SHARP

AR-FR24

Security Target

Version 0.06

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

SHARP CORPORATION

Revision history

Date	Ver.	Revision	Author	Reviewed	Approved
2007-03-14	0.01	• Original Draft	Nakagawa	Iwasaki	Kubota
2007-06-29	0.02	• Modified part of Sections 5.1.1.4, 8.3.1.10 and 8.3.1.11. (in response to Observation Reports ASE001-01 and ASE002-01)	Nakagawa	Iwasaki	Kubota
2007-07-17	0.03	• Modified part of Sections 5.1.1.4, 8.2.2 and 8.3.1.11. (in response to Observation Reports ASE002-01) • Modified descriptions in Sections 1.5.2, 2.2.1, 2.2.2 and 2.3.	Nakagawa	Iwasaki	Kubota
2007-08-01	0.04	• Modified descriptions in Section 2.2.2.	Nakagawa	Iwasaki	Kubota
2007-08-31	0.05	• Modified descriptions in Section 6.3.	Nakagawa	Iwasaki	Kubota
2007-09-19	0.06	• Modified part of Sections 6.3 and 8.3.2.	Nakagawa	Iwasaki	Kubota

© 2007, Sharp Corp., all rights reserved.

Table of Contents

© 2007, Sharp Corp., all rights reserved.

© 2007, Sharp Corp., all rights reserved.

List of Tables

List of Figures

© 2007, Sharp Corp., all rights reserved.

1 Security Target Introduction

1.1 ST Identification

This section provides information needed to identify this security target (ST) and the target of CC evaluation (TOE).

ST Title:	AR-FR24 Security Target
ST Version:	0.06
Publication Date:	2007-09-19
Author:	Sharp Corporation
TOE Identification:	AR-FR24 VERSION M.10
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 — also known as ISO/IEC 15408:2005
ST Evaluator:	Japan Electronics and Information Technology Industries Association, IT Security Center
Keywords:	SHARP, SHARP Corporation, Digital Multifunction Device, Multifunction Device, Multifunction Printer, MFP, MFD, encryption, data encryption, data clearing

1.2 ST Overview

This ST explains about the above TOE, i.e., AR-FR24.

A Multi Function Device (hereafter referred to as “MFD”) is an office machine for sale which has functions such as copy, printer, image scanning and fax. The TOE is an optional product sold separately to strengthen the data security function of the MFD made by Sharp Corporation. The TOE is intended to counter attempts to steal image data spooled in storage devices in a MFD.

The main security function of this TOE is as follows. This ST describes them.

- Encryption of the image data
- Erasure of the image data by overwriting when the data is deleted.

1.3 CC Conformance Claim

This ST satisfies the followings:

a) CC Version 2.3, Part 2 Conformant

b) CC Version 2.3, Part 3 Conformant

c) EAL3 Augmented with ADV_SPM.1

d) With Interpretations-0512

e) Conformant to no PP

1.4 Reference Materials

The materials listed in Table 1-1 have been referred to prepare this ST. Hereafter references to [CC_PART1], [CC_PART2] and [CC_PART3] shall be interpreted as being modified by [CC_INTPR], unless otherwise noted.

© 2007, Sharp Corp., all rights reserved.

Table 1-1: Reference Materials

Identifier	Title
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3, CCMB-2005-08-001. (Japanese Version 1.0, December 2005)
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3, CCMB-2005-08-002. (Japanese Version 1.0, December 2005)
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3, CCMB-2005-08-003. (Japanese Version 1.0, December 2005)
[CC_INTPR]	Interpretations-0512, dated December 2005, Information Security Certification Office, IT Security Center, Information-technology Promotion Agency, Japan

1.5 Conventions, Terminology, and Acronyms

This section identifies the conventions and defines the terminology and acronyms used in this ST.

1.5.1 Conventions

This section describes the conventions used in this ST.

The following conventions are used to distinguish text with special meaning.

a) *Plain italicized text* is used to emphasize text.

The following conventions are used to express the use of operations that are allowed for the CC functional and assurance components.

b) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. One or more assignment values are shown in brackets []. The parameter name is indicated in parentheses ( ) after each value unless the name is self-evident.

c) The refinement operation is used to add detail to a component, and thus further restricts the TOE. Additional text is indicated in bold. Deleted text is indicated in parentheses ( ).

d) The selection operation is used to select one or more options when multiple options are provided in a component. Selections are underlined and shown in brackets [].

e) Iteration is used to cover different aspects of the same requirement. An iteration number inside parentheses ( ) is appended to the component name, short name, and element name as a unique identifier.

1.5.2 Terminology

Terminology unique to this document is defined in Table 1-2. Acronyms used in this ST are indicated in Table 1-3.

Table 1-2: Terminology

Term	Definition
Auto Clear at Job End	The function that clears (by overwriting) image data of each job stored in some MSD of the MFD, invoked when a job is finished or cancelled.
Board	A printed circuit board on which components are mounted by soldering.
Clear All Memory	The function to overwrite the all image data that is stored to the MSD in the MFD. This function is invoked by the operation of the key operator.
Engine	A device that forms print images on receiver papers, with mechanism of paper feeding/ejection. Also called as “print engine” or “engine unit”.
FAX board	One of the units of an MFD that can be equipped with the TOE. It provides the fax function. Support for the FAX board is the standard, optional or unavailable depending on the MFD model.
FAX_RAM	The RAM on the FAX board. A volatile memory.
FAX_ROM	The ROM on the FAX board. It is provided physically as part of the TOE.

© 2007, Sharp Corp., all rights reserved.

Term	Definition
Firmware	The software that is embedded to the machines to control the machine's hardware. In this document, firmware especially indicates the controller firmware.
Flash memory	A type of non-volatile memory that allows the entire memory to be erased at once and also allows rewriting to any part of memory.
GDI board	One of the units of an MFD that can be equipped with the TOE. It is equipped with USB and parallel I/F and provides part of the print function. It is included in some of the MFD models which do not contain the PCL board.
Image data	Digital data, especially in this document, of two-dimensional image that each function of the MFD manages.
IMC board	One of the units of an MFD that can be equipped with the TOE. It is provided physically as part of the TOE. It provides the image processing function.
IMC_RAM	The RAM on the IMC board. A volatile memory.
IMC_ROM	The ROM on the IMC board. It is provided physically as part of the TOE.
Job	The sequence from beginning to end of the use of an MFD function (copy, print, scan send and fax). In addition, the instruction for a functional operation is sometimes called a job.
Key operator	An authorized user who is allowed to access the security management function and MFD management function of the TOE.
Key operator code	A password used for authentication of the key operator.
Key operator program	The TOE security management function. It also provides the MFD management function. To access the key operator programs, identification and authentication of the key operator shall be successful.
MCU board	One of the units of an MFD that can be equipped with the TOE. It provides the control function of the entire MFD.
MCU_RAM	The RAM on the MCU board. A volatile memory.
MCU_ROM	The ROM on the MCU board. It is provided physically as part of the TOE.
Memory	A memory device; in particular a semiconductor memory device.
Non-volatile memory	The memory device that retains its contents even when the power is turned off.
Operation panel	The user interface unit in front of the MFD. This contains the start key, numerical key, function key and liquid crystal display with touch operation system.
PCL board	One of the units of an MFD that can be equipped with the TOE. It is equipped with NIC, USB and parallel I/Fs and provides the print and scan send functions. Support for the PCL board is the standard, optional or unavailable depending on the MFD model.
PCL_RAM	The RAM on the PCL board. A volatile memory.
PCL_ROM	The ROM on the PCL board. It is provided physically as part of the TOE.
Scanner unit	The device that scans the original and gets the image data. This is used for copy, scan send or fax transmission.
Spool	Storing the job's image data to the MSD temporary to increase the input and output efficiency.
Unit	A substance provided standard that can be attached to or detached from a printed circuit board; or an option that is installed and is ready for operation. This can also be a system that includes a mechanism and is ready for operation.
Volatile memory	A memory device, the contents of which vanish when the power is turned off.

