Data Security Kit
AR-FR22
Security Target

Version 0.09

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

SHARP Corporation

History of revisions

Date	Version	Revision	Authored by	Approved by
Jan. 31, 2005	0.01	· Preparation of first edition	Iwasaki	Yamanaka
Feb. 21, 2005	0.02	· Modified printer function · Change of Guidance · Misprint correction	Iwasaki	Yamanaka
April.5, 2005	0.03	· Revision of indicated contents · Change of TOE version	Iwasaki	Yamanaka
April 13, 2005	0.04	· Change of Guidance · Corrected MFD model names	Iwasaki	Yamanaka
April 25, 2005	0.05	· Revision of indicated contents	Iwasaki	Yamanaka
June 22, 2005	0.06	· Revision of indicated contents	Iwasaki	Yamanaka
June 23, 2005	0.07	· Revision of indicated contents	Iwasaki	Yamanaka
June 29, 2005	0.08	· Revision of indicated contents	Iwasaki	Yamanaka
July 21, 2005	0.09	· Revision of indicated contents	Iwasaki	Yamanaka

Table of Contents

List of Tables

List of Figures

1 ST Introduction

1.1 ST Identification

Information for the purpose of identifying this document and the TOE is given below.

ST title:	Data Security Kit AR-FR22 Security Target
Version:	0.09
Publication date:	July 21, 2005
Author:	SHARP Corporation
TOE Identification:	AR-FR22 VERSION S.10
CC Identification:	CC Version 2.1, ISO/IEC 15408:1999, JIS X 5070:2000, CCIMB Interpretations-0407
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 the SHARP Data Security Kit AR-FR22.

A Multi-Function Device (hereafter referred to as “MFD”) is a commercially sold office machine that is capable of copy, print, scan send, PC FAX, fax transmission, and fax reception functions. The TOE is a firmware upgrade kit that enhances the data security function of the MFD. This kit prevents leaking of information from actual image data that was spooled to the memory device in MFD.

1.3 CC Conformance

This document satisfies the following:

a) CC Version 2.1, Part 2 Conformant

b) CC Version 2.1, Part 3 Conformant

c) EAL3 Augmented
Augmented components: ADV_SPM.1

d) There is no PP to which this ST refers.

1.4 Reference

The materials listed in Table 1 were referred to during the creation of this document.

Table 1: Reference

Name	Title of Document
[CC_PART1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model August 1999, Version 2.1 CCIMB-99-031 (January 2001, Translation Version 1.2, Information-technology Promotion Agency, Security Center)
[CC_PART2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements August 1999, Version 2.1 CCIMB-99-032 (January 2001, Translation Version 1.2, Information-technology Promotion Agency, Security Center)

Name	Title of Document
[CC_PART3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements August 1999, Version 2.1 CCIMB-99-033 (January 2001, Translation Version 1.2, Information-technology Promotion Agency, Security Center)
[HOSOKU-0407]	CCIMB Interpretations-0407

1.5 Conventions, Terminology, and Acronyms

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

1.5.1 Conventions

This section describes the conventions used in this document. This section describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning.

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

b) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [ ] indicates an assignment.

c) The refinement operation is used to add detail to a requirement, and thus further restricts a requirement.

d) The selection operation is used to select one or more options provided by the CC in stating a requirement. Selection operation is shown with [<u>underline</u>].

e) Iterated functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis.

1.5.2 Terminology

Terminology unique to this document is defined in Table 2.

Table 2: Terminology

Term	Definition
Image data	The digital data that results from scanning an original on the MFD for a copy, print, scan, or fax transmission job. This is the data that is transmitted over or received from the telephone line during a PC FAX operation, fax transmission, or fax reception. Image data also refers to the data after it has been converted into a format that can be handled by the MFD.
Engine	A device that prints an image on paper, including the paper feeding and paper output mechanisms. This is also called a print engine or an engine unit.
Key operator	A user that is authorized to access the TOE security management functions and the MFD management functions.
Key operator code	A password used for authentication of the key operator.
Key operator programs	Security management functions of the TOE, as well as MFD management functions. To access the key operator programs, identification and authentication as a key operator are required.
Job	The sequence from beginning to end of the use of an MFD function (copy, print, scan send, PC FAX, fax transmission, or fax reception). In addition, the instruction for a functional operation is sometimes called a job.
Data Security Kit	The AR-FR22 which is upgrade kit for use only with SHARP MFDs.
Memory	A memory device; in particular a semiconductor memory device
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.
Board	A printed circuit board on which components are mounted by soldering.

Term	Definition
Actual image data	The part of image data that is actual image data, excluding the control area.
Clear all memory	An operation that clears (by overwriting) all actual image data areas where spooled data is stored in the MSD of an MFD. Since only a key operator can execute, it is also called clear all memory by key operator operation.
Operation panel	A user interface device that includes a display, buttons/keys, and buttons in a touch panel. This is also the unit that includes the above.
Non-volatile memory	Memory that retains its contents even when the power is turned off. Non-volatile memory is often made from semiconductor elements or magnetic memory.

1.5.3 Acronyms

Acronyms used in this ST are indicated in Table 3.

Table 3: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard established by NIST (National Institute of Standards and Technology)
DSK	Data Security Kit
EEPROM	Electrically Erasable Programmable ROM, a type of non-volatile memory that allows electrical rewriting to any part of memory if performed infrequently.
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.
I/F	Interface
IFAX	Internet FAX
MSD	Mass Storage Device. For this TOE, MSDs are the volatile memory, and Flash memory. These are managed by a file system.
OS	Operating System
RAM	Random Access Memory
ROM	Read Only Memory
TIFF-FX	The graphics format specified by the Internet FAX standard.

2 TOE Description

2.1 TOE Overview

2.1.1 TOE Type

The TOE is a data security kit (DSK) which takes the form of a firmware product for the MFD.

2.1.2 Overview of the TOE Security Functions

The TOE security functions primarily consist of the cryptographic operation function and the data clear function. The objective of these functions is to prevent the leaking of information from actual image data remaining in the MFD.

The cryptographic operation function encrypts the actual image data of a PC FAX, fax transmission, or fax reception operation before it is spooled to Flash memory.

The data clear function writes random values or a fixed value or a fixed value over actual image data, when the copy, print, scan send, PC FAX, fax transmission, fax reception job is completed.

