Digital Multifunction Device
Data Security Kit
AR-FR4/AR-FR5

Security Target

Version 0.04

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.

July 30, 2004

Sharp Corporation

History of revisions

Date	Version	Revision
March 4, 2004	0.01	Preparation of first edition
May 18, 2004	0.02	Correction of indicated contents
May 20, 2004	0.03	Correction of indicated contents
July 30, 2004	0.04	Correction of indicated contents

Table of Contents

List of tables

List of figures

1 ST Introduction

1.1 ST Identification

This section presents information for the purpose of identifying the ST and TOE.

ST title	Digital Multifunction Device Data Security Kit AR-FR4/AR-FR5 Security Target	
Version	0.04	
Publication date	July 30, 2004	
Author	Sharp Corporation	
TOE Identification	Japan	Data Security Kit AR-FR4 version M.20
	Overseas	Data Security Kit AR-FR4 version M.20, Data Security Kit AR-FR5 version E.20
	The TOE identification varies due to differences in language and product name, however, the product is the same.)	
CC Identification	CC version 2.1, ISO/IEC 15408:1999, JIS X 5070:2000	
Assurance Level	EAL4	
ST Evaluator	Fuji Research Institute Corporation Information Security Evaluation Center	
Keywords	Sharp, Sharp Corporation, Digital Multifunction Device, Multifunction Device, Multifunction Printer, MFP, MFD, object reuse, residual information protection, encryption, data encryption, data clearing	

1.2 ST Overview

This ST explains the AR-FR4 and AR-FR5 Data Security Kits for Sharp Digital Multi-Function Devices.

A Multi-Function Device (hereafter referred to as “MFD”) is an office machine consisting of a print unit with copy, scan, and fax options.

The TOE is a firmware upgrade kit that enhances the security function of the MFD. In an office environment where security is required, this kit provides functions that greatly reduce the danger that information from residual data stored in the MFD will be disclosed to a person who gains unauthorized access to the machine during processing or after completion of a print, copy, scan or fax job. In particular, when the MFD receives a job the data is encrypted before being spooled, and after the job is processed, a random pattern of data or fixed values are written over the spooled data to prevent unauthorized reproduction of the document or image data. The functions of the security kit are described in detail in Chapter 2 and Chapter 6.

The TOE requires that access to the area of use of the TOE (the office in which it is installed) be controlled according to procedures determined by the office, and that the employees in the office be generally trustworthy.

1.3 CC Conformance Claim

This document satisfies the following:

a) Conformity to CC Version 2.1, Part 2

b) Conformity to CC Version 2.1, Part 3

c) EAL4 Conformity

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

1.4 References

The following documentation was used to prepare this ST:

[CC_PART1] Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model, dated August 1999, version 2.1, CCIMB-99-031

[CC_PART2] Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032

[CC_PART3] Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033

[HOSOKU-0210] CCIMB Interpretations-0210

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 to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning.

The notation, formatting, and conventions used in this ST are largely consistent with those used in the Common Criteria (CC).

Selected presentation choices are discussed here.

The CC allows several operations to be performed on security functional components; assignment, refinement, selection, and iteration as defined in paragrah 2.1.4 of [CC_PART2] are:

a) 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.
b) The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
c) The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.
d) 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.
e) *Plain italicized text* is used to emphasize text.

1.5.2 Terminology

Terminology that is specific to this ST is indicated in Table 1.

Table 1: Terminology

Term	Definition
Data Security Kit	The AR-FR4 or AR-FR5 Data Security Kit (DSK) for the Sharp Digital Multifunction Device.
Key operator	An authorized user who manages the Data Security Kit for Sharp Digital Multifunction Devices.
Key operator text instructions	A general term for instructions that the key operator must follow in the MFP operation manual, the DSK operation manual, and the DSK installation checklist.
Latent image data	Residual information remaining on a mass storage device (MSD) when a copy/print/scan/fax job is completed, cancelled, or interrupted.
Memory	A memory device; in particular a semiconductor memory device.
Spooled data	The document or image data that is spooled to the MSD in the MFD for each copy, print, scan, or fax job.
Unauthorized user	An entity that interacts with the TOE Security Function (TSF) in a benign or malicious manner.

1.5.3 Acronyms

Acronyms used in this ST are indicated in Table 2.

Table 2: 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.
HDD	Hard Disk Drive
MSD	Mass Storage Device
OS	Operating System
PIN	Personal Identification Number
RAM	Random Access Memory
ROM	Read Only Memory In particular, refers to Masked ROM where the contents of the memory are determined at the time of manufacture and cannot be erased or changed after manufacture.

2 TOE Description

This chapter identifies the TOE type and explains the contents of the TOE evaluation by means of a detailed description of the configuration to be evaluated.

2.1 TOE Overview

The TOE is provided as a product. This section describes the category of the TOE and the category of the form in which it is provided as a product.

2.1.1 TOE Type

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

The TOE is part of the firmware[1] of the MFD. Stated more precisely, the TOE is a firmware upgrade kit that adds a security function to the firmware of the MFD.

Part of the TOE is code that replaces part of the original firmware, and the remainder of the TOE is code that is added to the original firmware and is called up from the replacement part.

The TOE is to be installed in an office with high security requirements and is to be used by the employees that work there.

2.1.2 Product Form

The product, or DSK, is a security enhancement firmware upgrade kit that can be installed at the factory or in the field, and takes the form of a ROM product that replaces part of the ROM of the MFD.

A list of the MFD products that can be upgraded using this kit is shown in Table 3. These MFDs are a printer base to which copy, scan, and fax functions are added as required to meet the specific needs of the office where the machine is used. The ROM originally installed in these MFDs is one of two slightly different types, with the type installed depending the type of MFD.

Table 3: DSK models and corresponding MFD models

DSK model Version	Name	Corresponding MFD model
AR-FR4 version M.20	MFD Data Security Kit	MFD models sold outside of Japan AR-M350, AR-M450, AR-M280N, AR-M350N, AR-M450N, AR-M280U, AR-M350U, AR-M450U, AR-M300U, AR-M300N, DM-3551, DM-4551 MFD models sold in Japan AR-310M, AR-350M, AR-450M, AR-310S, AR-350S, AR-450S, AR-310F, AR-350F, AR-450F, DM-3551, DM-4551
AR-FR5 version E.20	[2]Printer Data Security Kit	Models sold outside of Japan AR-P350, AR-P450, DM-3500, DM-3501, DM-4500, DM-4501

[1] Software that is incorporated in hardware is generally called firmware. The TOE is firmware for the MFD, which is to say that the TOE is software incorporated in the MFD that controls the MFD hardware.

[2] When the MFD is configured only for the printer function, it is normally called a printer.

2.1.3 Variations in the Product Form

The DSK product is provided in two forms, the AR-FR4 and AR-FR5, depending on the MFD form. Both product forms consist of the same DSK, however, the form of the replacement ROM differs in accordance with the form of the ROM to be replaced.

When the MFD is configured only as a printer, the AR-FR5 is installed on MFDs sold outside Japan. When the MFD includes the copy function as well as the printer function (a scanner unit is installed that also enables installation of the fax expansion kit), the AR-FR4 is installed.

The MFD is equipped with a mass storage device such as an HDD, RAM (RAM disk) or Flash memory, which is determined by the configuration of function units. The image and document data of jobs run on the MFD are stored on the MSD. The DSK ensures the security of document and image data temporarily stored on the MSD inside the upgraded MFD.

2.1.4 Overview of the TOE Security Function

The TOE security function primarily consists of the data clear function and the data encryption function.

When a print, scan, or copy job is completed, the data clear function writes random data to the area where the *spooled data* is stored on the HDD or RAM (RAM disk). In the case of a fax job, which is stored in Flash memory, the data clear function writes fixed values to the area where the *spooled data* is stored.

The data encryption function encrypts document or image data before the data is stored on the MSD. As long as the encryption key is not obtained, the data encryption function makes it impossible to read document or image data before the data is cleared following completion of the job. As such, even before a job is completed, the *spooled data* stored on the MSD is protected from unauthorized or accidental disclosure.

The TOE security function also includes key generation and security management functions to enable efficient operation of the above two functions. A detailed description of these functions can be found in the TOE summary specifications in Chapter 6.

2.2 Scope and Boundary of the TOE Configuration

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

2.2.1 Physical Scope and Boundary

The physical configuration of the MFD is shown in Figure 1.

The control unit in the MFD that appears in the center of the diagram controls the entire MFD.

The TOE exists inside the replacement ROM module for the firmware on the controller board.