© 2007, Sharp Corp., all rights reserved.

Table 1-3: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard, established by NIST (National Institute of Standards and Technology, United States of America)
EEPROM	Electrically Erasable Programmable ROM, a type of non-volatile memory that allows low frequency of electrical rewriting at any address.
I/F	Interface
MSD	Mass Storage Device, in this document, this especially indicates the IMC_RAM, PCL_RAM and Flash memory in MFD.
NIC	Network Interface Card, or, Network Interface Controller
RAM	Random Access Memory, memory capable of being read and written randomly.
ROM	Read Only Memory
UI	User Interface
USB	Universal Serial Bus, a serial bus standard to connect between IT equipments.

© 2007, Sharp Corp., all rights reserved.

2 TOE Description

2.1 TOE Overview

2.1.1 TOE Type

The TOE is an IT product and firmware for the MFD that is stored to the ROM. By replacing the MFD standard firmware, it offers the security function and controls the entire MFD.

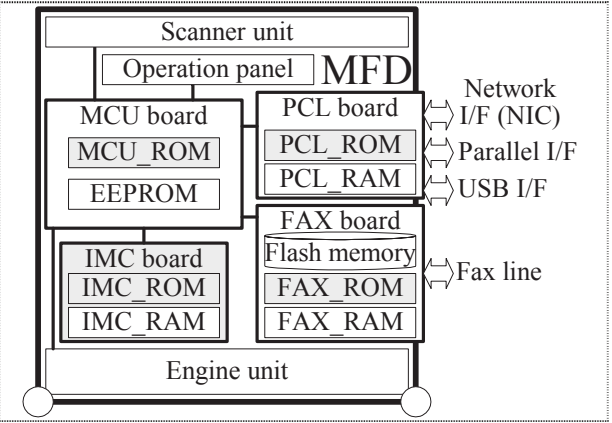

Figure 1: TOE and physical configuration of the MFD

2.1.2 Overview of the TOE Security Functions

The main security functions of the TOE are the cryptographic operation function and the data clear function. These functions are intended to prevent the disclosure of information from actual image data remaining in the TOE-equipped MFD.

The cryptographic operation function encrypts actual image data before it is spooled to the Flash memory when the MFD processes each fax job.

The data clear function writes random values or a fixed value over data areas where spooled actual image data is contained after each of the copy, print, scan send and fax jobs is finished.

2.2 TOE Configuration

This section describes the physical and logical configuration of the TOE.

2.2.1 Physical Configuration of the TOE

Figure 1 shows the physical configuration of the MFD with the TOE shaded. The physical scope of the TOE is as follows:

- MCU firmware: Firmware that controls the MCU board, which is contained in the MCU_ROM on the MCU board.
- IMC firmware: Firmware that controls the IMC board, which is contained in the IMC_ROM on the IMC board.
- PCL firmware: Firmware that controls the PCL board, which is contained in the PCL_ROM on the PCL board.
- FAX firmware: Firmware that controls the FAX board, which is contained in the FAX_ROM on the FAX board.

The TOE is provided by the MCU_ROM, PCL_ROM, FAX_ROM and IMC board. The MFD in which the TOE has not been installed yet contains the firmware which does not provide the security function. To install the TOE, the MCU_ROM and IMC board in the MFD shall be removed and replaced with the TOE part. When the MFD contains the PCL board or FAX board, the ROMs on them shall be replaced.

The TOE can be used on the following Sharp MFDs: AR-267FG, AR-267FP, AR-267G, AR-267S, AR-5625, AR-M256, AR-M257, AR-M257J and AR-M258.

2.2.2 Logical Configuration of the TOE

Figure 2 shows the logical configuration of the TOE. The thick-lined frame indicates the logical scope of the TOE. Rounded boxes indicate hardware devices that are out of the TOE. Rectangles indicate functions of the TOE; and ones shaded indicate security functions. Arrows in the figure indicate data flows.

© 2007, Sharp Corp., all rights reserved.

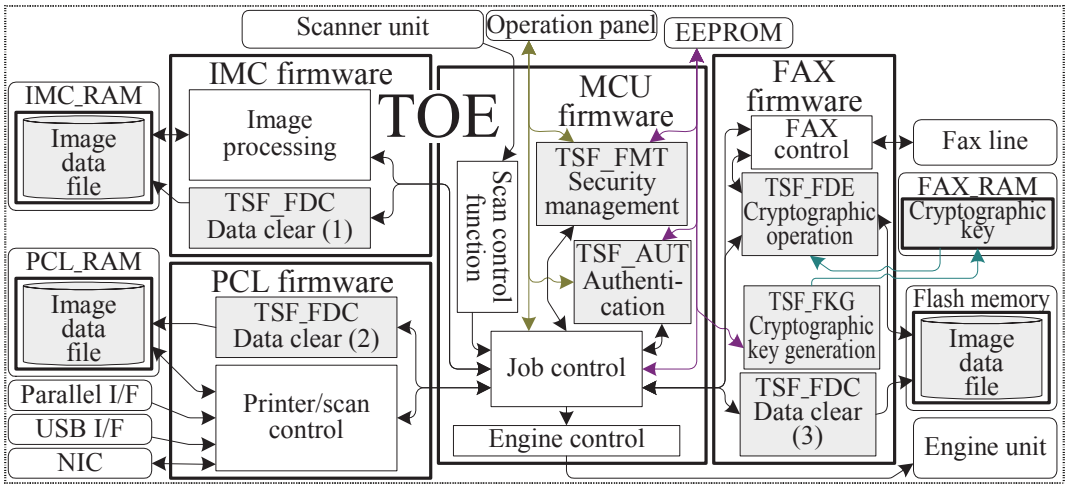

Figure 2: Logical configuration of the TOE

The TOE is firmware for the MFD. It provides security functions, while controlling the entire MFD. The logical scope of the TOE includes the following functions:

a) Cryptographic operation function (TSF_FDE): encrypts actual image data generated by the fax function, and then spools it to the Flash memory to store as image files. Moreover, the function reads and decrypts to use the actual image data spooled to the Flash memory.

b) Cryptographic key generation function (TSF_FKG): generates the cryptographic key for encryption and decryption provided by the cryptographic operation function. This function stores the generated key in the volatile memory (FAX_RAM).

c) Data clear function (1), data clear function (2) and data clear function (3) (TSF_FDC): overwrites the actual image data in the MSD when each of the copy, print, scan send and fax jobs is finished or cancelled (Auto Clear at Job End). This function also overwrites all actual image data in the MSD by the operation of the key operator (Clear All Memory).

d) Authentication function (TSF_AUT): identifies and authenticates a key operator (administrator) by means of the key operator code (a password).

e) Security management function (TSF_FMT): provides a function to change (modify) the key operator code after key operator authentication is successful.

f) Engine control function: controls the engine unit during copy job, print job and fax reception job.

g) Scan control function: controls the scanner unit during copy job, scan send job, and fax transmission job for scanning of an original.

h) Printer/scan control function: This function can operate on an MFD that can be equipped with the TOE and that has the PCL board standard or as an option.

