SHARP

MX-FR15

Security Target

Version 0.04

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

SHARP CORPORATION

Revision history

Date	Ver.	Revision	Author	Reviewed	Approved
2009/8/31	0.01	• Original Draft	Nakagawa	Sakamoto	Yamaguchi
2009/11/12	0.02	• In response to the Observation Report ASE001-01. • Modified descriptions in the TOE overview	Nakagawa	Sakamoto	Yamaguchi
2010/2/10	0.03	• In response to the Observation Report ASE002-01.	Nakagawa	Sakamoto	Yamaguchi
2010/3/10	0.04	• Complemented insufficiency in the content of the TOE description.	Nakagawa	Sakamoto	Yamaguchi

Table of Contents

List of Tables

List of Figures

1 ST Introduction

In accordance with the Common Criteria (CC) identified in Section 2.1, this chapter identifies this Security Target (ST) and the Target of Evaluation (TOE) claiming conformance to this ST. For that, this chapter presents ST reference, TOE reference, TOE overview and TOE description. See Sections 8.1 and 8.2 for terminology used in this ST.

1.1 ST Reference

This section provides information needed to identify this Security Target (ST).

Title: MX-FR15 Security Target

Version: 0.04

Publication Date: March 10, 2010

Author: Sharp Corporation

1.2 TOE Reference

This section provides information needed to identify the Target of Evaluation (TOE) claiming conformance to this ST.

Name: MX-FR15

Version: C.10

Developer: Sharp Corporation

1.3 TOE Overview

1.3.1 TOE Type

The TOE is an IT product to protect data in a Multi Function Device (MFD).

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

MFDs, Multi function Devices, are office machines mainly with copier, printer, scanner and fax functions.

1.3.2 Required non-TOE hardware/software/firmware

The TOE operates on the MFD (hardware) made by Sharp Corporation, namely, MX-M363U, MX-M363UJ, MX-M453U, MX-M453UJ, MX-M503U and MX-M503UJ.

1.3.3 Main Security Functions

The TOE security feature mainly provides the following functions aiming to counter unauthorized attempts to steal image data stored in the TOE-equipped MFD.

a) Cryptographic operation function: encrypts image data handled by the MFD before the MFD writes the data to the non-volatile memory in the MFD.

b) Data clear function: overwrites with random values or a fixed value image data areas in the MSD (the volatile memory or Flash memory) in the MFD.

1.3.4 TOE Usage

The TOE provides MFD functions such as copier, printer, scanner, fax transmission and reception, and PC-Fax in the same way as the standard firmware. This section describes an overview of how to invoke the security functions described in the previous section. Descriptions on MFD functions are discussed later.

a) Users' operation of MFD functions such as copier triggers an automatic operation of the cryptographic operation function and the data clear function of the TOE. The MFD temporality spools the image data to the MSD in the MFD while a job such as copy is in the process. The MFD reads out the image data to process the job and deletes the image data when the job is finished. The TOE encrypts image data to be spooled to the non-volatile memory (Flash memory) by the cryptographic operation function and

decrypts when it reads it out. The TOE overwrites image data to be deleted from the MSD by the data clear function.

b) The administrator operates on the operation panel of the MFD as necessary (including when the MFD is disposed) to execute “Clear All Memory”. Then, the TOE overwrites all image data in the MFD by the data clear function.

1.3.5 Overview of the MFD Functions and Applications

The usage environment of the MFD that the TOE is installed to is shown in Figure 1.

