.4	2004/04/04	Renewal of assurance measures
1.5	2004/05/20	Revised by CRV-T017-001 Renewal of assurance measures Revised to modify Chapter 2
1.6	2004/06/07	Revised to modify Chapter 8.2.4 Renewal of assurance measures Change of a TOE title Change of headers
1.7	2004/06/22	Renewal of assurance measures
1.8	2004/06/30	Revised to modify Chapter 3

Table of contents

1 ST Introduction

This section contains ST Identification, ST Overview, CC Conformance Claim, and Terminology.

1.1 ST Identification

This section contains ST Identification.

ST Title	EOS-1D Mark II firmware Security Target
ST Version	1.8
ST Issue Date	June 30, 2004
ST Issuer	Camera Development Center, Canon Inc.
TOE Title	EOS-1D Mark II firmware
TOE Version	1.0.1
Keyword	Digital Camera, Data Verification, Integrity, MAC, and EAL2+
Version of CC	ISO/IEC 15408-1:1999 ISO/IEC 15408-2:1999 ISO/IEC 15408-3:1999

(Note) "Common Criteria for Information Technology Security Evaluation Version 2.1 Part 1-3 (Japanese, Version 1.2, Information-Technology Promotion Agency, January 2003)" is used for a Japanese translation. Furthermore, "CCIMB Interpretaions-0210" is also used.

1.2 ST Overview

This document is the Security Target (ST) for EOS-1D Mark II digital camera (EOS digital camera) firmware. The security function that EOS digital camera firmware provides is as follows.

- To generate verification data to verify whether EOS digital camera image is modified.

The structure of this ST is as follows.
Section 1 provides ST Identification, ST Overview, CC Conformance Claim, and Terminology as a ST Introduction.
Section 2 provides TOE type, TOE Overview, TOE Configuration.
Section 3 provides the statement of TOE Security Environment.

Section 4 provides the statement of Security Objectives.

Section 5 provides the statement of IT Security Requirements.

Section 6 provides the statement of TOE Summary Specification.

Section 7 provides the statement of PP Claims.

Section 8 provides the statement of Rationale for Security Objectives, IT Security Requirements, and TOE Summary Specification.

1.3 CC Conformance Claim

The ST is :

CC part 2 conformant.

CC part 3 conformant with EAL2 augmented by ALC_DVS.1.

CCIMB-0210 application.

There is no PPs claimed to which this ST is conformant.

1.4 Terminology

This section defines terminology.

CC : Common Criteria

EAL : Evaluation Assurance Level

PP : Protection Profile

ST : Security Target

TOE : Target of Evaluation

MAC : Message Authentication Code

FIPS : The Federal Information Processing Standards

2 TOE Description

This section provides the statement of TOE type, TOE Overview, and TOE Configuration.

2.1 TOE Type

The type of the product that includes the TOE is a digital camera. The TOE is the firmware of the digital camera called EOS digital camera, and the type of the TOE is embedded software.

2.2 TOE Overview

While photos taken by a 35mm film camera require development and printing, photos taken by digital camera do not require them. Moreover, since photos taken by digital camera are digital data, these photos do not have secular degradation, these photos are easy to store and search, and these photos can be transmitted to a remote place using a communication channel. Since there are these various merits, the digital camera is used in many fields. For example, in the damage insurance industry, an accident vehicle is assessed based on photos taken by digital camera. In the construction industry, progress of construction or implementation of construction is checked based on photos taken by digital camera. In the Ministry of Land, Infrastructure and Transport in Japan, it is accepted to use the digital camera for record of the construction site.

However, the demerit of digitized photos is also pointed out. Since digitized photos have the feature that processing and alteration can be easily performed using photo retouch tools, the reliability of photos taken by digital camera is lower than that of photos taken by a 35mm film camera. Actually, an incident occurred that the injustice subsidy was received by altering the photo of the final appearance of the building taken by digital camera.

Of course, it is not impossible to alter photos taken by 35mm film camera. However the cost for altering is much bigger than the merit obtained by altered photos, or the altered result tends to look unnatural. Therefore, the actual alterations have not been made so often. And therefore, photos taken with the 35mm film camera are wildly adopted as the evidence. Hence, alteration ease of photos taken with the digital camera is becoming a big issue, especially for the damage insurance industry or the construction industry, so the countermeasure to prevent this problem is necessary.

EOS digital camera is a digital camera that was developed based on such a background,

and it can be used with the Data Verification Kit, which verifies integrity of image files.

At the beginning, we explain the whole Data Verification System that consists of EOS digital camera and the data verification kit. Figure 2-1 shows the whole Data Verification System.