- During a print job, this function creates a bitmap image for printing from the print data received through the network, USB or parallel interface.
- During a scan send job, this function converts the actual image data obtained by scanning into the specified format and transmits it through the network interface over the network.

i) Fax control function: Controls transmission over the FAX line for a PC-Fax or fax transmission job, and reception from the FAX line for a fax reception job.

j) Image processing function: Performs image processing for printing using special functions of the MFD.

k) Job control function: controls behavior of the MFD while it processes each of the copy, print, scan send and fax jobs.

© 2007, Sharp Corp., all rights reserved.

2.3 Overview of the MFD Functions and Applications

As well as the standard MFD firmware, the TOE has the following MFD functions: copy, print, scan send, and fax. The TOE executes a part of the TOE security functions (TSF) automatically while each of these MFD functions is being executed. This property of the TOE protects even a user with no knowledge or awareness about the TOE security functions. The usage environment of the MFD that the TOE is installed to is shown in Figure 3.

Each MFD function of the TOE is explained below. Most functions are available on the operation panel of the MFD. Some functions run when the MFD receives data. Moreover, some functions are available on the TOE Web, which is a Web site that the TOE serves for remote operation.

Each of the following functions receives the image data from the MFD's scanner unit or from outside of the MFD, spools the image data to the MSD in the MFD, and sends the image data to the MFD's engine unit (printing) or to the outside of the MFD (transmission).

a) Copy function: reads the original and prints that image by the operation from the operation panel.

b) Print function: prints the data received from outside of the MFD by way of the following means.
- Printer drivers: are installed on the clients for the MFD, and generate print data by the user's operation. The print data come to the MFD via the network, the USB, or the parallel I/F.
- E-mails: have print data as attached files, and come to the MFD via the network.
- Web: that is, the web page of "Submit Print Job", provided by the TOE for remote control, accepts files uploaded from clients via the network.

c) Scan send function: scans an original to obtain image data through operations on the operation panel, and transmits the image data file in either of the following ways:
- E-mail: transmits it as an attachment to an E-mail.
- File server: transmits it to an FTP server.
- Desktop: transmits it via FTP to a client (The MFD bundle software is required.)

d) Fax function: transmits and receives faxes through the telephone line.
- Fax transmission function: scans an original to obtain image data through operations on the operation panel, and transmits the image data as a facsimile.
- Fax reception function: receives a facsimile from another fax machine and prints it.
- PC-Fax function: transmits image data from a client as a facsimile. This function is also described as PCFAX.

Support for the FAX and PCL boards is the standard, optional or unavailable depending on the MFD model. The FAX board is necessary to perform the fax function and the PCL board is necessary for the scan send function. If a GDI board (not included in the TOE), instead of the PCL board, is installed, it is possible to process print jobs received from a USB or parallel I/Fs although the scan send function is not available.

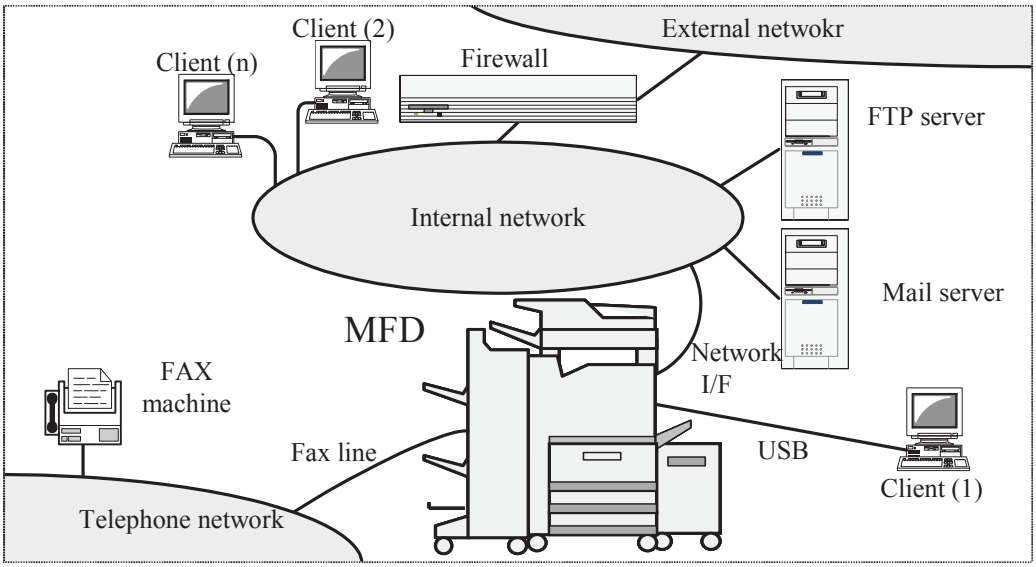

Figure 3: Usage environment of the MFD

© 2007, Sharp Corp., all rights reserved.

2.4 Assets Protected by the TOE

When the user uses the MFD, the MFD itself holds the image data file in a volatility memory or the Flash memory in MFD when each job, such as a copy, print, scan send, or fax is completed or when each job are cancelled. Assets protected by the TOE are the actual image data that remains after the data has deleted for the allocation release of the resource.

The explanation of actual image data is shown in the Figure 4. Image data consists of control area and actual image data. On the other hand, actual image data file is an object that is handled by the file system controlling the image, and the actual image data itself.

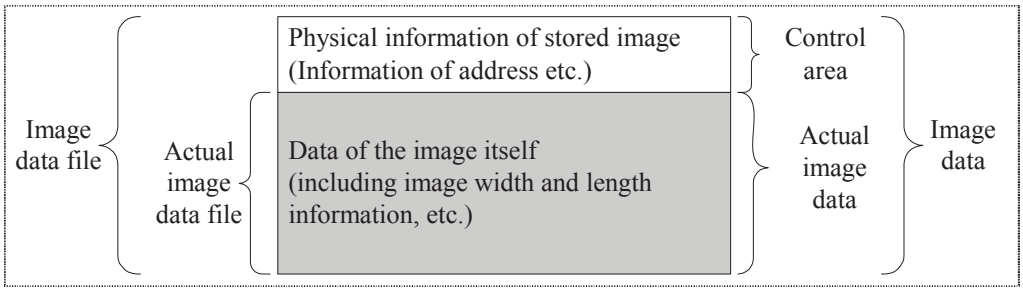

Figure 4: Illustration of the actual image data

The purpose of the TOE is to prevent the disclosure of information from residual actual image data (protected assets by the TOE) due to an attacker possessing a low level attack potential.

The assets stored in the volatile memory are not the subject of attack because low-level attackers can not read them out.

© 2007, Sharp Corp., all rights reserved.

3 TOE Security Environment

3.1 Assumptions

Use and operation of the TOE requires the environment described in Table 3-1.

Table 3-1: Assumptions

Identifier	Definition
A.OPERATOR	The key operator is a trustworthy person who does not take improper action with respect to the TOE.