In addition to the replacement ROM that contains the TOE, the scope of physical effect of the TOE consists of the MSD to which jobs are spooled (HDD, RAM disk, or Flash memory), the EEPROM where security settings are stored, and the operation panel.

a) Controller unit including the DSK
   The controller unit consists of a microprocessor and the firmware that is run by the microprocessor. The controller unit also includes volatile RAM that is required for the operation of the microprocessor. The EEPROM is described in a separate section.
   The microprocessor in the controller unit runs all the TSF.
   The cryptographic key is stored in volatile RAM.
   The DSK is installed by replacing the firmware. The physical form of the replacement ROM and the ROM that is replaced is one or two ROM modules. The AR-FR5 consists of one ROM module, and the AR-FR4 consists of two ROM modules. Each ROM module consists of a ROM chip mounted on an approximately 25 mm x 60 mm printed circuit board module

with an edge connector. The ROM that is replaced and the replacement ROM containing the DSK are installed on the controller unit by means of an edge connector.

b) MSD to which jobs are spooled
This is an HDD, a RAM disk, or Flash memory. The HDD card option is connected to the controller unit. In configurations that do not have an HDD, part of the controller unit's volatile RAM is used as a RAM disk.
The Flash memory used for fax jobs is located on the fax interface card. This card is included in the optional fax expansion kit, and serves to connect the fax expansion kit to the MFD's controller unit in addition to containing Flash memory for storing spooled fax data.

c) Operation panel
The operation panel can be used to operate the MFD/printer and configure security settings for the TOE. From the perspective of the TOE environment, the operation panel is a device for the purpose of configuring TOE security settings and performing authorization.
On printers that are not equipped with a scanner unit, the machine's alphanumeric display panel is used to operate the machine. On MFDs that are equipped with a scanner unit, the scanner unit's touch panel is used to operate the machine (the machine's alphanumeric display panel cannot be used). These operation panels are all controlled by the controller unit.

d) EEPROM containing the security settings
The security settings described above are stored in the controller unit's EEPROM. To view or change the security settings, the operation panel described above must be used; no other methods (such as remote operation via communication) are possible.

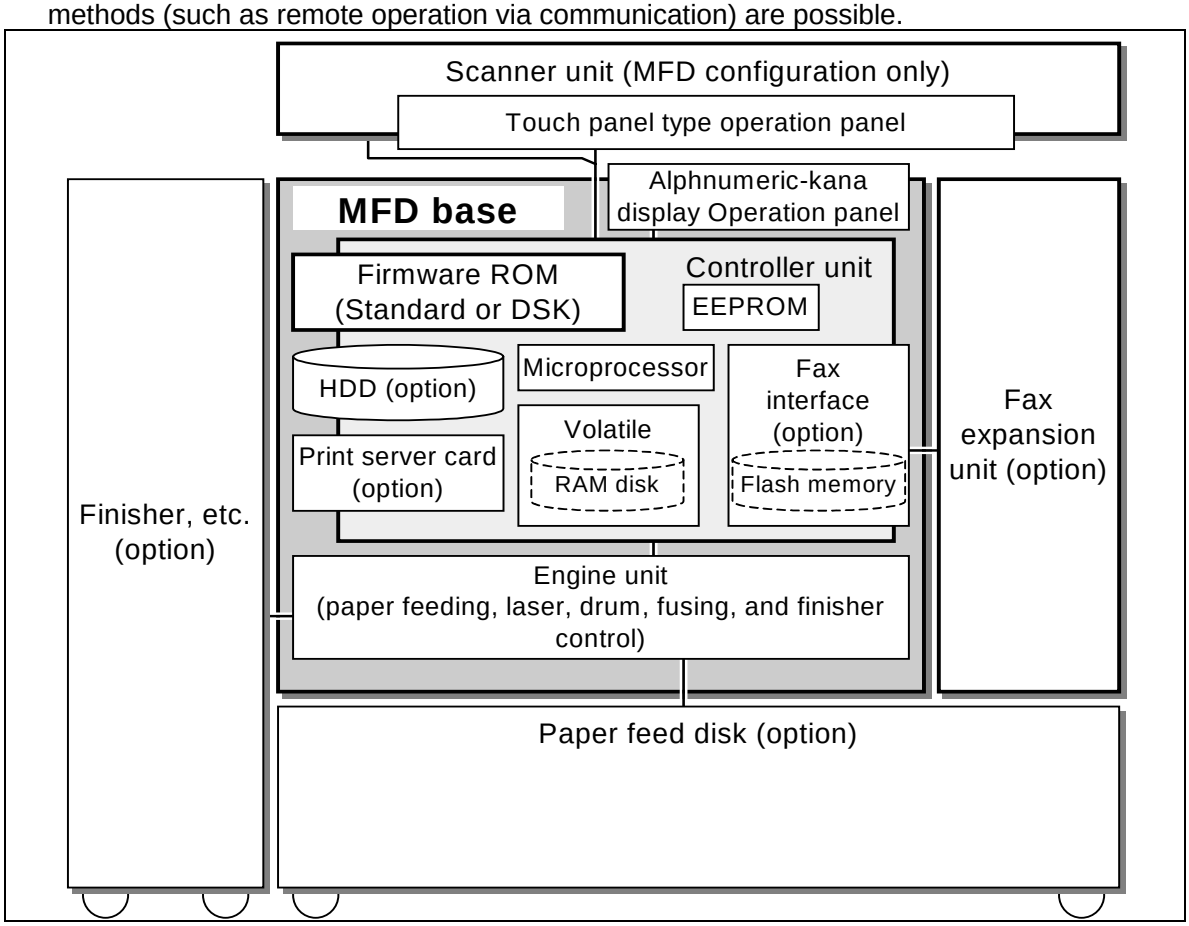

Figure 1: The TOE and physical configuration of the MFD

Considerations regarding the configuration of the machine outside the physical scope and boundaries of the TOE are stated below.

First, the distinction between the source of a job and the device that processes the job is explained. Although some units have both the attribute of a job source and a job processing device, this is because the operation of each option or unit differs.

1) Job sources
    a) Scanner unit
    The MFD operates as a copier, a network scanner, or a scanner for fax transmission
    b) Print server card (100 Base-TX / 10 Base-T network interface)
    The MFD receives a print request from the network
    c) IEEE1284 parallel interface
    The MFD receives a print request from the IEEE1284 parallel interface
    d) Fax expansion kit
    The fax reception function of the MFD operates through the mediation of the telephone line
2) Job processing devices
    a) Print server card (100 Base-TX / 10 Base-T network interface)
    When the MFD operates as a network scanner
    b) Fax expansion kit
    When the fax transmission function of the MFD operates
    c) Engine unit
    d) Paper feed disk
    e) Finisher

Print, copy, scan, and fax jobs that the MFD processes originate outside of the physical (and logical) scope of the TOE, and upon being received by the MFD, are spooled. The TOE intervenes at the stage where a job is spooled, and encrypts the spooled data. For example, a copy job, scan job, or fax transmission job originates in the scanner unit option, in the MFD controller unit, and in the operation panel.

After being spooled, the job is decrypted by the TOE and then is processed outside of the physical (and logical) scope of the TOE, which is to say that it is printed or transmitted. In the case of printing, the processing of a print job, copy job, or fax reception job consists of the MFD controller unit causing the MFD engine unit to print the spooled data of the job.

Each unit, including the engine unit, scanner unit option, print server card (100 Base-TX / 10 Base-T network interface), paper disk, and finisher, has a microprocessor and firmware. However, the DSK does not change the firmware of any of these units and does not affect their operation; and thus these units are not within the physical scope of the TOE.

The MFD controller unit includes an IEEE1284 parallel interface to receive print jobs. The controller unit can also be equipped with an optional fax expansion kit (which enables connection to the telephone line for the fax function) and a print server card (100 Base-TX / 10 Base-T network interface). Jobs are input to and output from the MFD via these interfaces. Print jobs are received via the parallel interface and network interface, fax reception jobs are received via the phone line, fax transmission jobs are sent via the phone line, and scan jobs are sent via the network interface.

2.2.2 Logical Scope and Boundaries

The logical configuration of the TOE is shown in Figure 2.

