This document is a translation of the evaluated and certified security target written in Japanese

EOS Original Data Security System Security Target

Version 1.7

Date May 17, 2007

Author Camera Development Center, Canon, Inc.

Revision History

Version	Date	Revision Details
1.0	Oct. 16, 2006	First edition.
1.0.1	Nov. 13, 2006	Covered parts of the specifications that are not yet determined.
1.1	Nov. 24, 2006	Covered OR (TCE-EOR-001-01, TCE-EOR-0002-01).
1.2	Dec. 08, 2006	Corrected written errors based on an internal review.
1.3	Dec. 15, 2006	Corrected errors based on an internal review.
1.4	Feb. 19, 2007	Covered OR (TCE-EOR-003-01, TCE-EOR-0004-01).
1.5	Feb. 23, 2007	Corrected errors based on an internal review.
1.6	Apr. 09, 2007	Covered OR (TCE-EOR-005-01, TCE-EOR-0006-01). Corrected errors based on an internal review.
1.7	May 17, 2007	Modified TOE name.

Table of Contents

1 ST introduction

This chapter covers the ST reference, TOE reference, TOE overview, and TOE description.

1.1 ST reference

This section describes ST identification information.

ST title	EOS Original Data Security System Security Target
ST version	1.7
ST publisher	Camera Development Center, Canon, Inc.
ST publishing date	May 17, 2007

1.2 TOE reference

This section describes the TOE identification information.

TOE title	EOS Original data Security System
TOE version	1.0
TOE developer	Camera Development Center, Canon, Inc.

This TOE is comprised of the EOS digital camera, administrator tool, browser tool, and OS card shown below.

Table 1-1 Component Parts of the EOS Digital Camera

Identifying Name	Identifying Information
EOS-1D Mark III hardware	EOS-1D Mark III
EOS-1D Mark III firmware	1.0.8

Table 1-2 Component Parts of the Administrator Tool

Identifying Name	Identifying Information
Original Data Security Administrator	1.0

Table 1-3 Component Parts of the Browser Tool

Identifying Name	Identifying Information
Original Data Security Utility	1.0

Table 1-4 Component Parts of the OS Card

Identifying Name	Identifying Information
Original Data Security Card hardware	OSC-128M
Original Data Security Card applet (applet name : FF34123456100101)	00000003

1.3 TOE 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 is a system that makes it possible to verify the originality of image files shot by the EOS digital camera and which keeps image files confidential, by offering the following security functions.

- 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 data related to the function of identifying and authenticating the 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 identifying and authenticating the users of the administrator tool and the browser tool.

The EOS digital camera can be used alone, but the administrator tool and browser tool require either Windows 2000, Windows XP, or Windows Vista running on a PC/AT-compatible machine. The OS card is used either in the EOS digital camera, or in an OS card reader/writer (referred to as a "reader/writer" below) that is connected to the PC/AT-compatible machine. Details regarding these components are given in section 1.4. Refer to Table 1-5 for the product names and included components.

Table 1-5 Products and Included Components

Product Name	Main Included Components
EOS-1D Mark III (complete set)	The EOS digital camera The administrator tool The browser tool
EOS digital camera accessory Original Data Security Kit OSK-E3 (referred to as "the OSK kit" below)	The administrator tool The browser tool The OS card The card reader/writer
EOS digital camera accessory Original Data Security Card OSC-128M	The OS card

1.4 TOE description

This chapter describes the objectives and methods for using the TOE, the physical and logical scope as the TOE's configuration, and the users of the TOE.

1.4.1 Objectives and methods for using the TOE

Since the images shot with the digital camera are digital, it is easy to process or modify them by using a photo retouching tool. Also, it is possible to use a variety of different media to send digital images, such as different types of flash memory, communication lines, and so on. Due to these characteristics, the falsification and leakage of shot images.

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 identify and authenticate the administrators and browsers, and so on.

Next, the image shooting and browsing (viewing) procedures are as described below.
Before an image is shot, the administrator of this system must initilize the OS card preferences and so on. The OS card’s initializations include the ID and PIN of the OS card’s administrator and registration of the card key. The browser’s ID and PIN and the EOS digital camera ID are also registered. The administrator’s ID and PIN, the browser’s ID and PIN, the EOS digital camera’s ID, and the card key are referred to as the “OS card data.” Register the EOS digital camera’s ID to register which EOS digital camera can use that OS card, and register the browser ID to register which browser can use that OS card. It is possible to register multiple browsers and EOS digital cameras in a single OS card. The card key is generated inside the OS card and registered. The MAC key is maintained in advance by the EOS digital camera and the OS card.
A photographer with the EOS digital camera and OS card will insert the OS card into the EOS digital camera. Once the OS card is inserted into the EOS digital camera, each device will verify and connect to the other. The EOS digital camera will verify that this is the OS card, and the OS card will verify that the corresponding EOS digital camera ID is registered. If either verification fails, then the EOS digital camera will show a message in its display. After each component verifies the other, the EOS digital camera will receive the card key from the OS card. When photographs are taken with the EOS digital camera set to “Add original image verification data,” the EOS digital camera will generate an image key internally and generate verification data for that image file by using the MAC key. The image key is used to encrypt the image file, resulting in an

encrypted image file. The card key is also used to encrypt the image key, resulting in an encrypted image key. An encrypted image file is then generated with verification data that is comprised of verification data, the encrypted image file, and the encrypted image key. The details of this image file encryption are described later in this document. This encrypted image file with verification data is recorded on the prescribed medium, as set by the EOS digital camera. Since the EOS digital camera supports various types of flash memory and communication lines, the medium is not restricted to any particular medium. It is possible to save the encrypted image file with verification data on flash memory installed in the EOS digital camera, or on a PC connected via the USB (Universal Serial Bus) interface, or on a remote PC via wireless LAN, for instance. Also note that not all image files taken by the EOS digital camera will have verification added and be encrypted. Only those image files selected by the photographer will be handled in this manner. It is possible to set "Add verification data" on or off in the EOS digital camera menu for "Add original image determination data." On the other hand, the image file is automatically encrypted when the OS card is inserted into the EOS digital camera, after the EOS digital camera and the OS card have verified each other. In other words, there is no need to set "encrypt the image file" in the EOS digital camera menu.