2.2 TOE Configuration

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

2.2.1 Physical Scope and Boundaries of the TOE

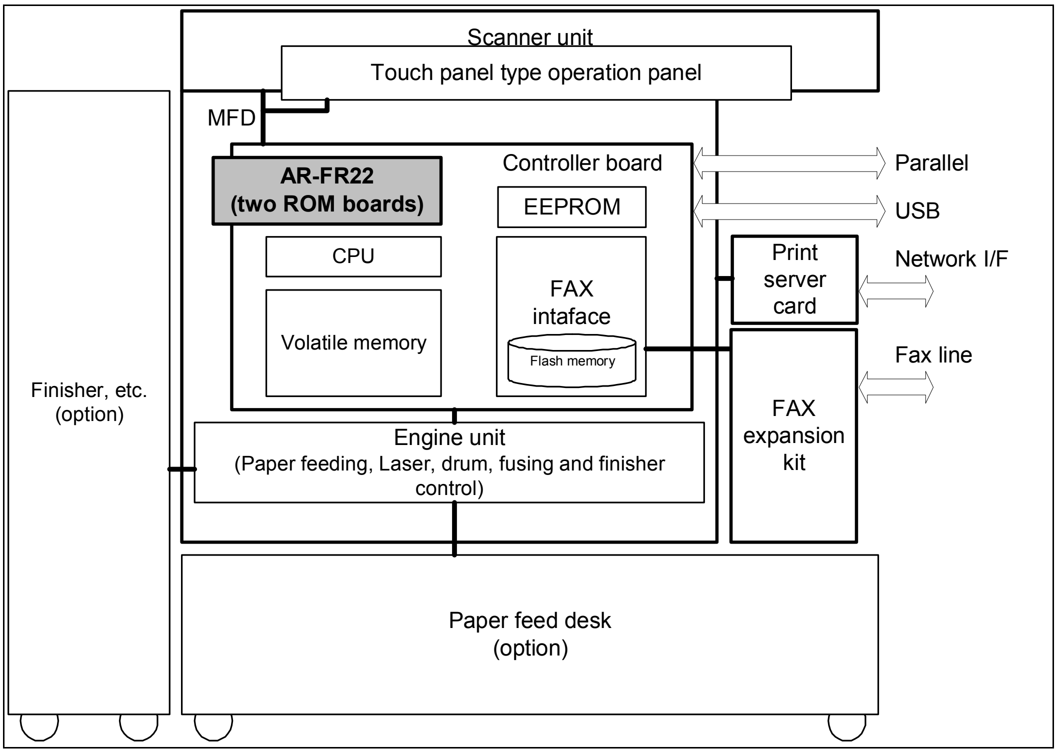

Figure 1: TOE and physical configuration of the MFD

The AR-FR22 (the TOE) is provided by two ROM boards. These are shaded in Figure 1.

The TOE can be used in the following SHARP MFDs: AR-M351U, AR-M451U, AR-355U, AR-455U, AR-355UJ, AR-455UJ, AR-311S, AR-351S, AR-451S, AR-311FP, AR-351FP, AR-451FP.

The physical scope of the TOE is as follows:

a) Controller firmware
Firmware that controls the Controller board, which is contained in the two ROM boards on the Controller board.

2.2.2 Logical Scope and Boundaries of the TOE

The logical configuration of the TOE is shown in Figure 2. The TOE is indicated by the thick-lined frame. The rectangles indicate firmware functions and the rectangles with rounded corners indicate hardware. Firmware functions that are security functions are shaded.

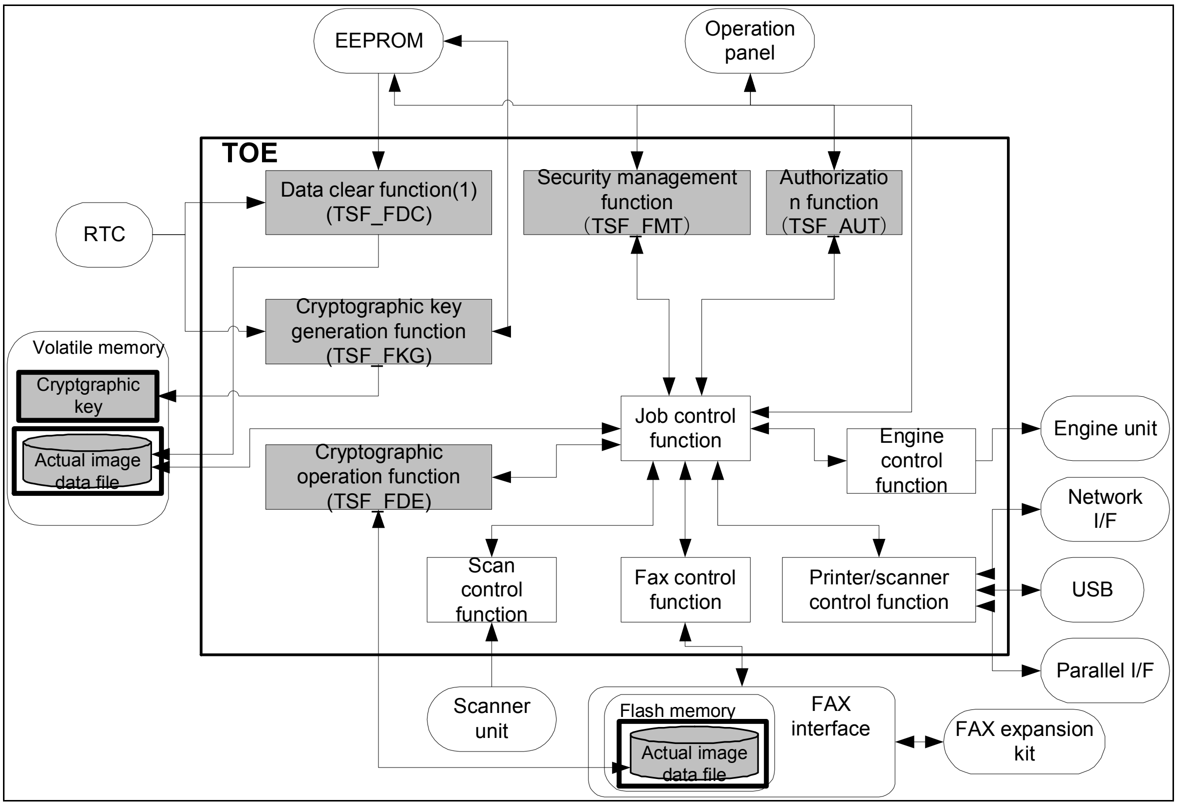

Figure 2: Logical configuration of the TOE

The TOE is an upgrade kit that adds security functions to the MFD. Along with providing security functions, it performs control of the entire MFD. The following functions are included within the logical scope of the TOE.

a) Cryptographic operation function (TSF_FDE)
This encrypts the actual image data of a PC FAX, fax transmission or fax reception job, spools the encrypted data to Flash memory, and manages it as an image data file. This function also reads the encrypted actual image data in Flash memory, decrypts it, and uses it.