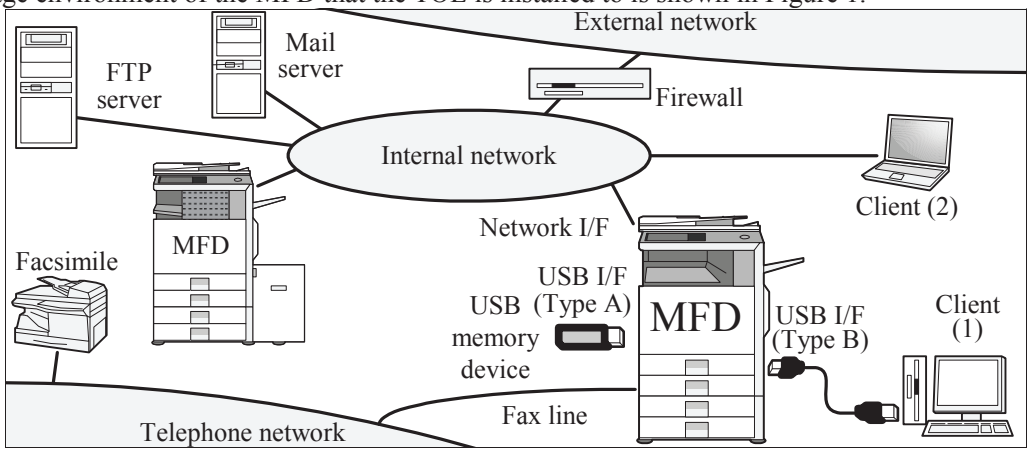

Figure 1: Usage environment of the MFD

Each MFD function of the TOE is explained below. Most functions are available on the operation panel of the MFD. Some functions run when receiving data.

1.3.5.1 Job function

The job function receives the image data from the MFD’s scanner unit or from outside of the MFD, spools the image data to the MSD in the MFD, and sends the image data to the MFD’s engine unit (printing) or to the outside of the MFD (transmission). The job control function and the MFD control function implement the job function.

a) Copier: reads the original and prints that image by the operation from the operation panel. If Tandem Copy mode is selected, it sends the image data to the MFD that the administrator specified beforehand.

b) Printer: prints the data received from the outside of the MFD.

Printer driver: generates the print data at a client and sends to the MFD via network or USB. If Tandem Print mode is selected, the printer driver sends the image data to two MFDs.

Push print: is to send print data from a client to the MFD via E-mail, FTP or Web. Tandem print requests from another MFD are printed in the same manner.

Pull print: acquires the print data in an FTP server or a network folder by operations on the operation panel.

c) Network scanner: scans an original to obtain image data by operations on the operation panel, and transmits the image data file in either of the following ways:

E-mail: transmits it as an attachment to an E-mail.

File server: transmits it to an FTP server.

Desktop: transmits it via FTP to a client running the software tool delivered together with the MFD or provided separately.

Network folder: transmits it into a shared folder of Microsoft Windows over the network.

USB memory: puts it into a USB memory device plugged into the MFD.

d) Fax transmission: scans an original to obtain image data through operations on the operation panel, and transmits the image data as a facsimile.

e) Fax reception: receives a facsimile from another fax machine and prints it.

f) PC-Fax: transmits image data from a client as a facsimile.

1.4 TOE Description

1.4.1 Physical Configuration of the TOE

The physical scope of the TOE is the controller firmware in the MFD as shaded in Figure 2. This is provided in two ROMs as "Data Security Kit MX-FR15 (DSK)", an optional product for MFDs made by Sharp, to strengthen its security functions.

- ROM: contains the controller firmware. When the TOE is installed in the MFD, two ROMs of the standard firmware are removed from the controller board and replaced with two ROMs of the DSK.