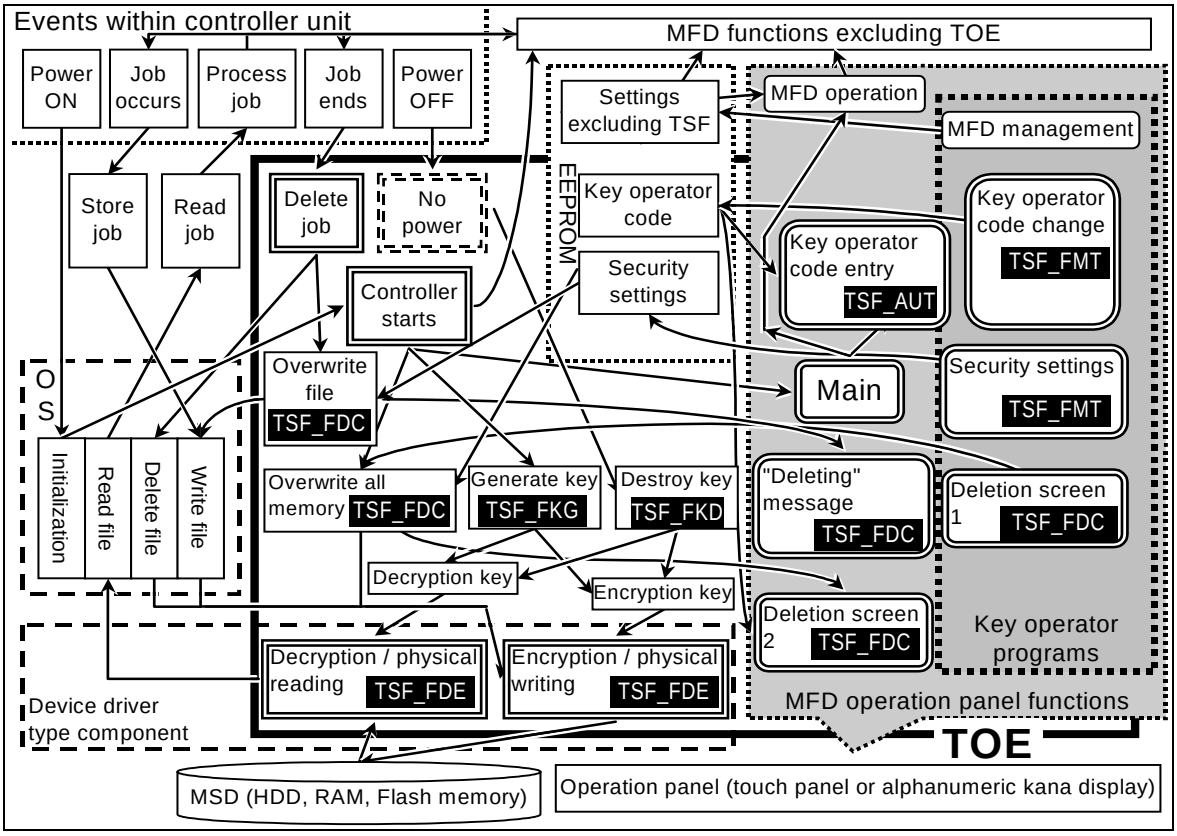

Figure 2: Logical configuration of the TOE

The controller unit firmware (including the TOE) is a single program that runs on the controller unit. The software operation environment of the TOE is the microprocessor used by the controller unit and the OS. The microprocessor is described in a) in 2.2.1.

The firmware broadly consists of three components. These are the above mentioned OS component, a component playing the role of software applications running on the OS, and a component that plays a device driver-like role, controlling the hardware together with the OS. The TOE consists of part of the software application component and part of the device driver component. The diagram shows only those parts of the OS function and device driver component that are necessary to explain the interface to the TSF.

MFD hardware shown in the diagram are the MSD and operation panel. All other descriptions are of software functions (program, data, and objects). Among the software functions, the OS function and device driver component are outlined by broken lines. All other software functions are the software application component. The rectangle with rounded corners indicates the operation panel function (user interface), while the other software functions are indicated by rectangles. Among these, the interface to the TSF is indicated by a double line. Acronyms of software functions in the TOE unique to specific TSF are indicated by outline characters.

The logical boundaries of the TOE are determined by the following TOE security functions (TSF):

a) Data Clear
b) Data Encryption (TSF_FDE)
c) Key Generation (TSF_FKG)
d) Key Destruction (TSF_FKD)
e) Authentication (TSF_AUT)
f) Security Management (TSF_FMT)

A detailed explanation of each TSF is provided in Chapter 6. The logical scope and boundary are explained here.

a) Data Clear (TSF_FDC)

During normal operation, the MFD spools document and image data to an MSD. The data of printer, copy, and scan jobs are spooled to an HDD or RAM disk, and the data of fax jobs are spooled to Flash memory.

When a job is completed, the data of the job is no longer needed and the MFD deletes the data file from the MFD. This is accomplished by rewriting the management area of the MSD so as to delete the file registration. This releases the management area and data area that the file occupied, freeing these areas for use by other jobs. However, there is no guarantee that the data area of the deleted file will be overwritten by a spooled data file of another job.

The data clear function (TSF_FDC) of the TOE adds a data area overwrite function to the file delete function of the MFD. This function overwrites the data area that was occupied by the deleted file. This function is called the *Auto Clear at Job End* function.

The data clear function (TSF_FDC) of the TOE also clears (by overwriting) the entire spooled data area of the HDD or RAM disk when the MFD is powered on. This function is called the *Power Up Auto Clear* function.

A function for manual clearing of the memory area of the HDD, RAM disk, and Flash memory is also provided. This function is called the *Clear All Memory* function. In particular, this ST indicates this as *Clear All Memory by Key Operator Operation*.

In relation to this TSF, installing the TOE in the MFD adds code for the overwrite function, and the existing file deletion code is replaced by code that includes a call to the overwrite function. When a job is completed, the TOE deletes the file and automatically clears (overwrites) the memory occupied by the file, and when the machine is powered on, the TOE automatically clears (overwrites) the entire spool area of the HDD or RAM disk. The TOE also provides the clear all memory function via the user interface.

Thus, with regard to this TSF, the overwrite function is included within the logical scope of the TOE. The entry point of the spooled data file deletion function is one logical boundary. This entry point is called when the MFD finishes a job. The entry point of controller startup is also a logical boundary. This is called in order to start up the file system management functions of the HDD/RAM and Flash memory when the MFD is powered on. The user interface of the TSF is as follows:

- Data clearing message
  This appears during *Auto Clear at Job End*. The message is called by the TSF within the TOE.
- *Clear All Memory* operation
  This is a user interface for *Clear All Memory by Key Operator Operation*. This is included in the *security settings* user interface in security management (TSF_FMT) described later.
- Clear screen 1
  This is displayed during the above operation. The screen allows the user to confirm or cancel the clear all memory operation. The screen is called by the TSF within the TOE.
- Clear screen 2
  This is displayed when the user confirms the *Clear All Memory* operation in clear screen 1, and during automatic memory clear when the machine is powered on. The screen indicates that all memory is being cleared and shows progress as a percentage. The screen is called by the TSF within the TOE.

b) Data Encryption (TSF_FDE)

When a job occurs, the job is spooled by creating a data file in the MSD. During the creation of the file, the data is encrypted and written to the MSD by the data encryption function (TSF_FDE) of the TOE. When the spooled job is actually processed, each block of data of the spooled job is read from the MSD and decrypted as it becomes needed. The decryption function is included within the encryption function (TSF_FDE). Encryption and decryption are called at the time of reading/writing the job file. The key used for encryption and decryption is stored in volatile RAM.

In relation to this TSF, installing the TOE in the MFD adds encryption and decryption code, and the existing file read/write code is replaced with code that includes calls to the encryption and decryption code. The encryption code is executed when spooled job data is written to the MSD, and the decryption code is executed when the spooled data is read from the MSD. The encryption and decryption codes include access to the key.

Thus, with regard to this TSF, the code for reading, writing, encrypting, and decrypting the spooled data file of a job and the key in volatile RAM are included within the logical scope of the TOE, and the entry points of the device drivers that provide, by MSD sector, the read/write function to the OS are the logical boundaries. These entry points are called via the OS when the MFD receives a job and stores the spooled data, and during processing of the job when the spooled data is read.

The encryption operation of the TOE guarantees that unauthorized access from the MFD operation panel or an external interface (network interface, IEEE1284 parallel interface, or telephone line interface) will not be possible.

c) Key Generation (TSF_FKG)

b) Key Destruction (TSF_FKD)

The key generation function and the key destruction function handle the key information of the MFD. A cryptographic key is generated (TSF_FKG) and stored in volatile RAM when the MFD is powered on. Using circuits that store electric charges as memory elements, volatile RAM stores information by means of electric charges. When the MFD is powered off or an interruption in the power supply occurs, the stored electric charges disappear and the key stored in volatile RAM can no longer be read, resulting in key destruction (TSF_FKD). The key generated by the key generation function (TSF_FKG) is used until key destruction (TSF_FKD) takes place.

In relation to TSF_FKG, installing the TOE in the MFD adds key generation code. In particular, the spool management initialization code that is executed when the controller is started up is replaced by a version of the code that calls the key generation code. This code is executed when the MFD and TOE are powered on.

The key generation code in the TOE and the key in volatile RAM are included within the logical scope of the TOE, and the entry point of controller start-up described above in the data clear section is the logical boundary. The logical scope of TSF_FKD is the key in volatile RAM, and TSF_FKD does not have a logical boundary.

The key generated by the TOE is stored in volatile RAM, and the implementation assures that unauthorized access from the MFD operation panel or an external interface (network interface, IEEE1284 parallel interface, or telephone line interface) will not be possible.

The key used for encryption and decryption of spooled data in the HDD or RAM disk uses date and time data and tick time, with the date and time data obtained from the RTC (clock circuit). This RTC continues to operate regardless of whether the MFD is powered on or off. Date and time data obtained from the RTC can be set by the key operator, however, it is in practice impossible to match the date and time data to the tick data, and thus the same key cannot be generated twice.

e) Authentication (TSF_AUT)

The MFD has an MFD management function that exists prior to installation of the DSK, and this function consists of settings that are called *key operator programs*. Within the organization that uses the MFD, the administrator of the MFD who is allowed to run the key operator programs is called the *key operator*. To run a key operator program, the key operator must obtain authorization by entering a 5-digit PIN number. This PIN is called the *key operator code*. The key operator code ensures that only the key operator can access the key operator programs.

General users can use the functions of the MFD other than the key operator programs without authorization.

The DSK protects its security management function with the same authorization as the above key operator code, unifying its authorization with key operator code authorization. In addition, access to the security management function is incorporated into the key operator program menu. In other words, the DSK adds security management function access to the key operator programs of the MFD, and implements the key operator code as a means of authorization.

As such, to access the security management function (TSF_FMT), the key operator must obtain authorization by entering the key operator code, and only the key operator is capable of this access.

The key operator code is stored in the EEPROM in the MFD. The TSF compares the code entered by the user to the code stored in the EEPROM, and authorizes the user if the two codes match.