b) Cryptographic key generation function (TSF_FKG)
This function generates the cryptographic key for encryption and decryption by the cryptographic operation function. The generated key is stored in volatile memory.

c) Data clear function (TSF_FDC)
These functions clear actual image data, which has been spooled to the MSD and managed as an image file for a copy, print, scan send, PC FAX, fax transmission, or fax reception job, by overwriting random values or fixed values to the corresponding actual image data area. (Auto clear at job end)
This function clears all areas to which data can be spooled by writing random or fixed values over the data in those areas. (Clear all memory by key operator operation)
This consists of the following two data clear functions:

- Auto clear at job end
(Clears the actual image data area used by a job when the job ends.)
During the processing of job, for actual image data spooled to volatile memory, this function clears the actual image data area by overwriting it with random values. For actual image data spooled to Flash memory, this function clears the actual image data area by overwriting each bit with a fixed value.

- Clear all memory by key operator operation
  (Note: This function clears the whole actual image data of any incomplete jobs or jobs that ended abnormally, and is used to prevent the leaking of information from actual image data when the MFD is disposed of or its ownership changes.)
  Volatile memory is cleared by writing random values over all actual image data areas of those memories, and Flash memory is cleared by writing fixed values over all actual image data areas of Flash memory. This function also can cancel (interrupt) the clear all memory by the key operator operation.

d) Authentication function (TSF_AUT)
Authenticates a key operator by means of the key operator code (password).

e) Security management function (TSF_FMT)
This provides a function for changing (modifying) the key operator code following authentication as a key operator.

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/scanner control function
This function can operate on an MFD that can be equipped with the TOE and that has the printer board standard or as an option. In addition, the network can operate on an MFD that has the network function as an option.

- During a print job, this function creates a bitmap image for printing from the print data received through the parallel, USB or network 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) Job control function
Jobs include copy jobs, print jobs, scan send jobs, PC FAX jobs, fax transmission jobs, and fax reception jobs. The job control function controls copy, print, scan send, PC FAX, fax transmission, and fax reception operation of the MFD.

2.3 Use the TOE

This section explains how the TOE operates and is used.

2.3.1 How the TOE is used

When users use the copy, printer, scan send, PC FAX, fax reception and fax transmission functions of the MFD, the TOE operates in the background without the need for attention on the part of the user. The usage environment of the TOE is shown in Figure 3.

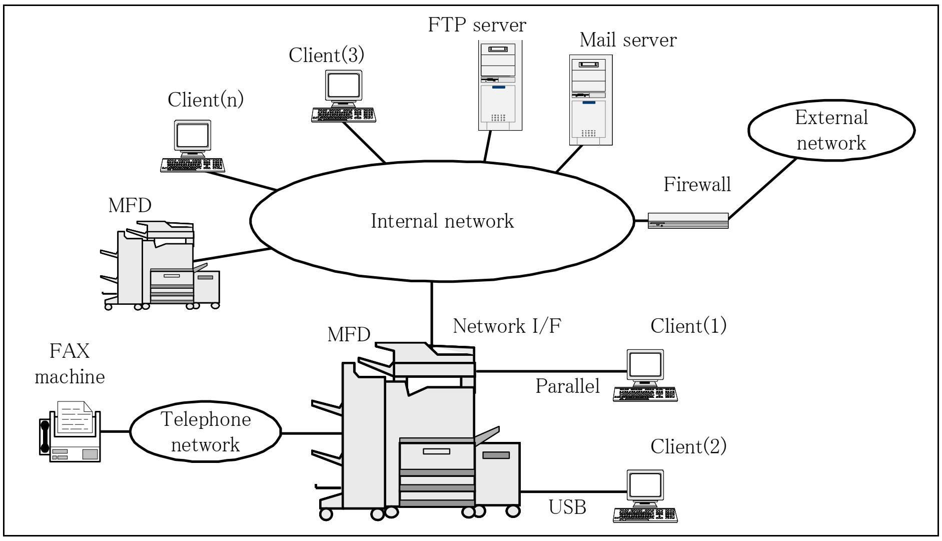

Figure 3: Usage environment of the TOE

a) Copy function

The copy function of the MFD is used to scan an original and print the resulting image.

In addition, one of a copy function includes a tandem copy function. This function can be executed out in two MFD which installed a network by a standard or an option among MFD which can install TOE. With a tandem copy function, two MFD is connected to inside network, MFD which read a manuscript transfers image data addressed to other MFD via inside network it is a function each halves the copy number of copies that a user specified, and it is shared, and to output print. When TOE is installed by both transmission side MFD and reception side MFD, a tandem copy function can be used. However, a tandem copy function as against MFD which does not install TOE from MFD which installed TOE does not work.

b) Printer function

The printer function of the MFD prints print data sent from a client.

This function can be used on an MFD that can be equipped with the TOE and that has the printer function standard or as an option. The MFD can receive print data by the four following methods:

1) On a client that has the MFD printer driver installed, print data is generated by the printer driver. The MFD receives the generated print data through a parallel, USB, or network interface. (print function)
2) The MFD has an E-mail account on a mail server connected to the same network, and the MFD periodically checks the server for received e-mail. If the MFD has received e-mail, it retrieves the e-mail together with the file (print data) attached to the e-mail. (E-mail print function)
3) To a FTP server connected to a network, MFD oneself receives a file in a FTP server (print data) over direct network I/F by operation from an operation panel of MFD. (FTP pull print function)
4) A File (print data) is sent to MFD from the Web browser of a client connected to the same network. The MFD receives a file (print data) from a client, which is not through the printer driver, through the network interface directly. (Direct print function of files on computers)

In addition, one of a print function includes a tandem print function. When this function prints tandem from the client whom printer driver for MFD is installed in, and it specifies becomes effective. With a tandem copy function, two MFD is connected to inside network, MFD which received print data from a client transfers image data addressed to other MFD via inside network it is a function each halves the copy number of copies that a user specified, and it is shared, and to output print. When TOE is installed by both transmission side MFD and reception side MFD, a tandem copy function can be used. However, a tandem copy function as against MFD which does not install TOE from MFD which installed TOE does not work.

c) Scan send function

Scan send function converts the actual image data that an MFD scanned to designated form in a user, it is function transferring to FTP server connected to network or mail server.

