[DSK_ST]

Digital Multifunction Device

Data Security Kit

AR-FR21

Security Target

Version 0.04

SHARP CORPORATION

Revision History

Date	Ver.	Revision	Author	Approved
1 Apr. 2005	0.01	• Original Draft	Nakagawa	Yamanaka
11 Apr. 2005	0.02	• Corrected MFD model names in TOE Description.	Nakagawa	Yamanaka
12 May 2005	0.03	• Modified descriptions on MFD optional parts.	Nakagawa	Yamanaka
28 June 2005	0.04	• Modified ST Identification, Logical Configuration of the TOE, and Assumptions.	Nakagawa	Yamanaka

Table of Contents

List of Figures

List of Tables

1 Security Target Introduction

1.1 ST Identification

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

ST Title:	Digital Multifunction Device Data Security Kit AR-FR21 Security Target
ST Version:	0.04
Publication Date:	28 June 2005
Author:	Sharp Corporation
TOE Identification:	AR-FR21 VERSION M.10
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 — also known as ISO/IEC 15408:1999; with CCIMB Interpretations as of 01 December 2003
ST Evaluator:	Mizuho Information & Research Institute, Inc.
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 Sharp Digital MFD Data Security Kit AR-FR21.

A Multi-Function Device (hereafter referred to as “MFD”) is a commercially sold office machine consisting of copy, printer, network scanning, and fax functions. The TOE is an 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 image data spooled in the MFD during processing of a print, copy, scan or fax job or image data stored in the MSD in the MFD by the filing function will be disclosed to a person who gains unauthorized access to the machine.

1.3 CC Conformance Claim

This ST is claiming the following conformance:

a) CC Version 2.1, ISO/IEC 15408:1999
b) With CCIMB Interpretations as of 01 December 2003
c) Part 2 Conformant
d) Part 3 Conformant
e) EAL3 Conformant
f) Conformant to no PP

1.4 Reference Materials

The materials listed in Table 1 have been referred to prepare this ST.

Table 1: Reference Materials

Identifier	Title
[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.
[INTPR_01DEC2003]	CCIMB Interpretations as of 01 December 2003

Hereafter, references to [CC_PART1], [CC_PART2] and [CC_PART3] shall be interpreted as being modified by [INTPR_01DEC2003], unless otherwise noted.

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.

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

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

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

b) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password.

- One or more assignment values are shown in brackets [ ].
- When a value or part of a value indicates a list, all list elements are shown within braces { }. Breaks between elements are indicated by commas or itemization.
- When values are assigned to a list of parameters, the parameter name is indicated in parentheses ( ) next to each value unless the name is self-evident.
- When multiple values are assigned to a single parameter, information to distinguish each value is provided in parentheses ( ) next to the value unless the information is self-evident. For example, this is done when a subject attribute and an object attribute are assigned to a security attribute parameter.

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

- Additional text is indicated in **bold**.
- When one section of text is replaced by another, such as the replacement of a general term with a more specialized term, the original text is shown in parentheses ( ) and the new text is shown immediately before it in **bold**.
- A list value is indicated in the same way as an assignment operation.
- When text is deleted as an editorial refinement, the deleted text is indicated in parentheses.

d) The selection operation is used to select one or more options when multiple options are provided in a component.

- Selections are denoted in slant blackest *[ ]* by *[underlined italicized text]*.

e) Iteration is used to cover different aspects of the same requirement.

- An iteration number inside parentheses ( ) is appended to the component name, short name, and element name as a unique identifier.

1.5.2 Terminology

Terminology unique to this document is defined in Table 2.

Table 2: Terminology

Term	Definition
Actual image data	The part of an image data file that does not include the management area.
Board	A printed circuit board on which components are mounted by soldering.
Clear All Memory	An operation that clears (by overwriting) all actual image data stored in all MSDs in an MFD.
Data Security Kit	The AR-FR21 upgrade kit for use only with Sharp MFDs.
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.
External network	A network other than an internal network of an organization, which is not managed by the organization.

Term	Definition
Filing	A function that stores image data handled by the MFD into the HDD, for users' later operations, such as a printing or a transmission. This is also called *Document Filing*.
Image data	The digital data that results from scanning an original on the MFD for a copy, print, scan, or fax transmission job. In the case of fax reception, the data received via the telephone line, or the received fax data after it has been decompressed. These types of data are also called image data when they have been compressed.
Internal network	A network that is protected from security threats from an external network. The intranet of an organization is an "internal network".
Job	The sequence from beginning to end of the use of an MFD function (copy, printer, direct print, network scanning, PC fax transmission, fax transmission, or fax reception). In addition, the instruction for a functional operation is sometimes called a job.
Key Operator	A user that is authorized to access the TOE security management functions and the MFD management functions. The administrator of the MFD and the TOE.
Key Operator Code	A password used for authentication of the Key Operator.
Key Operator Programs	Security administrative functions of the TOE, as well as MFD administrative functions. To access the Key Operator Programs, authentication as the Key Operator is required.
Memory	A memory device; in particular a semiconductor memory device.
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.
Protected network settings data	A part of MFD network related setting data of which this ST claims to be a part of assets protected by the TOE. The coverage will be shown in section 2.3.3.
Software button	The LCD display is a touch panel, and the software buttons are keys that appear in the display such as up and down arrow keys (▲ and ▼) and checkboxes.
Uncleared data	Data that remains in the MSD due to trouble that occurred before a copy or fax job finished, including cancellation of the job. This also refers to spooled data that exists before a job ends normally.
Unit	A module 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.
Web-Admin	A user that is authenticated, as an administrator of the MFD, with an administrative password, on the Web that the TOE provides for remote operation, where Admin is an abbreviation of Administrator.

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, United States of America)
DSK	Data Security Kit
EEPROM	Electrically Erasable Programmable ROM, a type of non-volatile memory that allows electrical rewriting to any part of memory.
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
LCD	Liquid Crystal Display
MSD	Mass Storage Device For the TOE, an MSD is an HDD or Flash memory.
NIC	Network Interface Card, or, Network Interface Controller
RAM	Random Access Memory
ROM	Read Only Memory
UI	User Interface

2 TOE Description

2.1 TOE Overview

2.1.1 TOE Type

The TOE is a data security kit that takes the form of a ROM *product* containing firmware for the MFD. The TOE is an upgrade kit that adds security functions to the MFD. By replacing the MFD standard firmware, it offers the security functions and controls the entire MFD.

2.1.2 Overview of the TOE Security Functions and Applications

As well as the standard MFD firmware, the TOE has the following functions: copy, printer, direct print, scan transmission, fax transmission, fax reception, and PC-Fax. It executes a part of the TOE security functions automatically while each of these MFD functions is being executed. This property of the TOE protects even a user with no knowledge or awareness about the TOE security functions. The usage environment of the TOE is shown in Figure 1.

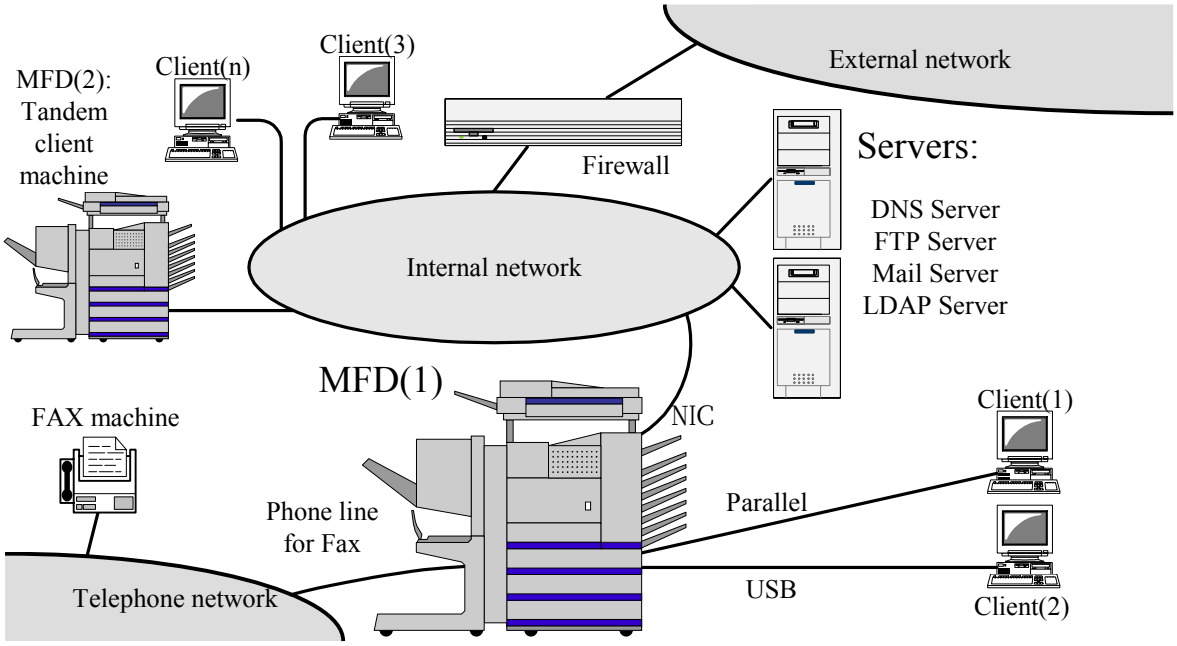

Figure 1: Usage environment of the TOE

Assume that sets of the TOE are installed in MFD (1) and MFD (2) in the diagram. Focusing on MFD (1), each function of the MFD is explained below:

2.1.2.1 Copy

The copy function, as well as the standard MFD firmware, is used to scan an original and print the resulting image. The major optional features are listed below:

a) Tandem Copy: When two MFDs are connected to the same internal network, the MFD that scans the original (the server machine) can transfer the actual image data over the network to the other MFD (the client machine) to halve the number of copies specified by the user and share the printing work. However, the TOE does not forward the actual image data to an MFD with the standard firmware.

b) Filing: This is an addition to the normal printout. The actual image data of an original can be saved in MFD. The Document Filing function (section 2.1.2.8) prints or deletes the saved data.

2.1.2.2 Printer

The printer function, as well as the standard MFD firmware, prints print data transferred from a client, in which the printer driver for the MFD shall be installed. The print data come up via the parallel I/F, USB, or the internal network. The major optional features are listed below:

a) Tandem Print: Just like the Tandem Copy function, the MFD that receives print data plays the server machine and halves with the client machine the number of copies specified by the user.

b) Hold before Print: Upon receiving a set of data, this function generates the printable actual image data from it and then saves the generated data in the MFD without printing it. It works as the *confidential print* if the data are stored with a password.

c) Hold after Print: Actual image data can be printed out as usual and then saved in the MFD.

d) Proof Print: This function prints out only one copy out of the designated number of prints and then retains the actual image data for the remaining number of prints, safeguarding against a large amount of misprinting.

The Document Filing function (section 2.1.2.8) prints or deletes the data saved in the MFD.

2.1.2.3 Direct Print

The direct print function, as well as the standard MFD firmware, retrieves a file of print data from a client, an FTP server or an E-mail attachment, and prints it out, without any printer driver as opposed to the printer function (section 2.1.2.2) This function can be performed in either of the following ways:

a) E-mail Print / Internet Fax Reception: The TOE periodically checks the mail server, receives E-mails, and prints the attached print files. E-mails sent as Internet faxes are processed in the same way.

b) FTP Pull Print: Through operations on the operational panel, the TOE accesses the FTP server, retrieves a file, and then prints it out.

c) FTP Push Print: This function prints print data that the clients send into the FTP server that the TOE provides.

d) Web Print: This function prints print data that the clients send into the Web server that the TOE provides.

2.1.2.4 Network Scanning

The network scanning function, as well as the MFD standard firmware, scans an original to obtain image data and performs an *E-mail/FTP Transmission* or an *Internet Fax Transmission*.

Here, *FTP Transmission* (to an FTP server), *Desktop Transmission* (to a client's desktop in FTP), and *E-mail Transmission* (for a mail server) are called *E-mail/FTP Transmission* in general. To use *Desktop Transmission*, the destination client must be running the Network Scanning Tool, which is software that accompanies the MFD network scanning function.