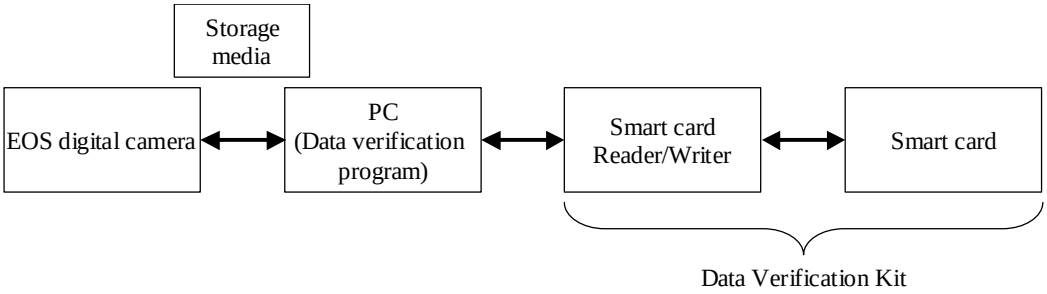

Figure 2-1 Data Verification System

The Data Verification System consists of EOS digital camera, PC (The Verification Program is installed), and the Data Verification Kit. The Data Verification Kit consists of a smart card R/W connected to the PC and a smart card connected into the smart card R/W. An equivalent product with a smart card can also be used. The Data Verification System aims at verifying integrity of image files taken by EOS digital camera. The PC (The Verification Program is installed) and the Data Verification Kit verify integrity of image files by using the verification data. That is, this system counters the threat, which photos taken by EOS digital camera may be altered, by the set of EOS digital camera, PC, and the Verification Kit. One person generates image files with the verification data by using EOS digital camera, the other person verifies integrity of the image files with the verification data by using PC and the Verification Kit. The person who verifies image files can be the same with or can be different from the person who generates the image files. It depends on the application of the Data Verification System. Moreover, the threat, which this system counters, is only integrity of image files. This system counters neither confidentiality nor availability, because this system does not assume these threats. Although image files that can be verified integrity are only image files taken by EOS digital camera, not all image files taken by EOS digital camera are the files that can be verified integrity. Only the image files that wants to verity integrity is applicable. That is, the user of the EOS digital camera choose whether verification data is generated or not, before taking photos.

Following example shows the use of the Data Verification System in the damage insurance industry. At first an accident investigator takes image files (accident photos) of the accident spot with EOS digital camera. In this case, the accident investigator takes photos in the state that the verification data is generated. Then the damage insurance company prepares a PC and the Data Verification Kit. A damage insurance company receives the image files (accident photos) with the verification data taken by an accident investigator, and verifies integrity of received image files (accident photos) with the verification data by using PC and the Data Verification Kit. If integrity of the image files is successlly verified, it is estimated that the image files are actually taken by EOS digital camera and no alternation is added.

The TOE is a firmware of EOS digital camera used by the Data Verification System. That is, the TOE is a firmware of EOS digital camera that bears only the generation function of verification data in the Data Verification System. Although the whole system counters the threat, which photos taken by EOS digital camera may be altered, the TOE itself cannot counter the threat. That is, the TOE bears only the generation function of verification data, which is a part of the functions that is required by the whole system.

The technology used by the Data Verification System has the following feature. Verification data of image files is generated using a key. Further the key is not stored directly, but stored as the relevant information (the seed of the key) to the key at EOS digital camera.

2.3 TOE Configuration

2.3.1 Physical boundary of the TOE

Figure 2-2 shows the physical components of both the TOE and the TOE platform.

Figure 2-2 Physical component including the TOE

As shown in Figure 2-2, the physical component that includes the TOE is a digital camera. The platform of the TOE is a hardware that consists of a digital camera, and does not contain both lens and storage media installed a digital camera. Further the storage media is the general term of external storage, and EOS digital camera has three types of external storage, which are CF (Compact Flash) Card, SD (Secure Digital) Card, and the direct transmission to PC. There are two types of methods to use EOS digital camera. One is the method that operates from a shutter button and/or a setting dial, the other is the method that operates it from PC linked to EOS digital camera. Figure 2-3 shows more detailed digital camera components.