This function can be used on an MFD that can be equipped with the printer and network function standard or as an option. As for the scan send ability, Scan-to-FTP transmitting a message to a FTP server, Scan-to-Desktop transmitting a message to a FTP server operating in a client and Scan-to-Email to transmit to an email server is possible. A scan tool is installed in a client in order to use Scan-to-Desktop, and it is had to operate a FTP server. In addition, one of scan transmitter ability includes an Internet FAX (IFAX) function. A scanned image is converted into a format with the authority of IFAX (TIFF-FX), for a designated partner, it is a function to emit in a protocol the same as transfer to an email server.

d) PC FAX function

The PC FAX function of the MFD is used to fax PC FAX data sent from a client. This function can be used on an MFD that can be equipped with the printer and FAX functions standard or as an option. The destination is selected at the client, and the function is executed on the MFD when it receives the PC FAX data from the client through a parallel, USB, or network interface.

e) Fax transmission function

The fax transmission function of the MFD is used to send a fax to a destination FAX machine that is selected using the MFD operation panel. This function can be used on an MFD that can be equipped with FAX function standard or as an option. The destination fax number is entered at the MFD operation panel. An auto-dial number stored using the MFD operation panel can also be used.

f) Fax reception function

The fax reception function of the MFD receives faxes sent by FAX machines and prints the faxes out. This function can be used on an MFD that can be equipped with FAX functions standard or as an option.

2.3.2 How the TOE is operated

Only a key operator that has been identified and authenticated (TSF_AUT) is able to use the TOE. After being authenticated, the key operator can configure/execute the following settings and functions by means of the TOE security management function (TSF_FMT) and data clear function (TSF_FDC).

- Clear all memory by key operator operation
- Changing (modifying) the key operator code

By a key operator program, functions such as job situation completion area elimination, address book / image transmission of a message registration data elimination, the data area elimination number of times, automatic elimination in power supply ON, the automatic elimination number of times in power supply ON, the automatic elimination number of times after each job completion, print hold prohibition setting, data list print prohibition setting, job situation completion area indication setting, use prohibition of a re-transmission of a message key, cancellation of hold print data operation prohibition provide besides, too, but these are non-security capability. In addition, as for the automatic elimination number of times in each job end and the elimination number of times in all data area elimination by operation of a key operator, a change is possible in the range of 7 from 1, but it is non-security capability for use in adjustment between overwrite elimination processing time.

2.4 Protected assets by the TOE

Protected assets by the TOE are actual image data that remains following deletion (due to de-allocation of the resource) of image data files stored in volatile memory or Flash memory in the MFD, which takes place after a user completes the MFD for a copy, print, scan send, PC FAX, fax transmission, or fax reception job or when the job is interrupted.

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.

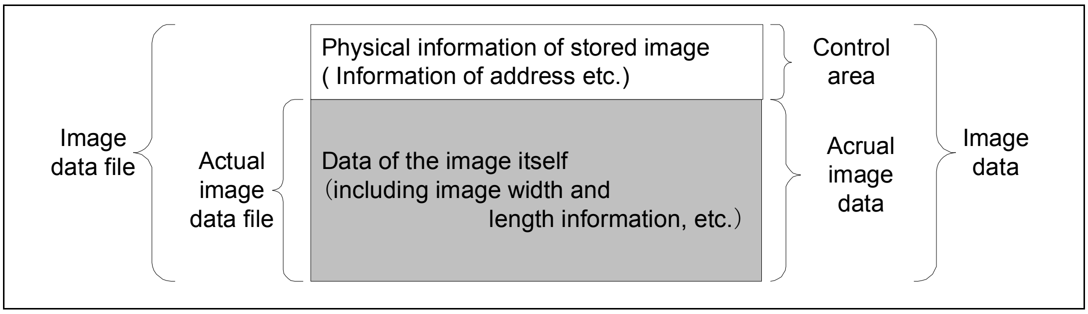
Image data file
Actual image data file
Physical information of stored image (Information of address etc.)
Data of the image itself （including image width and length information, etc.）
Control area
Acrual image data
Image data

Figure 4: Explanation of actual image data

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

In addition, the protected assets stored in the volatile memory cannot be read by an attacker possessing a low level attack potential and never be the target of attacking.

3 TOE Security Environment

This chapter discusses the TOE security environment.

3.1 Assumptions

Use and operation of the TOE requires the environment described in Table 4.

Table 4: Assumptions

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

3.2 Threats

Threats to the TOE are described in Table 5.

Table 5: Threats

Identifier	Definition
T.RECOVER	A low-level attacker will leak 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 Organizational Security Policies

Organizational security policies are described in Table 6.

Table 6: Organizational Security Policies

Identifier	Definition
P.RESIDUAL	Upon completion of a copy, print, scan send, PC FAX, fax transmission, or fax reception job, or following interruption of a job, 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.

4 Security Objectives

This chapter discusses the measures for the security objectives.

4.1 Security Objectives for the TOE

The security objectives for the TOE are shown in Table 7 .

Table 7: TOE Security Objectives

Identifier	Definition
O.RESIDUAL	Upon completion of a copy, print, scan send, PC FAX, fax transmission, or fax reception job, or following interruption of a job, the TOE shall overwritten the actual image data area spooled to the MSD. The TOE also shall perform overwriting of all image data areas of the MSD by the instruction of key operator.
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.

4.2 Security Objectives for the Environment

The security objectives for the environment are shown in Table 8.

Table 8: Security Objectives for the Environment

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

5 IT Security Requirements

5.1 TOE Security Requirements

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

5.1.1 TOE Security Functional Requirements

5.1.1.1 Class FCS: Cryptographic support

a) 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-J expansion algorithm] and a specified cryptographic key size [128 bits] that meet the following [Data Security Kit Encryption Standard].

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

b) 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 MSD and decryption of actual image data encrypted and spooled in the MSD] in accordance with a specified cryptographic algorithm [AES Rijndael algorithm] and cryptographic key size [128 bits] that meet [FIPS PUB 197].

Dependencies: 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

a) 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 MSD].

Dependencies: No dependencies

5.1.1.3 Class FIA: Identification and Authentication

a) FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [[3 (positive integer number)]] unsuccessful authentication attempts occur related to [the number of failed Key Operator authentication attempts following the last successful authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [actions shown in Table 9].

Dependencies: FIA_UAU.1 Timing of authentication

Table 9: Action of Authentication failure

Identifier	Actions
Unsuccessful authentication reached three times	Authentication trial receptionist stop for five minutes
Return to a normal state	Five minutes pass, the authentication failure number of times is cleared, and it is return automatically

b) 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

c) FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

FIA_UAU.7.1 The TSF shall provide only [display of an asterisk for each entered digit] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

d) FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of authentication

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

e) FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that the secret meets [the 5-digits number].