2.1.2.5 Fax Transmission

The fax transmission function, as well as the standard MFD firmware, sends a fax to a destination fax machine that is selected on the operation panel.

The major optional features are listed below:

a) Timer Transmission: The TOE holds a transmission in and starts it when the reservation time that the user has specified comes.

2.1.2.6 Fax Reception

The fax reception function, as well as the standard MFD firmware, receives a fax and prints it out.

2.1.2.7 PC-FAX

The PC-FAX (or PCFAX) function, as well as the standard MFD firmware, faxes or internet-faxes image data from a client, in which the PC-FAX driver for the MFD shall be installed. The data come up via parallel I/F, USB or the internal network.

The major optional features are listed below:

a) Document Filing: Actual image data can be printed out as usual and then saved in the MFD. The data saved in the MFD may later be printed or deleted with the Document Filing function (section 2.1.2.8).

2.1.2.8 Document Filing

The Document Filing function, as well as the standard MFD firmware, saves actual image data to the HDD in the MFD, and later calls them up to reuse them on the operation panel or from a client via the Web. The TOE provides *confidential mode*, a filing mode that protects the saved data by a password. A file saved in confidential mode is called a *confidential file*.

For saving data in a confidential file, the following four operations are available:

a) *Scan Save:* Actual image data obtained by scanning is saved to the HDD without being printed or transmitted.

b) Copy job (*FILE* specified): See *Copy* in section 2.1.2.1.

c) Printer job (*Hold before Print, Hold after Print* or *Proof Print* specified): See *Printer* in section 2.1.2.2.

d) PC-FAX job (*Document Filing* specified): See *PC-FAX* in section 2.1.2.7.

During each saving operation above, the TOE allows the user to types in a password, and saves the password together with the actual image data into a confidential file. For calling up a saved confidential file and using it, authentication by entry of the password is required before the operations on the file. Operations on saved files include the following:

a) Print: Prints the saved file, with the settings such as number of copies to print, as well as the copy function. Tandem printing feature is also available here.

b) Send: Transmits the saved file by fax, by E-mail/FTP transmission or by Internet fax.

c) Preview: Displays a rough picture of the actual image data in the saved file. Available only on the Web.

d) Property change: Has the saved file change from a confidential file to a file not confidential (without password), and vice versa.

e) Password change.

f) Delete.

2.1.2.9 Backup

The backup function, as well as the standard MFD firmware, creates a backup file in the client of a file stored in the HDD using the Document Filing function, and restores a backup file to the HDD. The former operation is called *exporting* or *backing up* the file. And the latter operation is called *importing* or *restoring* the file. These operations are instructed by the user on the clients.

A file is exported in the following sequence:

a) A user accesses the TOE Web from a client and operates as needed for the options, such as selecting a file in the HDD, and specifying the password.

b) The TOE confirms that the given password is correct for the selected confidential file, and then, sends the file, in its encrypted form as it has been, to the Web browser on the client.

c) The Web browser on the client downloads the file and saves it.

A file is imported in the following sequence:

a) A user accesses the TOE Web from a client and operates as needed for the options, such as selecting a file on the client.

b) The Web browser on the client uploads the selected file onto the TOE.

c) The TOE receives the file, encrypts if not yet done, and saves it.

2.1.2.10 Network Management

The network management function, as well as the standard MFD firmware, allows configuring the IP address to be allocated for the MFD, the IP address of the DNS servers that the MFD is to refer, and other network related settings. These configurations are required for utilizing MFD networking functionalities.

Some features of this function are provided via the operation panel. They are on a UI named *Network Settings* under the Key Operator Programs UI, and include minimum settings such as IP address setting. In addition, the *Tandem Setting* is allowed only in this Network Settings UI.

The TOE provides its Web for remote operation, when set to enable TCP/IP. Some of the pages in this Web are protected by an administrative password. In this ST, the user authenticated with this administrative password is named *Web-Admin,* and the protected pages are generally named *Web-Admin Pages.*

Most features of this network management function are provided via this Web for the Web-Admin, and allow the configurations such as the settings for the MFD to refer the DNS, WINS, SMTP and LDAP servers. In this ST, the pages that contain forms for these settings and the submission target pages of the forms are generally named *Network Management Pages.* All Network Management Pages are Web-Admin Pages.

2.2 TOE Configuration

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

2.2.1 Physical Configuration of the TOE

Figure 2 shows the physical configuration of the MFD. The AR-FR21, the TOE, is shaded in the figure.

The TOE runs on the following Sharp MFDs: AR-311N, AR-351N, AR-451N, AR-M351N, AR-M355N, AR-M355NJ, AR-M451N, AR-M455N, AR-M455NJ, AR-M351U, AR-M355U, AR-M355UJ, AR-M451U, AR-M455U and AR-M455UJ. Among these, every MFD model that has U in its name needs a Sharp genuine option that contains an HDD, in order that the TOE can run on it.

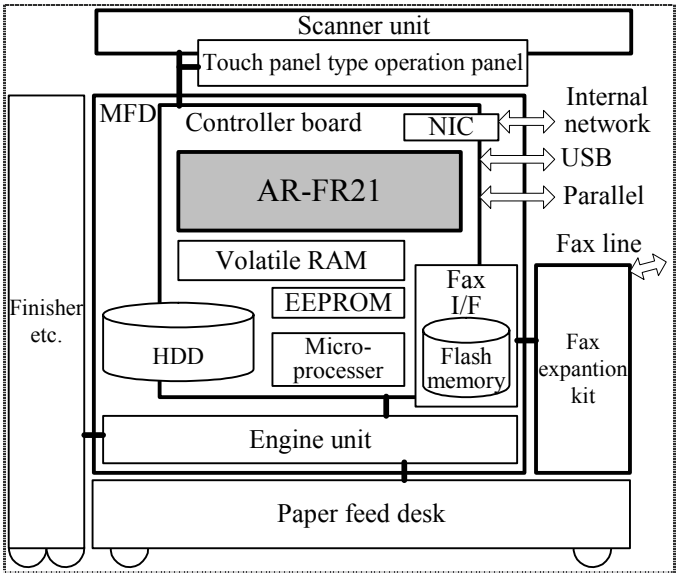

Figure 2: TOE and physical configuration of the MFD

The physical scope of the TOE is as follows:

a) Controller firmware: Controls the controller board of the MFD and is housed in two ROM boards that are attached to the controller board.

Component parts other than the TOE in the Figure 2 are described below:

b) Scanner unit: Scans an original to obtain the actual image data. Used for copy, scan transmission, fax transmission, and scan to HDD.

c) Touch panel type operation panel: Has the LCD equipped with button keys and a touch panel.

d) Controller board: Controls the entire MFD and is equipped with the microprocessor executing the firmware within the TOE, the volatile RAM, and the EEPROM retaining settings.

e) NIC: An Ethernet I/F for internal network connections.

f) Fax expansion kit and Fax I/F: Provide fax transmission/reception functions, equipped with the flash memory retaining the actual image data necessary for the fax transmission/reception job processing.

g) HDD: Retains the actual image data necessary for job processing other than fax transmission/reception. A user can also use the Document Filing function to retain the actual image data.

h) Engine unit: Prints out the actual image data. At the same time, it controls other parts like Paper tray or Finisher and is used for copy, printer, direct print, fax reception, and re-operational printout.

i) Paper tray: Stores pages of paper for printout, sending them to the engine unit.

j) Finisher and others: Available for finishing purposes such as stapling printed pages and punching holes.

2.2.2 Logical Configuration of the TOE

The logical configuration of the TOE is shown in Figure 3. The TOE is shaded in the diagram. Long rectangles indicate software and rectangles with rounded corners indicate hardware. In addition, the user

data that the TOE protects are stored in the devices out of the TOE, i.e. HDD, Flash memory and Administration EEPROM. These user data are also shaded in the diagram.

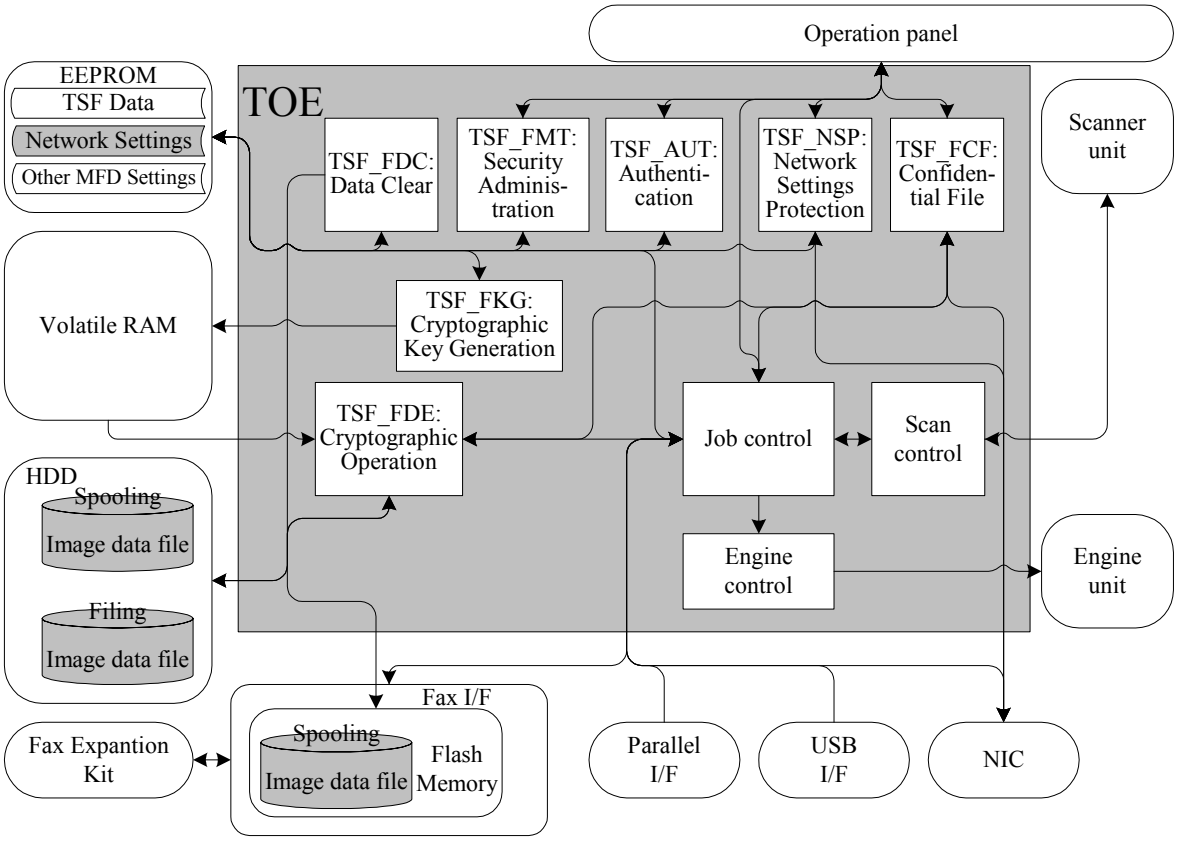

Figure 3: Logical configuration of the TOE

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): Encrypts actual image data that is being spooled or saved by the filing function and stores it in the MSD (HDD or Flash memory) by intervening with the device driver function controlling the MSDs (HDD and Flash memory) in the MFD. This function also decrypts data that was stored in the MSD by spooling or the filing function.

b) Cryptographic key generation function (TSF_FKG): Generates the cryptographic key for encryption and decryption by the cryptographic operation function (previous paragraph). The generated key is stored in volatile RAM.

c) Data clear function (TSF_FDC): When a job is completed and the image data, spooled in the HDD or the Flash memory in order to process the job, is deleted and when a user deletes an image data that the user saved in the HDD by the after-mentioned confidential file function, this function clears the actual image data area by overwriting random values or fixed values to that area *(Auto Clear at Job End).*
In addition, for uncompleted job image data and undeleted image data that a user saved, this function clears the actual image data area by overwriting random values or fixed values to that area *(Clear All Memory, Clear Document Filing Data and Power up Auto Clear).*
The following four data clear programs are provided:

- Auto Clear at Job End (for HDD and Flash memory): Clears the actual image data area used by a job after it is completed. It also clears the after-mentioned confidential file, saved by the confidential file function, when the user deletes the file.
- Clear All Memory (for HDD and Flash memory): Clears all actual image data that remain, when invoked by the operation of the administrator, the Key Operator. The administrator shall run this program when disposing of the TOE and/or the MFD or transferring ownership to another party.