The EOS digital camera can decrypt encrypted image files recorded on a specific type of medium, and show these files on the EOS digital camera display. The EOS digital camera has no function for outputting image files outside the EOS digital camera, however.

A browser with a PC and the OS card can use a card reader/writer to connect the OS card to the PC. When the browser tool is used to attempt to view an encrypted image file with verification data, the OS card identifies and authenticates the browser with the ID and PIN. If the identification and the authentification are succeed, the PC and OS card will decrypt the encrypted image key by using the card key. The image key will then be used to decrypt the encrypted image file, and the originality of the image file will be verified based on the MAC key and verification data.

By following these steps, it is possible to maintain the originality and confidentiality of the image files. The steps for simultaneously achieving both originality and confidentiality were described above, but there is no need to always maintain both of these characteristics at the same time. The photographer can set the menu of the EOS digital camera and attach or remove the OS card from the EOS digital camera to achieve just originality or confidentiality. Also, since the originality of an image file has

no relationship with the photographer or browser, when only the originality needs to be verified, or in other words, when verifying the originality of an image file with verification data, there is no need to identify and authenticate the browser (viewer).
The administrator can set the administrator ID and PIN of the OS card and the card key preferences, can add and delete browser IDs and PINs, can change administrator PINs and browser PINs, and register or delete the EOS digital camera ID. Multiple browsers can be registered on a single OS card along with the EOS digital camera. Furthermore, the administrator can initialize the OS card, as well as take or restore backups. Backups provide protection against failure of the OS card, and make it possible to restore on a physically different OS card, thereby resulting in a duplicate card. A duplicated OS card, which is to say an OS card holding the same OS card data, can be shared in advance between the photographer and browser in order to realize the real-time transmission and viewing (browsing) of encrypted image files. A browser can view (browse) image files and change his own PIN.

1.4.2 TOE configuration

1.4.2.1 Physical scope of the TOE

Figure 1-1 shows a diagram of the entire system. The colored parts represent the physical scope of the TOE.

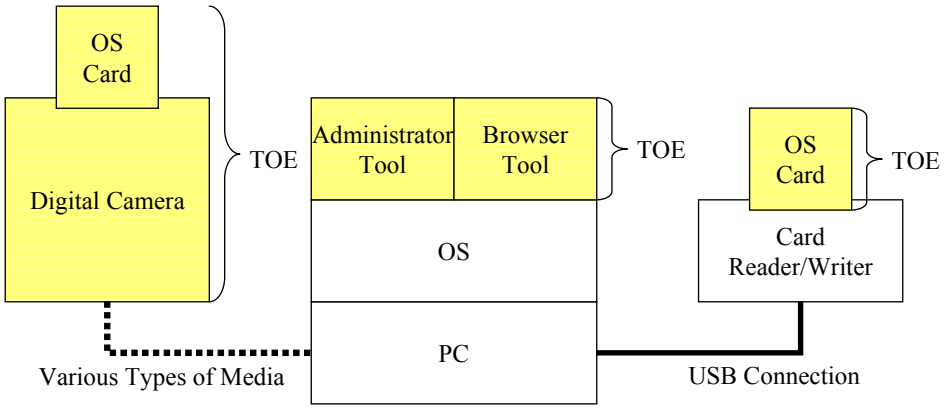

Figure 1-1 Diagram of the Entire EOS Digital Camera System

As shown in Figure 1-1, the 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. Figure 1-1 shows multiple OS

cards, but these can be physically different OS cards, or the same OS card. The administrator tool, browser tool, OS card, and card reader/writer can be obtained via the OSK kit. A description of each element is provided below.

- **The EOS digital camera**

  This is the TOE, a device that can shoot images and generate image files. Table 1-6 shows the details of the constituent elements of the EOS digital camera's hardware and software. These elements of the physical external interface, which is comprised of the shutter button, control buttons, dial, remote control port, synchronization port (for the flash), and other control parts; the LCD monitor, display panel, and other display parts; the CF (Compact Flash) card, SD (Secure Digital) card, and other external media parts; and the USB interface and other external connection device parts. Note that the firmware for the EOS-1D Mark III can be obtained from Canon's web site[1].

Table 1-6 Constituent Elements of the EOS Digital Camera

Identifying Name	Identifying Information
EOS-1D Mark III hardware	EOS-1D Mark III
EOS-1D Mark III firmware	1.0.8

- **Administrator tool**

  This application, which is a TOE, is used to manage the OS card. Table 1-7 shows the details of the constituent element of the administrator tool software. This element has a GUI (Graphical User Interface) as an external physical interface.

Table 1-7 Constituent Element of the Administrator Tool

Identifying Name	Identifying Information
Original Data Security Administrator	1.0

- **Browser tool**

  This application, which is a TOE, uses image files. Table 1-8 shows the details of the constituent element of the browser tool software. This element has a GUI (Graphical User Interface) as an external physical interface.

[1] http://canon.jp

Table 1-8 Constituent Element of the Browser Tool

Identifying Name	Identifying Information
Original Data Security Utility	1.0

- **OS card**

  This flash memory, which is a TOE, includes smart card functionality. Table 1-9 shows the details of the constituent elements of the OS card hardware and software. These elements have an external media connection as an external physical interface. The OS cards each have different individual information (referred to as the "OSCID" below).

Table 1-9 Constituent Elements of the OS Card

Identifying Name	Identifying Information
Original Data Security Card hardware	OSC-128M
Original Data Security Card applet (applet name : FF34123456100101)	00000003

- **PC**

  This is the PC/AT-compatible machine on which the administrator tool and browser tool run. This element uses a human interface comprised of a keyboard, mouse, display, and other components, and a peripheral device comprised of USB and so on as the external physical interface.

- **OS**

  This is the basic software (operating system) of the PC on which the administrator tool and browser tool run. The operating systems usable as a TOE are shown in Table 1-10. This element has a GUI (Graphical User Interface) as an external physical interface.

Table 1-10 List of Usable Operating Systems

List of Usable Operating Systems
Microsoft Windows 2000 Professional Service Pack 4
Microsoft Windows XP Professional Service Pack 2 (32-bit system)

List of Usable Operating Systems
Microsoft Windows XP Home Edition Service Pack 2 (32-bit system)
Microsoft Windows Vista (32-bit system)[2]

- **Card reader/writer**

  This device, which reads and writes the OS card, is connected to the PC via USB. This element uses a peripheral device interface such as USB and an external media connection as its external physical interface.