Dependencies: No dependencies

5.1.1.4 Class FMT: Security Management

a) FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

FMT_MOF.1.1 The TSF shall restrict the ability to [enable, disable] the function [Clear all memory by key operator operation] to [the key operator].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

b) 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

c) 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 [the key operator].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

d) FMT_SMR.1 Security roles

Hierarchical to: No other components

FMT_SMR.1.1 The TSF shall maintain the role [the key operator].

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

Dependencies: FIA_UID.1 Timing of identification

e) FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [The functions shown in Table 10, which manage the TOE management items].

Dependencies: No dependencies

Table 10: TOE management items

Functional requirement	Management item
FCS_CKM.1	None (the attributes of the encryption key have not been changed)
FCS_COP.1, FIA_UAU.7, FMT_MSA.2, FMT_SMF.1	None (no requirement for management items)
FDP_RIP.1	None (not have to be managed because a timing of overwriting is only upon the deallocation of the resource from an object)
FIA_AFL.1	None (There is not a management item on FIA_AFL.1 the authentication failure number of times does not need management in order to be fixed value, and stop time to a re-authentication is fixed time, it does not have to manage, it returns to a normal state automatically.)
FIA_UAU.2	Key operator code
FIA_UID.2	None (not managed because user identification information and identification operation is fixed)
FIA_SOS.1	None (the quality metric is fixed and thus not managed)
FMT_MOF.1, FMT_MTD.1	None (the role group reciprocally interacting with the TSF function (TSF data) is fixed, and thus there is no need for management)
FMT_SMR.1	None (the only user that performs a role is the key operator, and thus there is no need for management)

5.1.1.5 Class FPT: Protection of the TSF

a) 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 Security Assurance Requirements

Assurance components for the assurance level selected by this document are shown in Table 11. Table 11 shows the assurance requirements that must be satisfied to claim EAL3+ADV_SPM.1 compliance.

Table 11: Assurance Requirements

Component	Component Name	Dependencies:
ACM_CAP.3	Authorisation 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
ATE_DPT.1	Testing: high-level design	ADV_HLD.1, ATE_FUN.1
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

5.1.3 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_UAU.2, FIA_UAU.7, FIA_SOS.1 and FIA_AFL.1 use a probabilistic or permutational mechanism, and the explicit strength of function is SOF-basic. FCS_COP.1 is a functional requirement that uses a cryptographic algorithm, and thus not apply to this SOF level.

5.2 Security Requirements for the IT Environment

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

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)

The correspondence between security functional requirements and TOE security functions is shown in Table 12. Table 12 indicates the section that describes the correspondence between general description of security functional requirement and TOE security specifications.

Table 12: Security Functional Requirements and TOE Security Specifications

Functional Requirement	Security Functions				
	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_AFL.1			6.1.3	6.1.4	
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	
FIA_SOS.1					6.1.5
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_SMR.1				6.1.4	6.1.5
FMT_SMF.1					6.1.5
FMT_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 (shared key) to support the actual image data encryption function. When the MFD is powered on, a cryptographic key (shared key) is always generated. The cryptographic key is generated as a 128-bit of secure key using MSN-J 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 to generate in MSN-J expansion algorithm is used by code operation to spool in Flash memory. The cryptographic key is stored in volatile memory.

6.1.2 Cryptographic operation (TSF_FDE)

During the processing of a job, the actual image data of the job is always encrypted before being spooled to Flash memory. 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.

The cryptographic key is used in MSN-J expansion algorithm in code operation to Flash memory.

6.1.3 Data clear (TSF_FDC)

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

a) Auto clear at job end
When a copy job, print job or scan send job ends, the actual image data file in volatile memory is overwritten with random values.

When a PC FAX, fax transmission, or fax reception job ends, the actual image data file that was spooled to Flash memory overwritten with fixed values.

b) Clear all memory by key operator operation
To execute or cancel the clear all memory by key operator operation function, identification and authentication of the key operator is required.
When the key operator executes clear all memory by key operator operation after being identified and authenticated as the key operator, all actual image data that are used for spooling to volatile memory are overwritten with random values, and all actual image data that are used for spooling to Flash memory are overwritten by fixed values. To cancel clear all memory by key operator operation, key operator identification and authentication by entry of the key operator code are required following selection of the cancel operation. In key operator authentication, when the number of times of unsuccessful authentication trial after an authentication success of the last to a key operator is authentication failure which is three continuations, an authentication input receptionist is stopped for five minutes. A normal state is returned from an authentication input stop to automatically the re-authentication input is accepted. 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 by key operator operation is managed so that it is executed at job end or at the instruction of clear all memory by the key operator operation. And auto clear at job end and clear all memory by key operator operation always enforced.

The random values used to overwrite volatile memory 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. Key operator identification and authentication are enforced following selection of the key operator programs by requiring entry of the key operator code. In key operator authentication, when the number of times of unsuccessful authentication trial after an authentication success of the last to a key operator is authentication failure which is three continuations, an authentication input receptionist is stopped for five minutes. A normal state is returned from an authentication input stop to automatically the re-authentication input is accepted. 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 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 by key operator operation, 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 following key operator authentication (TSF_AUT).

6.1.5 Security management (TSF_FMT)

The key operator code is managed by the security management(TSF_FMT). The security management (TSF_FMT) can only be executed following key operator identification and authentication (TSF_AUT). 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.

- Changing (modifying) the key operator code
  This function provides the functions of key operator code query and modification. The newly inputted key operator code should be verified that it is 5-digits number.

When each setting value is changed, it is stored in EEPROM in the MFD.

6.2 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 13.