The user interface for authorization provided by the DSK is included within the logical scope of the TOE. The logical boundary of the TOE as related to the TSF is the access operation performed by the user using the authorization user interface.

f) Security Management (TSF_FMT)

Installation of the TOE in the MFD adds access to parameters that can be changed with the security management function, and also adds a user interface under the security management menu. In addition, in the user interface, installation of the TOE replaces the top menu of the key operator programs with a menu that also calls the security management function, and replaces the authorization screen with a screen that calls the new top menu.

The user interface of this TSF is as follows:

- Security settings
  These control the operation of the data clear function (TSF_FDC). The settings can be changed using the operation panel. When a setting is changed, the value stored in the EEPROM of the MFD is rewritten.
  This also includes the user interface of *Clear All Memory by Key Operator* described previously.
- Changing the key operator code
  The key operator code can be changed using the operation panel, upon which the code stored in the EEPROM of the MFD is rewritten.

The above user interfaces, and the user interfaces that form a path linking the authorization user interface to the above user interfaces, are included within the logical scope of the TOE. The logical boundary of the TOE in relation to the TSF is authorization (TSF_AUT). The operation performed by the user of the TSF to access the authorization screen forms a logical boundary of the TOE.

2.3 Lifecycle of the MFD and Assets Protected by the TOE

Assets protected by the TOE during the lifecycle of the MFD (from the time of purchase to the time of disposal) are as follows:

2.3.1 Purchase of the MFD and TOE or Start of Lease

There are no protected assets at the time of purchase or at the start of the lease of the MFD and TOE.

2.3.2 When the MFD and TOE are in Operation

When the MFD is in operation, assets to be protected are as follows:

a) When machine trouble occurs, spooled data generated in the MSD of a copy, print, scan, or fax job not yet completed

b) The following settings of the security management function of the TOE:
- *Power Up Auto Clear* enabled or disabled
- *Auto Clear at Job End* number of repetitions
- *Power Up Auto Clear* number of repetitions
- *Clear All Memory by Key Operator Operation* number of repetitions
- Key operator code

In the following cases, spooled data (a protected asset) will remain in the MSD.

1. When the power of the MFD is interrupted due to machine trouble before a copy, print, scan, or fax job is completed.

2. When a power interruption occurs before spooled data in the MSD is deleted using the MFD operation panel when the job retention function of the MFD is used.
   The job retention function can be used when a hard disk drive is installed in the MFD, and is used when printing from a computer (when the print function of the MFD is being used). The following job retention functions are available:
   - Hold after printing
     After printing is finished, this function holds the print data in the MSD until the MFD is powered off or until the data is deleted. The job can be reprinted as needed using the MFD operation panel.
   - Hold without printing
     When the MFD receives a print job, it holds the print data in the MSD without printing it. Printing can be initiated using the MFD operation panel. The print data is held until the MFD is powered off or the job is deleted.
   - Sample print
     When the MFD receives a print job from a computer, it prints only one set of copies. The print data is retained in the MSD, and the user can print the remaining sets using the MFD operation panel. The print data is held until the MFD is powered off or the job is deleted.

   When using any of these functions, printing or deletion of the print data is possible only if the passcode specified at the computer when the print job was sent is entered at the MFD operation panel. The job retention function is a regular function that is used to initiate printing using the MFP operation panel as described above; it is not a security function of the TOE.
   The passcode makes it possible to use the job retention function. Assets that are to be protected by the TOE are indicated above in a) and b), and these do not include misuse of a passcode. For this reason, the TOE does not protect against misuse of a passcode.

The MFD is equipped with an IEEE1284 parallel interface, a telephone line interface, and a network interface, however, during use of the MFD it is not possible to access spooled data in the MSD from these external interfaces be means of unintended use of the MFD.

2.3.3 Disposal of the MFD and TOE or Expiration of Lease

Assets to be protected at the time of disposal of the MFD and TOE or when the MFD is returned at the expiration of a lease are spooled data remaining in the MFD as described in 1 in 2.3.2 and 1.

3 TOE Security Environment

This chapter discusses the TOE security environment.

3.1 Assumptions

This section describes the security aspects of the intended environment of the TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, user, and key operator guidance. The following specific conditions are assumed to exist in an environment where this TOE is employed.

3.1.1 Environment Assumptions

The environmental assumptions delineated in Table 4 are required to ensure the security of the TOE.

Table 4: Environmental Assumptions

Definition	Description
A.OFFICE	The MFD with the TOE incorporated will be installed in a normal office environment. When the office employees are all out of the office, security measures such as locking the doors are taken. In addition, if someone needs to enter the office when no employees are present, there is a means of verifying that the person is an authorized employee.
A.PROCEDURE	The key operator carefully follows these procedures: • Verifies that the TOE is installed. • Configures suitable data clear and clear repetition settings. • Regularly changes the *key operator code*. • Uses a *key operator code* that cannot be guessed easily. • Does not disclose the *key operator code* to others.

3.2 Threats

Table 5 identifies the threats to the TOE. The threats to the TOE are considered to be users with public knowledge of how the TOE operates and possesses the skills and resources to physically remove the MSD from the MFD and use publicly available software and hardware tools to read the information. In addition, threats to management of the TOE security function are changing the data clear and clear repetition settings.

With respect to reading information in the MSD, a threat to the MSD exists if the MSD is stolen during operation of the MFD, if the MSD is temporarily removed, or if the MFD is disposed of, sold, or returned due to lease expiration.

With respect to TOE security management, a threat exists from operation of the MFD operation panel.

These security threats are mitigated by means of the objectives described in Chapter 4, Security Objectives.

Table 5: Threats to the TOE

Definition	Description
T.ALTER	It is possible that a malicious user may change the settings of the security management function of the TOE.
T.RECOVER	A malicious user may attempt to recover document or image data from the *residual data* in the MSD of a copy, print, scan, or fax job by physically removing the MSD from the MFD and using commercially available tools to read its contents.

3.3 Organizational Security Policies

There are no relevant organizational security policies.

4 Security Objectives

This chapter details the planned responses to security problems and threats. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

a) Security objectives for the TOE
b) Security objectives for the environment

4.1 Security objectives for the TOE

This section describes the security objectives of the TOE. The TOE accomplishes the security objectives defined in Table 6.

Table 6: Security objectives for the TOE

Definition	Description
O.AUTHENTICATION	To use the security function of the TOE, authorization must be performed by means of a *key operator code*.
O.REMOVE	Reading of job data must not be possible even if the MSD in the TOE-equipped MFD is accessed by a physical means other than via the MFD.
O.RESIDUAL	*Spooled data* from a job must be immediately cleared by overwriting a preset number of times once that job is completed. If the power is turned off or interrupted before the data is cleared, the data must be cleared by overwriting a preset number of times when the power is turned back on.

4.2 Security objectives for the environment

The security objectives for the environment are defined in Table 7.

Table 7: Security objectives for the environment

Definition	Description
OE.OPERATE	The key operator is a trustworthy person who will carry out the following without fail: • Verify that the TOE is installed. • Configure suitable data clear and clear repetition settings. • Regularly change the *key operator code*. • Will not use a *key operator code* that can be guessed easily. • Will not disclose the *key operator code* to others.
OE.SECURE	When the employees of an office where the TOE-incorporated MFD is installed are all out, security measures such as locking doors will be taken. In addition, if someone needs to enter the office when no employees are present, there is a means of verifying that the person is an authorized employee.

5 IT Security Requirements

This chapter defines the IT security requirements that shall be satisfied by the TOE or its environment.

The CC divides TOE security requirements into two categories:

a) TOE security functional requirements (SFR) (such as identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
b) TOE security assurance requirements (SAR) that provide grounds for confidence that the TOE and its supporting IT environment meet security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subsections.

5.1 TOE Security Functional Requirements (SFR)

The TOE satisfies the security functional requirements (SFR) delineated in Table 8. The rest of this section contains a description of each component and related dependencies.

Table 8: TOE Security Functional Requirements (SFR)

Functional Component ID	Functional Component Name
Cryptographic support (TSF_FDE, TSF_FKG, TSF_FKD)	
FCS_CKM.1(1)	Cryptographic Key Generation (1)
FCS_CKM.1(2)	Cryptographic Key Generation (2)
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
Data clear (TSF_FDC)	
FDP_RIP.1	Subset Residual Information Protection
Authentication (TSF_AUT)	
FIA_UAU.2	User Authentication before any Action
FIA_UAU.7	Protected Authentication Feedback
FIA_SOS.1	Verification of Secrets
Security Management (TSF_FMT)	
FMT_MOF.1(1)	Management of Security Functions Behavior (1)
FMT_MOF.1(2)	Management of Security Functions Behavior (2)
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles

5.1.1 Class FCS: Cryptographic Support

Application note
The key for encryption and decryption is generated when the DSK-equipped MFD is powered on. The key is stored in volatile RAM and is available until the MFD is powered off or power is otherwise removed. Once the key is lost, there is no way to recover it. Two encryption keys exist: one key for when an HDD or RAM is used as the MSD, and one key for when Flash memory is used for the MSD.

a) FCS_CKM.1(1) Cryptographic Key Generation (1)

Hierarchical to: No dependencies

FCS_CKM.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cyclical delay Fubonacci random number extension algorithm] and a specified

cryptographic key size [128 bits] that meet the following [AES Standard].