The OS card is flash memory with smart card functionality, and offers physical tamper-resistance. Also note that the EOS digital camera is dedicated hardware, and its specifications are unpublished.

1.4.2.2 Logical scope of the TOE

Figure 1-2 shows the functions of this entire system. The functions enclosed within thick borders are TOE functions, and the colored functions are this TOE's security functions.

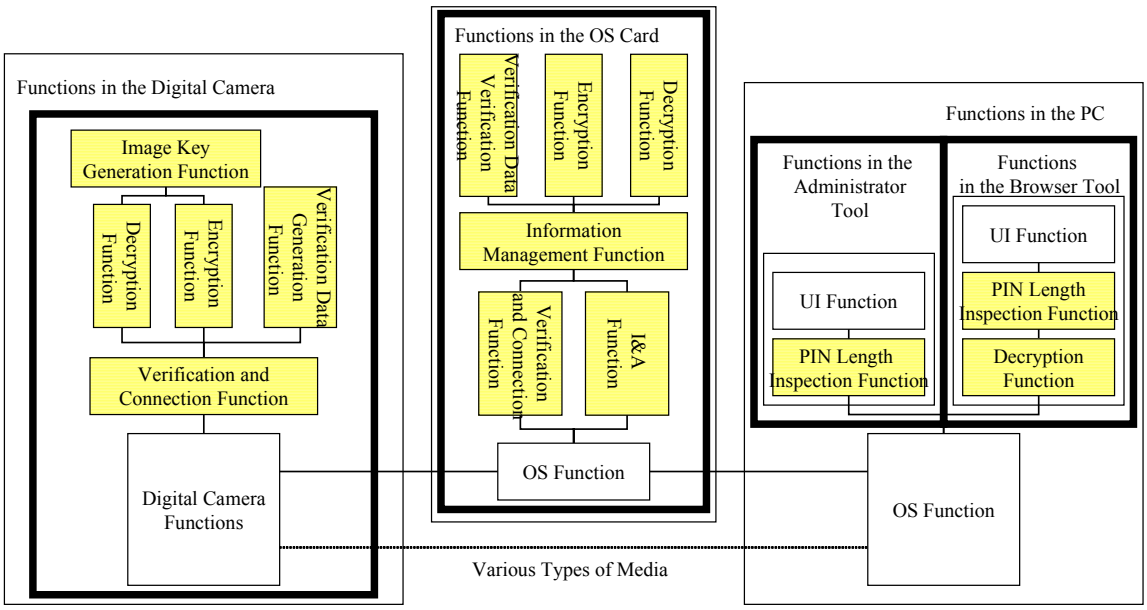

Figure 1-2 Block Diagram of EOS Digital Camera System Functions

[2] Except the Starter Edition

Each function is described below by physical configuration scope.

<The EOS Digital Camera>

- **Functions in the Digital Camera**

  By controlling each part of the EOS digital camera based on the input from the controls and PC connection, this function makes it possible to shoot images, generate image files, and output image files to the display, external media connection, and PC connection. It is also possible to decrypt as necessary and show image files and encrypted image files on the display from some types of media. It is not possible, however, to use image files and encrypted image files input from media for any purpose other than displaying.

- **Verification and Connection Function**

  This function verifies and connects the OS card.

- **Encryption Function**

  This function encrypts image files and image keys.

- **Image Key Generation Function**

  This function generates image keys.

- **Decryption Function**

  This function decrypts encrypted image files and encrypted image keys.

- **Verification Data Generation Function**

  This function generates verification data for verifying the originality of image files by using MAC keys.

<PC>

- **OS Function**

  This is the basic software, or “operating system” for running the TOE.

<administrator tool>

- **PIN Length Inspection Function**

  This function inspects the PIN to be registered by a user and ensures that it has between 8 and 15 characters.

<browser tool>

- **Decryption Function**

  This function decrypts encrypted image files.

- **PIN Length Inspection Function**

This function inspects the PIN to be registered by a user and ensures that it has between 8 and 15 characters.

<The OS card>

- **OS Function**

  This is the basic software, or "operating system" for running the TOE.

- **I&A Function**

  This function uses PIN authentication to identify and authenticate administrators and browsers. This function also manages the IDs and PINs of both administrators and browsers.

- **Verification and Connection Function**

  This function verifies that the EOS digital camera has been registered, and connects it.

- **Information Management Function**

  This function generates and manages card keys, and manages OS card data. Furthermore, it includes functionality to control the access by users of card keys and other OS card data. The IDs of EOS digital cameras that can use card keys etc. are maintained and managed, along with browser IDs. Only the administrator can set information related to this access control.

- **Encryption Function**

  This function encrypts card keys and OS card data, and generates encrypted OS card data. The encrypted key for the OS card data is generated based on seed information input from outside.

- **Decryption Function**

  This function decrypts encrypted OS card data.

- **Verification Data Verification Function**

  This function verifies the originality of image files based on MAC keys and verification data.

Note that the smart card functions such as the tamper-resistant functionality of the OS card are not the security functions of this TOE.

Next, the processing steps of image files are shown in Figure 1-3, and the symbols used in Figure 1-3 are described in Table 1-11. Also, since Figure 1-3 describes the image file processing steps, it only includes the decryption function, encryption function, verification data generation function, and verification data verification function, all of

which are directly involved with image files.