3.2 Threats

Threats to the TOE are described in Table 3-2.

Table 3-2: Threats

Identifier	Definition
T.RECOVER	A low-level attacker will disclose information through the use of a device other than the MFD to read actual image data remained in the flash memory in MFD.

3.3 Organisational Security Policies

Organisational security policies are described in Table 3-3.

Table 3-3: Organisational Security Policies

Identifier	Definition
P.RESIDUAL	Upon completion or interruption of each of the copy, print, scan send or fax jobs, the actual image data area spooled to the MSD shall be overwritten. When the MFD is disposed of or its ownership changes, all areas to which actual image data is spooled shall be overwritten by the key operator operation.

© 2007, Sharp Corp., all rights reserved.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are shown in Table 4-1.

Table 4-1: Security Objectives for the TOE

Identifier	Definition
O.REMOVE	To make it impossible to display an image in the event that the Flash memory of a TOE-equipped MFD is read using a device other than the MFD that spooled the data, the TOE shall encrypt the actual image data using a cryptographic key unique to the MFD before spool in the flash memory.
O.RESIDUAL	The TOE shall overwrite the actual image data area spooled to the MSD when each of the copy, print, scan send or fax jobs is finished or cancelled. The TOE also shall perform overwriting of all image data areas of the MSD by the instruction of key operator.

4.2 Security Objectives for the Environment

The security objectives for the environment are shown in Table 4-2.

Table 4-2: Security Objectives for the Environment

Identifier	Definition
OE.ERASEALL	When the MFD is disposed of or its ownership changes, the key operator shall overwrite all data spooling areas of the MSD.
OE.OPERATE	Those in charge of the organisation that owns TOE-equipped MFDs shall understand the role of the key operator and select a suitable person with the utmost care.

© 2007, Sharp Corp., all rights reserved.

5 IT Security Requirements

5.1 TOE Security Requirements

This section describes the IT security requirements that the TOE and its environment shall satisfy.

5.1.1 TOE Security Functional Requirements

This section describes the Security Functional Requirements that the TOE shall satisfy, based on the classes of [CC_PART2]. The minimum strength of function for the TOE is defined in section 5.1.2.

5.1.1.1 Class FCS: Cryptographic Support

●FCS_CKM.1	Cryptographic key generation
Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [MSN-A expansion algorithm] and specified cryptographic key sizes [128 bits] that meet the following: [Data Security Kit Encryption Standard].
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_COP.1	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [● Encryption of actual image data to be spooled in the Flash memory ● Decryption of actual image data encrypted and spooled in the Flash memory] in accordance with a specified cryptographic algorithm [Rijndael Algorithm] and cryptographic key sizes [128 bits] that meet the following: [FIPS PUB 197].
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

5.1.1.2 Class FDP: User data protection

●FDP_RIP.1	Subset residual information protection
Hierarchical to:	No other components.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [● Actual image data files in IMC_RAM ● Actual image data files in PCL_RAM ● Actual image data files in Flash memory].
Dependencies:	No dependencies.

© 2007, Sharp Corp., all rights reserved.

5.1.1.3 Class FIA: Identification and authentication

●FIA_SOS.1	Verification of secrets
Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [the 5-digit number].
Dependencies:	No dependencies.

●FIA_UAU.2	User authentication before any action
Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification

●FIA_UAU.7	Protected authentication feedback
Hierarchical to:	No other components.
FIA_UAU.7.1	The TSF shall provide only [the number of characters that are provided] to the user while the authentication is in progress.
Dependencies:	FIA_UAU.1 Timing of authentication

●FIA_UID.2	User identification before any action
Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.

5.1.1.4 Class FMT: Security management

●FMT_MOF.1	Management of security functions behaviour
Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [enable, disable] the functions [Clear All Memory] to [key operator].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

●FMT_MSA.2	Secure security attributes
Hierarchical to:	No other components.
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
Dependencies:	ADV_SPM.1 Informal TOE security policy model [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

●FMT_MTD.1	Management of TSF data
Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to [modify, query] the [key operator code] to [key operator].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
●FMT_SMF.1	Specification of Management Functions

© 2007, Sharp Corp., all rights reserved.

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [Modify the key operator code].
	Note: Consideration for management requirement is described in section 8.2.2.
Dependencies:	No dependencies.

●FMT_SMR.1	Security roles
Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [key operator].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification

5.1.1.5 Class FPT: Protection of the TSF

●FPT_RVM.1	Non-bypassability of the TSP
Hierarchical to:	No other components.
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies:	No dependencies.

5.1.2 TOE Minimum Strength of Function

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

Among the functional requirements that this TOE satisfies, only FIA_SOS.1, FIA_UAU.2 and FIA_UAU.7 use a probabilistic or permutational mechanism, and the explicitly stated functional strength is SOF-basic. FCS_COP.1 is a functional requirement that uses a cryptographic algorithm, and thus does not apply to this SOF level.

5.1.3 TOE Security Assurance Requirements

Assurance components for the assurance level selected by this document are shown in Table 5-1. Table 5-1 shows the assurance requirements that shall be satisfied to claim EAL3+ADV_SPM.1 compliance.

Table 5-1: Assurance Requirements

Component	Component Name	Dependencies:
ACM_CAP.3	Authorization controls	ACM_SCP.1, ALC_DVS.1
ACM_SCP.1	TOE CM coverage	ACM_CAP.3
ADO_DEL.1	Delivery procedures	No dependencies
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.2	Security enforcing high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	No dependencies
ADV_SPM.1	Informal TOE security policy model	ADV_FSP.1
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ALC_DVS.1	Identification of security measures	No dependencies
ATE_COV.2	Analysis of coverage	ADV_FSP.1, ATE_FUN.1

© 2007, Sharp Corp., all rights reserved.

Component	Component Name	Dependencies:
ATE_DPT.1	Testing: high-level design	ADV_HLD.1, ATE_FUN.I
ATE_FUN.1	Functional testing	No dependencies
ATE_IND.2	Independent testing - sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_MSU.1	Examination of guidance	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

5.2 Security Requirements for the IT Environment

The security objectives for the environment do not require any security requirements for the IT environment of the TOE.

© 2007, Sharp Corp., all rights reserved.

6 TOE Summary Specification

This chapter describes the security functions and assurance measures performed by the TOE to meet the security requirements.

6.1 TOE Security Functions (TSF)

Table 6-1 shows the correspondences between the security functional requirements and the TOE security functions. The section number where each correspondence is described is shown in the table.

Table 6-1: Security Functional Requirements and TOE Security Specifications

Function Requirement	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT
FCS_CKM.1	6.1.1				
FCS_COP.1		6.1.2			
FDP_RIP.1			6.1.3		
FIA_SOS.1					6.1.5
FIA_UAU.2			6.1.3	6.1.4	
FIA_UAU.7			6.1.3	6.1.4	
FIA_UID.2			6.1.3	6.1.4	
FMT_MOF.1			6.1.3	6.1.4	
FMT_MSA.2	6.1.1				
FMT_MTD.1				6.1.4	6.1.5
FMT_SMF.1					6.1.5
FMT_SMR.1				6.1.4	6.1.5
FPT_RVM.1	6.1.1	6.1.2	6.1.3	6.1.4	6.1.5

6.1.1 Cryptographic key generation (TSF_FKG)

The TOE generates a cryptographic key (common key) to support the actual image data encryption function. When the MFD is powered on, a cryptographic key (common key) is always generated. The cryptographic key is generated as a 128-bit of secure key using MSN-A expansion algorithm which is the cryptographic key generation algorithm to execute the AES Rijndael encryption algorithm, based on the Data Security Kit Encryption Standards. The cryptographic key is stored in FAX_RAM.