Dependencies: FCS_COP.1 Cryptographic Operation
FCS_CKM.4 Cryptographic key destruction

(In the security functional requirements (SFR), a dependency on FMT_MSA.2 is indicated, however, this TOE does not require FMT_MSA.2.) Details are given in 8.2.1.)

b) FCS_CKM.1(2) Cryptographic Key Generation (2)

Hierarchical to: No dependencies

FCS_CKM.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [MSN-T extension algorithm] and a specified cryptographic key size [128 bits] that meet the following [AES Standard].

Dependencies: FCS_COP.1 Cryptographic Operation
FCS_CKM.4 Cryptographic key destruction

(In the security functional requirements (SFR), a dependency on FMT_MSA.2 is indicated, however, this TOE does not require FMT_MSA.2.) Details are given in 8.2.1.)

c) FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No dependencies

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [power off or removed] that meets the following: [none].

Dependencies: FCS_CKM.1 Cryptographic Key Generation

(In the security functional requirements (SFR), a dependency on FMT_MSA.2 is indicated, however, this TOE does not require FMT_MSA.2.) Details are given in 8.2.1.)

d) FCS_COP.1 Cryptographic Operation

Hierarchical to: No dependencies

FCS_COP.1.1 The TSF shall perform [document and image data encryption and decryption] in accordance with a specified cryptographic algorithm [Rijndael algorithm] and cryptographic key size [128 bits] that meet the [AES Standard].

Dependencies: FCS_COP.1 Cryptographic Operation
FCS_CKM.4 Cryptographic Key Destruction

5.1.2 Class FDP: User Data Protection

a) FDP_RIP.1 Subset Residual Information Protection

Hierarchical to: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*de-allocation of the resource from*] the following objects: [Spool data of a print job, copy job, scan job, or fax job of the MFD].

Dependencies: No dependencies

5.1.3 Class FIA: Identification and Authentication

a) 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: No dependencies

(In the security functional requirements (SFR), a dependency on FIA.UID.1 is indicated, however, this TOE does not require FIA.UID.1 .) Details are given in 8.2.1.)

b) FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No dependencies

FIA_UAU.7.1 The TSF shall provide only [obscured feedback asterisks (*)] while the authentication is in progress.

Dependencies: FIA_UAU.2 User Authentication before any Action

c) FIA_SOS.1 Verification of Secrets

Hierarchical to: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that the secret matches the [5-digit key operator code].

Dependencies: No dependencies

5.1.4 Class FMT: Security Management

a) FMT_MOF.1(1) Management of Security Functions Behavior (1)

Hierarchical to: No dependencies

FMT_MOF.1(1) The TSF shall restrict the ability to [determine the behavior] of the function [enable/disable setting of Power On Data Clear] to the [key operator].

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

b) FMT_MOF.1(2) Management of Security Functions Behavior (2)

Hierarchical to: No dependencies

FMT_MOF.1.1(2) The TSF shall restrict the ability to [*operate*] the function [Clear All Memory by Key Operator Operation] to the [key operator].

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

c) FMT_MTD.1 Management of TSF Data

Hierarchical to: No dependencies

FMT_MTD.1.1 The TSF shall restrict the ability to [*query, modify,* [none]] the [key operator code, overwrite count of the HDD or RAM (RAM disk) during all data clear by key operator operation, overwrite count of the HDD

or RAM (RAM disk) during power on auto clear, and the overwrite count of the HDD or RAM (RAM disk) during auto clear after each job finishes] to the [key operator].

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

d) FMT_SMF.1 Specification of Management Functions

Hierarchical to: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [The management functions of the TOE indicated in Table 9].

Dependencies: No dependencies

Table 9: Management Functions of the TOE

Function Requirement	Management Function
FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(4)	None (attributes of the encryption key have not been changed, thus there are no management functions.)
FCS_COP.1, FIA_UAU.7, FMT_MSA.2, FMT_SMF.1	None (no requirement for management functions)
FDP_RIP.1	Functions that manage the following items related to overwrite clearing. • Enable/disable setting for power on auto clear • Overwrite count setting for auto clear at job end • Overwrite count setting for clear all memory by key operator operation • Overwrite count setting for power on auto clear
FIA_UAU.2	Key operator code change function
FIA_SOS.1	None (the quality scale is a constant value, thus there is no management function)
FMT_MOF.1(1), FMT_MOF.1(2), FMT_MTD.1	None (the role group reciprocally affecting and affected by the TSF function (TSF data) is fixed, thus there is no management function)
FMT_SMR.1	None (the only role that maintains the TOE is that of the key operator, thus there is no management function)

e) FMT_SMR.1 Security Roles

Hierarchical to: No dependencies

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

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

Dependencies: No dependencies

(In the security functional requirements (SFR), a dependency on FIA.UID.1 is indicated, however, this TOE does not require FIA.UID.1 .) Details are given in 8.2.1.)

5.2 TOE Security Assurance Requirements

Table 10 identifies the security assurance components drawn from [CC_Part 3] Security Assurance Requirements EAL4.

Table 10: EAL4 Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies:
ACM_AUT.1	Partial CM automation	ACM_CAP.3
ACM_CAP.4	Generation support and acceptance procedures	ACM_SCP.1, ALC_DVS.1
ACM_SCP.2	Problem tracking CM coverage	ACM_CAP.3
ADO_DEL.2	Detection of modification	ACM_CAP.3
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.2	Fully defined external interfaces	ADV_RCR.1
ADV_HLD.2	Security enforcing high-level design	ADV_FSP.1, ADV_RCR.1
ADV_IMP.1	Subset of the implementation of the TSF	AVD_LLD.1, ADV_RCR.1, ALC_TAT.1
AVD_LLD.1	Descriptive low-level design	ADV_HLD.2, 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
ALC_LCD.1	Developer defined life-cycle model	No dependencies
ALC_TAT.1	Well-defined development tools	ADV_IMP.1
ATE_COV.2	Analysis of coverage	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	Testing: high-level design	ADV_FSP.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, ATE_FUN.1
AVA_MSU.2	Validation of analysis	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_RCR.1
AVA_VLA.2	Independent vulnerability analysis	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1

5.3 Security requirements for the IT environment

There are no security requirements for the IT environment.

5.4 Explicitly Stated Requirements for the TOE

This ST does not contain explicitly stated requirements for the TOE. All security functional requirements (SFR) have been drawn from [CC_PART2].

5.5 Minimum Strength of Function

The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

Among the functional requirements that this TOE satisfies, only FIA_SOS.1 uses a probability or permutation mechanism, and the explicitly stated functional strength is SOF-basic. FCS_COP.1 is a functional requirement that uses an cryptographic algorithm, and thus not apply to this SOF level.

6 TOE Summary Specification

This chapter presents an overview to the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

6.1 TOE Security Functions (TSF)

This section presents the security functions performed by the TOE to satisfy the SFR in section 5.1. Traceability to SFR is also provided.

6.1.1 Cryptographic Support (TSF_FDE)

During normal operation, the MFD stores document or image data in an MSD as *spooled data*. Fax data is stored in Flash memory, and the document or image data of a copy, scan, or print job is stored as *spooled data* in an HDD or RAM disk. The DSK encrypts the data according to the AES standard using the Rijndael algorithm based on the key stored in volatile RAM, and spools it to the MSD.

When the spooled job is actually processed, each block of data of the spooled job is read from the MSD and decrypted as it becomes needed.

Functional Requirements Satisfied: FCS_COP.1

6.1.2 Cryptographic Key Generation (TSF_FKG)

The DSK generates cryptographic keys (common keys) to support the encryption function for document and image data. When the MFD is powered on, two cryptographic keys (common keys) are generated to implement the Rijdael algorithm according to the AES standard. One key is used for both encryption and decryption of spooled data that is stored in or read from the HDD or RAM disk in the MFD using the cyclical delay Fibonacci random number extension algorithm. The other key is used for both encryption and decryption of spooled data that is stored in or read from Flash memory in the MFD using the MSN-T extension algorithm. Both keys are 128 bits long. The keys are stored in volatile RAM.

Functional Requirements Satisfied: FCS_CKM.1

6.1.3 Cryptographic Key Destruction (TSF_FKD)

The DSK stores both of the above 128-bit keys in volatile RAM. Using circuits that store electric charges as memory elements, volatile RAM stores information by means of electric charges. When the MFD is powered off or an interruption in the power supply occurs, the stored electric charges disappear and the key stored in volatile RAM can no longer be read, resulting in key destruction.

Functional Requirements Satisfied: FCS_CKM.4

6.1.4 Data clear (TSF_FDC)

The DSK includes a data clear function that clears *spooled data*. This function consists of the following three programs:

a) Auto Clear at Job End
b) Power Up Auto Clear
c) Clear All Memory by Key Operator Operation

For *spooled data* stored in the HDD and RAM disk, random data is written over the data a preset number of times when the job is completed. For spooled data stored in Flash memory, constant values (zeros) are written over the data. This function is called the *Auto Clear at Job End* function.

In addition, each time the MFP is powered on, random data is written over the entire spooled data memory area of the HDD and RAM disk a preset number of times. This function is called the *Power Up Auto Clear* function.