Table 13: Assurance Measures

Component	Component Name	Assurance Measures
ACM_CAP.3	Authorisation controls	Digital MFD Data Security Kit AR-FR22 Configuration Management, Digital MFD Data Security Kit AR-FR22 VERSION S.10 Configuration List
ACM_SCP.1	TOE CM coverage	
ADO_DEL.1	Delivery procedures	Digital MFD Data Security Kit AR-FR22 Delivery Procedures
ADO_IGS.1	Installation, generation, and start-up procedures	AR-FR22 Installation Instruction Manual (Japanese), AR-FR22 Installation Instruction Manual (English, German, French, Spanish)
ADV_FSP.1	Informal functional specification	Digital MFD Data Security Kit AR-FR22 Security Functional Specifications
ADV_HLD.2	Security enforcing high-level design	Digital MFD Data Security Kit AR-FR22 High-level Design
ADV_RCR.1	Informal correspondence demonstration	Digital MFD Data Security Kit AR-FR22 Representation Correspondence Analysis
ADV_SPM.1	Informal TOE security policy model	Digital MFD Data Security Kit AR-FR22 Security Policy Model Specifications
AGD_ADM.1	Administrator guidance	AR-FR22 Data Security Kit Operation Manual, AR-FR22 Data Security Kit Notice, LASER PRINTER KEY OPERATOR'S GUIDE, LASER PRINTER OPERATION MANUAL (for general information and copier operation), OPERATION MANUAL (for printer), FACSIMILE EXPANSION KIT OPERATION MANUAL, OPERATION MANUAL (for network scanner)
AGD_USR.1	User guidance	
ALC_DVS.1	Identification of security measures	Digital MFD Data Security Kit AR-FR22 Development Security Specifications
ATE_COV.2	Analysis of coverage	Digital MFD Data Security Kit AR-FR22 Coverage Analysis
ATE_DPT.1	Testing: high-level design	Digital MFD Data Security Kit AR-FR22 High-level Design Testing Analysis
ATE_FUN.1	Functional testing	Digital MFD Data Security Kit AR-FR22 Functional Testing Specifications
ATE_IND.2	Independent testing - sample	TOE
AVA_MCU.1	Examination of guidance	AR-FR22 Data Security Kit Operation Manual, AR-FR22 Data Security Kit Notice, LASER PRINTER KEY OPERATOR'S GUIDE, LASER PRINTER OPERATION MANUAL (for general information and copier operation), OPERATION MANUAL (for printer), FACSIMILE EXPANSION KIT OPERATION MANUAL, OPERATION MANUAL (for network scanner)
AVA_SOF.1	Strength of TOE security function evaluation	Digital MFD Data Security Kit AR-FR22 Strength of Security Function Analysis
AVA_VLA.1	Developer vulnerability analysis	Digital MFD Data Security Kit AR-FR22 Vulnerability Analysis

6.3 Strength of Security Function

The following security functions are based on a probabilistic or permutational mechanism: authentication (TSF_AUT) and data clear (TSF_FDC), which correspond to FIA_UAU.2, FIA_UAU.7, FIA_AFL.1 and security management (TSF_FMT), which corresponds to FIA_SOS.1. Authentication and security management provide password-related mechanisms that are probabilistic or permutational. The strength of these security functions is SOF-basic.

[DSK_ST]

7 PP Claims

The TOE does not claim conformance to a PP.

8 Rationale

This chapter demonstrates the completeness and consistency of this ST.

8.1 Security Objectives Rationale

Table 14 demonstrates that the policies indicated in the security objectives are effective for the organizational security policies, assumptions, and threats indicated in the TOE security environment. Table 14 shows the section of this document that provides the rationale for the correspondence between the security objectives and the threats, assumptions, and organizational security policies.

Table 14: Security Objectives Rationale

Security Objective	Threat	Assumption	Organizational Security Policy
	T.RECOVER	A.OPERATOR	P.RESIDUAL
O.RESIDUAL			8.1.3
O.REMOVE	8.1.1		
OE.OPERATE		8.1.2	
OE.ERASEALL			8.1.3

8.1.1 T.RECOVER

To counter T.RECOVER, which is the threat that a low-level attacker may read the actual image data which is stored in the Flash memory among the protected asset of this TOE, O.REMOVE stipulates that actual image data must be encrypted using a cryptographic key that is unique to the MFD before it is spooled so that the data is meaningless even if read.

With respect to cryptographic key stored and actual image data that is spooled among the protected asset of this TOE, when the volatile memory are 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 on the memory during the run of MFD, 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 volatile memory cannot be read and therefore information leakage from the Flash memory can be prevented, and information leakage from the actual image data spooled in volatile memory can be prevented.

8.1.2 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 organization that owns the TOE-equipped MFD. Therefore, A.OPERATOR can be achieved.

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 all data spooling areas of the MSD 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.

8.2.1 Security Functional Requirements Rationale

The correspondence between security functional requirements and security objectives is shown in Table 15. Table 15 shows the section that provides the rationale for the correspondence between the security functional requirements and the security objectives.

Table 15: Security Functional Requirements Rationale

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

8.2.1.1 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 job end or at the execution of clear all memory by key operator operation by FDP_RIP.1.

b) The key operator is identified and authenticated by FIA_AFL.1, FIA_UAU.2, FIA_UAU.7, and FIA_UID.2.

c) Only the key operator can enable/disable the clear all memory function by FMT_MOF.1.

d) An inquiry and a change (modify) of a key operator code become possible by FMT_MTD.1.

e) In case the key operator code is changed (modified), FIA_SOS.1 verifies that the inputted key operator code is 5-digits number to enables to set a key operator code with the defined quality of standard.

f) Key operator is assigned the role of TOE management by FMT_MOF.1 and FMT_MTD.1 and this role is maintained by FMT_SMR.1. The operations like enable/disable of clear all memory or query/modify of key operator code are allowed only by the key operator. According to the instruction of the key operator, overwriting of all data area of MSD can be performed.

g) According to FMT_SMF.1 manage the key operator code of FIA_UAU.2. The key operator can be identified and authenticated surely.

h) FPT_RVM.1 supports that the functional requirements to achieve O.RESIDUAL cannot be bypassed.

Each phenomenon does not compete in being a stand-alone phenomenon about a) from g) mutually. There is not the possibility that a function requirement competes in what is executed by a single function requirement about a), c), d), e), g). Contention does not occur in order four functional requirements supplement each other, and to execute identification authentication as for b). Contention does not occur in three functional requirements being independent by reason of control of security feature by a manager and TSF data as for f). Contention does not occur in h) being a requirement for use in a mutual support. Contention of a functional requirement does not occur to achieve O.RESIDUAL as above.

8.2.1.2 O.REMOVE

O.REMOVE is 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. 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. To enforce FCS_COP.1, a cryptographic key is generated according to FCS_CKM.1. The seed of cryptographic key is generated by the TOE and is accepted as having secure value for security attributes according to FMT_MSA.2. And FPT_RVM.1 supports that the functional requirements to achieve O.REMOVE cannot be bypassed.

Because FCS_CKM.1 and FMT_MSA.2 are with a matter of dependence nature of FCS_COP.1, competition does not occur. As for FPT_RVM.1, competition does not occur in what is a matter for use in a mutual support. Contention of a functional requirement does not occur to achieve O.REMOVE as above.

8.2.2 Rationale for security functional requirement dependencies

Security functional requirement dependencies are shown in Table 16. Table 16 shows the dependencies that the security functional requirements must satisfy according to the CC, the dependencies that the TOE satisfies, and the section that provides the rationale for dependencies that are not satisfied.