6.1.2 Cryptographic operation (TSF_FDE)

During the processing of a PCFAX, fax transmission, or fax reception job, the actual image data of the job is always encrypted before being spooled to Flash memory on the FAX board. When the encrypted and spooled actual image data is processed (used) actually, it is always read and used after decrypting it. The actual image data is encrypted and decrypted using the AES Rijndael algorithm based on FIPS PUBS 197 and the 128 bits cryptographic key generated by TSF_FKG cryptographic key generation.

6.1.3 Data Clear (TSF_FDC)

The TOE provides the data clear function that clears spooled actual image data file. This function consists of the following two programs:

- Auto Clear at Job End:
  When a copy job or print job ends, the actual image data file for the job that was spooled to IMC_RAM is overwritten with random values.
  When a scan send job ends, the actual image data file for the job that was spooled to PCL_RAM is overwritten with random values.
  When a PCFAX, fax transmission, or fax reception job ends, the actual image data file for the job that was spooled to Flash memory is overwritten with fixed values.

© 2007, Sharp Corp., all rights reserved.

- Clear All Memory:
  To execute and cancel Clear All Memory, identification and authentication of the key operator is required.
  When invoking Clear All Memory, after being identified and authenticated as the key operator, all actual image data that are used for spooling to IMC_RAM and PCL_RAM are overwritten with random values, and all actual image data that are used for spooling to Flash memory on the FAX board are overwritten by fixed values.
  To cancel Clear All Memory, key operator identification and authentication by entry of the key operator code are required following selection of the cancel operation. While the key operator code is being entered, the TOE hides the entered digits and instead shows each entered digit as an asterisk "*" to indicate the number of digits entered. The key operator code is managed in EEPROM as authentication data for comparison with the inputted data, and the key operator identification/authentication functions and code entry hidden feedback function are always executed, so that cancellation of Clear All Memory is only possible when the user is identified and authenticated as a key operator.

The timing of Auto Clear at Job End and Clear All Memory is managed so that it is executed at job end or at the instruction of Clear All Memory. And Auto Clear at Job End and Clear All Memory always enforced.

The random value used to overwrite the IMC_RAM and PCL_RAM are generated based on the cyclical delay Fibonacci algorithm.

6.1.4 Authentication (TSF_AUT)

The TOE always requires key operator identification and authentication before the key operator programs (TOE security management functions) can be used. This specifies key operator and associates the role of key operator with a user. The key operator identification and authentication function requires that the key operator select the key operator programs and then input the key operator code. While the key operator code is being entered, the TOE hides the entered digits and shows each entered digit as an asterisk "*" to indicate the number of digits entered. The key operator identification/authentication functions and code entry hidden feedback function are always executed, so that operation of the key operator programs is only possible when the user is identified and authenticated as a key operator.

Clear all memory, which is a data clear function (TSF_FDC), and query and change of the key operator code, which are security management functions (TSF_FMT), can only be used after key operator authentication (TSF_AUT) succeeds.

6.1.5 Security management (TSF_FMT)

The security management (TSF_FMT) provides the functions of key operator code query and modification. The key operator code is managed by the security management (TSF_FMT). The security management (TSF_FMT) can only be executed after key operator identification and authentication (TSF_AUT) succeeds. Like authentication (TSF_AUT), this therefore specifies key operator and associates the role of key operator with a user and even after the key operator code is modified (changed), the role as a key operator is maintained.

The newly inputted key operator code should be verified that it is 5-digit number and then stored in EEPROM in the MFD.

6.2 TSF Strength of Security Functions

The following security functions are based on a probabilistic or permutational mechanism:

- Authentication function (TSF_AUT): Entry of the key operator code for authentication corresponds to FIA_UAU.2 and FIA_UAU.7.
- Data clear function (TSF_FDC): the same as above.
- Security management function (TSF_FMT): Modifying the key operator code corresponds to FIA_SOS.1.

The strength of these security functions is SOF-basic.

© 2007, Sharp Corp., all rights reserved.

6.3 Assurance Measures

The documents that serve as the assurance measure for each component of the security assurance requirements in this ST are shown in Table 6-2.

Table 6-2: Assurance Measures

Component	Assurance Measures
ACM_CAP.3 ACM_SCP.1	AR-FR24 AR-FR25 Configuration Management AR-FR24 VERSION M.10 Configuration List
ADO_DEL.1	AR-FR24 AR-FR25 Delivery Procedures
ADO_IGS.1	AR-FR24/FR25 Installation Manual AR-FR24/FR25 Installation Manual (for overseas)
ADV_FSP.1	AR-FR24 AR-FR25 Security Functional Specifications
ADV_HLD.2	AR-FR24 AR-FR25 High-level Design
ADV_RCR.1	AR-FR24 AR-FR25 Representation Correspondence Analysis
ADV_SPM.1	AR-FR24 AR-FR25 Security Policy Model Specifications
AGD_ADM.1 AGD_USR.1 AVA_MSU.1	AR-FR24 Data Security Kit Operation Manual AR-FR24 AR-FR25 Data Security Kit Notice Digital Multifunctional System Key Operator's Guide
ALC_DVS.1	AR-FR24 AR-FR25 Development Security Specifications
ATE_COV.2	AR-FR24 AR-FR25 Coverage Analysis
ATE_DPT.1	AR-FR24 AR-FR25 High-level Design Testing Analysis
ATE_FUN.1	AR-FR24 Functional Testing Specifications AR-FR24 AR-FR25 Testing Environment and Tools Manual
ATE_IND.2	TOE
AVA_SOF.1	AR-FR24 AR-FR25 Strength of Security Function Analysis
AVA_VLA.1	AR-FR24 AR-FR25 Vulnerability Analysis

© 2007, Sharp Corp., all rights reserved.

7 PP Claims

This ST and TOE do not claim conformance to any PP.

© 2007, Sharp Corp., all rights reserved.

8 Rationale

This chapter demonstrates the completeness and consistency of this ST.

8.1 Security Objectives Rationale

Table 8-1 demonstrates that the policies indicated in the security objectives are effective for the assumptions, threats and organisational security policies indicated in the TOE security environment. Table 8-1 shows the sections of this document that provide the rationale for the correspondences of the security objectives and the assumptions, threats and organisational security policies.

Table 8-1: Security Objectives Rationale

TOE security environment Security Objective	A.OPERATOR	T.RECOVER	P.RESIDUAL
O.REMOVE		8.1.2	
O.RESIDUAL			8.1.3
OE.ERASEALL			8.1.3
OE.OPERATE	8.1.1		

8.1.1 A.OPERATOR

A.OPERATOR stipulates that the key operator be a trustworthy person. OE.OPERATE enforces strict selection of the person who will be the key operator based on an understanding of the role of key operator on the part of those in charge of the organisation that owns the TOE-equipped MFD. Therefore, A.OPERATOR can be achieved.