- Clear Document Filing Data (for HDD): Clears the actual image data that remain in the HDD, when invoked by the operation of the administrator, the Key Operator. This program aims at batch-clearing the data saved by the users. However, this program can also clear the image data of the jobs spooled to HDD.
  The two programs, Clear All Memory and Clear Document Filing Data, are generically called *Data Clear Operations*.
- Power up Auto Clear (for HDD and Flash memory): Clears the actual image data area when the TOE is powered on, unless the TOE has any reserved transmission jobs or any Fax/Internet fax reception jobs not yet printed out. The Key Operator may enable/disable this function (whether or not executing this program at the time of power-on) and customize data area to be cleared by this program

d) Authentication function (TSF_AUT):
Authenticates a Key Operator by means of the Key Operator Code, i.e. a password.

e) Security administration function (TSF_FMT):
Provides following administrative functions that are essential for operating of the TOE:

- Set the number of times Auto Clear at Job End program is repeated
- Set the number of times data clear operations are repeated
- Set the data areas to be cleared by Power up Auto Clear program
- Set the number of times Power up Auto Clear program is repeated
- Change the Key Operator Code
- Release the lock of confidential files
- Reset the NIC (reset MFD network related settings, including Web-Admin password)

f) Network settings protection function (TSF_NSP):
Protects network-related settings of MFD not to be tampered by users other than the MFD administrator.

g) Confidential file function (TSF_FCF):
Provides password protection when a user stores image data in the MFD using the Document Filing function. The image data that is stored as a password protected file using this function is called a *confidential file*. The user establishes a password when storing the data, and the TOE then requires authentication by means of that password to reuse (print or transmit) the data.
If incorrect passwords for a confidential file are entered three times in a row, this function refuses further authentication attempts. This is called *locking.*
This function can be used for *confidential printing* of printer jobs.

Among the functions within the logical scope of the TOE, each function mentioned so far is characteristic of the TOE. Followings are also within the logical scope of the TOE, and are the functions that both the TOE and the standard MFD firmware have.

h) Scan control function:
Controls the scanner unit during scanning of originals for copy jobs, network scanning jobs, fax transmission jobs and Scan Save operations.

i) Engine control function:
Transfers actual image data to the engine unit and have them printed out, when processing copy jobs, printer jobs, direct print jobs, fax reception jobs and printing operations on saved files.

j) Job control function:
Controls the functions mentioned in section 2.1.2, such as copy function.

2.3 Assets Protected by the TOE

The following assets are protected by the TOE.

a) Actual image data that the MFD functions temporarily spools to process jobs.

b) Actual image data that users store as confidential files.

c) Network-related setting data of MFD

The concrete description of above each is found in sections 2.3.1, 2.3.2 and 2.3.3.

2.3.1 Actual Image Data That the MFD Functions Temporarily Spools to Process Jobs

The assets protected by the TOE include the actual image data that the TOE itself temporarily spools to the HDD or the Flash memory in the MFD for processing the jobs (mentioned in section 2.1.2) without intent of the user to save when the user uses the MFD functions of the TOE. These data are the user data, and possibly contains the users' sensitive information, such as the user's own information and the information of the customers of the user.

2.3.2 Actual Image Data That Users Store in Confidential Files

The assets protected by the TOE include the actual image data that the user saves to the MSD inside the MFD as files with a password ("*confidential files*"). As well as in the previous section, these are the user data, and possibly contain the users' sensitive information.

2.3.3 Network-Related Setting Data of MFD

Among the MFD configuration settings, these are MFD own network settings (IP address etc.), settings in the usage of the services of the external servers that MFD is to refer, and the Tandem Settings. These settings can be found in an MFD that can be equipped with the TOE and that either has the printer function as a standard feature or has the printer function installed as an option. The assets protected by the TOE include the following setting data:

a) TCP/IP Settings
b) DNS Settings
c) WINS Settings
d) SMTP Settings
e) LDAP Settings
f) Tandem Settings

In this ST, these data items are named *Protected Network Settings Data*. These are the settings data that the administrator sets to the MFD, and possibly affects MFD's function of Send to E-mail/FTP, fax transmission, internet fax transmission and tandem. Therefore, these settings possibly affect protection of the actual image data written in the previous sections each.

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: Environmental Assumptions

Identifier	Definition
A.NETWORK	The MFD, in which the TOE is installed, is connected to an internal network kept secure so as not to be wiretapped, and is protected against being accessed arbitrarily from any external networks.
A.OPERATOR	The Key Operator and the Web-Admin are trustworthy persons who will not take improper action with respect to the MFD and the TOE.
A.USER	Every user, who may be an administrator of the TOE and/or the MFD, handles the password in the following ways: • Every password shall be set up not easy to guess. • Every password shall be updated on regular basis. • Every password shall be maintained in safety.

3.2 Threats

Threats to the TOE are described in Table 5. This ST assumes attackers on the TOE who have generic knowledge of the TOE behaviours and the skills to remove the MSD physically from the MFD and use readily obtained software and hardware tools to replicate or steal the information in the MSD.

Table 5: Threats to the TOE

Identifier	Definition
T.RECOVER	An attacker physically removes the MSD from MFD to read the MSD and recover the actual image data stored in it.
T.SHUNT	An attacker tampers with the network-related settings of the MFD to make the MFD send the actual image data to the equipments that the attacker uses as means to attack, when a user operates the MFD to send the actual image data.
T.SPOOF	An attacker impersonates a user to print or transmit actual image data that the user has stored in the MSD.

3.3 Organizational Security Policies

This ST assumes no organizational security policy.

4 Security Objectives

This chapter discusses the security objectives for the TOE.

4.1 TOE Security Objectives

The security objectives of the TOE are shown in Table 6.

Table 6: TOE Security Objectives

Identifier	Definition
O.RESIDUAL	Spooled actual image data and actual image data stored in the MSD using the filing function shall be cleared (by overwriting) once it is no longer needed.
O.REMOVE	To make it impossible to display an image in the event that the MSD of a TOE-equipped MFD is read using a device other than the MFD that spooled the data or stored it by filing, the actual image data shall be encrypted before being stored using a cryptographic key unique to the MFD.
O.MANAGE	Only the Key Operator shall be provided security administrative functions to maintain secure operation of the TOE.
O.NSP	The network-related settings functionality of the MFD shall be provided only to Key Operator and the Web-Admin.
O.UAU	To protect actual image data stored by a user in the MFD using the filing function, a user authentication method shall be provided.

4.2 Environmental Security Objectives

TOE environmental security objectives are described in Table 7.

Table 7: Environmental Security Objectives

Identifier	Definition
OE.BROWSER	In the IT environment of the TOE, authentic input functionality shall be provided by Web browsers used when the Web-Admin accesses to the Web-Admin Pages and when the users call up the saved confidential files in the MFD.
OE.CIPHER	Under the internal network environment, in which the TOE is to be installed, there shall be implemented protections for the TOE communications data against wiretapping.
OE.CLIENT	In the IT environment of the TOE, clients that send print jobs or PC-Fax jobs to the TOE shall provide a function allowing the user to specify the filing password before sending the jobs to the TOE.
OE.FIREWALL	The connection between the internal network on which the TOE is installed and the external network shall be accomplished using communication devices with functions that protect the internal network against security threats from the external network.
OE.OPERATE	Those in charge of the organization shall select suitable persons for the role of the Key Operator and the Web-Admin with the utmost care, and shall have them understand each of the roles.
OE.USER	Those in charge of the organization shall have the Key Operator and the Web-Admin observe the following rules: • Every password shall be set up not easy to guess. • Every password shall be updated on regular basis. • Every password shall be maintained in safety. The Key Operator shall have the users of confidential files observe the rules above.

5 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

This section describes the TOE Security Functional Requirements for every class of [CC_PART2]. The minimum strength of function for the TOE is to be defined in section 5.1.3. All the TOE Security Functional Requirements, described in this section, are taken from [CC_PART2], and contain no extended requirements.

5.1.1.1 Class FCS: Cryptographic Support

- FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall**, whenever the TOE is powered on,** generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [MSN-D Extension Algorithm] and specified cryptographic key sizes [128 bits] that meet the following: [{Sharp Standard}].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

- FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [{ • Encrypting any unencrypted actual image data and the confidential file password before writing to the MSD • Decrypting any actual image data and the confidential file password after reading the MSD }] in accordance with a specified cryptographic algorithm [Rijndael Algorithm] and cryptographic key sizes [128 bits] that meet the following: [{FIPS PUB 197}].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.1.1.2 Class FDP: User data protection

- FDP_RIP.1 Subset residual information protection

Hierarchical to:	No other components.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting one or more times** upon the *[deallocation of the resource from]* the following objects: [{image data files}].
Dependencies:	No dependencies

5.1.1.3 Class FIA: Identification and authentication

- FIA_AFL.1(1) Authentication failure handling (1)

Hierarchical to: No other components.

FIA_AFL.1.1(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(1) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [stop accepting authentication attempts for at least 5 minutes].

Dependencies: FIA_UAU.1 Timing of authentication

- FIA_AFL.1(2) Authentication failure handling (2)

Hierarchical to: No other components.

FIA_AFL.1.1(2) The TSF shall detect when *[* [3 (*positive integer number*)] *]* unsuccessful authentication attempts occur related to [the number of failed Web-Admin authentication attempts following the last successful authentication].

FIA_AFL.1.2(2) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [stop accepting authentication attempts for at least 5 minutes].

Dependencies: FIA_UAU.1 Timing of authentication

- FIA_AFL.1(3) Authentication failure handling (3)

Hierarchical to: No other components.

FIA_AFL.1.1(3) The TSF shall detect when *[* [3 (*positive integer number*)] *]* unsuccessful authentication attempts occur related to [the number of failed authentication attempts for a confidential file following the last successful authentication for that confidential file].

FIA_AFL.1.2(3) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [stop accepting authentication attempts for that confidential file until the Key Operator releases it].

Dependencies: FIA_UAU.1 Timing of authentication

- FIA_SOS.1(1) Verification of secrets (1)

Hierarchical to: No other components.

FIA_SOS.1.1(1) The TSF shall provide a mechanism to verify that **the Key Operator Code** (secrets) **meets** (meet) [5-digit decimal number].

Dependencies: No dependencies

- FIA_SOS.1(2) Verification of secrets (2)

Hierarchical to: No other components.

FIA_SOS.1.1(2) The TSF shall provide a mechanism to verify that **the Web-Admin password** (secrets) **meets** (meet) [a length of at least 5 characters each of which is an upper-case alphabet, a lower-case alphabet, a digits or a punctuation mark].

Dependencies: No dependencies

- FIA_SOS.1(3) Verification of secrets (3)

Hierarchical to: No other components.

FIA_SOS.1.1(3) The TSF shall provide a mechanism to verify that **the password for a confidential file** (secrets) **meets** (meet) [5-digit decimal number].

Dependencies: No dependencies

- FIA_UAU.2(1) User authentication before any action (1)

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1(1) The TSF shall require **Key Operator** (each user) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of **Key Operator** (that user).

Dependencies: FIA_UID.1 Timing of identification

- FIA_UAU.2(2) User authentication before any action (2)

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1(2) The TSF shall require **Web-Admin** (each user) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of **Web-Admin** (that user).

Dependencies: FIA_UID.1 Timing of identification

- FIA_UAU.2(3) User authentication before any action (3)

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1(3) The TSF shall require each user **that stored a confidential file** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

- FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [{

- Web-Admin shall be re-authenticated before being allowed changing Web-Admin password.

}].

Dependencies: No dependencies

- FIA_UAU.7(1) Protected authentication feedback (1)

Hierarchical to: No other components.

FIA_UAU.7.1(1) The TSF shall provide only [asterisks as many as characters provided] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

- FIA_UID.2(1) User identification before any action (1)

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1(1) The TSF shall require **Key Operator** (each user) to identify itself before allowing any other TSF-mediated actions on behalf of **Key Operator** (that user).