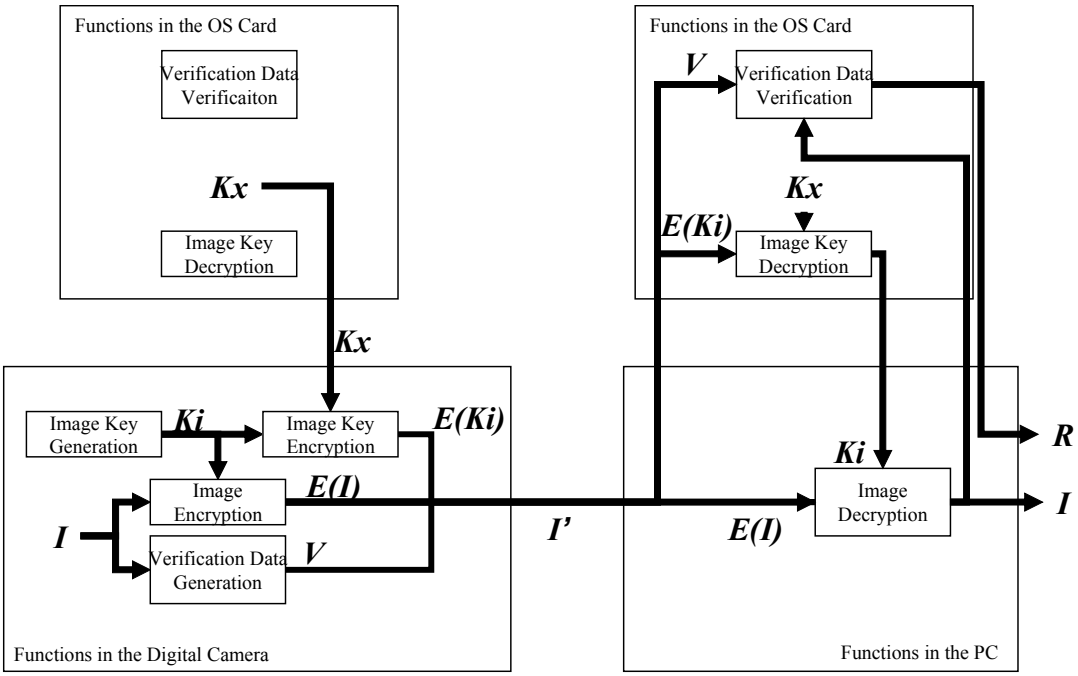

Figure 1-3 Image File Processing Steps

Table 1-11 Symbol Descriptions

Symbol	Description
Ki	The image key. This key is used to encrypt and decrypt image files.
Kx	The card key. This key is maintained inside the OS card, and is used to encrypt and decrypt the image key.
I	The image file.
V	Verification data.
R	Verification result. This is the result of verifying the originality of an image file,based on the verification data.
E(Ki)	The encrypted image key.
E(I)	The encrypted image file.
I'	The encrypted image file with verification data. This is formed from ***E(I)***, ***E(Ki)***, and ***V***.

As show in Figure 1-3, this system uses the image key to encrypt the image file, and uses a hierarchical encryption method to encrypt the image key with the card key. The

card key is generated when the administrator sets the OS card preferences (initial settings). The image key, on the other hand, is generated each time an image file is generated, which is to say that the image key is generated automatically inside the EOS digital camera each time a photograph is taken. The OS card outputs the card key to the EOS digital camera after the EOS digital camera is verified and connected, and with the EOS digital camera's confidentiality maintained. On the other hand, when an encrypted image file is decrypted, the card key is not output from the OS card to the PC. Also, although it is not shown in Figure 1-3, the MAC key differs between EOS digital cameras, and is recorded on the EOS digital camera and the OS card in advance. The card key and other items of OS data are encrypted with the encryption function inside the OS card, and are then output to the PC as backup data.

1.4.3 TOE users

The users of this system are as follows:

Photographer	The entity who uses the EOS digital camera and the OS card to generate image files.
Browser	The entity who uses the browser tool and the OS card to view or "browse" image files. This entity can modify his own PIN.
Administrator	In addition to the role of browser, the administrator entity uses the administrator tool and the OS card to initialize, backup, and restore the OS card data. This entity also manages the EOS digital camera IDs, administrator IDs and PINs, and browser IDs and PINs capable of accessing the OS card.

Note that it is expected that there will be situations where the photographer and administrator are the same person, the browser and administrator are the same person, or the photographer and browser are the same person.

2 Conformance claims

2.1 CC conformance claim

The CC conformance claims of this ST and TOE are listed below:

CC versions for which conformance is claimed for the ST and TOE :

[CC] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, September 2006, Ver.3.1 Revision 1, CCMB-2006-09-001

Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, September 2006, Ver.3.1 Revision 1, CCMB-2006-09-002

Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, September 2006, Ver.3.1 Revision 1, CCMB-2006-09-003

Conformance of the ST with respect to CC part 2 : CC Part 2 conformant

Conformance of the ST with respect to CC part 3 : CC Part 3 conformant

The following information was referred to during the creation of this ST :

[CEM] Common Methodology for Information Technology Security Evaluation Evaluation methodology, September 2006, Ver.3.1 Revision 1, CCMB-2006-09-004

2.2 PP claim, Package claim

The PP claim and Package claim of this ST and TOE are shown below:

PP claim : This ST conforms with no PP

Package claim : EAL2 Conformant

3 Security problem definition

This chapter describes the security problem definition.

3.1 Threats

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.2 Organisational security policies

No organizational security policy is envisioned based on this ST.

3.3 Assumptions

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 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.

3.3.5 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.

4 Security objectives

This chapter describes the security objectives.

4.1 Security objectives for the TOE

4.1.1 O.VERIFY_IMAGE

When an image file shot by the EOS digital camera is generated, this TOE generates verification data that can be used to verify the originality of the shot image file, and records the image file with verification data on the storage medium. The TOE verifies the originality of the image file based on the verification data when the image file is viewed.

4.1.2 O.ENC_IMAGE

When an image file shot by the EOS digital camera is generated, this TOE indirectly uses information stored on the prescribed OS card to encrypt the image file and record the encrypted image file on the storage medium. When the image file is viewed, the TOE indirectly uses information stored on the OS card to decrypt the encrypted image file. The TOE also maintains the confidentiality of the key used for encrypting and decrypting the image file.

4.1.3 O.I&A

Before accessing the card key stored on the OS card, the TOE identifies and authenticates of the user.

4.1.4 O.ACCESS_CONTROL

When the OS card is used via the browser tool or administrator tool on the PC, the TOE controls access by the user.

4.1.5 O.ENC_OSC

The TOE encrypts backup data when the OS card data is backed up, and decrypts this encrypted backup data when the OS card data is restored.

4.2 Security objectives for the operational environment

4.2.1 OE.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.

4.2.2 OE.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.

4.2.3 OE.MANAGER

The entity given the role of selecting the administrator (manager) must make sure to assign an administrator who will dutifully carry out permitted actions only. Also, an administrator must be assigned who will select and set a PIN that is difficult for third parties to guess.

4.2.4 OE.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.

4.2.5 OE.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, management must ensure that this card reader/writer will be connected to the PC in such a way that eavesdropping does not occur between the two.

