KYOCERA MITA

Data Security Kit (E)
Software Type IV
Security Target
Version 1.10

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

August 10, 2010

KYOCERA MITA Corporation

- Revision History -

Date	Version	Content of revision	Approver	Drafter
Sep. 16, 2009	0.40	・Newly drafted (derived from Type I	Itoh	Sone
Aug. 10, 2010	1.10	・Revised changes in Type I	Itoh	Sone

- TABLE OF CONTENTS -

- List of Figures -

- List of Tables -

1. ST INTRODUCTION

1.1. ST Reference

ST Title :	KYOCERA MITA Data Security Kit (E) Software Type IV Security Target
ST Version :	Version 1.10
Creation Date :	August 10, 2010
Author :	KYOCERA MITA Corporation

1.2. TOE Reference

TOE Name :	Data Security Kit (E) Software Type IV
TOE Version :	V1.00
Manufacturer :	KYOCERA MITA Corporation

1.3. TOE Overview

1.3.1 TOE Type

This TOE defined by this ST, includes the firmware that controls the Multi Function Printer (hereinafter referred to as "MFP") having mainly copy function, scan function and print function, and ASIC having the security algorithm function. The TOE is installed to be used for the MFPs manufactured by KYOCERA MITA Corporation, namely, "TASKalfa 552ci, CS 552ci, CDC 1850/DCC 2850". Major security features of the TOE protect the image data stored in the internal HDD inside the MFP from being removed through an unauthorized interface.

1.3.2 Usage and Major Security Features of TOE

The MFP in which this TOE is installed is able to perform coping (duplication), printing (paper outputting) and network scanning (electronization) of various documents handled by users. The MFP is located in general office and is not only utilized as a standalone but also connected to LAN or Local Port (USB Port) for the use in the network environment. In the network environment, the MFP is assumed to be used by connecting to client PCs or server on the internal network protected from unauthorized access on the external network by firewall.

In this user environment, the above-mentioned operational functions can be performed through operations on the operation panel or client PCs on the network.

Figure 1.1 shows a typical user environment.

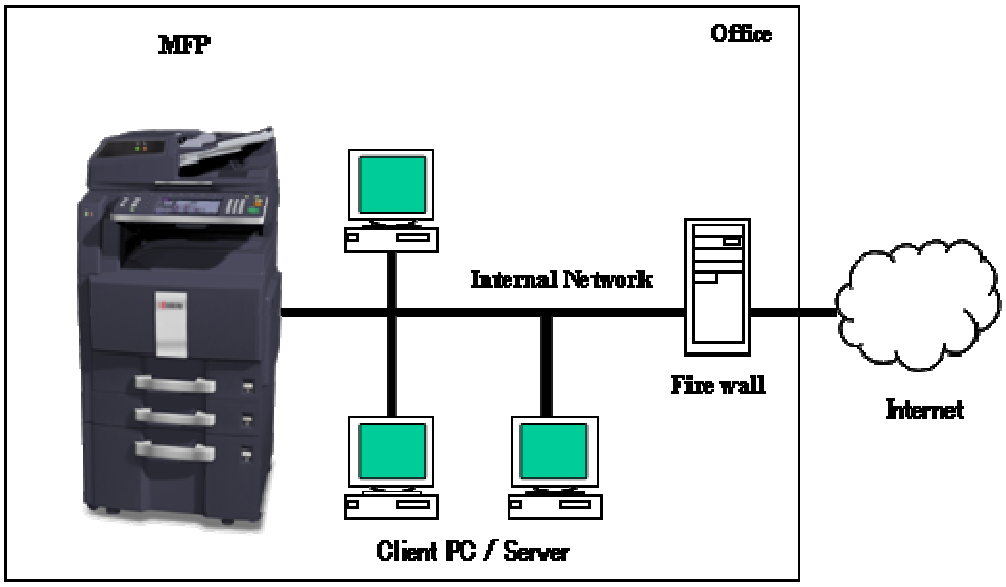

Figure 1.1 A common usage in offices

The TOE security functions can activate upon agreement and registration of the license of the optional "Data Security Kit (E)" for the MFP "TASKalfa 552ci, CS 552ci, CDC 1850/DCC 2850".