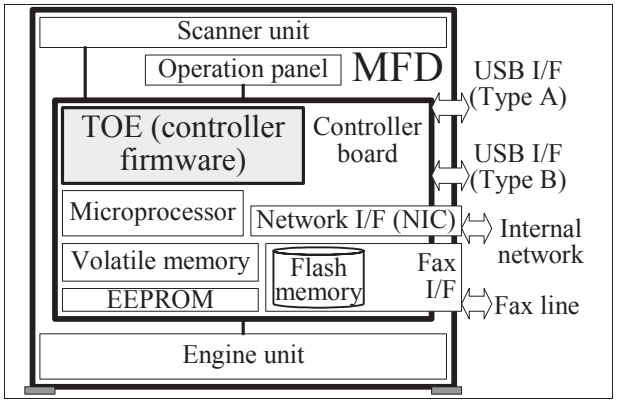

Figure 2: TOE and physical configuration of the MFD

1.4.2 Logical Configuration of the TOE

Figure 3 shows the logical configuration of the TOE. The thick-lined frame indicates the logical scope of the TOE. Rounded boxes indicate hardware devices that are out of the TOE. Rectangles indicate functions of the TOE; and ones shaded indicate security functions. Among the data in the volatile memory, Flash memory and EEPROM, the data that security functions handle (i.e. user data and TSF data) are also shaded. Arrows in the figure indicate data flows. Functions of the TOE usually put data in the volatile memory temporarily to pass the data to each other. However, the figure omits every such detail except security significance.

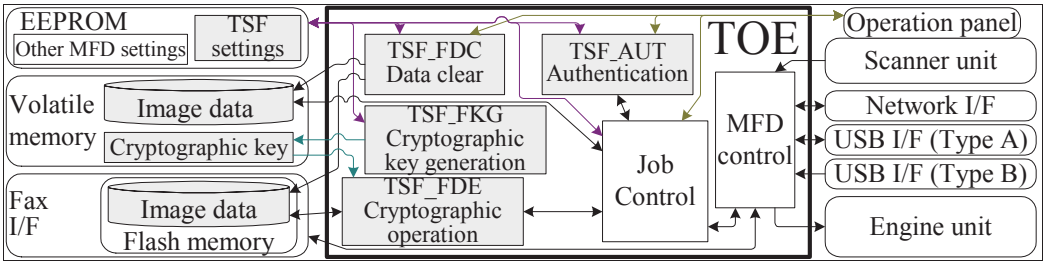

Figure 3: Logical configuration of the TOE

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

a) Cryptographic operation function (TSF_FDE): encrypts image data to be stored in the Flash memory and decrypts image data retrieved from the Flash memory. This function is invoked by the job control function when the MFD processes a job.

b) Cryptographic key generation function (TSF_FKG): generates the cryptographic key for the cryptographic operation function and stores the key in the volatile memory.

c) Data clear function (TSF_FDC): overwrites the MSD to prevent information leakage from the MSD. This function consists of data clear functions (Auto Clear at Job End and Clear All Memory). "Auto Clear at Job End" is activated automatically by being invoked by the job control function. "Clear All Memory" is only invoked by the administrator.

d) Authentication function (TSF_AUT): identifies and authenticates an administrator by means of the administrator password. This function includes a management function that changes the administrator password.

e) Job control function: provides UIs and control actions for each MFD job.

f) MFD control function: controls MFD hardware. This also converts the data format between the data to receive or transmit and the image data in the MFD for the jobs that require the communication.

1.4.3 Guidance Documents

Guidance documents as follows accompany the firmware as part of the TOE. Unique identifiers for the guidance documents and their versions are shown in brackets.

- MX-FR15 Data Security Kit Operation Manual [CINSE4812FC51]
- MX-FR15 Data Security Kit Notice [CINSE4813FC51]

1.4.4 Assets Protected by the TOE

This section describes assets protected by the TOE security function.

1.4.4.1 Overview of Protected Assets

The TOE itself temporarily spools image data to the volatile memory or the Flash memory in the MFD for processing the jobs (mentioned in this chapter) without intent of the user to save when the user uses the MFD functions of the TOE. All image data remaining after a job completion or cancellation is included in the assets protected by the ST. These data possibly contain the users' sensitive information, such as the user's own information and the information of the customers of the user.

MFDs "delete" these image data when the jobs are finished or cancelled to deallocate resources. To "delete" here means just to make the storage area "unused" by marking it "deleted" in the allocation table. This is to "delete" the image data that occupied the storage area, in the same way as data files on the hard disk connected to a general personal computer are deleted; the deleted image data can remain in the cleared area until the area is reused by other jobs.

Thus, this ST includes into the assets the deleted image data remaining in the volatile memory or the Flash memory in the MFD. The TOE is intended to prevent an attacker with the basic attack potential from leaking information of the remaining image data which is the assets protected by the TOE.