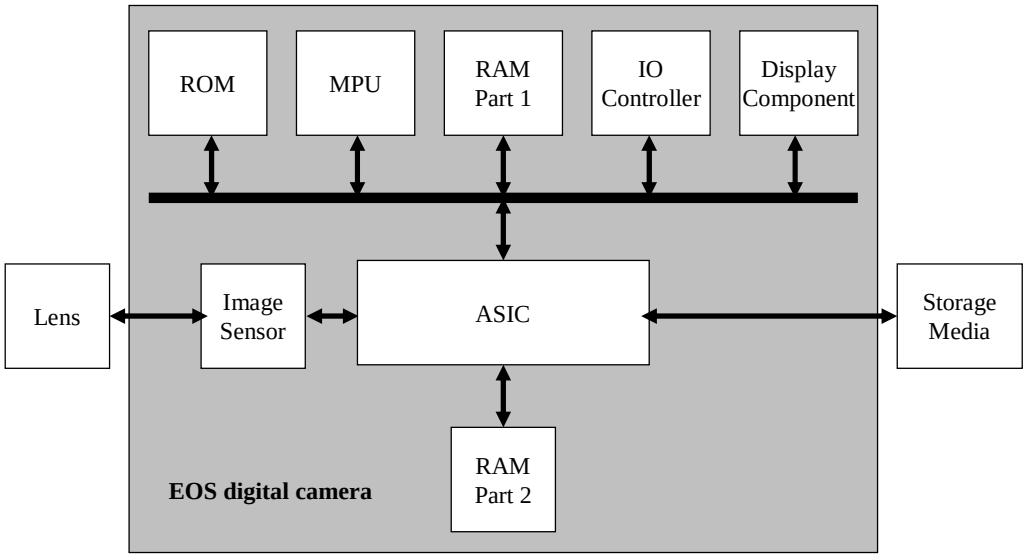

Figure 2-3 Physical components of the EOS digital camera

Each component is explained as follows.

MPU	MPU is the processing tip that bears the function to control each part of EOS digital camera.
ROM	ROM is the ROM (Read Only Memory) that stores data to drive EOS digital camera. In addition, the ROM includes OS (Operating System) that runs on above MPU.
RAM Part 1	RAM Part 1 is the RAM (Random Access Memory) that is used by above MPU.
IO Controller	IO Controller consists of two interfaces. One of them is the interface

which bears the communication between the EOS digital camera and an external equipment such as a PC, the other is the interface which communicate the commands of the user to the camera, such as the release button or the dials.

Display Component
: Display Component is the LCD (Liquid Crystal Display) to display image file or setting values, multiple display panels, and the video output.

Image sensor
: Image Sensor is the sensor that convert the inputted optical electric charge into voltage.

ASIC
: ASIC is the IC to eliminate the noise and to generate image file from the signal of Image Sensor.

RAM Part 2
: RAM Part 2 is the RAM that is used by above ASIC.

The Physical boundary of the TOE is the software that runs on MPU shown in Figure 2-3, i.e. firmware. Table 2-1 shows the physical components of EOS digital camera, which include the TOE.

Table 2-1 Components of the EOS digital camera

Identification	Parts number/version
Body of EOS digital camera	EOS-1DMK2
EOS-1D Mark II firmware (TOE)	1.0.1

If the version of "Body of EOS digital camera" is identified, all components shown in Figure 2-3 are uniquely identified.

2.3.2 Logical boundary of the TOE

Figure 2-4 shows the logical components of EOS digital camera that include the TOE.

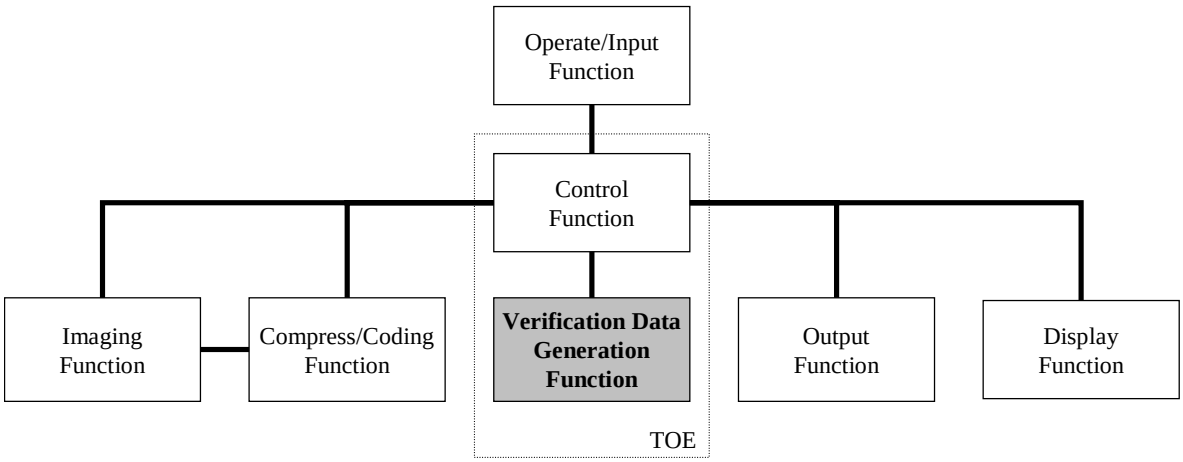

Figure 2-4 Logical components of the EOS digital camera

Each logical component is explained as follows.