4.3 Security objectives rationale

This section describes the correspondence relationships between “security objectives” and “security problem definitions of threats, organizational security policies (OSPs), and assumptions” from the perspectives of necessity and sufficiency.

4.3.1 The necessity of security countermeasure policies

Table 4-1 maps “security objectives” and “security problem definitions of threats, organizational security policies (OSPs), and assumptions”. This shows how each security objective corresponds to at least one threat, organizational security policy

(OSP), or assumption.

Table 4-1 Correspondence between Security Objectives and Threats, Organizational Security Policies, and Assumptions

	T.MODIFY_IMAGE	T.DISCLOSE_IMAGE	T.DISCLOSE_OSC	T.ILLEGAL_ACCESS	T.BACKUP	A.PHOTOGRAPHER	A.VIEWER	A.MANAGER	A.PLATFORM	A.PERIPHERAL
O.VERIFY_IMAGE	×									
O.ENC_IMAGE		×								
O.I&A			×							
O.ACCESS_CONTROL				×						
O.ENC_OSC					×					
OE.PHOTOGRAPHER						×				
OE.VIEWER							×			
OE.MANAGER								×		
OE.PLATFORM									×	
OE.PERIPHERAL										×

4.3.2 The sufficiency of security countermeasure policies

This section shows the basis for claiming that the security objectives fully satisfy the security problem definitions.

T.MODIFY_IMAGE is guarded against by O.VERIFY_IMAGE. The reason for this is that O.VERIFY_IMAGE enables the generation of an image file with verification data that enables the verification of the image file's originality when the image file of an image shot by the EOS digital camera is generated. Also, when an image file with verification data is viewed, it is possible to verify the originality of the image file based on the verification data. The makes it possible to detect falsification of an image file shot with the EOS digital camera, thereby inhibiting the threat in question. Therefore, O.VERIFY_IMAGE satisfies the demands of T.MODIFY_IMAGE.

T.DISCLOSE_IMAGE is guarded against by O.ENC_IMAGE. The reason for this is that O.ENC_IMAGE encrypts image files when they are shot by the EOS digital camera and generated, and decrypts these encrypted image files for viewing. This makes it possible to maintain the confidentiality of image files shot with the EOS digital camera, thereby preventing the threat in question. Therefore, O.ENC_IMAGE satisfies the demands of T.DISCLOSE_IMAGE.

T.DISCLOSE_OSC is guarded against by O.I&A. The reason for this is that O.I&A identifies and authenticates the user before allowing access to the card key stored on the OS card. This prevents the unauthorized access of the OS card by third parties using the PC, thereby preventing the threat in question. Therefore, O.I&A satisfies the demands of T.DISCLOSE_OSC.

T.ILLEGAL_ACCESS is guarded against by O.ACCESS_CONTROL. The reason for this is that O.ACCESS_CONTROL controls access to the OS card by a user of the browser tool or administrator tool on the PC. This prevents processing that exceeds the scope of the browser's privileges, thereby preventing the threat in question. Therefore, O.ACCESS_CONTROL satisfies the demands of T.ILLEGAL_ACCESS.

T.BACKUP is guarded against by O.ENC_OSC. The reason for this is that O.ENC_OSC encrypts backup data when a backup is taken, and decrypts the encrypted backup data during restoration. This makes it possible to maintain the confidentiality of the backup data, thereby preventing the threat in question. Therefore, O.ENC_OSC satisfies the demands of T.BACKUP.

It is self-evident that A.PHOTOGRAPHER is guarded against by OE.PHOTOGRAPHER. The reason for this is that OE.PHOTOGRAPHER roughly restates the text of A.PHOTOGRAPHER. Therefore, OE.PHOTOGRAPHER satisfies the demands of A.PHOTOGRAPHER.

It is self-evident that A.VIEWER is guarded against by OE.VIEWER. The reason for this is that OE.VIEWER roughly restates the text of A.VIEWER. Therefore, OE.VIEWER satisfies the demands of A.VIEWER.

A.MANAGER is guarded against by OE.MANAGER. OE.MANAGER requires the

appointment of an administrator who will dutifully carry out only permitted actions, thereby guaranteeing that no malicious actions will be performed. Therefore, OE.MANAGER satisfies the demands of A.MANAGER.

It is self-evident that A.PLATFORM is guarded against by OE.PLATFORM. The reason for this is that OE.PLATFORM roughly restates the text of A.PLATFORM. Therefore, OE.PLATFORM satisfies the demands of A.PLATFORM.

It is self-evident that A.PERIPHERAL is guarded against by OE.PERIPHERAL. The reason for this is that OE.PERIPHERAL roughly restates the text of A.PERIPHERAL. Therefore, OE.PERIPHERAL satisfies the demands of A.PERIPHERAL.

5 Extended components definition

This chapter describes the extended components. This ST does not define extended components.

6 Security requirements

This chapter describes security requirements.

6.1 Security functional requirements

This section describes the security functional requirements. Note that all the security funcitonal requirements are as stipulated in CC Part 2.

6.1.1 FCS_COP.1a Cryptographic operation (MAC)

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [assignment: the generation and the verification 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].

6.1.2 FCS_CKM.1b Cryptographic key generation (Image Encryption)

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys *(Image Key)* in accordance with a specified cryptographic key generation algorithm [assignment: PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1] and specified cryptographic key sizes [assignment: 128 bits] that meet the following: [assignment: FIPS PUB 186-2].

6.1.3 FCS_CKM.4b Cryptographic key destruction (Image Encryption)

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys *(Image Key)* in accordance with a specified cryptographic key destruction method [assignment: Zeroization] that meets the following: [assignment: none].

6.1.4 FCS_COP.1b Cryptographic operation (Image Encryption)

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [assignment: the encryption and the decryption of the image file] in accordance with a specified cryptographic algorithm [assignment: AES] and cryptographic key sizes [assignment: 128 bits] that meet the following: [assignment: FIPS PUB 197].

6.1.5 FCS_CKM.1c Cryptographic key generation (Image Key Encryption)

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys *(Card Key)* in accordance with a specified cryptographic key generation algorithm [assignment: PRNG based on ANSI X9.31] and specified cryptographic key sizes [assignment: 128 bits] that meet the following: [assignment: ANSI X9.31].