The TOE provides the protected functions against leakage of the user image data temporarily stored in the internal HDD inside the MFP during and after processing of each function. When storing the image data into the internal HDD, the image data is encrypted. When receiving an instruction for deletion of the image data, it disables re-usage of the data so that even if the HDD is removed and directly accessed through an interface of the HDD, leakage of the image data can be protected.

1.3.3 Required Non-TOE Hardware/Software/Firmware

To activate the TOE, a certain models of the MFP manufactured by KYOCERA MITA Corporation are needed. Products in which this TOE can be installed are listed in Table 2.1.

Table 1.1 TOE Compatible Products

TOE Name/Version	Compatible Products
Data Security Kit (E) Software Type IV/ V1.00	TASKalfa 552ci CS 552ci CDC 1850/DCC 2850

In order to use the normal functions of the MFP, printer driver and TWAIN driver (identified by Guidance), SMTP server, SMB server and FTP server are needed for client PCs and server in the common usage in offices as shown in Figure 1.1.

1.4. TOE Description

1.4.1. People Associated with the TOE

Roles of people related to the use of the MFP in which the TOE is installed, are defined as follows:

- Machine administrator:
  A person registered as an administrator of the MFP in which the TOE is installed. The administrator holds privileges regarding the MFP. He/she installs and uses devices comprising the MFP in which the TOE is installed, as well as the TOE, and operates and manages them.

- TOE User:
  A person who can use the MFP in which the TOE is installed. He/she can utilize the copy function, print function, network scan function and document management box function.

- Service Person:
  A person certified by KYOCERA MITA Corporation as a service person of the MFP in which the TOE is installed. When the service person installs the TOE, she/he activates and setups (enables operation of) the TOE. Also, she/he performs maintenance of devices comprising the MFP in which the TOE is installed, as well as the TOE.

1.4.2. Physical Configuration of the TOE

The conceptual figure of physical configuration of the TOE is shown in Figure 1.2.