It is also possible to write random data a preset number of times to the entire spooled data memory area of the HDD and RAM disk, and write constant values (ones) to all bits of the spooled data memory area of Flash memory using the Flash memory block clear function, by an operation performed by the key operator. This function is called the *Clear All Memory* function. In particular, this ST indicates this as *Clear All Memory by Key Operator Operation*.

The number of times that random data overwriting is repeated can be set by the key operator.

The reason that random data instead of fixed values are used to clear the HDD is to reduce the concern the residual magnetism will be amplified. The number of repetitions of random data overwriting can be increased to further reduce residual magnetism. The RAM disk is handled in the same way using the same overwriting method.

Due to the structure of Flash memory, only a zero can be written to a bit that has “1” as a value; writing “1” to a bit with “0” as a value is not possible. Changing the value of bits from “0” to “1” is only possible by collectively changing all values in a block of bits. Since using block clearing to clear the spooled data of one job would also clear data of other jobs, a single job is cleared by writing zeros over the data.

Cautionary points regarding this TSF (the data clear function) are given in the following.

The *Auto Clear at Job End* function operates immediately after a job is completed, however, in the event that the power is turned off or interrupted before a job is completed, the job will remain without being overwritten. In the case of an HDD, if the power is unintentionally removed even after a job is completed it is possible that automatic clearing may not be finished. Once a power interruption occurs, spooled data in an HDD or RAM disk is treated as invalid and thus a job that remains on an HDD or RAM disk due a power interruption will no longer be cleared by *Auto Clear at Job End*. For this reason the *Power Up Auto Clear* function is necessary, and the key operator should use this function according to the instructions in the key operator guide.

For a fax job in Flash memory, even if a power interruption occurs the job will not be treated as cleared until processing actually ends, and thus the job will be cleared by the *Auto Clear at Job End* function without fail. For this reason, Flash memory is not subject to the *Power On Auto Clear* function (there is no need to clear Flash memory when the power is turned on, and furthermore, this would not be acceptable). However, when the *Clear All Memory* function is executed, even jobs that are not complete are cleared.

Next, the relationship of jobs held using the job retention function to this TSF (the data clear function) is discussed.

A normal print job is treated as done once printing finishes normally and the TSF clears the spooled data. By contrast, a job held using the MFD’s job retention function is not treated as done until it is deleted from the hold job list, at which point the spooled data is cleared by the TSF. A job is deleted from the hold job list by means of a *Delete* operation at the MFP panel, or a *Delete After Printing* operation using the MFP panel followed by printing ending normally. In addition to these operations, a DSK *Clear All Memory* operation will clear spooled data, including the hold job.

If the power is removed without deleting a hold job, the job will be treated as an incomplete job and will remain on an HDD as described above. With respect to these matters, caution must be exercised and the instructions in the key operator documentation must be followed.

As is written in the key operator instructions, it is recommended that the key operator perform *Clear All Memory* before turning off the power to ensure that data does not remain due to any of the above causes.

The following is an overview of the *job retention* function.

The job retention function can be used only for print jobs when an HDD is installed in the MFD. This function makes it possible to control the timing of the start of printing and the end of a job (job done) from the MFD operation panel. The job retention function has three modes: *Hold After Printing*, *Hold Without Printing*, and *Sample Print*. When *Hold After Printing* is used, the job is printed normally and then stored in the HDD instead of being deleted. The job can be reprinted using the MFD operation panel. When *Hold Without Printing* is used, the MFD spools the job to the HDD without starting printing. Printing is started using the MFD operation panel and the job

can also be reprinted at a later time. *Sample Print* is used when printing multiple copies of a job to prevent a large number of misprints. When the function is used, the MFD initially only prints the first set of copies. Printing of the remaining sets is started using the MFD operation panel, and reprinting is also possible at a later time. With all modes a password can be assigned to the job, and in particular assigning a password allows *Hold Without Printing* to be used as a confidential print function. Three operations are possible at the operation panel in all modes: *Delete*, *Print and Delete*, and *Print and Save*. When *Delete* is used, or *Print and Delete* is used and printing ends normally, the job is considered done and the spooled data is cleared by the TSF.

Functional requirements satisfied: FDP_RIP.1, FMT_MOF.1(2), FMT_SMR.1

6.1.5 Authentication (TSF_AUT)

The TOE requires that the key operator enter a 5-digit PIN (key operator code) to access the key operator programs. By correctly entering the key operator code, the key operator is authorized. During entry of the key operator code, the TOE displays the entered digits as asterisks (*) so that the code is not visible.

In addition, with respect to the data clear function (TSF_FDC), entry of the key operator code is required for authorization in order to cancel execution of the power on auto clear function or the clear all memory by key operator operation function.

The key operator code authorization is a *probability or permutation type mechanism*. The strength of function (SOF) is SOF-basic.

Functional requirements satisfied: FMT_SMR.1, FIA_UAU.2, FIA_UAU.7, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MTD.1

6.1.6 Security Management (TSF_FMT)

Security Management (TSF_FMT) allows the following security functions to be selected after the key operator has been authorized by entry of the key operator code.

a) Enable/disable setting for power on auto clear

The number of times writing of random data to the HDD or RAM disk is repeated for the data clear function can also be set.

b) Overwrite count setting for auto clear at job end
c) Overwrite count setting for clear all memory by key operator operation
d) Overwrite count setting for power on auto clear

In addition, the authorization data (key operator code) can be changed.

e) Changing the key operator code

The key operator code is a 5-digit decimal number, and the TOE verifies that the number of digits is five.

In the event that the key operator code is forgotten, there is no way to query, delete, erase, or otherwise restore it.

The values of the above settings are stored in EEPROM in the MFD.

Functional requirements satisfied: FMT_SMR.1, FMT_MOF.1(1), FMT_MTD.1, FIA_SOS.1, FMT_SMF.1

6.2 Assurance Measures

The TOE satisfies the assurance requirements of the EAL4 assurance level. This section identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Life Cycle Support, Testing, and Vulnerability Assessment Assurance Measures applied by Sharp Corporation to satisfy the EAL4 assurance requirements. The assurance components of EAL4 and assurance measures are shown in Table 11.

Table 11: Assurance components and assurance measures

Assurance component	Assurance Measure
ACM_AUT.1 Partial CM automation	Digital MFD Data Security Kit Configuration Management Automation Tools Manual
ACM_CAP.4 Generation support and acceptance procedures	Digital MFD Data Security Kit Configuration Management Automation Tools Manual
ACM_SCP.2 Problem tracking CM coverage	Digital MFD Data Security Kit CM Coverage Manual
ADO_DEL.2 Detection of modification	Digital MFD Data Security Kit Delivery Procedures Manual
ADO_IGS.1 Installation, generation, and start-up procedures	Digital MFD Data Security Kit Verification Materials for Conformity of Delivery Procedures
ADV_FSP.2 Fully defined external interfaces	Digital MFD Data Security Kit Security Function Specifications
ADV_HLD.2 Security enforcing high-level design	Digital MFD Data Security Kit High-level Design Manual
ADV_IMP.1 Subset of the implementation of the TSF	Digital MFD Data Security Kit Source Code Manual
ADV_LLD.1 Descriptive low-level design	Digital MFD Data Security Kit Low-level Design Manual
ADV_RCR.1 Informal correspondence demonstration	Digital MFD Data Security Kit Expressed Correspondence Analysis Manual
ADV_SPM.1 Informal TOE security correspondence policy model	Digital MFD Data Security Kit Security Policy Model Specifications
AGD.ADM.1 Administrator guidance	Digital MFD Data Security Kit Verification Materials for Class Conformity of Guidance Text AR-FR4 Data Security Kit Operation Manual, AR-FR5 Data Security Kit Operation Manual, Installation Checklist, Supplemental Sheet, LASER PRINTER Operation manual (for printer operation and general information)
AGD_USR.1 User guidance	
ALC_DVS.1 Identification of security measures	Digital MFD Data Security Kit Development Security Specifications
ALC_LCD.1 Developer defined life-cycle model	Digital MFD Data Security Kit Life-cycle Management Instructions
ALC_TAT.1 Well-defined development tools	Digital MFD Data Security Kit Development Tools Materials
ATE_COV.2 Analysis of coverage	Digital MFD Data Security Kit Coverage Analysis Manual
ATE_DPT.1 Testing: high-level design	Digital MFD Data Security Kit High-level Design and Testing Analysis Manual
ATE_FUN.1 Functional testing	Digital MFD Data Security Kit Functional Testing Specifications
ATE_IND.2 Independent testing - sample	Digital MFD Data Security Kit Independent Testing Environment and Tools Manual
AVA_MSU.2 Validation of analysis	Digital MFD Data Security Kit TOE Misuse Analysis Manual AR-FR4 Data Security Kit Operation Manual, AR-FR5 Data Security Kit Operation Manual, Installation Checklist, Supplemental Sheet, LASER PRINTER Operation manual (for printer operation and general information)

Assurance component	Assurance Measure
AVA_SOF.1 Strength of TOE security function evaluation	Digital MFD Data Security Kit Strength of TOE security function evaluation
AVA_VLA.2 Independent vulnerability analysis	Digital MFD Data Security Kit Vulnerability Analysis Manual

7 PP Claims

The TOE does not claim conformance to a PP.