6.1.6 FCS_CKM.4c Cryptographic key destruction (Image Key

Encryption)

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys *(Card Key)* in accordance with a specified cryptographic key destruction method [assignment: Zeroization] that meets the following: [assignment: none].

6.1.7 FCS_COP.1c Cryptographic operation (Image Key Encryption)

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [assignment: the encryption or the decryption of the Image Key] in accordance with a specified cryptographic algorithm [assignment: Triple DES] and cryptographic key sizes [assignment: 168 bits (3 keys)] that meet the following: [assignment: NIST SP800-67].

6.1.8 FCS_COP.1d Cryptographic operation (OS Card data)

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [assignment: the encryption and the decryption of the OS Card data] in accordance with a specified cryptographic algorithm [assignment: Triple DES] and cryptographic key sizes [assignment: 168 bits (3 keys)] that meet the following: [assignment: NIST SP800-67].

6.1.9 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: EOS Digital Camera System Access Control Policy] on [assignment:

Subject : App process corresponding to the PC tool

Object : Image file (*I*), OS Card data (*C*), Seed of the OS Card data encryption key (*S*)

Operation : Encrypt (*Enc*), Decrypt (*Dec*), Generate (*Gen*) the verification data of the object, Verify (*Ver*) the object based on the verification data, Export (*Exp*), Import (*Imp*)].

6.1.10 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [assignment: EOS Digital Camera System Access Control Policy] to objects based on the following: [assignment: subjects, objects, and security attributes shown in Table 6-1, Table 6-2, and Table 6-3].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules shown in Table 6-1, Table 6-2, and Table 6-3].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment:

The App process can verify (*Ver*) the image file (*I*) based on the verification data].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment:

The App process with any ID can not encrypt (*Enc*) the image file (*I*).

The App process with any ID can not generate (*Gen*) the verification data of the image file (*I*)].

Table 6-1 EOS Digital Camera System Access Control List 1

Subject	Sec. Attributes	Condition	Object
			I
App process	Viewer ID	If Viewer ID is enrolled.	*Dec*
App process	Administrator ID	If Administrator ID is enrolled.	*Dec*

Table 6-2 EOS Digital Camera System Access Control List 2

Subject	Sec. Attributes	Condition	Object
			C
App process	Administrator ID	If Administrator ID is enrolled.	*Exp/Imp*

Table 6-3 EOS Digital Camera System Access Control List 3

Subject	Sec. Attributes	Condition	Object
			S
App process	Administrator ID	If Administrator ID is enrolled.	*Imp*

6.1.11 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the [assignment: EOS Digital Camera System Access Control Policy] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes

6.1.12 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the [assignment: EOS Digital Camera System Access Control Policy] when importing user data, controlled under the

SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: none].

6.1.13 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: 3]] unsuccessful authentication attempts occur related to [assignment: the each authentication of the administrator and the viewer].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: return the authentication result after waiting 5 seconds in the next authentication attempt].

Note : When the user is authenticated successfully, the TSF shall clear the unsuccessful authentication counter for the user.

6.1.14 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: Administrator ID, Viewer ID].

6.1.15 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: the Authentication Metric defined below].

Authentication Metric

(1) The length of it between 8 characters and 15 characters.

6.1.16 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: the actions defined in Table 6-4] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Table 6-4 List of TSF mediated actions #1

TSF mediated actions
To get the OSCID of the OS card
To get the version information of the OS card
To generate the verification data of the image file
To verify the image file based on the verification data

6.1.17 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: the actions defined in Table 6-5] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Table 6-5 List of TSF mediated actions #2

TSF mediated actions
To get the OSCID of the OS card
To get the version information of the OS card
To generate the verification data of the image file
To verify the image file based on the verification data

6.1.18 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: Administrator ID, Viewer ID].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: none].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: none].

6.1.19 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: modify, delete, [assignment: run initial-setting, initialize, add]] the [assignment: Administrator ID, Administrator PIN, Viewer ID, Viewer PIN, Card Key, EOS Digital Camera ID] to [assignment: the administrator].

6.1.20 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: management items of column in Table 6-6].

Table 6-6 List of the management functions

management items of the TOE
To add Viewer ID/PIN, and EOS Digital Camera ID
To delete Viewer ID/PIN, and EOS Digital Camera ID
To modify Administrator PIN, Viewer PIN, and EOS Digital Camera ID
To run initial-setting of Administrator ID/PIN and Card Key
To initialize Administrator ID/PIN, Viewer ID/PIN, Card Key, and EOS Digital Camera ID

6.1.21 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.22 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: disclosure] when it is transmitted between separate parts of the TOE *(the digital camera and the OS card)*.

6.2 Security assurance requirements

This section describes the TOE security assurance requirements. The evaluation assurance level of this TOE is EAL 2. The security assurance requirements of this TOE are shown in Table 6-7. Also, all security assurance requirements are as stipulated in CC Part 3.

Table 6-7 List of TOE Security Assurance Requirement Components

Assurance Class	Assurance Requirement Componets	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.3 Security requirements rationale

6.3.1 Sufficiency of the TOE security objectives for covering security functional requirements

This section describes the correspondence of security functional requirements and TOE security objectives from the perspectives of necessity and sufficiency.

6.3.1.1 The necessity of security functional requirements

Table 6-8 maps the TOE security objectives and security functional requirements. This shows how each security functional requirement corresponds to at least one TOE security objectives.

Table 6-8 Correspondence between Security Functional Requirements and TOE Security Objectives

	O.VERIFY_IMAGE	O.ENC_IMAGE	O.I&A	O.ACCESS_CONTROL	O.ENC_OSC
FCS_COP.1a	×				
FCS_CKM.1b		×			
FCS_CKM.4b		×			
FCS_COP.1b		×			
FCS_CKM.1c		×			
FCS_CKM.4c		×			
FCS_COP.1c		×			
FCS_COP.1d					×
FDP_ACC.1				×	
FDP_ACF.1				×	
FDP_ETC.1				×	×
FDP_ITC.1				×	×
FIA_AFL.1			×		

	O.VERIFY_IMAGE	O.ENC_IMAGE	O.I&A	O.ACCESS_CONTROL	O.ENC_OSC
FIA_ATD.1			×		
FIA_SOS.1			×		
FIA_UAU.1			×		
FIA_UID.1			×		
FIA_USB.1			×		
FMT_MTD.1		×	×		
FMT_SMF.1		×	×		
FMT_SMR.1		×	×		
FPT_ITT.1		×			

6.3.1.2 The sufficiency of security functional requirements

This section shows the basis for claiming that the security functional requirements fully satisfy the TOE security objectives.