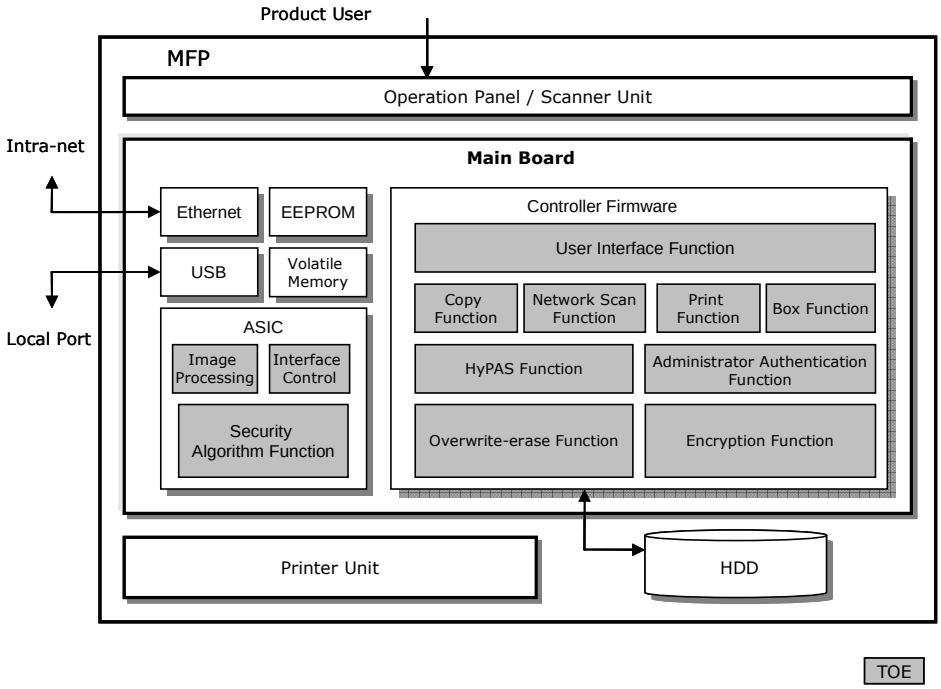

Figure 1.2 Physical Configuration of the TOE

The MFP in which the TOE is installed consists of an operation panel, a scanner unit, a printer unit, a main board and HDD hardware.

Controller firmware on the main board to control a copy function, a network scan function, a print function, a document management box function, an administrator authentication function, a HyPAS function, an overwrite-erase function and an encryption function are included in the TOE.

Additionally, special custom IC (ASIC) which share with the control firmware in installing the security functions is included in the TOE. The ASIC includes a security algorithm function module, an image processing module and an interface controller module. From the above-mentioned, the security algorithm function module overwrites over the specified area in the HDD regarding the overwrite-erase function, and encrypts the image data when reading and writing into the HDD regarding the encryption function.

The firmware term as described in this ST includes the meaning of ASIC as well as the controller firmware.

Non-TOE is: the MFP identified by the table 1.1, language file used for performing user interface function and application software installed by performing HyPAS function.

Physical tamper resistance in hardware (including ASIC) comprising the MFP is not evaluated.

1.4.3. Logical Configuration of the TOE

The conceptual figure of logical configuration of the TOE is shown in Figure 1.3.

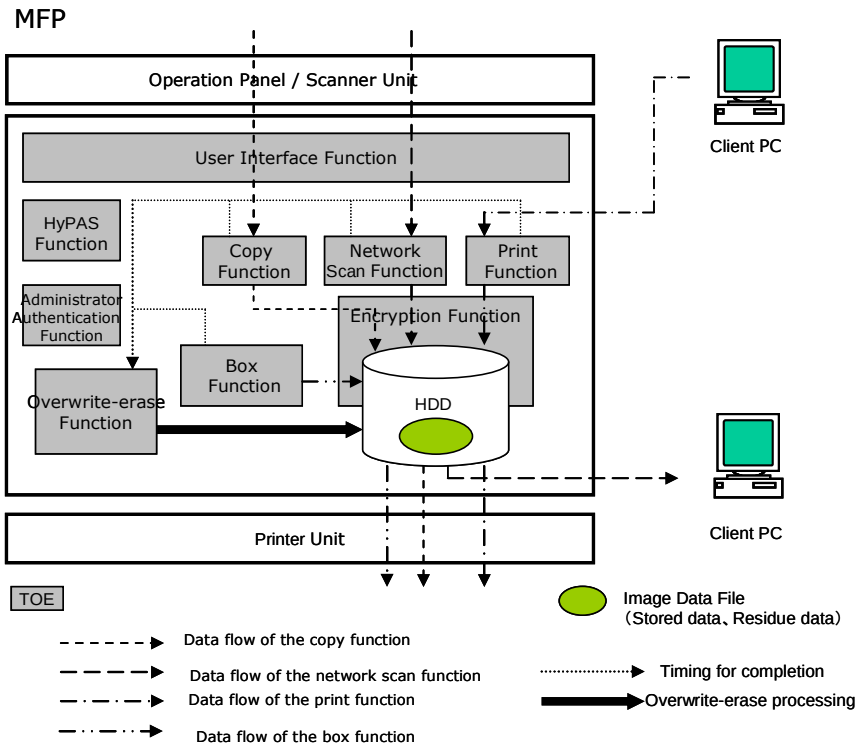

Figure 1.3 Logical Configuration of the TOE

1.4.3.1. Basic Functions provided by the TOE

The TOE provides the following basic functions.