Table 16: Security Functional Requirement Dependencies

Functional Requirement	Stipulated dependencies	Satisfied dependencies	Rationale for dependencies not satisfied
FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FMT_MSA.2	8.2.2.1
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FMT_MSA.2	8.2.2.1
FDP_RIP.1	No dependencies	No dependencies	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2(*)	
FIA_UAU.2	FIA_UID.1	FIA_UID.2(*)	
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2(*)	
FIA_UID.2	No dependencies	No dependencies	
FIA_SOS.1	No dependencies	No dependencies	
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1, FMT_MSA.1, FMT_SMR.1	ADV_SPM.1, FMT_SMR.1	8.2.2.2
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	
FMT_SMR.1	FIA_UID.1	FIA_UID.2(*)	
FMT_SMF.1	No dependencies	No dependencies	
FPT_RVM.1	No dependencies	No dependencies	

(*) Dependencies on FIA_UID.1 and FIA_UAU.1 are satisfied by the hierarchical components FIA_UID.2 and FIA_UAU.2.

8.2.2.1 Rationale for no dependencies on FCS_CKM.4

The cryptographic key is stored in volatile memory and when the power is off, electrical charge of volatile memory in which the cryptographic key is stored disappears and the cryptographic key is destructed. Therefore it doesn’t require any dependence.

8.2.2.2 Rationale for no dependencies on FMT_MSA.1 and FDP_ACC.1

The seed of cryptographic key is a security attribute related to cryptographic operation that is managed by the TOE. The key operator is not permitted to change the seed of cryptographic key, and thus FMT_MSA.1 is not required. Similarly access control is not needed, and thus FDP_ACC.1 is not required.

8.2.3 Mutual effect of security requirements

Table 17 shows the mutual effect of security requirements.

Table 17: Mutual effect of security requirements

Functional Requirement	Requirement providing protection	
	Bypassing	Deactivation
FCS_CKM.1	FPT_RVM.1	None
FCS_COP.1	FPT_RVM.1	None
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1
FIA_AFL.1	FPT_RVM.1	None
FIA_UAU.2	FPT_RVM.1	None
FIA_UAU.7	FPT_RVM.1	None
FIA_UID.2	FPT_RVM.1	None
FIA_SOS.1	FPT_RVM.1	None
FMT_MOF.1	FPT_RVM.1	None
FMT_MSA.2	None	None
FMT_MTD.1	FPT_RVM.1	None
FMT_SMR.1	None	None
FMT_SMF.1	None	None

8.2.3.1 Bypassing

Bypassing of the functional requirements in Table 17 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 actual image data before it is spooled. In addition, the encrypted image data is always decrypted before use, and thus bypassing is not possible.

c) Sub-set residual information protection FDP.RIP.1 is always invoked during auto clear at job end and clear all memory by key operator operation, and thus bypassing is not possible.

d) FIA_AFL.1, FIA_UAU.2, FIA_UAU.7, and FIA_UID.2 related to key operator identification and authentication are always invoked during identification and authentication of key operator, 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 behavior FMT_MOF.1 always requires key operator identification and authentication before clear all memory is executed. To cancel clear all memory, key operator authentication is also always invoked after selection of the cancellation operation, and thus bypassing is not possible.

g) Management of TSF data FMT_MTD.1 always requires identification and authentication of the key operator, the setting is stored in EEPROM, and thus bypassing is not possible.

8.2.3.2 De-activation

Regarding deactivation in Table 17, FDP_RIP.1 ensures protection from acts of deactivation in that access is restricted only to the key operator according to FMT_MOF.1.

8.2.3.3 Tampering

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

8.2.4 TOE security assurance requirements Rationale

The TOE is an MFD firmware upgrade kit, and is a 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 dependency on ADV_SPM.1 that is indicated in the functional requirement FMT_MSA.2.

Each requirement does not compete in assurance requirements aside from ADV_SPM.1 applying a package of EAL3 mutually. Competition with other requirements does not occur in ADV_SPM.1 being assurance requirements of individual specifications named a TSP model.

8.2.5 Rationale for Minimum Strength of Function

It is expected that the Data Security Kit AR-FR22 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 AR-FR22 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. Each explicit strength of function of FIA_AFL.1, FIA_UAU.2, FIA_UAU.7 and FIA_SOS.1 is SOF-base and they don’t conflict 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 11, the rationale is shown below.

8.3.1.1 FCS_CKM.1

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

8.3.1.2 FCS_COP.1

Spooled actual image data 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

For auto clear at job end, residual information protection is accomplished by overwriting the actual image data file stored in volatile memory (copy jobs, print jobs, scan send jobs) and Flash memory (PC FAX, fax transmission, and fax reception jobs) by TSF_FDC. For clear all memory by key operator operation, residual information protection is accomplished by overwriting all actual image data stored in volatile memory and Flash memory by TSF_FDC. Therefore, FDP_RIP.1 is satisfied.

8.3.1.4 FIA_AFL.1

Access to security management function (key operator program) by TSF_AUT, and key operator authentication for use in interruption of the all data areas clearing function by key operator operation by TSF_FDC, the handling in authentication failure is carried out, and thus FIA_AFL.1 is satisfied.

8.3.1.5 FIA_UAU.2

Authentication by the entry of the key operator code is performed to access the security management functions (key operator programs) by TSF_AUT, and thus FIA_UAU.2 is satisfied. In addition, entry of the key operator code is required to cancel clear all memory by key operator operation (TSF_FDC), and thus FIA_UAU.2 is satisfied.

8.3.1.6 FIA_UAU.7

During key operator authentication by TSF_AUT, each entered digit is displayed as "*" to provide protected feedback. In addition, during entry of the key operator code to cancel clear all memory by key operator operation (TSF_FDC), the TOE hides the entered digits and displays "*" instead for each entered digit to indicate the number of digits entered, and thus FIA_UAU.7 is satisfied.

8.3.1.7 FIA_UID.2

The key operator is identified by TSF_AUT when the key operator programs are selected and by TSF_FDC when cancellation is selected, and thus FIA_UID.2 is satisfied.

8.3.1.8 FIA_SOS.1

When the key operator code is changed (modified) by TSF_FMT, it is verified that the key operator code is 5-digits number, and thus FIA_SOS.1 is satisfied.

8.3.1.9 FMT_MOF.1

The execution of clear all memory by key operator operation (by TSF_FDC) is possible after identification and authentication of key operator by TSF_AUT, and cancellation of clear all memory is possible by identification and authentication of key operator by TSF_FDC, and thus FMT_MOF.1 is satisfied.

8.3.1.10 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.

8.3.1.11 FMT_MTD.1

A 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.