O.VERIFY_IMAGE is guarded against by FCS_COP.1a.
TSF generates the Keyed-Hash Message Authentication Code based on FCS_COP.1a, thereby making it possible to verify the originality of the image file based on verification data. Therefore, FCS_COP.1a satisfies the demands of O.VERIFY_IMAGE.

O.ENC_IMAGE is guarded against by FCS_CKM.1b, FCS_CKM.4b, FCS_COP.1b, FCS_CKM.1c, FCS_CKM.4c, FCS_COP.1c, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FPT_ITT.1.
According to FCS_CKM.1b, FCS_CKM.4b, and FCS_COP.1b, TSF generates the image key based on "PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1," implements encryption and decryption of the image file according to the "encryption algorithm AES," and destroys the image key by zeroing. According to FCS_CKM.1c, FCS_CKM.4c, and FCS_COP.1c, TSF generates the card key based on "PRNG based on ANSI X9.31," and destroys the card key by zeroing. According to FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1, the administrator manages the card

key. Furthermore, the card key is stored on the OS card with its confidentiality maintained, and to transfer this card key to the EOS digital camera, TSF implements the transfer of the card key with its confidentiality intact between the TOEs that are the OS card and the prescribed EOS digital camera, according to FPT_ITT.1. In order to determine whether or not the EOS digital camera is the prescribed one, the administrator manages the ID of the EOS digital camera according to FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. Therefore, FCS_CKM.1b, FCS_CKM.4b, FCS_COP.1b, FCS_CKM.1c, FCS_CKM.4c, FCS_COP.1c, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FPT_ITT.1 satisfy the demands of O.ENC_IMAGE.

O.I&A is guarded against by FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1, FIA_USB.1, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.
TSF authenticates the identities of the administrator and browsers according to FIA_UAU.1 and FIA_UID.1. Also, in order to support identification & authentication, TSF regulates the operations to be performed when identification & authentication fails according to FIA_AFL.1, defines the binding of the user subject when identification & authentication succeeds and defines user attributes according to FIA_ATD.1 and FIA_USB.1, and regulates the quality of authentication information according to FIA_SOS.1. Furthermore, TSF implements the management of identification & authentication by the administrator according to FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. Therefore, FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1, FIA_USB.1, FMT_SMF.1, and FMT_SMR.1 satisfy the demands of O.I&A.

O.ACCESS_CONTROL is guarded against by FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, and FDP_ITC.1.
TSF implements access control according to FDP_ACC.1 and FDP_ACF.1 as related to image files, OS card data, and the seed for the OS card data encryption key. TSF implements access control according to FDP_ETC.1 and FDP_ITC.1 as related to exporting and importing OS card data. Furthermore, according to FDP_ITC.1, TSF implements access control as related to importing the encryption key seed for OS card data. Therefore, FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, FDP_ITC.1, and FDP_ITT.1 satisfy the demands of O.ACCESS_CONTROL.

O.ENC_OSC is guarded against by FCS_COP.1d, FDP_ETC.1, and FDP_ITC.1. According to FCS_COP.1d and FDP_ETC.1, TSF encrypts the OS card data with the “encryption algorithm Triple DES,” and exports this data as backup data. On the other

hand, TSF imports encrypted OS card data and decrypts it with the "decryption algorithm Triple DES." Also, this encryption key seed is input according to FDP_ITC.1. Therefore, FCS_COP.1d, FDP_ETC.1, and FDP_ITC.1 satisfy the demands of O.ENC_OSC.

6.3.2 The rationales for the dependency

Table 6-9 shows the dependencies of TOE security functional requirements. The "SFR" row shows the IDs of TOE security functional requirements selected by this ST. The "CC Regulation Dependencies" row shows the dependencies regulated by the CC. Finally, the "ST Dependencies" row shows IDs that are satisfied by the ST. Note that "-" in the table indicates that the dependency component is not designated in CC part 2, or that the dependency component is not selected by the ST.

Table 6-9 TOE Security Function Requirement Dependencies

SFR	CC Regulation Dependencies	ST Dependencies
FCS_COP.1a	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	-
FCS_CKM.1b	[FCS_CKM.2, FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1b, FCS_CKM.4b
FCS_CKM.4b	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1], FMT_MSA.2	FCS_CKM.1b
FCS_COP.1b	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1b, FCS_CKM.4b
FCS_CKM.1c	[FCS_CKM.2, FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1c, FCS_CKM.4c
FCS_CKM.4c	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1], FMT_MSA.2	FCS_CKM.1c
FCS_COP.1c	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1c, FCS_CKM.4c
FCS_COP.1d	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FDP_ITC.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1
FDP_ETC.1	[FDP_ACC.1, FDP_IFC.1]	FDP_ACC.1
FDP_ITC.1	[FDP_ACC.1, FDP_IFC.1], FMT_MSA.3	FDP_ACC.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1

SFR	CC Regulation Dependencies	ST Dependencies
FIA_ATD.1	-	-
FIA_SOS.1	-	-
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	-	-
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_ITT.1	-	-

Since the assurance package EAL 2 was selected for the TOE security assurance requirement dependencies with no excess or deficiency, these requirement dependencies are satisfied.
Therefore, the TOE security requirements satisfy the necessary dependencies, other than the exceptions described below.

FCS_COP.1a does not satisfy any dependencies. Since this TOE uses keys stored in advance in the OS card with its tamper-resistant characteristics and the EOS digital camera, the requirements related to generating and inputting keys (FDP_ITC.1/FDP_ITC.2/FCS_CKM.1) are unnecessary. The OS card and the EOS digital camera have tamper-resistant properties, and so no threat of unauthorized reading of the encryption key is envisioned. For this reason, the requirement for destroying the key (FCS_CKM.4) is unnecessary. Furthermore, this TOE does not have any security attributes related to keys. For this reason, the requirement regarding security attributes (FMT_MSA.2) is unnecessary.
Therefore, this ST does not require the FCS_COP.1a dependency.

FCS_CKM.1b, FCS_CKM.4b, FCS_COP.1b, FCS_CKM.1c, FCS_CKM.4c, and FCS_COP.1c do not satisfy the dependency on FMT_MSA.2. This TOE ford not have security attributes related to keys.
Therefore, this ST does not require the dependency on FMT_MSA.2.