Dependencies: No dependencies

- FIA_UID.2(2) User identification before any action (2)

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1(2) The TSF shall require **Web-Admin** (each user) to identify itself before allowing any other TSF-mediated actions on behalf of **Web-Admin** (that user).

Dependencies: No dependencies

- FIA_UID.2(3) User identification before any action (3)

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1(3) The TSF shall require each user **that stored a confidential file** to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.1.4 Class FMT: Security management

- FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to ***[disable]*** the functions [{

- Clear All Memory
- Clear Document Filing Data
- Power Up All Clear

}] to [Key Operator].

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

- FMT_MTD.1(1) Management of TSF data (1)

Hierarchical to: No other components.

FMT_MTD.1.1(1) The TSF shall restrict the ability to ***[modify, query]*** the [{

- Number of times Auto Clear at Job End program is repeated
- Number of times data clear operations are repeated
- Data areas to be cleared by Power up Auto Clear program
- Number of times Power up Auto Clear program is repeated
- Key Operator Code

}] to [Key Operator].

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

- FMT_MTD.1(2) Management of TSF data (2)

Hierarchical to: No other components.

FMT_MTD.1.1(2) The TSF shall restrict the ability to ***[modify]*** the [{Web-Admin password}] to [Web-Admin].

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

- FMT_MTD.1(3) Management of TSF data (3)

Hierarchical to: No other components.

FMT_MTD.1.1(3) The TSF shall restrict the ability to ***[modify, delete]*** the [{password for a confidential file}] to [the user that stored the confidential file].

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

- FMT_MTD.1(4) Management of TSF data (4)

Hierarchical to: No other components.

FMT_MTD.1.1(4) The TSF shall restrict the ability to ***[*** [reset to factory default (*other operations*)] ***]*** the [{Web-Admin password}] to [Key Operator].

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

- 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: [{shown in Table 8}].

  Dependencies: No dependencies

- FMT_SMR.1(1) Security roles (1)

  Hierarchical to: No other components.

  FMT_SMR.1.1(1) The TSF shall maintain the roles [Key Operator].

  FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

  Dependencies: FIA_UID.1 Timing of identification

- FMT_SMR.1(2) Security roles (2)

  Hierarchical to: No other components.

  FMT_SMR.1.1(2) The TSF shall maintain the roles [Web-Admin].

  FMT_SMR.1.2(2) The TSF shall be able to associate users with roles.

  Dependencies: FIA_UID.1 Timing of identification

- FMT_SMR.1(3) Security roles (3)

  Hierarchical to: No other components.

  FMT_SMR.1.1(3) The TSF shall maintain the roles [each user that stored a confidential file].

  FMT_SMR.1.2(3) The TSF shall be able to associate users with roles.

  Dependencies: FIA_UID.1 Timing of identification

5.1.1.5 Class FPT: Protection of the TSF

- FPT_RVM.1 Non-bypassability of the TSP

  Hierarchical to: No other components.

  FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

  Dependencies: No dependencies

- FPT_SEP.1 TSF domain separation

  Hierarchical to: No other components.

  FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

  FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

  Dependencies: No dependencies

Table 8: Management Functions of the TOE

Origin	Management Function	Role
FCS_CKM.1	None (the cryptographic key does not have attributes that require management)	—
FCS_COP.1	None (no management requirements)	—

[DSK_ST]

Origin	Management Function	Role
FDP_RIP.1	• Modify and query the number of times Auto Clear at Job End program is repeated • Modify and query the number of times data clear operations are repeated • Modify and query the data areas to be cleared by Power up Auto Clear program • Modify and query the number of times Power up Auto Clear program is repeated • Disable Clear All Memory • Disable Clear Document Filing Data • Disable Power Up All Clear (The timing to perform protection is fixed to the release of allocation.)	Key Operator
FIA_AFL.1(1)	None (the threshold and action are fixed)	—
FIA_AFL.1(2)	None (the threshold and action are fixed)	—
FIA_AFL.1(3)	• Release the lock of confidential files (The threshold and action are fixed)	Key Operator
FIA_SOS.1(1)	None (the quality metric is fixed)	—
FIA_SOS.1(2)	None (the quality metric is fixed)	—
FIA_SOS.1(3)	None (the quality metric is fixed)	—
FIA_UAU.2(1)	• Modify and query the Key operator code	Key Operator
FIA_UAU.2(2)	• Modify the Web-Admin password	Web-Admin
	• Reset the Web-Admin password to factory default	Key Operator
FIA_UAU.2(3)	• Change the password for a confidential file • Delete the password for a confidential file	The user that saved the confidential file
FIA_UAU.6	None (requires re-authentication whenever the Web-Admin password change function is being used)	—
FIA_UAU.7(1)	None (no management requirements)	—
FIA_UID.2(1)	None (user identification information and identification operation are fixed)	—
FIA_UID.2(2)	None (user identification information and identification operation are fixed)	—
FIA_UID.2(3)	None (user identification information and identification operation are fixed for each confidential file)	—
FMT_MOF.1	None (the role group that mutually influences and is influenced by the TSF functions is fixed to the Key Operator alone)	—
FMT_MTD.1(1)	None (the role group that mutually influences and is influenced by the TSF data is fixed to the Key Operator alone)	—
FMT_MTD.1(2)	None (the role group that mutually influences and is influenced by the TSF data is fixed to the Web-Admin alone)	—
FMT_MTD.1(3)	None (the role group that mutually influences and is influenced by the TSF data is fixed to the user alone who saved the confidential file)	—
FMT_MTD.1(4)	None (the role group that mutually influences and is influenced by the TSF data is fixed to the Key Operator alone)	—
FMT_SMF.1	None (no management requirements)	—
FMT_SMR.1(1)	None (the user who plays part of the role is fixed to the Key Operator alone)	—
FMT_SMR.1(2)	None (the user who plays part of the role is fixed to the Web-Admin alone)	—
FMT_SMR.1(3)	None (the user who plays part of the role is fixed to the user alone who saved the confidential file)	—
FPT_RVM.1	None (no management requirements)	—
FPT_SEP.1	None (no management requirements)	—

5.1.2 TOE Security Assurance Requirements

Assurance components for the assurance level selected by this document are shown in Table 9. Table 9 shows the assurance requirements that must be satisfied to claim EAL3 compliance. All dependencies are satisfied.

Table 9: Assurance Requirements

Component	Component Name	Dependencies
ACM_CAP.3	Authorization controls	ALC_DVS.1
ACM_SCP.1	TOE CM coverage	ACM_CAP.3
ADO_DEL.1	Delivery procedures	None
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	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ALC_DVS.1	Identification of security measures	None
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	None
ATE_IND.2	Independent testing - sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.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(1), FIA_UAU.2(2), FIA_UAU.2(3), FIA_UAU.6, FIA_SOS.1(1), FIA_SOS.1(2) and FIA_SOS.1(3) use a probabilistic or permutational mechanism, and the explicitly stated functional strength is SOF-basic. FCS_COP.1 is a functional requirement that uses a cryptographic algorithm, and thus does not apply to this SOF level.

5.2 Security Requirements for the IT Environment

5.2.1 Security Functional Requirements for the IT Environment

This section describes the IT security requirements that the IT environment of the TOE must satisfy. In the IT environment for the TOE, following three types of entities have requirements to satisfy:

a) Web browsers:
are used on the clients for accessing the TOE Web. Most Web browsers being popularly used satisfy the requirements below. For example, Microsoft Internet Explorer Version 6.0 for Microsoft Windows clients does.

b) Print clients:
are the clients that transfer print data to the TOE for the printer function (section 2.1.2.2) of the TOE. Typically, the printer driver, that is the software that runs on the client and generates print data, should be what provides UI satisfying the requirements. The printer drivers that Sharp provides for MFD models (see section 2.2.1) on which the TOE can operate satisfy the requirements below. The above-mentioned printer driver accompanies MFDs that are equipped standard with the printer function and also accompanies the Sharp genuine printer options for the MFD.

c) PC-FAX clients:
are the clients that transfer image data to the TOE for the PC-FAX function (section 2.1.2.7) of the TOE. Typically, the PC-FAX driver, that is the software that runs on the client and generates image data for PC-FAX transmission, should be what provides UI satisfying the requirements. The PC-FAX drivers that Sharp provides for MFD models (see section 2.2.1) on which the TOE can operate satisfy the requirements below. The above-mentioned PC-FAX driver accompanies MFDs that are equipped standard with the printer function and also accompanies the Sharp genuine printer options for the MFD.

Security functional requirements that these entities shall satisfy follow:

- FIA_UAU.7(2) Protected authentication feedback (2)

  Hierarchical to: No other components.

  FIA_UAU.7.1(2) The **Web browsers** (TSF) shall provide only [dummy characters that show nothing other than number of characters provided] to the user while the authentication is in progress.

  Dependencies: FIA_UAU.1 Timing of authentication

- FIA_SOS.1(4) Verification of secrets (4)

  Hierarchical to: No other components.

  FIA_SOS.1.1(4) The **print clients and PC-Fax clients** (TSF) shall provide a mechanism to verify that **the password for a confidential file** (secrets) **meets** (meet) [5-digit decimal number].

  Dependencies: No dependencies

5.2.2 Security Assurance Requirements for the IT Environment

The IT environment of the TOE has no security assurance requirement to satisfy.

6 TOE Summary Specification

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

6.1 TOE Security Functions (TSF)

The correspondence between the TOE security functional requirements and the TOE security functions is shown in Table 10. The section number where each correspondence is described is shown in the table.

Table 10: Functional Requirements and Summary Specification

Function Requirement	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT	TSF_NSP	TSF_FCF
FCS_CKM.1	6.1.1						
FCS_COP.1		6.1.2					
FDP_RIP.1			6.1.3				
FIA_AFL.1(1)			6.1.3	6.1.4			
FIA_AFL.1(2)						6.1.6	
FIA_AFL.1(3)				6.1.4	6.1.5		6.1.7
FIA_SOS.1(1)					6.1.5		
FIA_SOS.1(2)						6.1.6	
FIA_SOS.1(3)							6.1.7
FIA_UAU.2(1)			6.1.3	6.1.4			
FIA_UAU.2(2)						6.1.6	
FIA_UAU.2(3)							6.1.7
FIA_UAU.6						6.1.6	
FIA_UAU.7(1)			6.1.3	6.1.4			6.1.7
FIA_UID.2(1)			6.1.3	6.1.4			
FIA_UID.2(2)						6.1.6	
FIA_UID.2(3)							6.1.7
FMT_MOF.1			6.1.3				
FMT_MTD.1(1)				6.1.4			
FMT_MTD.1(2)						6.1.6	
FMT_MTD.1(3)							6.1.7
FMT_MTD.1(4)				6.1.4			
FMT_SMF.1			6.1.3		6.1.5	6.1.6	6.1.7
FMT_SMR.1(1)			6.1.3	6.1.4	6.1.5		
FMT_SMR.1(2)						6.1.6	
FMT_SMR.1(3)							6.1.7
FPT_RVM.1			6.1.3	6.1.4		6.1.6	6.1.7
FPT_SEP.1			6.1.3	6.1.4		6.1.6	6.1.7

6.1.1 Cryptographic Key Generation (TSF_FKG)

TSF_FKG generates cryptographic keys (common keys), that FCS_CKM.1 requires, for supporting the cryptographic operation on actual image data. When the MFD is powered on, the MSN-D Extension Algorithm is used to generate a cryptographic key (common key) for execution of the AES Rijndael Algorithm. This cryptographic key is 128 bits long and is stored in volatile RAM.

6.1.2 Cryptographic Operation (TSF_FDE)

During the processing of a job, MFD spools the actual image data of the job in the MSD. Before the data is spooled to the MSD, the cryptographic key stored in volatile RAM is used to encrypt the data by means

of the AES Rijndael algorithm. When the MFD actually processes, or consumes, the spooled data, each block of the data is read from the MSD and decrypted as it becomes necessary during processing of the job.

The actual image data and passwords, which the users save by the confidential file function, are encrypted before being filed in the MSD, as well as the data being spooled. At each performance of authentication of the user that saved a confidential file before any operation on the saved file, the password for the confidential file is retrieved by reading the encrypted password and decrypting it. When the saved confidential file is called up and being printed or transmitted, each block of the data is read from the MSD and decrypted as it becomes necessary during processing, as well as the spooled data.