- User Interface function

  A function that receives inputs or operations from the operation panel for machine administrators, TOE users and service persons to utilize the MFP functions. It also makes displays on the operation panel.

- Administrator Authentication Function

  A function that identifies and authenticates a machine administrator by a password of the machine administrator inputted from the operation panel.

However, this function is not the security function that is provided by the TOE.

- Copy Function
  A function that reads image data from the scanner of the MFP, and outputs from the printer unit of the MFP by inputting or operating from the operation panel.
- Network Scan Function
  A function that transmits image data to client PCs by inputting or operating from the operation panel.
- Print Function
  A function that outputs image data transmitted from the client PCs connected over LAN or local, from the printer unit of the MFP by operating from the client PCs.
- Document Management Box Function
  A function that stores image data in the HDD for a long period of time.
  The image data inputted from the operation panel or the client PCs connected over LAN or local is stored in the HDD for a long period of time by inputting/operating from the operation panel or operating through the client PCs. The image data stored in the HDD for a long period of time can be printed out and forwarded to the client PCs. Anyone can be unrestricted access to the image data. The image data stored over a long period of time can be deleted as well.
- HyPAS Function
  The MFP in which the TOE is installed, can be used by installing an application which makes daily operations more efficient. HyPAS function is the function that installs an application and activates it in the MFP. The application software that is installed is however, outside of the TOE scope.

1.4.3.2. Security Functions provided by the TOE

The TOE provides the following functions as the security function.

- Encryption Function
  There is an encryption function for a purpose of being against threats of leakage of the image data stored in the HDD.
  The encryption function is the function that encrypts and stores the image data when operating the basic functions such as the copy function, the network scan function, the print function and the document management box function, and when storing the image data in the HDD. The encryption function also reads out the image data by decrypting the encrypted image data when performing the above-mentioned basic functions, and when reading out the image data stored in

the HDD

A cryptographic key used for encryption is generated to be an identical and unique number on the MFP basis, every time each MFP is powered on, and is stored in a volatile memory. That is, the cryptography key is not stored inside the MFP in a state that power of the MFP is turned off.

- Overwrite-erase Function
  In addition to the logical and conventional deletion process, there is the overwrite-erase function for a purpose of further enhancing security.
  The overwrite-erase function is the function that logically deletes not only the management information of the stored image data in the HDD, but also entirely overwrites and erases the actual image data area so that it disables re-usage of the data when receiving an instruction for deletion of the stored image data in the HDD after process of the basic functions such as the copy function, the network scan function, the print function and the document management box function is completed, or after the cancellation made by cancel operation during these processing are completed.

1.4.4. Guidance

Guidance comprising this TOE is shown as below.

Type	Name	Version	Destination
User Manual	Data Security Kit (E) Operation Guide	Rev.2 2010.8	Japan
	Data Security Kit (E) Operation Guide	Rev.2 2010.8	Overseas
	Notice	303MS56320 2010.1	Japan/Overseas
	Data Security Kit (E) Operation Guide Set-Up Edition	303MS56710 2008.12	Japan/Overseas
	TASKalfa 250ci/300ci/400ci/500ci/552ci Operation Guide	302KY56010 Rev.1 2009.11	Japan
	250ci/300ci/400ci/500ci/552ci Operation Guide	302KY56040 Rev.1 2009. 11	Overseas
	CDC 1725/DCC 2725 CDC 1730/DCC 2730 CDC 1740/DCC 2740 CDC 1840/DCC 2840 CDC 1850/DCC 2850 Operation Guide	302KY56160 First Edition 2009. 12	Overseas
Service Manual	TASKalfa 552ci Service Manual	2KYSM001 Rev.1 2010.7	Japan
	TASKalfa 552ci Service Manual	2KYSM061 Rev.1 2010.7	Overseas

1.4.5. Assets Protected by the TOE

A common MFP temporarily stores the data in the storage area before operating the function of copy, print and network scan. After the job is completed, the data will be deleted. The management area is however, only logically deleted. Thus either during the operation of each function, or in the event that real-time processing (output) can not be done due to a printer being out of paper, etc., the image data stays stored in the HDD, and even after the processing is completed, the actual data area will remain as residual information. The residual information, as well as the temporary stored image data, contains the identical data as the data processed by the each function. Therefore, it is potentially possible for the entire

data to be stolen if the HDD is pulled out from the MFP.