8.1.2 T.RECOVER

Even if a low-level attacker can read out the actual image data stored in the flash memory of the assets that is protected by the TOE, O.REMOVE counters T.RECOVER by spooling the image data after encrypting it to be illegible using the unique cryptographic key to the MFD.

With respect to cryptographic key stored in the FAX_RAM and actual image data that is spooled to PCL_RAM and IMC_RAM among the assets protected by this TOE, when the memory (volatile memory) is removed, the data are lost (because in volatile memory the electrical charges disappear and thus the data is lost) and there are no interface to read the data directly from the memory MFD in operation, and it requires a high level of technology like specifying the data area and under transferring data to read the cryptographic key or actual image data by attaching probes directly to the terminals or harness of MFD. Therefore, it is impossible for attacker possessing a low-level technical potential.

For this reason the cryptographic key stored in FAX_RAM cannot be read and therefore information disclosure from the flash memory can be prevented, and information disclosure from the actual image data spooled in PCL_RAM and IMC_RAM can be prevented.

8.1.3 P.RESIDUAL

P.RESIDUAL stipulates the enforcement of overwriting of actual image data spooled to the MSD after each job end by O.RESIDUAL. When the MFD is disposed of or its ownership changes, OE.ERASEALL stipulates that the key operator clear entire all data spool areas of the MSD by overwriting by O.RESIDUAL. Therefore, P.RESIDUAL can be achieved.

8.2 Security Requirements Rationale

In the following, it is demonstrated that the IT security requirements attain the security objectives.

© 2007, Sharp Corp., all rights reserved.

8.2.1 Security Functional Requirements Rationale

The correspondence between security functional requirements and security objectives is shown in Table 8-2. Table 8-2 shows the section that provides the rationale for the correspondence between the security functional requirements and the security objectives.

Table 8-2: TOE Security Functional Requirements Rationale

Objective Requirement	O.REMOVE	O.RESIDUAL
FCS_CKM.1	8.2.1.1	
FCS_COP.1	8.2.1.1	
FDP_RIP.1		8.2.1.2
FIA_SOS.1		8.2.1.2
FIA_UAU.2		8.2.1.2
FIA_UAU.7		8.2.1.2
FIA_UID.2		8.2.1.2
FMT_MOF.1		8.2.1.2
FMT_MSA.2	8.2.1.1	
FMT_MTD.1		8.2.1.2
FMT_SMF.1		8.2.1.2
FMT_SMR.1		8.2.1.2
FPT_RVM.1	8.2.1.1	8.2.1.2

8.2.1.1 O.REMOVE

The intent of O.REMOVE is to counter T.RECOVER; in other words the prevention of the display of an image from actual image data spooled to Flash memory in the MFD even if Flash memory is accessed using a device other than the MFD that spooled the data. This can be achieved by the combination of the following functional requirements.

- Actual image data is encrypted by FCS.COP.1 before being spooled, and thus even if it is accessed from a device other than the MFD that spooled the data, display of an image is prevented.
- FCS_CKM.1 generates the cryptographic key to achieve FCS_COP.1.
- The seed of the cryptographic key is generated by TOE itself and accepted as security attribute according to FMT_MSA.2.
- FTP_RVM.1 supports not to be able to bypass functional requirements to achieve O.REMOVE.

Since FCS_CKM.1 and FMT_MSA.2 depend on FCS_COP.1, these three do not cause any conflicts. Since FPT_RVM.1 is innately to be mutually supportive with other requirements, and does not conflict. Thus, functional requirements do not give O.REMOVE any conflicts.

8.2.1.2 O.RESIDUAL

O.RESIDUAL can be achieved by the combination of the following functional requirements.

a) The protection of user data is enabled by overwriting of the area where the actual image data are spooled at the execution of Auto Clear at Job End or Clear All Memory by FDP_RIP.1.

b) The key operator is identified and authenticated by FIA_UAU.2, FIA_UAU.7, and FIA_UID.2.

c) The ability to manage FDP _RIP.1 (enabling and disabling Clear All Memory) is restricted to the key operator by the following functional requirements.

- Only the key operator can enable/disable Clear All Memory by FMT_MOF.1.
- Only the key operator can query/change (modify) the key operator code by FMT_MTD.1.
- In case the key operator code is changed (modified), FIA_SOS.1 verifies that the inputted key operator code is 5-digit number to enables to set a key operator code with the defined quality of standard.
- FMT_SMF.1 ensures identification and authentication of the key operator by managing the key operator code according to FIA_UAU.2.

d) FTP_RVM.1 supports not to be able to bypass functional requirements to achieve O.RESIDUAL.

Since all four events of c) above are independent of one another and are the events in management of a), a) and the events of c) do not make any conflict with one another. Since these independent events each correspond only one functional requirement, their functional requirements do not make any conflicts.

There cannot be any conflicts between b), a) and c), because b) is independent from both a) and c) and the three functional requirements affect each other in a complementary manner to perform the identification and authentication function. Each event in a), b) and c) does not compete.

There cannot be any conflicts with d), a requirement for use in a mutual support.

Thus, functional requirements do not give O. RESIDUAL any conflicts.

© 2007, Sharp Corp., all rights reserved.

8.2.2 Rationale for Consistence of TOE security Management Functions

Some of TOE security functional requirements require the security management function. [CC_PART2] suggests the management activities foreseen by each functional component as the management requirements for each component.

T he management functions required by all TOE security functional requirement components are shown in Table 8-3 with the consideration for management requirement. The management functions specified by FMT_SMF.1 correspond to the management functions required shown in the table.

Thus, TOE security requirements are internally consistent with security management functions.

Table 8-3: Management Functions of the TOE

Management Function Origin	Management Function required	Consideration for management requirement
FCS_CKM.1	—	The attributes of the encryption key is not changed.
FCS_COP.1	—	(no management requirements)
FDP_RIP.1	—	The timing to perform protection is fixed to the release of allocation.
FIA_SOS.1	—	The quality metric is fixed.
FIA_UAU.2	• Modify the key operator code.	Management Function required agrees with management requirement.
FIA_UAU.7	—	(no management requirements)
FIA_UID.2	—	Identification of the key operator is fixed.
FMT_MOF.1	—	No role groups
FMT_MSA.2	—	(no management requirements)
FMT_MTD.1	—	No role groups
FMT_SMF.1	—	(no management requirements)
FMT_SMR.1	—	No user groups
FPT_RVM.1	—	(no management requirements)

8.2.3 Rationale for Security Functional Requirement Dependencies

Security functional requirement dependencies are shown in Table 8-4. Table 8-4 shows the dependencies that the security functional requirements must satisfy according to the CC, the dependencies that the TOE satisfies, the dependencies that the TOE does not satisfy, and the section that provides the rationale for dependencies that are not satisfied. The dependency that is marked with "*" in the table is satisfied by the hierarchically upper component.

Table 8-4: Security Functional Requirement Dependencies

Dependencies Requirement	Stipulated	Satisfied	Unsatisfied	Justification
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FMT_MSA.2	FCS_CKM.4	8.2.3.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FMT_MSA.2	FCS_CKM.4	8.2.3.1
FDP_RIP.1	—	—	—	—
FIA_SOS.1	—	—	—	—
FIA_UAU.2	FIA_UID.1 *	FIA_UID.2	—	—
FIA_UAU.7	FIA_UAU.1 *	FIA_UAU.2	—	—
FIA_UID.2	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	ADV_SPM.1	FDP_ACC.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	8.2.3.2
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1	FIA_UID.1 *	FIA_UID.2	—	—
FPT_RVM.1	—	—	—	—

8.2.3.1 Justification for No Satisfaction on FCS_CKM.4

The cryptographic key is stored in volatile memory. When the power is off, electrical charge of volatile memory in which the cryptographic key is stored disappears and the cryptographic key is destroyed.