By contrast, when the data is exported, it is transmitted to the client, without getting decrypted, being kept encrypted as it is. For this reason, neither the actual image data nor the password of any confidential file is possible to be leaked due to the backup function.

When the data is imported, the data is checked whether it has been encrypted, and gets encrypted if not yet. This mechanism is for migration of the document filing data files saved before the TOE is installed.

6.1.3 Data Clear (TSF_FDC)

The TOE provides the Data Clear function that clears image data files that are spooled or saved. This function consists of following four programs:

a) Auto Clear at Job End program

b) Clear All Memory program

c) Clear Document Filing Data program

d) Power up Auto Clear program

Every program above overwrites the actual image data on the HDD with random values generated based on the lagged-Fibonacci type of random number generator with rotation of bits. The repeat count set by the Security Administration (TSF_FMT) function applies here. Each program above generates random values each time of the repeats. When the actual image data on the Flash memory are being cleared, the data are overwritten once with a fixed value.

The following sections elaborate upon each program:

6.1.3.1 Auto Clear at Job End program

This program overwrites the actual image data that has been:

a) Spooled to the HDD or the Flash memory in order to process a job, when the job ends, and

b) Saved to the HDD using the confidential file function, when the user deletes the data.

6.1.3.2 Clear All Memory program

When the Key Operator invokes this program, it overwrites and clears the actual image data on the HDD that has been spooled or saved, and the actual image data in Flash memory that has been spooled.

This program accepts Cancel operation. Before allowing cancelling this program while running, the TSF always requires entering Key Operator Code whenever a Cancel operation is taken.

While Key Operator Code is being entered, the TOE shows as many asterisk "＊" characters as digits entered, however does not show the digits entered. The clearing operation is only cancelled if Key Operator authentication is successful. If an incorrect Key Operator Code is entered three times in a row to this Key Operator authentication, this program stops accepting further authentication attempts for five minutes (see section 6.1.4 for more detail).

6.1.3.3 Clear Document Filing Data program

When the Key Operator invokes this program, it overwrites and clears the actual image data. Its clears all actual image data spooled to the HDD, all actual image data saved by the filing function, or both. One of these three options shall be specified by the Key Operator.

This program accepts Cancel operation as well as Clear All Memory program.

6.1.3.4 Power up Auto Clear program

This program overwrites and clears the actual image data when the TOE is powered on, unless the TOE has any reserved transmission jobs or any Fax/Internet fax reception jobs not yet printed out.

This program is enabled or disabled, in other words this program does or does not run when the TOE is powered on, according to the settings by the Security Administration (TSF_FMT) function. The target data area of this program is also according to those settings.

This program clears every MSD as well as the Clear All Data program, or the specified range in the HDD as well as the Clear Document Filing program.

This program accepts Cancel operation as well as Clear All Memory program.

6.1.4 Authentication (TSF_AUT)

The TOE always requires that the Key Operator enter a 5-digit PIN, i.e. Key Operator Code, before allowing any access to the Key Operator Programs. By correctly entering the Key Operator Code, the Key Operator is authenticated. Only the Key Operator authenticated is allowed to access functionalities of TSF_FMT (section 6.1.5) and the Network Settings UI of TSF_NSP (section 6.1.6).

While the Key Operator Code is being entered, protected feedback is provided. While Key Operator Code is being entered, the TOE shows as many asterisk "＊" characters as digits entered, however does not show the digits entered.

If an incorrect Key Operator Code is entered three times in a row, this TSF stops further authentication attempts for five minutes. The TSF manages the number of authentication failures. When authentication is successful, the authentication failure count is reset to zero. This TSF manages the time remaining until further authentication attempts are accepted. If the power of the TOE is removed while time remains, the time remaining will be reset to five minutes the next time the TOE is powered on.

TSF_FDC (section 6.1.3) provides a similar mechanism that stops accepting authentication attempts. These two mechanisms are coupled each other; they both count in their authentication failures on single shared count of them, and when one stops accepting authentication attempts the other also does. For instance, if TSF_FDC is stopping accepting authentication attempts and the user selects the Key Operator Programs before the remaining time reaches to zero, this TSF does not accept the authentication attempt.

6.1.5 Security Administration (TSF_FMT)

After the procedure of identification and authentication for the Key Operator by selecting Key Operator Programs and by the Authentication of Key Operator Code entry (TSF_AUT), Security Administration function (TSF_FMT) allows the following administrative security management functions:

a) Number of times Auto Clear at Job End program is repeated:
accepts any integer between 1 and 7 inclusive as the number of times overwriting the actual image data on the HDD for the *Auto Clear at Job End* program. The setting can be queried and modified. The setting is stored in EEPROM in the MFD.

b) Number of times data clear is repeated:
accepts any integer between 1 and 7 inclusive as the number of times overwriting the actual image data on the HDD for the *Clear All Memory* program and the *Clear Document Filing Data* program. The setting can be queried and modified. The setting is stored in EEPROM in the MFD.

c) Power up Auto Clear:
accepts settings to enable or disable *Power up Auto Clear* program for each data area. The settings are stored in EEPROM in the MFD.

d) Number of times Power up Auto Clear program is repeated:
accepts any integer between 1 and 7 inclusive as the number of times overwriting the actual image data on the HDD for the *Power up Auto Clear* program. The setting can be queried and modified. The setting is stored in EEPROM in the MFD.

e) Key Operator Code change:
The Key Operator Code can be queried and modified. This ST defines 5 digits decimal number as the quality metric of Key Operator Code. This TSF checks the quality of the new Key Operator Code. The setting is stored in EEPROM in the MFD.

f) Release the lock on document filing output operation:
Using this function, only the Key Operator is allowed to unlock the confidential files locked because of authentication failures in a row. Whether each confidential file is locked is recorded in the HDD inside the MFD.

g) Reset the NIC:
This function resets all of MFD network related settings to factory default. Thus the Protected Network Settings Data, include the Web-Admin password, are all reset.

The functions above correspond to the management functions for the Key Operator that TOE Security Functional Requirement FMT_SMF.1 provides.

6.1.6 Network Settings Protection (TSF_NSP)

Upon the network settings of the MFD, this TSF protects the *Protected Network Settings Data* listed in section 2.3.3 against modification by anyone other than the MFD administrators. This TSF consists of following two programs:

a) Network Settings UI

b) Network Management Pages

These two programs, implemented in the ROM of the TOE, are the only means to modify the Protected Network Setting Data. Thus, the Protected Network Setting Data are protected against modification by anyone other than the MFD administrators.

The following sections elaborate upon each program:

6.1.6.1 Network Settings UI

On the operation panel, the TOE provides the *Network Settings* UI, only after the Key Operator is successfully identified and authenticated (TSF_AUT) by selecting the Key Operator Programs and entering the Key Operator Code.

6.1.6.2 Network Management Pages

The TOE Web provides the *Network Management Pages*. This TSF requires any access to the Network Management Pages to identify and authenticate the user itself who is attempting the access with the user identification and the password of the Web-Admin, before allowing the access. The user is allowed the access only if the identification and the authentication succeed. On the TOE Web, the Network Management Pages are the only I/F to modify the Protected Network Setting Data. Thus, on the TOE Web, the Protected Network Setting Data are protected against modification by anyone other than the Web-Admin.

If Web-Admin authentication fails three times in a row, this program stops further authentication attempts will not be accepted for five minutes, as well as TSF_AUT does.

The password change function is provided in the *Password Setup* page among the Network Management Pages. Re-authentication with the current Web-Admin password is required before performing the functions in the Password Setup page.

The Password Setup page allows changing the Web-Admin password. To change the Web-Admin password, the new password, allowed to contain alphabets and punctuation marks as well as digits, will be rejected as an error if shorter than five letters.

6.1.7 Confidential Files (TSF_FCF)

When a user saves actual image data in the MFD as a confidential file, the data is protected by a password and authentication is required before calling it up and using it.

At the saving of data, i.e. the creation of a confidential file, this TSF requests the user to set a password, and verifies that the password meets the quality metric, 5-digit decimal number.

This TSF provides functionalities of the operations on saved confidential files on the operation panel and the TOE Web.

Whenever a user attempts some operation on a saved confidential file, this TSF requests the user to enter the password. This TSF shows as many asterisk “∗” characters as digits entered, however does not show the digits entered. In case a user attempts some operation on a saved confidential file via the operation

panel, this TSF allows the operations described in section 2.1.2.8 except Preview, only when a password is given and it is identical to the password during the saving of the file.

If an incorrect password is entered three times in a row during the authentication before an operation on a saved confidential file, this TSF locks the file to prohibit any operation. A count is kept of the number of authentication failures for each file. When authentication is successful, the authentication failure count of the file is reset to zero. This TSF can lock a file, but cannot release the lock. The lock can only be released by the Security Administration (TSF_FMT) function.

This TSF allows changing the password, as one of the operations on a saved confidential file. This TSF verifies the new password meets the quality metric, 5-digit decimal number.

This TSF allows changing the property, as one of the operations on a saved confidential file. The password is deleted when the property is changed to other than Confidential. In the other direction, a password must be set to change the property to Confidential, and then this TSF verifies the password meets the quality metric, 5-digit decimal number.

6.2 Assurance Measures

The documents that serve as the assurance method for each component of the security assurance requirements in this ST are shown in Table 11.

Table 11: Assurance Measures

Component	Assurance Measures
ACM_CAP.3	AR-FR21 Configuration Management Document
ACM_SCP.1	AR-FR21 VERSION M.10 Configuration List
ADO_DEL.1	AR-FR21 Delivery Procedures Document
ADO_IGS.1	AR-FR21 Delivery Instruction Document, AR-FR21 Installation Instruction Manual (*1)
ADV_FSP.1	AR-FR21 Security Function Specifications
ADV_HLD.2	AR-FR21 High-level Design Document
ADV_RCR.1	AR-FR21 Representation Correspondence Analysis Document
AGD_ADM.1 AGD_USR.1 AVA_MSU.1	Following guidance documents (*2): • AR-FR21 Data Security Kit Operation Manual • AR-FR21 Data Security Kit Notice • AR-FR21 Web Help (General) • AR-FR21 Web Help (Document Filing) • Laser Printer Key Operator's Guide • Laser Printer Operation Manual (for general information and copier operation) • Laser Printer Operation Manual (for printer) • Laser Printer Operation Manual (for network scanner) • AR-FX12 Facsimile Expansion Kit Operation Manual
ALC_DVS.1	AR-FR21 Development Security Specifications
ATE_COV.2	AR-FR21 Testing Coverage Analysis Document
ATE_DPT.1	AR-FR21 High-level Design Testing Analysis Document
ATE_FUN.1 ATE_IND.2	AR-FR21 Functional Testing Specifications, AR-FR21 Testing Environment and Tools Manual
AVA_SOF.1	AR-FR21 Security Strength of Function Analysis Document
AVA_VLA.1	AR-FR21 Vulnerability Analysis Document

(*1) Written in 5 languages: English, Spanish, French, German and Japanese.

(*2) Assurance measures include English edition and Japanese edition of each guidance documents.

Documents without any mark are written in Japanese.

6.3 Strength of Security Functions

Probabilistic and permutational mechanisms used to implement TSFs are described below.

a) Key Operator Code:
TSFs implemented using the Key Operator Code are Key Operator authentication (TSF_AUT and TSF_FDC) and Key Operator Code change (TSF_FMT). The strength of these security functions is *SOF-basic.*

b) Web-Admin password
TSFs implemented using Web-Admin password are Web-Admin authentication, Web-Admin re-authentication, and Web-Admin password change (all TSF_NSP). The strength of these security functions is *SOF-basic.*

c) Confidential file password:
TSFs implemented using confidential file passwords are the confidential file save function, the authentication before an operation on a saved confidential file, and password change operations (all TSF_FCF). The strength of these security functions is *SOF-basic.*

7 PP Claims

The TOE does not claim conformance to any PP.

8 Rationale

This chapter demonstrates the completeness and consistency of this ST.

8.1 Rationale for Security Objectives

Table 12 verifies the effectiveness of the policies indicated in the security objectives are effective in countering the threats and assumptions indicated in the TOE security environment. Table 12 shows each section number that provides the rationale for the correspondence between threats and assumptions and the security objectives.