Thus, the assets that should be protected by the TOE are described as follows:

- Residue data

  Remaining data after image data stored in the HDD temporarily or for a long period of time is logically deleted from the HDD.

- Temporary stored data

  Image data that is temporarily stored in the HDD when operating the copy, print and network scan functions.

The above-mentioned data is stored in the image data file in the HDD.

2. CONFORMANCE CLAIMS

2.1. CC Conformance Claims

This ST and TOE conform to the following evaluation standards for information security (CC):

Part 1: Introduction and general model, Version 3.1 Japanese Translation revision 1.2, dated March 2007,

Part 2: Security functional requirements, Version 3.1 Japanese Translation revision 2.0, dated March 2008

Part 3: Security assurance requirements, Version 3.1 Japanese Translation revision 2.0, dated March 2008

The security functional requirements of this ST conform to CC Part 2.
The security assurance requirements of this ST conform to CC Part 3.

2.2. PP Claims

There is no applicable Protection Profile.

2.3. Package Claims

This ST conforms to EAL 3.

2.4. Conformance Rationale

There is no applicable PP rationale since this ST does not conform to PP.

3. SECURITY PROBLEM DEFINITION

This chapter describes threats, organizational security policies and assumptions.

3.1. Threats

Threats to the TOE are identified as follows. The level of the attacking capability of the attackers assumed for this TOE is at a low level.

T.RESIDUAL : Unauthorized access to the residue data

Attackers may remove the HDD and be unauthorized to recover, decode, read out and steal the remaining data in the HDD even after deletion of the image data by using the tools that are easily available.

T.TEMP : Unauthorized access to the temporary stored data

Attackers may remove the HDD and be unauthorized to read out and steal the image data temporarily stored in the HDD by using the tools that are easily available.

3.2. Organizational Security Policies

There is no organizational security policy the TOE must comply with.

3.3. Assumptions

The assumptions for the TOE are described as follows:

A.LOCATION : Safe security of the TOE in the operational environment

To protect the hardware inside the MFP from being possibly attacked (i.e. violating the TOE security), it is assumed that the TOE operates in mutually watchable and manageable environment. Regarding the attacking to the hardware, it is assumed that the attacker opens up the MFP to make it connect to devices for analyzing or replacing the MFP board.

A.NETWORK : Safety of the TOE from the external network

It is assumed that the TOE is used by connecting to the internal network that is protected against unauthorized access from the external network.

A.CE : The service person reliability

It is assumed that the service person is a reliable person and does not act

unfaithfully.

4. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE, the security objectives for the operational environment and the security objectives rationale.

4.1. Security Objectives for the TOE

The security objectives for the TOE are described as follows:

O.REMAIN : Overwrite-erase of the residue data

The TOE must ensure that any previous information content of a resource (the actual data area) is made unavailable upon the deallocation of the resource from the image data file stored in the HDD.

O.ENCRYPT : Prevention of the stored data from being decoded

The TOE must ensure that the image data stored in the HDD is encrypted and is not illegally decoded.

4.2. Security Objectives for the Operational Environment

The security objectives to be implemented by the TOE operational environment are described as follows:

OE.LOCATION : Protection of the TOE and assets in the environment

The MFP must operate under control in mutually watchable environment and the hardware in the MFP must be protected from analyzing and alteration.

OE.NETWORK : Prevention of the TOE from the external network

The TOE-connected internal network must prevent the attacks from the external network by placing the devices such as the firewall etc.

OE.CE. : Confirmation of the service person

When the service person performs maintenance on the TOE, confirmation must be made if the person is an authorized service person.