© 2007, Sharp Corp., all rights reserved.

Therefore, there is no necessity to use a key destruction method that meets standards, and FCS_CKM.4 is not required to specify standards.

8.2.3.2 Justification for No Satisfaction of Dependencies on FMT_MSA.2

The seed of cryptographic key is a security attribute related to cryptographic operation that is managed by the TOE. Even the key operator is not allowed to change the seed of cryptographic key, and thus FMT_MSA.1 and FMT_SMR.1 are not required. Similarly, the cryptographic key and seed of cryptographic key are not accessed by the user or key operator and not accepted from the outside of TOE, and thus either FDP_ACC.1 or MDP_IFC.1 is not required.

8.2.4 Mutual Effect of Security Requirements

Table 8-5 shows the mutual effect of security requirements.

8.2.4.1 Bypassing

Bypassing of the functional requirements in Table 8-5 is discussed below.

a) Cryptographic key generation FCS_CKM.1 is always invoked when the power is turned on and thus bypassing is not possible.

b) Cryptographic operation FCS_COP.1 always encrypts the actual image data before the data is spooled to the Flash memory and decrypts the data after the data is read, and thus bypassing is not possible.

c) Sub-set residual information protection FDP_RIP.1 is invoked every time a job is finished or cancelled or every time the key operator selects Clear All Memory, and thus bypassing is not possible.

d) FIA_UAU.2, FIA_UAU.7 and FIA_UID.2 related to the key operator identification and authentication are always invoked whenever identification and authentication of the key operator is executed, and thus bypassing is not possible.

e) Verification of secrets FIA_SOS.1 is always invoked without fail when the key operator code is changed (modified), and thus bypassing is not possible.

f) Management of security functions behaviour FMT_MOF.1 always requires the key operator authentication FIA_UAU.2 before operation for enabling Clear All Memory. When cancellation of Clear All Memory is selected, FMT_MOF.1 also invokes the key operator authentication before the program is cancelled. Thus, bypassing is not possible.

g) Management of TSF data FMT_MTD.1 always requires key operator authentication FIA_UAU.2, and thus bypassing is not possible.

Table 8-5: Mutual effect of security requirements

Defence Requirement	Bypass	Disabling
FCS_CKM.1	FPT_RVM.1	—
FCS_COP.1	FPT_RVM.1	—
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1
FIA_SOS.1	FPT_RVM.1	—
FIA_UAU.2	FPT_RVM.1	—
FIA_UAU.7	FPT_RVM.1	—
FIA_UID.2	FPT_RVM.1	—
FMT_MOF.1	FPT_RVM.1	—
FMT_MSA.2	—	—
FMT_MTD.1	FPT_RVM.1	—
FMT_SMF.1	—	—
FMT_SMR.1	—	—
FPT_RVM.1	—	—

8.2.4.2 De-activation

Regarding deactivation in Table 8-5, FDP_RIP.1 ensures protection from acts of deactivation in that access is restricted only to the key operator according to FMT_MOF.1.

8.2.4.3 Tampering

This TOE has only permitted the behaviour management of the security function only to the key operator. Improper subjects do not exist, and therefore, the access control is not needed, and TSF is not tampered.

8.2.5 TOE Security Assurance Requirements Rationale

The TOE is an optional product for MFD that is sold separately; in other words commercial product. The threat is that a low-level attacker may use a device other than the MFD to physically, and read and leak information in the MSD of the MFD. For this reason, the quality assurance level selected for the TOE is EAL3 + ADV_SPM.1, a sufficient level for commercial use. ADV_SPM.1 is selected due to the

© 2007, Sharp Corp., all rights reserved.

dependency on ADV_SPM.1 that is indicated in the functional requirement FMT_MSA.2. All dependencies are satisfied as Table 5-1.

The assurance requirements aside from ADV_SPM.1 are from the EAL3 package, and do not make any conflict with one another. ADV_SPM.1 is an assurance requirements for individual specifications of TSP models, and does not conflict with other requirements.

8.2.6 Rationale for Minimum Strength of Function

It is expected that this TOE will be used in general commercial systems, and thus malicious acts will be attacks that make use of public information. For this reason, the attack potential of attacker is “low-level”. The minimum strength of function level of this TOE is SOF-basic, and it can cope with the malicious acts that make use of public information by attackers possessing a low-level attack potential. Explicit strength of function of each FIA_SOS.1, FIA_UAU.2 and FIA_UAU.7 is SOF-basic and they do not conflict with the minimum strength of function.

8.3 TOE Summary Specification Rationale

This section demonstrates that the TOE security functions and their assurance measures meet the IT security requirements.

8.3.1 TOE Summary Specification Rationale

As for the correspondence between the security functional requirements and the TOE security specifications at Table 6-1, the rationale is shown below.

8.3.1.1 FCS_CKM.1

When the MFD is powered on, TSF_FKG generates a 128 bits cryptographic key (common key) using the MSN-A expansion algorithm. The MSN-A expansion algorithm is based on the SHARP Corporation Encryption Standards for MFD Data Security Kits, and thus FCS_CKM.1 is satisfied.

8.3.1.2 FCS_COP.1

The actual image data to be spooled is encrypted and decrypted by TSF_FDE according to the AES Rijndael algorithm standardized in FIPS PUB 197, and thus FCS_COP.1 is satisfied.

8.3.1.3 FDP_RIP.1

TSF_FDC protects remaining information by overwriting it as follows, and thus FDP_RIP.1 is satisfied.

- Auto Clear at Job End program overwrites the actual image data files stored in the IMC_RAM (for copy and print jobs), PCL_RAM (for scan send jobs) or Flash memory (for fax jobs).
- Clear All Memory program overwrites all actual image data stored in the IMC_RAM, PCL_RAM or Flash memory.

8.3.1.4 FIA_SOS.1

When the key operator code is changed by TSF_FMT, TSF_FMT verifies that the key operator code meets 5-digit number and does not accept any key operator codes that do not satisfy that quality metric, and thus FIA_SOS.1 is satisfied.

8.3.1.5 FIA_UAU.2

TSF_AUT enforces the authentication by entering the key operator code before the operation of the function for the key operator. TSF_FDC enforces the authentication by entering the key operator code when running Clear All Memory is cancelled. Thus, FIA_UAU.2 is satisfied.

8.3.1.6 FIA_UAU.7

TSF_AUT only indicates as many substitute characters as characters entered for the protected feedback while authentication of the key operator. So does TSF_FDC when it is authenticating the key operator to cancel a clearance, and thus FIA_UAU.7 is satisfied.

© 2007, Sharp Corp., all rights reserved.

8.3.1.7 FIA_UID.2

TSF_AUT requires the operation for the identification of the key operator before the operation of the function for the key operator. The cancel operation of Clear All Memory by TSF_FDC corresponds to the identification of the key operator. Thus, FIA_UID.2 is satisfied.