Table 12: Security Objectives Rationale

Security Objective	Threat T.RECOVER	Threat T.SHUNT	Threat T.SPOOF	Assumption A.NETWORK	Assumption A.OPERATOR	Assumption A.USER
O.RESIDUAL	8.1.1					
O.REMOVE	8.1.1					
O.MANAGE	8.1.1					
O.NSP		8.1.2				
O.UAU			8.1.3			
OE.BROWSER		8.1.2	8.1.3			
OE.CIPHER				8.1.4		
OE.CLIENT			8.1.3			
OE.FIREWALL				8.1.4		
OE.OPERATE					8.1.5	
OE.USER						8.1.6

8.1.1 T.RECOVER

O.MANAGE counters the threat T.RECOVER by implementing management of the TOE functions by the Key Operator for operation of the TOE. O.RESIDUAL clears the actual image data not to be read out. In addition, even if any actual image data not yet cleared were read out, O.REMOVE counters the threat by encrypting the data before writing to the MSD, so that the data is not in a form that has meaning to a human viewing it. Thus leakage of information in the MSD is prevented.

8.1.2 T.SHUNT

To counter the threat T.SHUNT, O.NSP protects the network-related settings functions so that only the approved administrators (the Key Operator and the Web-Admin) can access the protected functions. The Web-Admin shall observe OE.BROWSER and use a Web browser with authentic input functionality. Thus an attacker is prevented from changing network related settings.

8.1.3 T.SPOOF

To counter the threat T.SPOOF, O.UAU and OE.CLIENT gives the user authentication data to files stored in the MFD, and O.UAU and OE.BROWSER authenticate the user. When the user stores a file in the MFD, the user sets a password that only he or she knows. Thus an attacker is prevented from impersonation.

8.1.4 A.NETWORK

The assumption A.NETWORK requires the security for the internal network where the TOE is installed. So OE.FIREWALL protects the internal network against security threats from the external network. And OE.CIPHER protects the TOE communications data under the internal network environment. Thus the necessary security is kept in the internal network where the TOE is installed.

8.1.5 A.OPERATOR

The assumption A.OPERATOR requires that the Key Operator and the Web-Admin are trustworthy persons. OE.OPERATE satisfies it by enforcing strict selection of the person who will be the Key Operator and the Web-Admin based on an understanding of their roles.

8.1.6 A.USER

A.USER provides the particulars that the users shall comply over passwords. It is satisfied on all users that use any password if those in charge of the organization have the Key Operator and the Web-Admin observe rules of OE.USER and the Key Operator and the Web-Admin have the users of confidential files observe the rules.

8.2 Rationale for IT Security Requirements

The IT security requirements are to be verified for its effectiveness in attaining the security objectives.

8.2.1 Rationale for TOE Security Functional Requirements

This section demonstrates that the TOE security functional requirements attain the security objectives of the TOE.

The correspondence between the TOE security functional requirements and the TOE security objectives is shown in Table 13. Table 13 indicates the section that contains the rationale for each correspondence.

Table 13: Rationale for TOE Security Functional Requirements

Policy / Requirement	O.RESIDUAL	O.REMOVE	O.MANAGE	O.NSP	O.UAU
FCS_CKM.1		8.2.1.2			
FCS_COP.1		8.2.1.2			
FDP_RIP.1	8.2.1.1				
FIA_AFL.1(1)			8.2.1.3	8.2.1.4	
FIA_AFL.1(2)				8.2.1.4	
FIA_AFL.1(3)			8.2.1.3		8.2.1.5
FIA_SOS.1(1)			8.2.1.3	8.2.1.4	
FIA_SOS.1(2)				8.2.1.4	
FIA_SOS.1(3)					8.2.1.5
FIA_UAU.2(1)			8.2.1.3	8.2.1.4	
FIA_UAU.2(2)				8.2.1.4	
FIA_UAU.2(3)					8.2.1.5
FIA_UAU.6				8.2.1.4	
FIA_UAU.7(1)			8.2.1.3	8.2.1.4	8.2.1.5
FIA_UID.2(1)			8.2.1.3	8.2.1.4	
FIA_UID.2(2)				8.2.1.4	
FIA_UID.2(3)					8.2.1.5
FMT_MOF.1			8.2.1.3		
FMT_MTD.1(1)			8.2.1.3		
FMT_MTD.1(2)				8.2.1.4	
FMT_MTD.1(3)					8.2.1.5
FMT_MTD.1(4)			8.2.1.3		
FMT_SMF.1			8.2.1.3	8.2.1.4	8.2.1.5
FMT_SMR.1(1)			8.2.1.3		
FMT_SMR.1(2)				8.2.1.4	

Policy Requirement	O.RESIDUAL	O.REMOVE	O.MANAGE	O.NSP	O.UAU
FMT_SMR.1(3)					8.2.1.5
FPT_RVM.1			8.2.1.3	8.2.1.4	8.2.1.5
FPT_SEP.1			8.2.1.3	8.2.1.4	8.2.1.5

8.2.1.1 O.RESIDUAL

O.RESIDUAL is an objective to overwrite the area where the actual image data stored in MSD are archived, i.e. the image data file. In accordance with it, FDP_RIP.1 requires to activate overwriting for user data protection when each job finishes, when a confidential file is deleted, when a user invokes Clear All Memory or Clear Document Filing Data, and when powered on.

8.2.1.2 O.REMOVE

O.REMOVE is an objective to prevent the actual image data stored in the MSD of the MFD from being displayed in images even if an access is made from a source other than the TOE that executed the retention of the actual image data.

The actual image data within the MFD are encrypted due to FCS_COP.1 and are never retained in the MSD without being encrypted. Thus, attackers are prevented from trying to display in images the image data files that are not yet cleared by FDP_RIP.1. To implement FCS_COP.1, an encryption key is generated from a cryptographic key of FCS_CKM.1.

8.2.1.3 O.MANAGE

O.MANAGE stipulates that the Key Operator manages the TOE functions indicated below to ensure secure operation of the TOE.

a) The Key Operator is authenticated according to FIA_UAU.2(1), FIA_UAU.7(1), FIA_UID.2(1) and FIA_AFL.1(1). Thus only the Key Operator is allowed the following actions.
   - FMT_MTD.1(1) allows only the Key Operator to query and modify the number of times HDD is overwritten upon Auto Clear at Job End, the number of times HDD is overwritten upon data clear operations, and the Key Operator Code.
   - FMT_MTD.1(4) allows only the Key Operator to use the function that initializes the Web-Admin password to factory default.
   - FIA_AFL.1(3) allows only the Key Operator to release the lock on a confidential file set up after a series of failed authentication.
   - FMT_MOF.1 allows only the Key Operator to disable the following functions: Clear All Memory, Clear Document Filing Data and Power Up All Clear

b) FPT_RVM.1 is a requirement to ensure that identification and authentication of the Key Operator described in a) above are invoked and succeeded before each function that shall be allowed only to the Key Operator.

c) FPT_SEP.1 requires the security domain to protect each of the functions described in a) above.

d) Among the management functions defined in FMT_SMF.1(1), ones for the Key Operator correspond to the security objective O.MANAGE.

e) The appropriate SOF for the Key Operator Code is attained as follows:
   - FIA_AFL.1(1) requires to stop accepting authentication attempts for a period of time when unsuccessful authentication attempts repeated, to counter against a brute force attack on the Key Operator Code.
   - FIA_SOS.1(1) requires mechanisms that enforce the quality metric on the Key Operator Code.

f) The Key Operator is granted the role of the TOE administration in accordance with FMT_MOF.1 and FMT_MTD.1(1). And the role is to be maintained in accordance with FMT_SMR.1(1). Thus the management functions are always executed by the authorized Key Operator.

8.2.1.4 O.NSP

The combination of the following features satisfies O.NSP:

a) Password protection for the Network Settings UI:

- The Key Operator Code is used to identify and authenticate the Key Operator in accordance with FIA_UAU.2(1), FIA_UAU.7(1), FIA_UID.2(1) and FIA_AFL.1(1). The identification and authentication shall be carried out before providing the Network Settings UI allowing the modification of the Protected Network Settings Data.
- FPT_RVM.1 requires ensuring the above-mentioned identification/authentication to be always invoked and succeeded before providing the Network Settings UI allowing the modification of the Protected Network Settings Data.
- FPT_SEP.1 requires the security domain for the protection of the Network Settings UI.

b) Password protection for the Network Management Pages:

- A password is used to identify and authenticate the Web-Admin in accordance with FIA_UAU.2(2), FIA_UID.2(2) and FIA_AFL.1(2). The identification and authentication shall be carried out before providing the Network Management Pages allowing the modification of the Protected Network Settings Data. The IT environment requirement FIA_UAU.7(2) is adopted instead of FIA_UAU.7(1) here.
- FPT_RVM.1 requires ensuring the above-mentioned identification/authentication to be always invoked and succeeded before providing the Network Management Pages allowing the modification of the Protected Network Settings Data.
- FMT_SMF.1 requires the function to modify the Web-Admin password in relation to FIA_UAU.2(2). FMT_MTD.1(2) allows only the Web-Admin to use the function, and FIA_UAU.6 requires the re-authentication.
- The role Web-Admin is allowed managing the Web-Admin password, among the TSF data, and is maintained in accordance with FMT_SMR.1(2).
- FPT_SEP.1 requires the security domain for the protection of the Network Management Pages.

c) Attainment of an appropriate SOF:

- FIA_AFL.1(1) requires to stop accepting authentication attempts for a period of time when unsuccessful authentication attempts repeated, to counter against a brute force attack on the Key Operator Code.
- FIA_AFL.1(2) requires to stop accepting authentication attempts for a period of time when unsuccessful authentication attempts repeated, to counter against a brute force attack on the Web-Admin password.
- FIA_SOS.1(1) requires mechanisms that enforce the quality metric on the Key Operator Code.
- FIA_SOS.1(2) requires mechanisms that enforce the quality metric on the Web-Admin password.

8.2.1.5 O.UAU

The combination of following three features satisfies O.UAU:

a) Password protection for operations on saved confidential files:

- FIA_UID.2(3) and FIA_UAU.2(3) require the protection of the operations on saved confidential files by identifying and authenticating the user that stored the confidential file through the confidential file password.
- FPT_RVM.1 requires ensuring the above-mentioned identification/authentication to be always invoked and succeeded before allowing the operations on saved confidential files.
- FMT_SMF.1 requires the function to modify / delete the confidential file password in relation to FIA_UAU.2(3). Only the user that stored the confidential file is allowed for its use in accordance with FMT_MTD.1(3).
- The role of each user that stored a confidential file is allowed managing the confidential file password among TSF data, and is maintained in accordance with FMT_SMR.1(3).
- FPT_SEP.1 requires the security domain for the protection of the operations on saved confidential files.

b) Authentication input I/F suitable for entering passwords:

- FIA_UAU.7(1) requires an authentication input I/F suitable for entering passwords.

c) Attainment of an appropriate SOF:

- FIA_AFL.1(3) requires to lock a file when unsuccessful authentication attempts repeated, to counter against a brute force attack on the authentication mechanism for the file.
- FIA_AFL.1(3) allows only the identified and authenticated Key Operator to have the lock released.
- FIA_SOS.1(3) requires mechanisms that enforce the quality metric on the confidential file password.

8.2.2 Rationale for security functional requirement dependencies

Security functional requirement dependencies are shown in Table 14. Table 14 indicates the dependencies that are stipulated by the CC, the dependencies that are satisfied by the TOE, and for dependencies that are not satisfied by the TOE, the section that provides justification for non-satisfaction.