FCS_COP.1d does not satisfy dependencies on FCS_CKM.4 and FMT_MSA.2. The OS card and the EOS digital camera have tamper-resistant properties, and so no threat of unauthorized reading of the encryption key is envisioned. For this reason, the

requirement for destroying the key (FCS_CKM.4) is unnecessary. Furthermore, this TOE does not have any security attributes related to keys. For this reason, the requirement regarding security attributes (FMT_MSA.2) is unnecessary.
Therefore, this ST does not require the dependencies on FCS_CKM.4 and FMT_MSA.2.

FDP_ACF.1 and FDP_ITC.1 do not satisfy the dependency on FMT_MSA.3.
This TOE does not have security attributes related to access control objects. Therefore, the requirement related to object security attributes (FMT_MSA.3) is not necessary.
Therefore, this ST does not require the dependency on FMT_MSA.3.

6.3.3 The rationale of TOE assurance requirements

This TOE envisions both commercial and private usage. Also, this TOE targets the originality and confidentiality of image files, and does not directly handle information with economic value. For this reason, this TOE envisions low-level attackers without advanced technical knowledge, as described in Chapter 3.
When low-level attackers of this sort are envisioned, EAL 2 is appropriate from both cost and time investment perspectives.

7 TOE summary specification

This chapter divides the TOE security functions into categories, which are each then described.

7.1 Image File Verification Functions

This TOE has a function for generating verification data, and a function for verifying the originality of image files based on this verification data.

The "verification data generation function" complies with "FIPS PUB 198," and is comprised of "The Keyed-Hash Message Authentication Code" by using "fixed key lengths of 128 bits or more." Verification data is generated by the "function for verifying originality of an image file based on verification data" in the same way as the "function for generating verification data," and verification involves the comparison of this generated verification data and the verification data affixed to the image file (in compliance with FCS_COP.1a). 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 identification & authentication is not carried out (in compliance with FIA_UAU.1 and FIA_UID.1).

7.2 Image File Encryption Functions

This TOE includes image file encryption functions. These image file encryption functions include the image file encryption/decryption and image key encryption/decryption functions shown in Figure 1-3. The image file encryption and decryption functions are comprised of the following elements:

- An AES encryption/decryption function (in compliance with FCS_COP.1b) 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 (in compliance with FCS_CKM.1b)
- A key zeroization function that zeroes out keys (in compliance with FCS_CKM.4b)

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 (in compliance with FCS_COP.1c)

- A key generation function compliant with ANSI X9.31, with a PRNG based on ANSI X9.31 (in compliance with FCS_CKM.1c)
- A key zeroization function that zeroes out keys (in compliance with FCS_CKM.4c)

7.3 I&A Functions

This TOE has a function that allows the OS card to authenticate the identification of the user. The identification information and PIN are used to identifies and authenticate an administrator or browser. This TOE can also perform the following processes without authenticating a user's identity (in compliance with FIA_ATD.1, FIA_UAU.1, FIA_UID.1, and FIA_USB.1):

- 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 (in compliance with FIA_AFL.1).

7.4 PIN Length Inspection Function

This TOE verifies that a registered PIN is between 8 and 15 characters long (in compliance with FIA_SOS.1).

7.5 Verification and Connection Functions

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 (in compliance with FPT_ITT.1).

7.6 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 image files (*I*), OS card data (*C*), and OS card data encryption key seed information (*S*) (in compliance with FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, and FDP_ITC.1):

Table 7-1 EOS Digital Camera System Access Control List 1

		Condition	Object
Subject	**Sec. Attributes**		*I*
App process	Viewer ID	If Viewer ID is enrolled.	*Dec*
App process	Administrator ID	If Administrator ID is enrolled.	*Dec*

Table 7-2 EOS Digital Camera System Access Control List 2

		Condition	Object
Subject	**Sec. Attributes**		*C*
App process	Administrator ID	If Administrator ID is enrolled.	*Exp/Imp*

Table 7-3 EOS Digital Camera System Access Control List 3

		Condition	Object
Subject	**Sec. Attributes**		*S*
App process	Administrator ID	If Administrator ID is enrolled.	*Imp*

The symbols in the tables have the following meanings:

- 「*Dec*」 : Decrypt.
- 「*Exp*」 : Export.
- 「*Imp*」 : Import.

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 (in compliance with FDP_ACF.1).

Encryption and decryption of OS card data complies with NIST SP800-67, and is

comprised of Triple DES, using a 168-bit key length (in compliance with FCS_COP.1d). Also, this encryption key is generated with information inputted from outside as the seed (in compliance with FDP_ITC.1).

7.7 Administration Functions

Administrators can execute the following operations as administration functions (in compliance with FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1):

- Add and delete a browser's ID and PIN as a set.
- Change administrator and browser PINs.
- Set the initial settings (preferences) of 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

8 Reference, and Glossary/Abbreviation

8.1 Reference

This section provides reference material that was used in the creation of this ST.

[CC] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, September 2006, Ver.3.1 Revision 1, CCMB-2006-09-001

Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, September 2006, Ver.3.1 Revision 1, CCMB-2006-09-002

Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, September 2006, Ver.3.1 Revision 1, CCMB-2006-09-003

[CEM] Common Methodology for Information Technology Security Evaluation Evaluation methodology, September 2006, Ver.3.1 Revision 1, CCMB-2006-09-004

8.2 Glossary/Abbreviation

This section describes the abbreviations and terms used by this ST.

AES: An encryption algorithm referred to as the “Advanced Encryption Standard”

ANSI: American National Standards Institute

CF: A type of memory card referred to as “Compact Flash”

DES: An encryption algorithm referred to as the “Data Encryption Standard”

FIPS: The Commerce Department’s Federal Information Processing Standards

MAC: Message Authentication Code

NIST: The U.S. National Institute of Standards and Technology

OS Card (Original Data Security Card): A memory card with smart card functionality

PIN (Personal Identification Number): Password/code number

PRNG: Pseudo-Random Number Generator

SD: A type of memory card referred to as “Secure Digital”

SHA: A hash function referred to as “Secure Hash Algorithm”

USB (Universal Serial Bus): An interface standard for connecting peripheral devices to a PC