4.3. Security Objectives Rationale

The corresponding relations between assumptions, threats and organizational security policies, and security objectives are shown in the table below. It indicates

that the security objectives correspond to at least one of assumptions, threats and organizational security policies.

Table 4.1 Correspondences between threats and organizational security policies, and security objectives

Treats/Organizational Security Policies / Security Objectives	T.RESIDUAL	T.TEMP	A.LOCATION	A.NETWORK	A.CE
O.REMAIN	X				
O.ENCRYPT		X			
OE.LOCATION			X		
OE.NETWORK				X	
OE.CE					X

"Table 4.1 correspondences between threats and organizational security policies, and security objectives" rationale is described below.

T.RESIDUAL

To counter the threat of T.RESIDUAL, it is necessary to disable recovery, decoding and reading out of the information of the stored residue data in the HDD. This threat can be countered by O.REMAIN. It is ensured that any previous information in the area being released from the resource allocation of the stored image data file in the HDD can not be reused so that the residue data can be protected from being recovered, decoded and read out.

T.TEMP

To counter the threat of T.TEMP, it is necessary to disable reference and output of the information of the temporary stored image data. This treat can be countered by O.ENCRYPT. It is ensured that the stored image data in the HDD is encrypted and is not decoded except being decrypted by using the identical encryption key so that the image data can be protected from being referenced and outputted.

A.LOCATION

The assumption of A.LOCATION requires that the TOE operates under control in mutually watchable environment to prevent the hardware inside the MFP from the TOE security breach. The purpose is to restrict the attack methods and the attack chances in order to protect the hardware in the MFP from unauthorized analysis and alteration. By OE.LOCATION, the MFP operates under control in mutually watchable environment and the MFP is defended against the attacks to the hardware inside the MFP such as analyzing and alternation to the hardware so that the attack methods and the attack chances are restricted and then A.LOCATION can be achieved.

A.NETWORK

The assumption of A.NETWORK requires that the TOE is connected to the internal network protected from unauthorized access via the external network. The purpose is to prevent the TOE from access by uncertain number of unauthorized persons in order to restrict the attack methods and the attack possibilities by uncertain number of unauthorized agents through the external network. By OE.NETWORK, the TOE-connected internal network has the devices such as firewall to defend the attacks to the TOE against the access from the external network so that the attack methods and the attack possibilities by uncertain number of threat agents from the external network are restricted and then A.NETWORK can be achieved.

A.CE

The assumption of A.NETWORK requires that the service person who performs maintenance on the TOE is reliable person. The purpose is that the service person who performs maintenance on the TOE does not act unfaithfully. By OE.CE, when the service person performs maintenance on the TOE, confirmation will be made if the person is the authorized service person so that the service person who performs maintenance on the TOE will be restricted as the person who does not act unfaithfully. Then A.CE can be achieved.

5. EXTENDED COMPONENTS DEFINITION

Extended components are not defined.

6. SECURITY REQUIREMENTS

This chapter describes the TOE security requirements.

6.1. TOE Security Functional Requirements

FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: list of standards]
- *Kyocera Mita's Standard*

[assignment: cryptographic key generation algorithm]
- *Kyocera Mita's standard cryptographic key generation*

[assignment: cryptographic key sizes]
- *128 bits*

FCS_COP.1　Cryptographic Operation

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

FCS_COP.1.1　The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment:cryptographic algorithm] and cryptographic key sizes [assignment:cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: list of standards]
- FIPS PUB 197

[assignment: cryptographic algorithm]
- AES

[assignment: cryptographic key sizes]
- 128bits

[assignment: list of cryptographic operations]
- encryption of the image data when writing into the HDD.
- decryption of the image data when reading out from the HDD.

FDP_RIP.1　Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.1.1　The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: list of objects].