8.3.1.8 FMT_MOF.1

Enabling Clear All Memory by TSF_FDC is possible only after authentication of the key operator by TSF_AUT is successful.

Disabling Clear All Memory by TSF_FDC is possible only after authentication of the key operator by TSF_FDC is successful.

Thus, FMT_MOF.1 is satisfied.

8.3.1.9 FMT_MSA.2

It is explained that a cryptographic key is sure to be generated based on the secure seed for ADV_SPM.1, and FMT_MSA.2 is satisfied by cryptographic key generation TSF_FKG.

8.3.1.10 FMT_MTD.1

The key operator identified and authenticated by TSF_AUT is able to query and modify the key operator code by TSF_FMT, and thus FMT_MTD.1 is satisfied.

8.3.1.11 FMT_SMF.1

TSF_FMT contains the ability to modify the key operator code, and thus FMT_SMF.1 is satisfied.

8.3.1.12 FMT_SMR.1

Identification and authentication of key operator by TSF_AUT specifies the key operator. This associates the user with the role. In addition, even if the key operator code is changed (modified) by TSF_FMT, association and maintenance of the role continues, and thus FMT_SMR.1 is satisfied.

8.3.1.13 FPT_RVM.1

The supports by FPT_RVM.1, mentioned in section 8.2.4.1, are implemented by the TSFs as follows:

a) TSF_FKG always generates the cryptographic key according to FCS_CKM.1 when the power is turned on.

b) TSF_FDE always encrypts the actual image data when the data is spooled to the Flash memory according to FDC_COP.1 and reads and decrypts the actual image data in the Flash memory only when to process it.

c) TSF_FDC always overwrites according to FDP_RIP.1 every time a job is finished or cancelled and every time Clear All Memory is cancelled by the operation of the key operator.

d) TSF_AUT and TSF_FDC always enforces the identification operation of the key operator according to FIA_UID.2, authentication of the key operator code according to FIA_UAU.2 and protection of the feedback of the key operator code according to FIA_UAU.7 when the key operator is identified and authenticated.

e) TSF_FMT always verifies that the key operator code meets the quality metric, 5-digit number according to FIA_SOS.1 when the key operator code is changed.

f) TSF_FDC provides the interface to enable Clear All Memory according to FMT_MOF.1 only when the authentication of the key operator by TSF_AUT is invoked and successful. Disabling of Clear All Memory is allowed only when the authentication of the key operator by TSF_FDC is invoked and successful.

g) TSF_FMT provides the interface to modify the key operator code according to FMT_MTD.1 only when the authentication of the key operator by TSF_AUT is invoked and successful.

© 2007, Sharp Corp., all rights reserved.

8.3.2 TOE Assurance Measures Rationale

The assurance measures in section 6.3 satisfy TOE security assurance requirements by means of the following contents of each assurance measures (referred as A.m. in this section).

a) ACM_CAP.3, ACM_SCP.1

A.m.: AR-FR24 AR-FR25 Configuration Management

AR-FR24 VERSION M.10 Configuration List

Contents: It specifies the measures and procedures to distinguish every configuration item uniquely and to assure that users can be aware of which instance of the TOE they are using.

It specifies that changes only for the items that are under control of this assurance measure can be managed and that evaluation evidences that TOE implementation and the other assurance components of ST requires are modified by the managed way with appropriate authorization.

b) ADO_DEL.1

A.m.: AR-FR24 AR-FR25 Delivery Procedures

Contents: It specifies the measures and procedures to maintain the security of TOE when TOE is delivered from the developer to the users.

c) ADO_IGS.1

A.m.: AR-FR24/AR-FR25 Installation Manual

AR-FR24/AR-FR25 Installation Manual (for overseas)

Contents: It specifies the measures and procedures of installation of TOE.

d) ADV_FSP.1

A.m.: AR-FR24 AR-FR25 Security Functional Specifications

Contents: It specifies the behaviour of TSF and the interfaces that user-visible interfaces.

e) ADV_HLD.2

A.m.: AR-FR24 AR-FR25 High-level Design

Contents: It specifies the assurance that TOE provides the architecture that is suitable for the implementation of TOE functional requirements, from the view point of main structural units (subsystems) of TOE and the view point of associating these units with the functions that they provides.

f) ADV_RCR.1

A.m.: AR-FR24 AR-FR25 Representation Correspondence Analysis

Contents: It specifies the correspondence among TOE Summary Specifications, Functional Specifications and High-level Design.

g) ADV_SPM.1

A.m.: AR-FR24 AR-FR25 Security Policy Model Specifications

Contents: It specifies the correspondence among Function Specifications, Security Policy Model and these policies of the TSP. It provides the assurance that only the secure value can be accepted as the security attributes.

h) AGD_ADM.1

A.m.: AR-FR24 Data Security Kit Operation Manual

AR-FR24 AR-FR25 Data Security Kit Notice

Digital Multifunctional System Key Operator's Guide

Contents: They are the documents (operation manuals) that are written for the sake of maintaining and administering of TOE properly by TOE administrators.

i) AGD_USR.1

A.m.: (The same as AGD_ADM.1)

Contents: They are the documents (operation manuals) that are written for the secure use of TOE for TOE users.

j) ALC_DVS.1

© 2007, Sharp Corp., all rights reserved.

A.m.: AR-FR24 AR-FR25 Development Security Specifications

Contents: It specifies the physical, procedural and personnel security measures used in the development environment of TOE.

k) ATE_COV.2

A.m.: AR-FR24 AR-FR25 Coverage Analysis

Contents: It is the document that describes that it is enough to demonstrate that TSF operates as stated in the Functional Specifications, in the tests described in the Functional Testing Specifications.

l) ATE_DPT.1

A.m.: AR-FR24 AR-FR25 High-level Design Testing Analysis

Contents: It is the document that describes that it is enough to demonstrate that TSF operates as stated in the High-level Design Specifications, in the tests described in the Functional Testing Specifications.

m) ATE_FUN.1

A.m.: AR-FR24 Functional Testing Specifications

AR-FR24 AR-FR25 Testing Environment and Tools Manual

Contents: They are the documents that describe about the tests to establish that all the execution of the security function is as stated in the specifications.

n) ATE_IND.2

A.m.: TOE

Contents: TOE suitable for testing

o) AVA_MSU.1

A.m.: (The same as AGD_ADM.1)

Contents: They are the documents (operation manuals) that are written about the maintenance and administration method for the proper use of TOE for the TOE administrators and the secure use of TOE for the TOE users.

p) AVA_SOF.1

A.m.: AR-FR24 AR-FR25 Strength of Security Function Analysis

Contents: It is what strength of function analysis for probabilistic and permutational mechanism is performed.

q) AVA_VLA.1

A.m.: AR-FR24 AR-FR25 Vulnerability Analysis

Contents: It is what describes the existence of obvious security vulnerability of TOE security and the analysis that they can not be abused in the intended environment for the TOE.

8.3.3 Rationale for Strength of TOE Security Function

As described in section 6.2, the TSFs that are implemented using a probabilistic or permutational mechanisms are authentication (TSF_AUT), data clear (TSF_FDC) and security management (TSF_FMT). These functions have security strength of function of SOF-basic.

Thus, the minimum value of these security strengths of function is SOF-basic and the TOE security strength of function and the minimum strength of function defined in section 5.1.2 are consistent.

© 2007, Sharp Corp., all rights reserved.