Imaging Function

Imaging Function is the function that generates digital data. That is, it is the function that takes the light captured by Image Sensor into EOS digital camera as image data. Furthermore, other than above input function, there are filter function to delete an unnecessary light, a conversion function to convert into digital data, etc. However, since these are not related to the security function, the ST does not describe in detail.

Compress/Coding Function

Compress/Coding Function is the function that compresses digital data by the compression algorithm, and generates image file by coding.

Operate/Input Function

Operate/Input Function is the function that the user of EOS digital camera operates EOS digital camera by using shutter button, dials, etc. Moreover, Operate/Input Function has the communication function between EOS digital camera and PC. Although there is the function to input image file to EOS digital camera, but there is no function to input image file to EOS digital camera for generating verification data.

Display Function

Display Function is the function that shows image files, setting values, and state of EOS digital camera on Display Component.

Output Function

Output Function is the function that stores image file on the storage media. In case of adding verification data, this function stores image file with verification data on the storage media. In other case of not adding verification data, this function stores image file without verification data on the storage media.

Verification Data Generation Function

Verification Data Generation Function is the function that generates verification data of image file by using the key. This function inputs image file without verification data, and outputs verification data. Moreover, this function generates the key from the seed of the key.

Control Function

Control Function is the function that controls Imaging Function, Compress/Coding Function, Operate/Input Function, Display Function, Output Function, and Verification Data Generation Function. For example, in case "Take a photo" command is given by Operate/Input Function, this function provides image file to the user of EOS digital camera by using above functions.

Image data means the digital data such as the digital data by Image Sensor or the digital data by Compress/Coding Function. Image file means the Image data with additional attributes.

Next, Table 2-2 shows the correspondence between the logical components (Figure 2-4) and the physical components.

Table 2-2 Correspondence between physical components and logical components

Logical components	Physical components
Imaging Function	Imaging Sensor
Compress/Coding Function	ASIC, RAM Part 2
Operate/Input Function	IO Controller
Display Function	Display Component
Output Function	ASIC
Verification Data Generation Function	Firmware (TOE)
Control Function	Firmware (TOE)

As shown in Figure 2-4 and Table 2-2, the functions of the firmware that is the TOE, are Verification Data Generation Function and Control Function. The Verification Data Generation Function shown with the shade in Figure 2-4 is security function.

2.3.3 Role of the TOE

The product that includes the TOE is EOS digital camera. Therefore the owner of EOS digital camera is the user of the TOE. Usually, since the owner of EOS digital camera is the only user of the EOS digital camera, the owner of EOS digital camera is considered to be the administrator of the TOE. Therefore, the owner of EOS digital camera is the user of the TOE and also the administrator of the TOE. Hereafter, we call the owner of the EOS digital camera as user.

2.3.4 Assets of the TOE

Asset of the TOE is as follows.

Key	Key is information used for generation of verification data. The TOE does not store the key directly on EOS digital camera, the TOE stores the relevant information (the seed of the key) changed by the obfuscation operation, which makes it difficult to acquire the information before conversion form the information after conversion.

3 TOE Security Environment

This section provides the statement of the TOE security environment.

3.1 Assumptions

3.1.1 A.TAMPER

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

3.2 Threat

There is no threat that the ST assumes.

3.3 Organisational Security Policies

3.3.1 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.

3.3.2 P.SECURE_KEY

The key must be protected securely.

4 Security Objectives

This section provides the statement of the security objectives.

4.1 Security Objectives for the TOE

4.1.1 O.GEN_VD

The TOE must generate verification data by using the key in order to verify integrity of the image file that is taken only by the EOS digital camera. Additionally the verification data must be the data that a malicious attacker who is not expert cannot generate illegally. The TOE does not provide the function that reads the image file from image storage media in order to generate verification data.

4.1.2 O.GEN_KEY

The TOE must generate the key from the seed of the key by de-obfuscation operation that is the inverse operation of the obfuscation operation, and is the operation that is difficult to guess its procedure.