8 Rationale

This section demonstrates the completeness and consistency of this ST.

8.1 Security Objectives Rationale

Table 12 demonstrates that all security objectives for the TOE are traced back to identified threats to be countered or organizational security policies. Table 13 demonstrates that all security objectives are traced back to an assumed environment or organizational security policies.

Table 12: Security Objectives Rationale

TOE Security Objective	Threat or Organizational Security Policy Assumption	Rationale
O. RESIDUAL	T.RECOVER	O.RESIDUAL helps to counter the threat T.RECOVER by overwriting document and image data in the MSD, thereby limiting the window of opportunity of this threat. The data clear function overwrites all *residual data* making it impossible to read the data.
O.REMOVE	T.RECOVER	O.REMOVE counters the threat T.RECOVER by encrypting document and image data stored in the MSD. Reading of job data will be impossible even if the MSD in the TOE-equipped MFD is accessed by a means other than via the MFD.
O.AUTHENTICATION	T.ALTER	O.AUTHENTICATION counters the threat T.ALTER by means of key operator authentication through the entry of a key operator code to enable use of the TOE security function.

Table 13: Security Objectives Rationale for the Environment

Security objectives for the environment	Environment or security policy threat assumption	Rationale
OE. SECURE	A.OFFICE	A. OFFICE requires that when the employees of the office in which the TOE-equipped MFD is installed are all out, security measures such as locking the doors are taken, and if someone needs to enter the office when no employees are present, there is a means of verifying that the person is an authorized employee. OE.SECURE directly expresses this, and requires that when the employees of the office are all out, security measures such as locking the doors are taken, and if someone needs to enter the office when no employees are present, there is a means of verifying that the person is an authorized employee.
OE. OPERATE	A. PROCEDURE	PROCEDURE requires that the key operator perform the following: • Verify that the TOE is installed. • Configure suitable data clear and clear repetition settings. • Regularly change the *key operator code*. • Use a key operator code that cannot be guessed easily. Will not disclose the key operator code to others. OE. OPERATE requires that a trustworthy person who will perform the above without fail be selected as key operator.

8.2 Security Requirements Rationale

This section demonstrates that the security functional requirements of the TOE and the security assurance requirements of the TOE are satisfactory.

8.2.1 Rationale for TOE Security Functional Requirements

Table 14 demonstrates that the security objectives of the TOE are satisfied by the security functional requirements. Table 15 shows the security requirement to security objective mapping, and that each TOE security functional requirement is traced back to a security objective of the TOE.

In the security functional requirements (SFR), dependencies on various functional requirements are indicated, however, the TOE does not require some of these dependencies. The rationale for this is explained in the following.

(1) Rationale for no dependency on FMT_MSA.2

Security functional requirements that require a dependency:
FCS_CKM.1, FCS_CKM.4

Rationale for not requiring a dependency:
FMT_MSA.2 requires that only safe values be used for security attributes. FCS_CKM.1 is satisfied by TSF_FKG and FCS_CKM.4 is satisfied by TSF_FKD. Neither TSF_FKG nor TSF_FKD have security attributes. Therefore, there is no requirement for dependency on FMT_MSA.2.

(2) Rationale for no dependency on FIA_UID.1

Security functional requirements that require a dependency:
FIA_UAU.2, FMT_SMR.1

Rationale for not requiring a dependency:
The only user identification required by the MFD is that of the key operator; authorization satisfies this requirement and thus identification, hence FIA_UID.1, is not necessary.

Table 16 shows the correspondence between the mutual dependencies of the functional components and the degree of satisfaction of the dependencies.

The rationale for the dependencies in the various security functional requirements (SFR) in Table 16 is given below.

a) Dependency on FCS_COP.1, FCS_CKM.1, FCS_CKM.4
A key is generated by cryptographic key generation (FCS_CKM.1(1) and FCS_CKM.1(2)), and cryptographic operation (FCS_COP.1) is performed using that key. The key is destroyed (FCS_CKM.4) when the power of the MFD is turned off or interrupted.
b) Dependency on FMT_MOF.1(1), FMT_MOF.1(2), FMT_SMR.1
Enabling or disabling of Power On Auto Clear (FMT_MOF.1(1)), which controls the behavior of a security function, and Clear All Memory by Key Operator Operation (FMT_MOF.1(2)), shall only be managed by the key operator (FMT_SMR.1).
c) Dependency on FIA_UAU.7, FIA_UAU.2
When a user accesses the key operator programs, the TOE always requires entry of the key operator code, and asterisks (*) are displayed as feedback of the entered numbers.

8.2.2 Suitability of TOE Security Assurance Requirements

The intention of the TOE security policies (TSP) is to provide assurance that there will never be spooled data that is not encrypted, there will never be finished jobs that are not cleared, there will be no access to security management functions without authorization, and there will be no unexpected access to authorization data (the key operator code).

To assure the effectiveness of these TSPs at the site of the customer, measures are required to ensure firmware quality and prevent security deficiencies due to alteration from the site of development to the site of the customer.

Assurance of the effectiveness of the TOE security policies at the site of the customer shall consist of quality control evaluation of the product lifecycle, design evaluation of not only high-level design but of low-level and source code level design, vulnerability analysis of not only the developers but also the evaluators, and evaluation of the procedures for delivery, installation, and start-up without alteration.

For this purpose, this ST selects EAL4, which is necessary for and satisfies this assurance.

The TOE uses assurance level EAL4 and the dependencies on the security assurance requirements (SAR) are satisfied. Table 17 indicates the dependencies of the security assurance requirements (SAR) of EAL4.

Table 14: Rationale for Security Functional Requirements (SFR)

TOE Security Objective	Rationale
O.RESIDUAL	Spooled data that must be cleared is for a print job, copy job, scan job, or fax job, and thus is satisfied by FDP_RIP.1. The management functions of FDP_RIP.1 (functions that manage enable/disable of power on auto clear, overwrite count setting for auto clear at job end, overwrite count setting for clear all memory by key operator operation, and overwrite count setting for power on auto clear) are managed by FMT_SMF.1, and enable clearing to be executed reliably. Clearing behavior settings and clearing count settings are satisfied by FMT_MOF.1(1), FMT_MOF.1(2), and FMT_MTD.1, and their role is satisfied by FMT_SMR.1.
O.REMOVE	A key that satisfies FCS_CKM.1(1) and FCS_CKM.1(2) is used for encryption according to FCS_COP.1, and the key is destroyed according to FCS_CKM.4.
O.AUTHENTICATION	FIA_UAU.2, FMT_MTD.1, and FMT_SMR.1 all express all or part of the policy whereby only the key operator is allowed to use the security management functions. FIA_UAU.7 and FIA_SOS.1 also contribute to this policy. The key operator code change function of FIA_UAU.2 is managed by FMT_SMF.1, ensuring that only a legitimate key operator is authorized.

Table 15: Mapping of TOE Security Functional Requirements (SFR) to Security Objectives

TOE Security Functional Requirement (SFR)	O.RESIDUAL	O.REMOVE	O.AUTHENTICATION	Rationale for tracing the SFR back to the security policy
FDP_RIP.1 Subset residual information protection	X			Directly expresses O.RESIDUAL.
FIA_UAU.2 User authentication before any action			X	The policy determines that authentication is required before the TOE security functions can be used.
FIA_UAU.7 Protected authentication feedback			X	Required to prevent leaking of the key operator code.
FIA_SOS.1 Verification of secrets			X	Required to maintain the SOF of the key operator code.
FMT_MOF.1(1) Management of security functions behavior (1)	X			The policy determines that only the role key operator can determine behavior through the enable/disable setting of power on auto clear.
FMT_MOF.1(2) Management of security functions behavior (2)	X			The policy determines that only the role key operator can use clear all memory by key operator operation.

TOE Security Functional Requirement (SFR)	O.RESIDUAL	O.REMOVE	O.AUTHENTICATION	Rationale for tracing the SFR back to the security policy
FMT_MTD.1 Management of TSF data	X		X	The policy determines that only the role key operator can change the overwrite count settings and key operator code.
FMT_SMF.1 Specification of management functions	X		X	The policy determines functions that manage security management functions related to overwrite clearing (enable/disable power on auto clear, overwrite count setting for auto clear at job end, overwrite count setting for clear all memory by key operator operation, and overwrite count setting for power on auto clear). The policy also determines functions for changing the key operator code.
FMT_SMR.1 Security roles	X		X	The policy determines that the key operator role will handle management of clearing behavior, clearing count settings, and change of key operator code. The policy also determines the relationship of user to key operator.
FCS_CKM.1(1) Cryptographic key generation		X		The policy determines that a key will be generated for the encryption that is required to prevent external reading of job data.
FCS_CKM.1(2) Cryptographic key generation		X		The policy determines that a key will be generated for the encryption that is required to prevent external reading of job data.
FCS_CKM.4 Cryptographic key destruction		X		The policy determines that the key that can decrypt job data will be destroyed to prevent external reading of job data.
FCS_COP.1 Cryptographic operation		X		The policy determines the necessary cryptographic operation to prevent external reading of job data.