[assignment: list of objects]
- *image data file stored in the HDD*

[selection: allocation of the resource to, deallocation of the resource from]
- *deallocation of the resource from*

6.2. TOE Security Assurance Requirements

The evaluation assurance level of the TOE is EAL3 and the evaluation assurance level of the TOE is EAL3.

Table 6.1 TOE Security Assurance Requirements

Class	Component Name (Including Family)	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.3	Authorization Controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	ALC_LCD.1 Developer defined life-cycle model
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.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	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. Security Functional Requirements Rationale

The correspondences between security objectives and TOE security functional requirements are shown below.

Table 6.2 Correspondences between security objectives and TOE security functional requirements

Type	Security Objectives / TOE Security Functional Requirements	O.REMAIN	O.ENCRYPT
TOE Security Functional Requirements	**FCS_CKM.1**		**X**
	FCS_COP.1		**X**
	FDP_RIP.1	**X**	

"Table 6.2 Correspondences between security objectives and TOE security functional requirements" rationale is described below.

O.REMAIN

It is ensured that any previous information content of a resource is made unavailable upon the deallocation of the resource from the image data file stored in the HDD in accordance with FDP_RIP.1 Subset residual information protection. Therefore O.REMAIN can ensure that the residue data shall not be reused.

O.ENCRYPT

It can be ensured that the image data stored in the HDD is encrypted in accordance with FCS_COP.1 cryptographic operation policy. To accomplish FCS_COP.1, it is ensured that a cryptographic key enabling encryption is generated according to FCS_CKM.1. At this time, the cryptographic key is generated every time power is turned on, using the Kyocera Mita's standard cryptographic key generation algorithm.

Therefore O.ENCRYPT can ensure that the stored data shall not be illegally decoded.

6.3.2. Dependent Relations between TOE Security Functional Requirements

The dependent relations between the TOE security functional requirements are shown below.

Table 6.3 Dependent relations between TOE security functional requirements

No	TOE Security Functional Requirements	Hierarchical	Dependent Relations	Reference No.	Note
1	**FCS. CKM.1**	None	FCS_COP.1 FCS_CKM.4	2 Not needed	 Refer to 6.3.2.1
2	**FCS_COP.1**	None	FCS_CKM.1 FCS_CKM.4	1 Not needed	 Refer to 6.3.2.1
3	**FDP_RIP.1**	None	None	—	

6.3.2.1.Rationale for why dependency on FCS_CKM.4 is not needed

The cryptographic key is generated when the main power is tuned on, and is stored for encryption operation that is to read and write the image data on the HDD while the power is turned on. Beside this purpose, there is no interface available to allow unauthorized users to get access. Thus the requirement for the cryptographic key destruction is not needed.

6.3.3. Rationale for Security Assurance Requirements

Since this TOE aims to counter the threats from low level attackers to access image data, the TOE is required to ensure the counter-measure against the low level attacks. EAL3 includes analysis of the security measures of the TOE at development phase (performing and analyzing systematic tests, and evaluating the management of the development environment and the developed products) and also includes analysis whether the sufficient guidance information is included so that the security can be used safely. The assurance requirement conforms to EAL3. Thus selection of EAL3 is reasonable.

7. TOE SUMMARY SPECIFICATION

This chapter describes the summary specification for the security functions that are provided by the TOE.

Table 6.1 shows the relations between the TOE security functions and the security functional requirements.

Table 7.1 TOE security functions and security functional requirements

Security Functions / Functional Requirements	TSF.ENCRYPT	TSF.AGAIN
FCS_CKM.1	**X**	
FCS_COP.1	**X**	
FDP_RIP.1		**X**

7.1. Encryption Function

TSF.ENCRYPT

Encryption function is the function that performs the basic functions such as the copy function, the network scan function, the print function and the management document box function, and encrypts image data when storing the image data in the HDD.