4.2 Security Objectives for the Environment

4.2.1 OE.PHS_TAMPER

The user of the TOE must use the EOS digital camera with following hardware features. The hardware of the EOS digital camera must be the dedicated hardware, and must be protected from the direct-hardware-attack while the TOE is working. I.e. the hardware of a digital camera must have both the dedicated circuit structure and the dedicated camera body structure, and must protect the key from the direct-hardware-attack while the TOE is working.

4.2.2 OE.LOG_TAMPER

The user of the TOE must use the EOS digital camera with following software features. The software of the EOS digital camera must be the dedicated software, and only the software that the developer offered is enable to be installed.

5 IT Security Requirements

This section provides the statement of the IT security requirements.

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

This section provides the TOE security functional requirements. All TOE security functional requirements have been taken from CC Part 2.

5.1.1.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: Camera Development Center original key generation algorithm] and specified cryptographic key sizes [assignment: fixed value beyond 128 bits] that meet the following: [assignment: Camera Development Center original standards].

Dependencies: [FCS_CKM.2 Cryptographic key distribution
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.1.2 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [assignment: the generation of the verification data for the image file] in accordance with a specified cryptographic algorithm [assignment: The Keyed-Hash Message Authentication Code] and cryptographic key sizes [assignment: fixed value beyond 128 bits] that meet the following: [assignment: FIPS PUB 198].

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.2 Minimum Strength of Function Claim

The minimum strength of function for the TOE is SOF-basic.

In addition, FCS_COP.1 is the security functional requirement that uses cryptographic algorithm. The assessment of cryptographic algorithm is not covered in the CC.

5.1.3 TOE Security Assurance Requirements

This section provides the TOE security assurance requirements. The evaluation assurance level for the TOE is EAL2 augmented by ALC_DVS.1. Table 5-1 shows the TOE security assurance requirements. All TOE security assurance requirements have been taken from CC Part 3.

Table 5-1 List of the TOE security assurance components

Assurance class	Assurance component	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	In-formal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	In-formal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.2 Security Requirements for the IT environment

This section provides the security requirements for the IT environment.

There are no security requirements for the IT environment.

6 TOE Summary Specification

This section provides the statement of the TOE summary specification.

6.1 TOE Security Function

This section provides the security functions that are provided by the TOE.

6.1.1 SF.GEN_DV

The SF generates verification data as an evidence of the image file integrity by using following key. The TOE provides only the generation function of the verification data, but does not provide the verification function of the verification data. The algorithm for generating 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 SF generates the key from the seed of the key using the Camera Development Center original key generation algorithm i.e. 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.

6.2 Correspondence Between TOE Security Function and TOE Functional Requirements

Table 6-1 shows the correspondence between IT security functions and TOE security functional requirements.

Table 6-1 Correspondence between IT security functions and TOE security functional requirements

	FCS_CKM.1	FCS_COP.1
SF.GEN_DV	x	x

6.3 Strength of Function Claims

The IT security function realized by a probabilistic or permutational mechanism is SF.GEN_DV. The strength of function of SF.GEN_DV is SOF-Basic.

In addition, SF.GEN_DV is the IT security function that uses the secure hash function (cryptographic algorithm). The algorithm of the secure hash function (cryptographic algorithm) is out of scope of the strength of function.

6.4 Assurance Measures

This section provides the TOE assurance measures. Table 6-2 shows the TOE security assurance measures. These TOE security assurance measures are satisfied with TOE security assurance requirements described in Section 5.1.3.

Table 6-2 Correspondence between TOE security assurance measures and TOE security assurance requirements

TOE security assurance measures	TOE security assurance requirements
EOS digital camera configuration management documentation, ver 1.3, 2004/06/18	ACM_CAP.2
EOS digital camera delivery procedure documentation, ver 1.4, 2004/06/18	ADO_DEL.1 ADO_IGS.1
EOS digital camera firmware functional specification, ver 1.7, 2004/06/30	ADV_FSP.1
EOS digital camera high-level design, ver 1.5, 2004/06/30	ADV_HLD.1
EOS digital camera correspondence analysis, ver 1.6, 2004/06/30	ADV_RCR.1
EOS digital camera user guidance, ver 1.2, 2004/04/26	AGD_ADM.1 AGD_USR.1
EOS digital camera development security documentation, ver 1.2, 2004/05/20	ALC_DVS.1
EOS digital camera test documentation, ver 1.3, 2004/06/30	ATE_COV.1 ATE_FUN.1
EOS digital camera (TOE)	ATE_IND.2
EOS digital camera vulnerability analysis, ver 1.2, 2004/06/30	AVA_SOF.1 AVA_VLA.1

7 PP Claims

This section provides the statement of the PP claims.