Table 16: Status of Security Functional Requirement (SFR) Dependencies

Functional Component ID	Functional Component Name	Dependency to be satisfied	Dependencies that the TOE satisfies	Location of explanation why dependency need not be satisfied	Degree of dependency satisfaction
FCS_CKM.1(1)	Cryptographic key generation (1)	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FCS_CKM.4	8.2.1.1	--
FCS_CKM.1(2)	Cryptographic key generation (2)	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FCS_CKM.4	8.2.1.1	--
FCS_CKM.4	Cryptographic key destruction	FCS_COP.1, FCS_CKM.1, FMT_MSA.2	FCS_COP.1, FCS_CKM.1	8.2.1.1	--
FCS_COP.1	Cryptographic operation	FCS_CKM.1, FCS_CKM.4	FCS_CKM.1, FCS_CKM.4	--	Satisfied
FDP_RIP.1	Subset residual information protection	No dependencies	--	--	--

Functional Component ID	Functional Component Name	Dependency to be satisfied	Dependencies that the TOE satisfies	Location of explanation why dependency need not be satisfied	Degree of dependency satisfaction
FIA_UAU.2	User authentication before any action	FIA_UID.1	No dependencies	8.2.1.2	--
FIA_UAU.7	Protected authentication feedback	FIA_UAU.2	FIA_UAU.2	--	Satisfied
FIA_SOS.1	Verification of Secrets	No dependencies	--	--	--
FMT_MOF.1(1)	Management of security functions behavior (1)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	--	Satisfied
FMT_MOF.1(2)	Management of security functions behavior (2)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	--	Satisfied
FMT_MTD.1	Management of TSF data	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	--	Satisfied
FMT_SMF.1	Specification of management functions	No dependencies	--	--	--
FMT_SMR.1	Security roles	FIA_UID.1	No dependencies	8.2.1.2	--

Table 17: EAL4 Security Assurance Requirement (SAR) Dependencies

Assurance Component ID	Assurance Component Name	Dependencies:	Degree of dependency satisfaction
ACM_AUT.1	Partial CM automation	ACM_CAP.3	Satisfied
ACM_CAP.4	Generation support and acceptance procedures	ACM_SCP.1, ALC_DVS.1	Satisfied
ACM_SCP.2	Problem tracking CM coverage	ACM_CAP.3	Satisfied
ADO_DEL.2	Detection of modification	ACM_CAP.3	Satisfied
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	Satisfied
ADV_FSP.2	Fully defined external interfaces	ADV_RCR.1	Satisfied
ADV_HLD.2	Security enforcing high-level design	ADV_FSP.1, ADV_RCR.1	Satisfied
ADV_IMP.1	Subset of the implementation of the TSF	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1	Satisfied
ADV_LLD.1	Descriptive low-level design	ADV_HLD.2, ADV_RCR.1	Satisfied
ADV_RCR.1	Informal correspondence demonstration	No dependencies	--
ADV_SPM.1	Informal TOE security policy model	ADV_FSP.1	Satisfied
AGD_ADM.1	Administrator guidance	ADV_FSP.1	Satisfied
AGD_USR.1	User guidance	ADV_FSP.1	Satisfied
ALC_DVS.1	Identification of security measures	No dependencies	--
ALC_LCD.1	Developer defined life-cycle model	No dependencies	--
ALC_TAT.1	Well-defined development tools	ADV_IMP.1	Satisfied
ATE_COV.2	Analysis of coverage	ADV_FSP.1, ATE_FUN.1	Satisfied

Assurance Component ID	Assurance Component Name	Dependencies:	Degree of dependency satisfaction
ATE_DPT.1	Testing: high-level design	ADV_FSP.1, ATE_FUN.1	Satisfied
ATE_FUN.1	Functional testing	No dependencies	--
ATE_IND.2	Independent testing - sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	Satisfied
AVA_MSU.2	Validation of analysis	ADO_IGS.1, AGD_FSP.1, AGD_ADM.1, AGD_USR.1	Satisfied
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1	Satisfied
AVA_VLA.2	Independent vulnerability analysis	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1	Satisfied

8.2.3 Rationale for Minimum Strength of Function

As it is assumed that the MFD Data Security Kit will be used in a normal office environment, conceivable threats will take the form of an attack using public information from the operation panel of the MFD. For this reason, the attacker is considered to be unskilled. The attacker will not be able to circumvent authorization and use the TOE management functions, and thus the minimum strength of function level is “SOF-basic” in order to counter threats that use public information from an unskilled attacker.

8.3 Rationale for TOE Summary Specifications

This section demonstrates that the TOE security functions (TSF) and assurance measures satisfy the security functional requirements (SFR).

8.3.1 Rationale for TOE Summary Specifications

Table 18 provides a mapping of security functional requirements (SFR) and a rationale showing that they are each satisfied by a security function (SFR).

Table 18: Rationale for satisfaction of all security functional requirements (SFR) by TOE security functions (TSF)

Security Functional Requirement (SFR)	TOE Security Function (TSF)	Rationale
FCS_CKM.1(1) Cryptographic key generation	TSF_FKG Cryptographic key generation	Cryptographic keys (common keys) are automatically generated when the power is turned on.
FCS_CKM.1(2) Cryptographic key generation	TSF_FKG Cryptographic key generation	Cryptographic keys (common keys) are automatically generated when the power is turned on.
FCS_CKM.4 Cryptographic key destruction	TSF_FKD Cryptographic key destruction	The cryptographic keys are destroyed when the power is removed.
FCS_COP.1 Cryptographic operation	TSF_FDE Cryptographic operation	The cryptographic key generated by TSF_FKG encrypts and decrypts data according to the Rijndael algorithm.
FDP_RIP.1 Subset residual information protection	TSF_FDC Data clear	Residual information is protected by overwriting the spooled data stored in the MSD.
FIA_UAU.2 User Authentication before any action	TSF_AUT Authentication	When a user attempts to access the TOE management function, the user is prompted to enter the key operator code. The TOE management function activates upon verification that the entered code is valid.

Security Functional Requirement (SFR)	TOE Security Function (TSF)	Rationale
FIA_UAU.7 Protected authentication feedback	TSF_AUT Authentication	Feedback during authentication is protected by displaying each entered digit of the key operator code as an asterisk (*) on the operation panel.
FIA_SOS.1 Verification of secrets	TSF_FMT Security Management	When the key operator code is changed by TSF_FMT, it is verified that the new key operator code has 5 digits. A code that is not 5 digits is not accepted.
FMT_MOF.1(1) Management of security functions behavior (1)	TSF_AUT authentication, TSF_FMT data clear	Only a key operator is allowed by TSF_AUT to change the enable/disable setting for power on auto clear by TSF_FMT.
FMT_MOF.1(2) Management of security functions behavior (2)	TSF_AUT authentication, TSF_FDC data clear	Only a key operator is allowed by TSF_AUT to perform a clear all memory operation by TSF_FDC.
FMT_MTD.1 Management of TSF data	TSF_AUT authentication, TSF_FMT security management	Only a key operator is allowed by TSF_AUT to change the key operator code, the overwrite count for clear all memory by key operator operation, the overwrite count for power on auto clear, and the overwrite count for auto clear at job end by TSF_FMT.
FMT_SMF.1 Specification of management functions	TSF_FMT Security management	TSF_FMT manages functions that control the enable/disable setting for power on auto clear, overwrite count setting for data clear at job end, the overwrite count setting for clear all memory by key operator operation, the overwrite count setting for power on auto clear, and change of key operator code.
FMT_SMR.1 Security roles	TSF_AUT authentication, TSF_FMT security management, TSF_FDC data clear	Only a key operator is allowed by TSF_AUT to perform clear all memory by key operator operation by TSF_FDC, or to change by TSF_FMT the enable/disable setting for power on auto clear, the key operator code, the overwrite count setting for clear all memory by key operator operation, or the overwrite count setting for data clear at job end.

8.3.2 TOE Assurance Requirements

Section 5.2 of this document identifies the assurance measures implemented by Sharp Corporation to satisfy the assurance requirements of EAL4 as delineated in Annex B of [CC_PART3]. Table 19 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.2.

Table 19: Assurance Measure Compliance Matrix

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Lifecycle Support	Testing	Vulnerability Assessment
ACM_AUT.1	X						
ACM_CAP.4	X						
ACM_SCP.2	X						
ADO_DEL.2		X					
ADO_IGS.1		X					
ADV_FSP.2			X				
ADV_HLD.2			X				
ADV_IMP.1			X				
ADV_LLD.1			X				
ADV_RCR.1			X				
ADV_SPM.1			X				

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Lifecycle Support	Testing	Vulnerability Assessment
AGD_ADM.1				X			
AGD_USR.1				X			
ALC_DVS.1					X		
ALC_LCD.1					X		
ALC_TAT.1					X		
ATE_COV.2						X	
ATE_DPT.1						X	
ATE_FUN.1						X	
ATE_IND.2						X	
AVA_MSU.2							X
AVA_SOF.1							X
AVA_VLA.2							X

8.3.3 Strength of TOE Security Functions

The TOE provides key operator authentication (TSF_AUT) as probability and permutation based mechanisms. The strength of these security functions is SOF-basic. The minimum strength of function of the TOE is SOF-basic. As these two strength of function levels do not conflict, a strength of function of SOF-basic for the security function is reasonable.

8.4 Rationale for Explicitly Stated Requirements

This ST does not contain explicitly stated requirements.