Table 14: Security Functional Requirement Dependencies

Dependencies Requirement	Stipulated	Satisfied	Unsatisfied	Justifi-cation
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1	FCS_CKM.4, FMT_MSA.2	8.2.2.1
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1	ditto	ditto
FDP_RIP.1	—	—	—	—
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.2(1)	—	—
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.2(2)	—	—
FIA_AFL.1(3)	FIA_UAU.1	FIA_UAU.2(3)	—	—
FIA_SOS.1(1)	—	—	—	—
FIA_SOS.1(2)	—	—	—	—
FIA_SOS.1(3)	—	—	—	—
FIA_SOS.1(4)*	—	—	—	—
FIA_UAU.2(1)	FIA_UID.1	FIA_UID.2(1)	—	—
FIA_UAU.2(2)	FIA_UID.1	FIA_UID.2(2)	—	—
FIA_UAU.2(3)	FIA_UID.1	FIA_UID.2(3)	—	—
FIA_UAU.6	—	—	—	—
FIA_UAU.7(1)	FIA_UAU.1	FIA_UAU.2(1), FIA_UAU.2(3)	—	—
FIA_UAU.7(2)*	FIA_UAU.1	FIA_UAU.2(2)	—	—
FIA_UID.2(1)	—	—	—	—
FIA_UID.2(2)	—	—	—	—
FIA_UID.2(3)	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(1)	—	—
FMT_MTD.1(1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(1)	—	—
FMT_MTD.1(2)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(2)	—	—
FMT_MTD.1(3)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(3)	—	—
FMT_MTD.1(4)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(1)	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1(1)	FIA_UID.1	FIA_UID.2(1)	—	—
FMT_SMR.1(2)	FIA_UID.1	FIA_UID.2(2)	—	—
FMT_SMR.1(3)	FIA_UID.1	FIA_UID.2(3)	—	—
FPT_RVM.1	—	—	—	—
FPT_SEP.1	—	—	—	—

Note: Functional requirements with an asterisk are for the IT environment, while others are for the TOE.

8.2.2.1 Rationale for FCS_COP.1 not requiring dependencies on FCS_CKM.4 and FMT_MSA.2

The cryptographic key is stored in the volatile RAM, and is lost when the power of the TOE/MFD is turned off. Each memory cell in volatile RAM is a circuit that store electricity, and memorizes information by electric charge. The volatile RAM loses the electric charge accumulation so that the cryptographic key becomes unreadable when the power of the TOE/MFD is turned off. Therefore, there

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

This cryptographic key consists of only a 128-bit key that is generated on powered on and is cleared during power-off. It does not have any security attributes such as dates. Therefore, there are not any security attributes that shall be ensured secure values in accordance with FMT_MSA.2.

8.2.3 Mutual Effect of TOE Security Functional Requirements

Table 15 shows the mutual effect of TOE security functional requirements.

Table 15: Mutual Effect of TOE Security Functional Requirements

Defence Requirement	Bypass	Disabling	Interference
FCS_CKM.1	—	—	—
FCS_COP.1	—	—	—
FDP_RIP.1	—	FMT_MOF.1	—
FIA_AFL.1(1)	—	—	—
FIA_AFL.1(2)	—	—	—
FIA_AFL.1(3)	—	—	—
FIA_SOS.1(1)	—	—	—
FIA_SOS.1(2)	—	—	—
FIA_SOS.1(3)	—	—	—
FIA_UAU.2(1)	FPT_RVM.1	—	FPT_SEP.1
FIA_UAU.2(2)	FPT_RVM.1	—	FPT_SEP.1
FIA_UAU.2(3)	FPT_RVM.1	—	FPT_SEP.1
FIA_UAU.6	—	—	—
FIA_UAU.7(1)	—	—	—
FIA_UID.2(1)	FPT_RVM.1	—	FPT_SEP.1
FIA_UID.2(2)	FPT_RVM.1	—	FPT_SEP.1
FIA_UID.2(3)	FPT_RVM.1	—	FPT_SEP.1
FMT_MOF.1	—	—	—
FMT_MTD.1(1)	—	—	—
FMT_MTD.1(2)	—	—	—
FMT_MTD.1(3)	—	—	—
FMT_MTD.1(4)	—	—	—
FMT_SMF.1	—	—	—
FMT_SMR.1(1)	—	—	—
FMT_SMR.1(2)	—	—	—
FMT_SMR.1(3)	—	—	—
FPT_RVM.1	—	—	—
FPT_SEP.1	—	—	—

8.2.3.1 Bypass

Mutual supports to protect against attempts of bypassing shown in Table 15 are described below:

a) In accordance with FIA_UAU.2(1), authenticating the Key Operator must be invoked and succeed before allowing any TSF-mediated actions on behalf of the Key Operator. It is ensured in accordance with FPR_RVM.1.

b) In accordance with FIA_UAU.2(2), authenticating the Web-Admin must be invoked and succeed before allowing any TSF-mediated actions on behalf of the Web-Admin. It is ensured in accordance with FPR_RVM.1.

c) In accordance with FIA_UAU.2(3), authenticating the user that stored a confidential file must be invoked and succeed before allowing any TSF-mediated actions on behalf of that user. It is ensured in accordance with FPR_RVM.1.

d) In accordance with FIA_UID.2(1), identifying the Key Operator must be invoked and succeed before allowing any TSF-mediated actions on behalf of the Key Operator. It is ensured in accordance with FPR_RVM.1.

e) In accordance with FIA_UID.2(2), identifying the Web-Admin must be invoked and succeed before allowing any TSF-mediated actions on behalf of the Web-Admin. It is ensured in accordance with FPR_RVM.1.

f) In accordance with FIA_UID.2(3), identifying the user that stored a confidential file must be invoked and succeed before allowing any TSF-mediated actions on behalf of that user. It is ensured in accordance with FPR_RVM.1.

The other functional requirements in this ST are not of types that are bypassed.

8.2.3.2 Disabling

Mutual supports to protect against attempts of disabling shown in Table 15 are described below:

The user data protection of FDP_RIP.1 does not give any measure to deactivate the calling after a job completion or when deleting a confidential file. FMT_MOF.1 allows only the Key Operator to deactivate the following programs by stopping each function while in execution: Clear All Memory, Clear Document Filing Data, and Power up Auto Clear.

The other functional requirements in this ST do not give any measure for deactivation.

8.2.3.3 Interfere

Mutual supports to protect against attempts of interference shown in Table 15 are described below:

a) An authorised subject generated by the Key Operator identification of FIA_UID.2(2) and the authentication of FIA_UAU.2(1) needs the security domain for the protection from interference by any unauthorised subjects. It is ensured in accordance with FPT.SEP.1.

b) An authorised subject generated by the Web-Admin identification of FIA_UID.2(2) and the authentication of FIA_UAU.2(2) needs the security domain for the protection from interference by any unauthorised subjects. It is ensured in accordance with FPT.SEP.1.

c) For each user that stored a confidential file, an authorised subject generated by the user identification of FIA_UID.2(3) and the authentication of FIA_UAU.2(3) needs the security domain for the protection from interference by any unauthorised subjects. It is ensured in accordance with FPT.SEP.1.

Upon the other functional requirements in this ST, no unauthorised subject exists.

8.2.4 Rationale for TOE security assurance requirements

The TOE is an MFD firmware upgrade kit, and is a commercial product. Threats can be countered by a combination of simple mechanisms, including data clearing (overwriting), encryption, and password protection.

For this reason, the quality assurance level selected for the TOE is EAL3, a sufficient level for commercial use.

8.2.5 Rationale for minimum strength of function

This ST stipulates assumptions and environmental security objectives for the purpose of limiting the ability of attackers to attack the TOE. However, this does not imply that there is no need to counter attackers with a *low* attack potential.

A sufficient strength of function for this purpose is SOF-basic. This ST requires the TOE a minimum strength of function of SOF-basic, and this is consistent.

8.2.6 Rationale for security requirements for the IT environment

This section demonstrates that the security requirements for the IT environment enable the attainment of the environmental security objectives. Among the environmental security objectives, OE.BROWSER and OE.CLIENT are for the IT environment. The other objectives are relevant to operation of the TOE.

OE.BROWSER requires authentic input functionality for the Web-Admin authentication and the confidential file password authentication. This authentic input functionality is considered to need the following:

a) I/F suitable for entering passwords:

- FIA_UAU.7(2) requires protected authentication feedback of the Web browsers.

OE.CLIENT includes a requirement for an interface that enables the user to specify a password to be assigned to a confidential file of a print job or a PC-Fax job. The following items are required of this interface:

a) Attainment of an appropriate SOF:

- FIA_SOS.1(4) requires the print client and the PC-Fax client to verify the quality of a file password.

In contrast to the TOE which handles both setting of the password and authentication, the print client and the PC-Fax client only handle setting of the password, and thus the above is sufficient.

Also, the quality inspection when setting up a Web-Admin password is a TOE security functional requirement FIA_SOS.1(2).

The dependencies among these security functional requirements are all satisfied as shown in the Table 14.

There is no reason to require any security assurance requirements of the IT environments, and there is no dependency by any other IT security requirements. Therefore, no security assurance requirement for the IT environment is necessary.

8.3 Rationale for TOE Summary Specification

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

8.3.1 Rationale for TOE security functions

The satisfaction of the TOE security functional requirements by the TOE security functions (TSFs) is shown in Table 16. Table 16 indicates the section that provides the rationale for the satisfaction of each TOE security functional requirement by the corresponding TOE security functions.

Table 16: TOE Security Functional Requirements and TOE Security Functions

Function Requirement	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT	TSF_NSP	TSF_FCF
FCS_CKM.1	8.3.1.1						
FCS_COP.1		8.3.1.2					
FDP_RIP.1			8.3.1.3				
FIA_AFL.1(1)			8.3.1.4	8.3.1.4			
FIA_AFL.1(2)						8.3.1.5	
FIA_AFL.1(3)				8.3.1.6	8.3.1.6		8.3.1.6
FIA_SOS.1(1)					8.3.1.7		
FIA_SOS.1(2)						8.3.1.8	
FIA_SOS.1(3)							8.3.1.9
FIA_UAU.2(1)			8.3.1.10	8.3.1.10			
FIA_UAU.2(2)						8.3.1.11	
FIA_UAU.2(3)							8.3.1.12
FIA_UAU.6						8.3.1.13	
FIA_UAU.7(1)			8.3.1.14	8.3.1.14			8.3.1.14
FIA_UID.2(1)			8.3.1.15	8.3.1.15			
FIA_UID.2(2)						8.3.1.16	
FIA_UID.2(3)							8.3.1.17
FMT_MOF.1			8.3.1.18				
FMT_MTD.1(1)				8.3.1.19			
FMT_MTD.1(2)						8.3.1.20	

Function Requirement	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT	TSF_NSP	TSF_FCF
FMT_MTD.1(3)							8.3.1.21
FMT_MTD.1(4)				8.3.1.22			
FMT_SMF.1			8.3.1.23		8.3.1.23	8.3.1.23	8.3.1.23
FMT_SMR.1(1)			8.3.1.24	8.3.1.24	8.3.1.24		
FMT_SMR.1(2)						8.3.1.25	
FMT_SMR.1(3)							8.3.1.26
FPT_RVM.1			8.3.1.27	8.3.1.27		8.3.1.27	8.3.1.27
FPT_SEP.1			8.3.1.28	8.3.1.28		8.3.1.28	8.3.1.28

8.3.1.1 FCS_CKM.1

When the TOE is powered on, a 128-bit cryptographic key (common key) is generated using the MSN-D Extension Algorithm of TSF_FKG, and thus FCS_CKM.1 is satisfied.

8.3.1.2 FCS_COP.1

TSF_FDE encrypts the data, including the actual image data and confidential file passwords, that are being written to the MSD and are not encrypted yet. Each time a data segment is needed for processing a job, authenticating each user that saved a confidential file, and processing an operation on a saved confidential file, TSF_FDE reads and decrypts it from the MSD.

The TOE executes no other decryption other than the above.

The above mentioned encryption and decryption follow the Rijndael algorithm standardized by FIPS PUB 197. Thus FCS_COP.1 is satisfied.

8.3.1.3 FDP_RIP.1

TSF_FDC disables the regeneration of actual image data stored in an image data file in the MSD (either HDD or Flash memory) by overwriting the file at least once when the Auto Clear at Job End program runs.

TSF_FDC disables the regeneration of actual image data stored in all image data files in the MSD (both HDD and Flash memory) by overwriting all the files at least once when the Clear All Memory program runs.

TSF_FDC disables the regeneration of actual image data stored in all image data files in the MSD area designated by the Key Operator when the Clear Document Filing Data program or the Power up Auto Clear program runs.

Thus FDP_RIP.1 is satisfied.