There are no PP claimed.

8 Rationales

This section provides the rationales of the security objectives, IT security requirements, and TOE summary specification.

8.1 Security Objectives Rationales

Table 8-1 shows the correspondence between security objectives and security environment (assumptions, threat, and organisational security policy).

Table 8-1 Correspondence between security objectives and security environment

	A.TAMPER	P.GEN_VD	P.SECURE_KEY
O.GEN_VD		x	
O.GEN_KEY			x
OE.PHS_TAMPER	x		x
OE.LOG_TAMPER	x		x

Table 8-1 shows that each security objective covers at least one security environment.

Following rationale statements show that for each security environments, it contains an appropriate justification that the security objectives are suitable to counter those security environments.

A.TAMPER is countered by OE.PHS_TAMPER and OE.LOG_TAMER. Because OE.PHS_TAMPER ensured that the hardware of the EOS digital camera is the dedicated hardware, and is protected from the direct-hardware-attack while the TOE is working. OE.LOG_TAMPER ensured that the software of the EOS digital camera is the dedicated software, and is enable to be installed only the software that the developer offered. Additionally both OE.PHS_TAMPER and OE.LOG_TAMPER ensured that the user of the TOE must use the EOS digital camera that has above hardware and software features. Therefore OE.PHS_TAMPER and OE.LOG_TAMPER are satisfied

with A.TAMPER.

P.GEN_VD is countered by O.GEN_VD. Because O.GEN_VD ensured that the TOE generates verification data by using the key in order to verify integrity of the image file that is taken only by the EOS digital camera. And the verification data is data that a malicious user without advanced special knowledge cannot generate illegally. Therefore O.GEN_VD is satisfied with P.GEN_VD. In addition, the TOE has no function to read the image file from the storage media in order to generate verification data.

P.SECURE_KEY is countered by O.GEN_KEY, OE.PHS_TAMPER and OE.LOG_TAMER. Because O.GEN_KEY ensured that the TOE generates the key from the seed of the key by de-obfuscation operation that is the inverse operation of the obfuscation operation, and is the operation that is difficult to guess its procedure. OE.PHS_TAMPER ensured that the hardware of the EOS digital camera is the dedicated hardware, and is protected from the direct-hardware-attack while the TOE is working. OE.LOG_TAMPER ensured that the software of the EOS digital camera is the dedicated software, and is enable to be installed only the software that the developer offered. Therefore O.GEN_KEY, OE.PHS_TAMPER and OE.LOG_TAMPER are satisfied with P.SECURE_KEY.

8.2 Security Requirements Rationales

8.2.1 Rationales for Functional Requirements

TOE security functional requirements are the functional requirements to counter the security objectives. Table 8-2 shows the correspondence between TOE security functional requirements and security objectives.

Table 8-2 Correspondence between TOE security functional requirements and security objectives

	O.GEN_VD	O.GEN_KEY
FCS_CKM.1		x
FCS_COP.1	x	

Table 8-2 shows that each TOE security requirements cover at least one security objective.

Following rationale statements show that for each security objectives, it contains an appropriate justification that TOE security requirements are suitable to counter those security objectives.

O.GEN_VD is countered by FCS_COP.1. Because FCS_COP.1 ensured that the TSF generate verification data for image file in accordance with "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. Therefore FCS_COP.1 are satisfied with O.GEN_VD.

O.GEN_KEY is countered by FCS_CKM.1. Because FCS_CKM.1 ensured that the TSF generate the key from the seed of the key in accordance with "the Camera Development Center original key generation algorithm" i.e. the de-obfuscation algorithm. Therefore FCS_CKM.1 are satisfied with O.GEN_KEY.

8.2.2 Rationales for Functional Requirements Dependencies

Table 8-3 shows the dependencies between the TOE security requirements. The symbol "*" in the table means the dependency of the security requirements that are not satisfied. The symbol "!" in the table means the selected dependency from the optional dependencies.

Table 8-3 TOE functional requirements dependencies

TOE security requirements	The dependencies of TOE security requirements
FCS_CKM.1	[FCS_CKM.2 or !FCS_COP.1], *FCS_CKM.4, *FMT_MSA.2
FCS_COP.1	[FDP_ITC.1 or !FCS_CKM.1], *FCS_CKM.4, *FMT_MSA.2
ACM_CAP.2	Nothing
ADO__DEL.1	Nothing
ADO_IGS.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Nothing
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_DVS.1	Nothing

TOE security requirements	The dependencies of TOE security requirements
ATE_COV.1	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	Nothing
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

Table 8-2 shows that TOE security requirements exclude some following exceptions are satisfied with the dependencies. Following rationale statements show the justification where security requirement dependencies are not satisfied.