(1) FCS_CKM.1 Cryptographic Key Generation

The TOE generates a 128-bit cryptographic key to be used in the AES algorithm by using the Kyocera Mita's standard cryptographic key generating algorithm. The key is generated based on an identical and unique number on the MFP basis, every time each MFP power is turned on, and is kept in a volatile memory. However, information for the cryptographic key is set only when starting operation, and shall not be changed during the operation.

(2) FCS_COP.1 Cryptographic Operation

When storing image data in the HDD, the TOE encrypts the image data, using the 128-bit cryptographic key generated at the time of booting (FCS_CKM.1) and the

AES encryption algorithm based on FIPS PUBS 197, and write into the HDD. When reading out the stored image data from the HDD, the TOE decrypts the image data, similarly using the 128-bit cryptographic key generated at the time of booting and the AES encryption algorithm.

7.2. Overwrite-erase Function

TSF.AGAIN

Overwrite-erase function is the function that overwrites on the actual image data area with meaningless character strings when receiving an instruction for deletion of the stored image data in the HDD after jobs of the basic functions such as the copy function, the network scan function, the print function and the document management box function are completed or after the cancelation made by cancellation operation during these processing, and that disables re-usage of the data after the management information of the image data is erased subsequent to complete deletion of the actual data area.

(1) FDP_RIP.1 Subset Residual Information Protection

The TOE stores the used image data to be overwritten and erased in the specific area on the HDD, and then conducts to overwrite and erase by the process of auditing it. When receiving an instruction for operation of another basic function and so when waiting for the overwrite-erase function to be performed, or when the existence of the used image data is found because of turning off the power during overwrite-erase processing, the overwrite-erase shall be conducted by the audit process at the time of coming out of the waiting status or at the time of turning on the power.

8. ACRONYMS AND TERMINOLOGY

8.1. Definitions of terms

The definitions of the terms used in this ST are indicated in Table 8.1.

Table 8.1 Definitions of terms used in this ST

Terms	Definitions
Image data	It indicates the image information that is processed inside the MFP when TOE users use copy function, network scan function, print function and document management box function.
Temporary storage	Keeping the received image data temporarily on the HDD without outputting it or forwarding it as is, or keeping the image data temporarily on the HDD during the image processing. This is executed automatically during the process of the MFP without the users being conscious about it. This should be compared to long period storage.
Long period storage	Keeping the image data on the HDD. The users will have to consciously conduct the storage operation for this storage. This should be compared to temporary storage.
Client PC	It indicates the computers that connect to the network, and utilize the TOE services (functions) of the TOEs that are connected to the network.
Network scan	A function to transmit the scanned image data or the stored image data in the document management box, to the client PCs. There is PC transmission that transmits them via the LAN, e-mail transmission that transmits them via e-mails, and a TWAIN function that captures images of the originals by operations from the client PC.
Management area	An area within the image data where management information for that data is recorded. A logical deletion of image data means making this area unrecognizable.

Actual data area	An area within the image data where data composing the actual image is recorded. When image data is logically deleted, this area will remain. This remaining area will be called "residue area".
Overwrite-erase	This is to overwrite on the actual image data area with meaningless character strings when receiving an instruction for deletion of the stored image data in the HDD, and to delete the management information of the image data after the actual data area is completely erased. Thus it disables re-usage of the data.
Operation panel	This is installed on the uppermost part of the MFP, and is constituted by a liquid crystal panel. It is an external interface, and users can utilize the TOE via this operation panel.

8.2. Definitions of acronyms

The definitions of the acronyms used in this ST are indicated in Table 8.2.

Table 8.2 Definitions of acronyms used in this ST

Acronyms	Definitions
CC	Common Criteria
ST	Security Target
EAL	Evaluation Assurance Level
SFR	Security Functional Requirement
SAR	Security Assurance Requirement
TOE	Target of Evaluation
TSF	TOE Security Function
AES	Advanced Encryption Standard
EEPROM	Electronically Erasable Programmable ROM
HDD	Hard Disk Drive
MFP	Multi Function Printer
USB	Universal Serial Bus