8.3.1.12 FMT_SMR.1

Identification and authentication of key operator by TSF_AUT specifies the key operator. This associates the user with the role, and thus FMT_SMR.1 is satisfied. 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 FMT_SMF.1

FMT_SMF.1 contains the ability to manage the key operator code by TSF_FMT, which is management requirement of FIA_UAU.2, and thus is satisfied. With respect to the cryptographic key attributes, generation of the cryptographic key is assured by ADV_SPM.1 and there is no need to manage attribute changes, therefore there is no management requirements for FCS_CKM.1 or FMT_MSA.2. There is not a management item on FIA_AFL.1 the authentication failure number of times does not need management in order to be fixed value, and stop time to a re-authentication is fixed time, it does not have to manage, it returns to a normal state automatically. User identification information does not have to be managed, because identification operation is fixed, and there is no management requirements for FIA_UID.2. Timing of overwriting does not have to be managed, because a timing of overwriting is only upon the deallocation of the resources from an object, and there is no management requirements on FDP_RIP.1. With respect to the verification metric for secrets, the code consists of fixed values (5-digits and number) and thus there is no need for management and no management requirements for FIA_SOS.1. Role groups that mutually interact with TSF functions and TSF data are fixed, and thus there is no need for management and no management requirements for FMT_MOF.1 or FMT_MTD.1. Users having a role are the key operator only, and as there is no need for management, there are no management requirements for FMT_SMR.1.

8.3.1.14 FPT_RVM.1

According to the following IT security functions, corresponding functional requirements are certainly performed and never be bypassed, and thus FPT_RVM.1 is satisfied.

a) When the MFD is powered on, a cryptographic key is always generated by TSF_FKG and thus FCS_CKM.1 is satisfied.

b) When actual image data is spooled to Flash memory, it is always encrypted by TSF_FDE. When actual image data that has been spooled to Flash memory is read and the job is processed, it is always decrypted by TSF_FDE. Therefore, FCS_COP.1 is satisfied.

c) When auto clear at job end or clear all memory by key operator operation is executed, data overwriting is always enforced by TSF_FDC, and thus FDP_RIP.1 is satisfied.

d) When key operator identification and authentication are performed, key operator identification and authentication are always executed by TSF_AUT and TSF_FDC, and thus FIA_AFL.1, FIA_UAU.2 and FIA_UID.2 are satisfied.

e) During key operator authentication, the entered digits are always displayed as “*” by TSF_AUT and TSF_FDC, and thus FIA_UAU.7 is satisfied.

f) When the key operator code is changed (modified), TSF_FMT always verifies that the key operator code is 5-digits number, and thus FIA_SOS.1 is satisfied.

g) When clear all memory by key operator operation is executed or cancelled, key operator identification and authentication are always executed by TSF_AUT and TSF_FDC before execution or cancellation of clear all memory by TSF_FDC, and thus FMT_MOF.1 is satisfied.

h) Change (modifying) of key operator code is always executed by TSF_FMT after identification and authentication of key operator by TSF_AUT and thus FMT_MTD.1 is satisfied.

8.3.2 TOE assurance measures Rationale

The assurance measures in section 6.2 satisfies TOE security assurance requirements by means of the following contents of each assurance measures.

a) ACM_CAP.3, ACM_SCP.1

Assurance measures: Digital MFD Data Security Kit AR-FR22 Configuration Management,
Digital MFD Data Security Kit AR-FR22 VERSION S.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

Assurance measures: Digital MFD Data Security Kit AR-FR22 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

Assurance measures: AR-FR22 Installation Instruction Manual (Japanese),
AR-FR22 Installation Instruction Manual (English, German, French, Spanish)

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

d) ADV_FSP.1

Assurance measures: Digital MFD Data Security Kit AR-FR22 Security Functional Specifications

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

e) A DV_HLD.2

Assurance measures: Digital MFD Data Security Kit AR-FR22 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

Assurance measures: Digital MFD Data Security Kit AR-FR22 Representation Correspondence Analysis

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

g) ADV_SPM.1

Assurance measures: Digital MFD Data Security Kit AR-FR22 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

Assurance measures: AR-FR22 Data Security Kit Operation Manual,
AR-FR22 Data Security Kit Notice,
LASER PRINTER KEY OPERATOR'S GUIDE,
LASER PRINTER OPERATION MANUAL (for general information and copier operation),
OPERATION MANUAL (for printer),
FACSIMILE EXPANSION KIT OPERATION MANUAL,
OPERATION MANUAL (for network scanner)

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

Assurance measures: AR-FR22 Data Security Kit Operation Manual,
AR-FR22 Data Security Kit Notice,
LASER PRINTER KEY OPERATOR'S GUIDE,
LASER PRINTER OPERATION MANUAL (for general information and copier operation),
OPERATION MANUAL (for printer),
FACSIMILE EXPANSION KIT OPERATION MANUAL,
OPERATION MANUAL (for network scanner)

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

j) ALC_DVS.1

Assurance measures: Digital MFD Data Security Kit AR-FR22 Development Security Specifications,
Development security for Data Security Kit

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

k) ATE_COV.2

Assurance measures: Digital MFD Data Security Kit AR-FR22 Coverage Analysis

Contents: It is the documents which 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

Assurance measures: Digital MFD Data Security Kit AR-FR22 High-level Design Testing Analysis

Contents: It is the documents which 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

Assurance measures: Digital MFD Data Security Kit AR-FR22 Functional Testing Specifications,
Digital MFD Data Security Kit AR-FR22 Independent Testing Environment and Tools

Contents: It is the documents which describes about the tests to establish that all the execution of the security function is as stated in the specifications.

n) ATE_IND.2

Assurance measures: TOE

Contents: TOE suitable for testing

o) AVA_MSU.1

Assurance measures: AR-FR22 Data Security Kit Operation Manual,
AR-FR22 Data Security Kit Notice,
LASER PRINTER KEY OPERATOR'S GUIDE,
LASER PRINTER OPERATION MANUAL (for general information and copier operation),
OPERATION MANUAL (for printer),
FACSIMILE EXPANSION KIT OPERATION MANUAL,
OPERATION MANUAL (for network scanner)

Contents: It is the documents (operation manuals) which is 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

Assurance measures: Digital MFD Data Security Kit AR-FR22 Strength of Security Function Analysis

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

q) AVA_VLA.1

Assurance measures: Digital MFD Data Security Kit AR-FR22 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

Probabilistic and permutational mechanisms provided by the TOE are used in the key operator authentification (TSF_AUT), data clear (TSF_FDC) and key operator code change (modifying) (TSF_FMT) security functions. The strength of these security functions is SOF-basic.

On the other hand, the minimum strength of function for the TOE is SOF-basic. As each strength of function level do not conflict, SOF-basic which is a strength of security function is appropriate.