The FCS_CKM.1 includes neither the dependency to FCS_CKM.1 nor the dependency to FMT_MSA.2. However the TOE stored the key generated by FCS_CKM.1 only on a volatile RAM. Moreover the key is stored while the TOE is working. And the key is canceled at the time when the TOE is down. The key destruction is not a means of IT functionality, but a means using the physical characteristics of a volatile RAM. Additionally the TOE has no security attribute of the key. Therefore the TOE needs neither the dependency to FCS_CKM.1 nor the dependency to FMT_MSA.2.

The FCS_COP.1 includes neither the dependency to FCS_CKM.4 nor the dependency to FMT_MSA.2. As described above, the key destruction is not a means of IT function, but a means using the physical characteristics of a volatile RAM. Additionally the TOE has no security attribute of the key. Therefore the TOE needs neither the dependency to FCS_CKM.4 nor the dependency to FMT_MSA.2.

8.2.3 Mutual support of Security Requirements

From Section 8.2.2, TOE security functional requirements, exclude some exceptions, mutually support with the TOE security functional requirements that have the dependencies.

Additionally, although there is no explicit dependency, the mutual support of security functional requirements is described from the following point of view.
The TOE does not need the functions of the user data access control and/or flow control, so the TOE chooses neither FDP_ACC.1 nor FDP_IFC.1. That is, the TOE considers that there is no malicious subject inside the TOE. Therefore it is not necessary that the

TOE choose neither FPT_RVM.1 nor FTP_SEP.1.
The key generated by FCS_CKM.1 of the TOE does not have any security attributes. So the TOE does not have any management functions about FCS_CKM.1 such as a management of the security attributes of the key. Moreover the TOE does not have any management functions about FCS_COP.1. Therefore it is not necessary that the TOE does not choose FMT_MOF.1.
Furthermore, it is not necessary to enable detection that aimed at disabling of other security functional requirements, such as FAU class.

8.2.4 Rationale for Minimum Strength of Function Claim

It assumes that the total security functions of the generation and the verification of verification data are used by the commercial system. The total security functions are not the function that deals with information with economical value directly, but the function that enable to verify integrity of the image file.
From the above background, the TOE assumes the attacker who is not expert, as shown in Section 4.1.1. Moreover the direct-hardware-attack and the attack from other software are covered by the environment, as shown in Section 4.2.
As mentioned above, the attacker that the TOE must counter is the low-level attacker. Therefore it is appropriate that the minimum strength of function is SOF-basic.

8.2.5 Rationale for Assurance Requirements

As mentioned in Section 8.2.4, the TOE assumes the low level attacker. EAL2 is appropriate from both the low-level attacker definition and the investment (time and /or cost). However it is necessary for the TOE both to generate the key securely in development phase, and to maintain information about the key and the key generation algorithm securely. Therefore EAL2 augmented by ALC_DVS.1 is appropriate.

8.3 TOE Summary Specification Rationale

8.3.1 Rationale for TOE Security Function

Table 8-4 shows the correspondence between IT security function and TOE security functional requirements.

Table 8-4 Correspondence between IT security function and security functional requirements part 2

	FCS_CKM.1	FCS_COP.1
SF.GEN_DV	x	x

Table 8-4 shows that each security function covers at least one security functional requirements.

Following rationale statements show that for each security functional requirement, it contains an appropriate justification that the security functions are suitable to counter those security functional requirements.

FCS_CKM.1 is countered by SF.GEN_DV. Because SF.GEN_DV generates the key from the seed of the key using the Camera Development Center original key generation algorithm i.e. the de-obfuscation algorithm. The key length is fixed value beyond 128 bits. Therefore SF.GEN_DV is satisfied with FCS_CKM.1.

FCS_COP.1 is countered by SF.GEN_DV. Because SF.GEN_DV generates verification data as an evidence of the image file integrity by using following key. The algorithm for generating 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. Therefore SF.GEN_DV is satisfied with FCS_COP.1.

8.3.2 Rationale for Combination of TOE Security Function

Table 8-4 shows that the TOE has the only IT security function. Therefore it is not necessary to consider the combination of the security functions.

8.3.3 Rationale for Strength of Function Claims

In this TOE, the IT security function that is realized by a probabilistic or permutational mechanisms is SF.GEN_DV. The strength of function is claimed SOF-basic in Section 6.3. Moreover the minimum strength of function is claimed SOF-basic in Section 5.1.2.