8.3.1.4 FIA_AFL.1(1)

Both TSF_FDC and TSF_AUT authenticate the Key Operator. They both support the authentication failure handling as defined by FIA_AFL.1(1). So FIA_AFL.1(1) is satisfied.

8.3.1.5 FIA_AFL.1(2)

TSF_NSP allows the access to the Network Management Pages within the TOE Web only after the Web-Admin is successfully identified and authenticated upon the access through a Web browser. This authentication supports the authentication failure handling as defined by FIA_AFL.1(2). So FIA_AFL.1(2) is satisfied.

8.3.1.6 FIA_AFL.1(3)

When TSF_FCF authenticates each user that saved a confidential file before allowing an operation to the file, TSF_FCF counts the number of failed authentication attempts for each confidential file. TSF_FCF locks a confidential file when authentication failures repeated 3 times in a row on the file. The lock can be released only with *Release the lock on document filing output operation* function of TSF_FMT by only the Key Operator who TSF_AUT has successfully authenticated. Thus FIA_AFL.1(3) is satisfied.

8.3.1.7 FIA_SOS.1(1)

When the Key Operator Code is being changed, TSF_FMT verifies that the number of digits of the Key Operator Code is five. This satisfies FIA_SOS.1(1).

8.3.1.8 FIA_SOS.1(2)

When the Web-Admin password is being changed, TSF_NSP verifies that the number of password characters is 5-digit or more. Both upper and lower case of alphabets, numeric digits, and punctuation marks are accepted for passwords. Thus FIA_SOS.1(2) is satisfied.

8.3.1.9 FIA_SOS.1(3)

When a confidential file is stored, a confidential file password is changed, and a file property is changed from non-confidential to confidential, TSF_FCF verifies that the number of digits of the password is five. This satisfies FIA_SOS.1(3).

8.3.1.10 FIA_UAU.2(1)

FIA_UAU.2(1) is satisfied by TSF_FDC and TSF_AUT as follows:

The following actions (TSFs) need to authenticate the Key Operator before being allowed:

a) Authentication function (TSF_AUT):
   TSF_AUT executes authentication when the user makes an operation to select the Key Operator Programs.

b) Cancel operation of Data Clear function (TSF_FDC):
   TSF_FDC executes authentication when the user makes an operation to cancel a running program that is either *Clear All Memory*, *Clear Document Filing Data* or *Power up Auto Clear*.

All of these types of authentication are implemented by TSF, and allows the action only if the authentication succeeds. As for the Key Operator authentication which the TOE does, the above is all. And all the above are the authentication before allowing the action. Thus FIA_UAU.2(1) is satisfied.

8.3.1.11 FIA_UAU.2(2)

TSF_NSP allows the access to the Network Management Pages within the TOE Web only after the Web-Admin is identified and authenticated successfully when being accessed through a Web browser. Thus FIA_UAU.2(2) is satisfied.

8.3.1.12 FIA_UAU.2(3)

When a user is making an operation on a saved confidential file through the operation panel or the Web, the user is authenticated with the password that only the user who saved the file knows. TSF_FCF authenticates the user in this way before accepting the operation. Unless the authentication succeeds, TSF_FCF does never accept the operation. Thus FIA_UAU.2(3) is satisfied.

8.3.1.13 FIA_UAU.6

The Web-Admin password change I/F is provided after the Web-Admin is identified and authenticated. Here, the Web-Admin password change is allowed through the Web-Admin re-authentication by TSF_NSP. This is the only way to change the Web-Admin password. Thus FIA_UAU.6 is satisfied.

8.3.1.14 FIA_UAU.7(1)

The TOE provides the following authentication I/F:

a) The Key Operator authentication by TSF_AUT

b) The Key Operator authentication for a cancel operation by TSF_FDC

c) Password entry by TSF_FCF for an operation on a saved confidential file

All of the above displays an asterisk “＊” instead of echoing back the character input. Thus FIA_UAU.7(1) is satisfied.

8.3.1.15 FIA_UID.2(1)

FIA_UID.2(1) is satisfied by TSF_FDC and TSF_AUT as follows:

FIA_UAU.2(1) is satisfied by TSF_FDC and TSF_AUT as follows:

The following actions (TSFs) need to authenticate the Key Operator before being allowed:

a) Authentication function (TSF_AUT):
The Key Operator is identified by user's operation to select the Key Operator Programs. TSF_AUT implements the functionality of this operation.

b) Cancel operation of Data Clear function (TSF_FDC):
The Key Operator is identified by user's operation to cancel a running program that is either *Clear All Memory*, *Clear Document Filing Data* or *Power up Auto Clear*. TSF_FDC implements the functionality of this operation.

As for the Key Operator identification which the TOE does, the above is all. And all the above are the authentication before allowing the action. Thus FIA_UID.2(1) is satisfied.

8.3.1.16 FIA_UID.2(2)

TSF_NSP allows the access to the Network Management Pages within the TOE Web only after the Web-Admin is identified and authenticated successfully when being accessed through a Web browser. Thus FIA_UID.2(2) is satisfied.

8.3.1.17 FIA_UID.2(3)

When a user is making an operation on a saved confidential file through the operation panel or the Web, the user is authenticated with the password that only the user who saved the file knows. TSF_FCF authenticates the user in this way before accepting the operation. Unless the authentication succeeds, TSF_FCF does never accept the operation. Thus FIA_UID.2(3) is satisfied.

8.3.1.18 FMT_MOF.1

After the Key Operator is identified and authenticated, TSF_FDC allows cancelling a running program that is either *Clear All Memory*, *Clear Document Filing Data* or *Power up Auto Clear*. Thus FMT_MOF.1 is satisfied.

8.3.1.19 FMT_MTD.1(1)

The functions in the Key Operator Programs only allows modifying and/or querying the number of times Auto Clear at Job End program is repeated, the number of times data clear operations are repeated, the data areas to be cleared by Power up Auto Clear program, and the number of times Power up Auto Clear program is repeated. The names of the functions are respectively "Number of times Auto Clear at Job End program is repeated", "Number of times data clear is repeated", "Power up Auto Clear" and "Number of times Power up Auto Clear program is repeated".

The Key Operator Programs are allowed after TSF_AUT identifies and authenticates the Key Operator. Thus FMT_MTD.1(1) is satisfied.

8.3.1.20 FMT_MTD.1(2)

TSF_NSP provides the Web-Admin password change I/F after TSF_NSP identifies and authenticates the Web-Admin. Then the Web-Admin password change is allowed through the Web-Admin re-authentication by TSF_NSP. This is the only way to change the Web-Admin password. Thus FMT_MTD.1(2) is satisfied.

8.3.1.21 FMT_MTD.1(3)

After TSF_FCF identifies and authenticates each user that saved a confidential file, TSF_FCF allows changing the password and changing the property to delete the password. Thus FMT_MTD.1(3) is satisfied.

8.3.1.22 FMT_MTD.1(4)

The Web-Admin password can be reset to factory default only with *Reset the NIC* operation in the Key Operator Programs. The Key Operator Programs are allowed after TSF_AUT identifies and authenticates the Key Operator. Thus FMT_MTD.1(4) is satisfied.

8.3.1.23 FMT_SMF.1

Table 17 shows that the TSFs implement all the management functions that FMT_SMF.1 specifies. Therefore, FMT_SMF.1 is satisfied.

Table 17: Specification and implementation of management functions

Specified management functions	TSF	Functions implemented as TSF
Modify and query the number of times Auto Clear at Job End program is repeated	TSF_FMT	Number of times Auto Clear at Job End program is repeated
Modify and query the number of times data clear operations are repeated	TSF_FMT	Number of times data clear is repeated
Modify and query the data areas to be cleared by Power up Auto Clear program	TSF_FMT	Power up Auto Clear
Modify and query the number of times Power up Auto Clear program is repeated	TSF_FMT	Number of times Power up Auto Clear program is repeated
Disable Clear All Memory	TSF_FDC	Cancel Clear All Memory
Disable Clear Document Filing Data	TSF_FDC	Cancel Clear Document Filing Data
Disable Power Up All Clear	TSF_FDC	Cancel Power Up All Clear
Release the lock of confidential files	TSF_FMT	Release the lock on document filing output operation
Modify and query the Key operator code	TSF_FMT	Key Operator Code change
Reset the Web-Admin password to factory default	TSF_FMT	Reset the NIC
Modify the Web-Admin password	TSF_NSP	The *Password Setup* page
Change the password for a confidential file	TSF_FCF	Password
Delete the password for a confidential file	TSF_FCF	Property Change

8.3.1.24 FMT_SMR.1(1)

The Key Operator, who is the administrator of the TOE, only knows the Key Operator Code. TSF_AUT and TSF_FDC identify and authenticate the Key Operator, to associate it to its role, and to maintain its role. And TSF_FMT modifies the Key Operator Code, also to do the above. Thus FMT_SMR.1(1) is satisfied.

8.3.1.25 FMT_SMR.1(2)

The Web-Admin only knows the Web-Admin password. TSF_NSP identifies and authenticates the Web-Admin, to associate it to its role, and to maintain its role. And TSF_NSP modifies the Web-Admin password, also to do the above. Thus FMT_SMR.1(2) is satisfied.

The function that initializes the Web-Admin password to factory default (by TSF_NSP) is only allowed to the Key Operator who is identified and authenticated as the TOE security administrator with the Key Operator Code.

Thus FMT_SMR.1(2) is satisfied.

8.3.1.26 FMT_SMR.1(3)

Each user who saved a confidential file only knows the password of the file. TSF_FCF identifies and authenticates the user who saved the file, to associate it to its role, and to maintain its role. And TSF_FCF modifies the password, also to do the above. Thus FMT_SMR.1(3) is satisfied.

8.3.1.27 FPT_RVM.1

The supports by FPT_RVM.1, mentioned in section 8.2.3.1, are implemented by the TSFs as follows:

a) TSF_FDC always invokes the Key Operator authentication, when a user makes an operation to cancel a running program (*Clear All Memory*, *Clear Document Filing Data* or *Power up Auto Clear*), and does never cancel the program unless the authentication succeeds.

b) TSF_AUT always invokes the Key Operator authentication, when a user makes an operation to select the Key Operator Programs (including the Security Administration functions and the Network Settings UI), and does never provides the Key Operator Programs UI.

c) TSF_NSP requires the Web-Admin identification/authentication of any the HTTP requests to the Network Management Pages, and does never allow any access to the Network Management Pages unless the Web-Admin identification/authentication succeeds.

d) TSF_FCF always invokes the confidential file password authentication, when a user requests an operation on a saved confidential file through the operation panel or the Web, and does never accept the request unless the authentication succeeds.

Thus all requirements of the supports by FPT_RVM.1, mentioned in section 8.2.3.1, are satisfied.

8.3.1.28 FPT_SEP.1

The supports by FPT_SEP.1, mentioned in section 8.2.3.3, are implemented by the TSFs as follows:

a) TSF_FDC implements the Key Operator authentication to maintain a security domain, which protects the cancel operation of a running program (*Clear All Memory*, *Clear Document Filing Data* or *Power up Auto Clear*).

b) TSF_AUT implements the Key Operator authentication to maintain a security domain, which protects the Key Operator Programs (including the Security Administration functions and the Network Settings UI).

c) TSF_NSP implements the Web-Admin identification/authentication to maintain a security domain, which protects the Network Management Pages.

d) TSF_FCF implements the confidential file password authentication to maintain a security domain, which protects operations on saved confidential files.

Thus all requirements of the supports by FPT_SEP.1, mentioned in section 8.2.3.3, are satisfied.

8.3.2 Rationale for TOE assurance measures

The effectiveness of the assurance measures in section 6.2 is demonstrated in this section. As shown in Table 11, all of the TOE security assurance requirements correspond to assurance measures by means of the indicated documents, and the documents shown for the assurance measures provide the rationale required by the TOE security assurance requirement EAL3 that is stipulated by this ST.

8.3.3 Rationale for TOE security strength of function

As stated in section 6.3, all TSFs implemented using a probabilistic or permutational mechanisms have security strength of function of SOF-basic. The minimum value of these security strengths of function is SOF-basic.

This is sufficient for the minimum strength of function of the TOE, which is SOF-basic. Thus the TOE security strength of function and the minimum strength of function are consistent.