These claims are consistent.

8.3.4 Rationale for Assurance Measures

Table 8-5 shows the correspondence between TOE security assurance measures and TOE security assurance requirements.

Table 8-5 Correspondence between TOE security assurance measures and TOE security assurance requirements part 2

TOE security assurance measures	TOE security assurance requirements
EOS digital camera configuration management documentation, ver 1.3, 2004/06/18	ACM_CAP.2
EOS digital camera delivery procedure documentation, ver 1.4, 2004/06/18	ADO_DEL.1 ADO_IGS.1
EOS digital camera firmware functional specification, ver 1.7, 2004/06/30	ADV_FSP.1
EOS digital camera high-level design, ver 1.5, 2004/06/30	ADV_HLD.1
EOS digital camera correspondence analysis, ver 1.6, 2004/06/30	ADV_RCR.1
EOS digital camera user guidance, ver 1.2, 2004/04/26	AGD_ADM.1 AGD_USR.1
EOS digital camera development security documentation, ver 1.2, 2004/05/20	ALC_DVS.1
EOS digital camera test documentation, ver 1.3, 2004/06/30	ATE_COV.1 ATE_FUN.1
EOS digital camera (TOE)	ATE_IND.2
EOS digital camera vulnerability analysis, ver 1.2, 2004/06/30	AVA_SOF.1 AVA_VLA.1

Table 8-5 shows that each TOE security assurance measure covers at least one TOE security assurance requirements.

Following rationale statements show that for each security assurance requirement, the TOE security assurance measures are suitable to counter those security assurance requirements.

ACM_CAP.2 is countered by the following document.

- EOS digital camera configuration management documentation, ver 1.3, 2004/06/18

This document describes version of the TOE, a configuration list that describe the configuration items, and the method used to uniquely identify the configuration items. Therefore this document is satisfied with ACM_CAP.2.

ADO_DEL.1 and ADO_IGS.1 are countered by the following document.

- EOS digital camera delivery procedure documentation, ver 1.4, 2004/06/18

This document describes all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site and the steps necessary for secure installation, generation, and start-up of the TOE. Therefore this document is satisfied with ADO_DEL.1 and ADO_IGS.1.

ADV_FSP.1 is countered by the following document.

- EOS digital camera firmware functional specification, ver 1.7, 2004/06/30

This document describes the TSF and its external interfaces. Therefore this document is satisfied with ADV_FSP.1.

ADV_HLD.1 is countered by the following document.

- EOS digital camera high-level design, ver 1.5, 2004/06/30

This document describes the structure of the TSF in terms of subsystems and the security functionality provided by each subsystem of the TSF. This document identifies all interfaces to the subsystems of the TSF. Moreover this document identifies any underlying hardware, firmware, and/or software required by the TSF. Therefore this document is satisfied with ADV_HLD.1.

ADV_RCR.1 is countered by the following document.

- EOS digital camera correspondence analysis, ver 1.6, 2004/06/30

This document demonstrates that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. Therefore this document is satisfied with ADV_RCR.1.

AGD_ADM.1 and AGD_USR.1 are countered by the following document.

- EOS digital camera user guidance, ver 1.2, 2004/04/26

In EOS digital camera, it is considered that the owners of EOS digital camera are the

user of TOE, and the administrator of TOE. So this document for the owners of EOS digital camera describes the administrative/non-administrative functions and interfaces available to the owners of the TOE. Therefore this document is satisfied with AGD_ADM.1 and AGD_USR.1.

ALC_DVS.1 is countered by the following document.

- EOS digital camera development security documentation, ver 1.2, 2004/05/20

This document describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore this document is satisfied with ALC_DVS.1.

ATE_COV.1 and ATE_FUN.1 are countered by the following document.

- EOS digital camera test documentation, ver 1.3, 2004/06/30

This document describes the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. Moreover this document describes test plans, test procedure descriptions, expected test results and actual test results. Therefore this document is satisfied with ATE_COV.1 and ATE_FUN.1.

ATE_IND.2 is countered by the followings.

- EOS digital camera (TOE)

This is the TOE that is suitable for testing. Therefore this is satisfied with ATE_IND.2.

AVA_SOF.1 and AVA_VLA.1 are countered by the following document.

- EOS digital camera vulnerability analysis, ver 1.2, 2004/06/30

This document describes analysis for each mechanism identified in the ST as having a strength of TOE security function claim. Moreover this document describes the vulnerability analysis. Therefore this document is satisfied with AVA_SOF.1 and AVA_VLA.1.