Concrete contents are described for each asset as follows:

1.4.4.2 Image Data Remaining in the Flash Memory

In processing PC-Fax, fax transmission and reception jobs, the Flash memory is used to store spooled image data which is transmitted or received by fax. Since image data remains in the non-volatile Flash memory after a fax transmission or reception is finished or cancelled, information will be leaked if an attacker reads it. Regardless of the organisational security policies, such as whether image data is encrypted and whether there are any threats of being read, overwritten of image data shall be mandatory. Thus, this ST includes the remaining data in the assets protected by the TOE.

1.4.4.3 Image Data Remaining in the Volatile Memory

Same as above, in processing copier, printer and scanner jobs, the volatile memory is used to store spooled image data. Even if the image data remains in the volatile memory after each of the jobs is finished or cancelled, an attacker with the basic attack potential cannot read and therefore the data will not be targeted. However, following the above organisational security policies, this ST includes the image data remaining in the volatile memory in the assets protected by the TOE.

1.4.5 Related parties of the TOE

This section describes those related to the TOE and the TOE-equipped MFD.

- Owner: is an organisation which possesses the TOE and the MFD and puts them under management.
- Person in charge of the organisation: belongs to the owner and owes the responsibility for management of MFD.
- Administrator: is assigned operation and management of the TOE and MFD, appointed by the person in charge of the organisation.
- User: uses the MFD functions (Section 1.3.5) of the TOE and MFD.

2 Conformance Claims

This ST satisfies the followings.

2.1 CC Conformance Claim

The versions of the CC to which this ST and the TOE claim conformance are as follows:

- Part 1: Introduction and general model
  September 2006 Version 3.1 Revision 1 Japanese Translation 1.2
- Part 2: Security functional components
  September 2007 Version 3.1 Revision 2 Japanese Translation 2.0
- Part 3: Security assurance components
  September 2007 Version 3.1 Revision 2 Japanese Translation 2.0

The conformance of this ST to CC Part 2 is CC Part 2 conformant.

The conformance of this ST to CC Part 3 is CC Part 3 conformant.

2.2 PP Claim

This ST does not claim conformance to any PP.

2.3 Package Claim

This ST claims conformance to the assurance requirements package of EAL3.

3 Security Problem Definition

This chapter defines security problems of the TOE.

3.1 Threats

Threats to the TOE are described in Table 3-1. This ST supposes attackers who possess the basic attack potential.

Table 3-1: Threats

Identifier	Definition
T.RECOVER	An attacker removes the Flash memory in the MFD and installs it in other devices (other than the MFD where the memory is originally mounted) to read and leak the image data remaining in the Flash memory.

3.2 Organisational Security Policies

Organisational security policies are described in Table 3-2.

Table 3-2: Organisational Security Policies

Identifier	Definition
P.RESIDUAL	Upon completion or interruption of a job, the area in the MSD to which the image data area are spooled shall be overwritten one or more times. When the MFD is disposed of or its ownership changes, all spool areas in the MSD shall be overwritten one or more times.

3.3 Assumptions

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

Table 3-3: Assumptions

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

4 Security Objectives

This chapter describes the measures to implement the security objective policies.

4.1 Security Objectives for the TOE

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

Table 4-1: Security Objectives for the TOE

Identifier	Definition
O.MANAGE	The TOE shall provide the function that identifies and authenticates the authorized administrator.
O.REMOVE	The TOE shall encrypt actual image data using a cryptographic key unique to the MFD before spooling it to the Flash memory in the TOE-equipped MFD so that the image can not be regenerated from the data even if it is read using other devices than the MFD which originally spooled.
O.RESIDUAL	The TOE shall overwrite the area in the MSD to which the user data area spooled one or more times when a job is finished or cancelled. The TOE shall provide the function to overwrite all spool areas in the MSD one or more times by the administrator's operation.

4.2 Security Objectives for the Operational Environment

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

Table 4-2: Security Objectives for the Operational Environment

Identifier	Definition
OE.ERASEALL	When the MFD is disposed of or its ownership changes, the administrator shall overwrite all spool areas in the MSD one or more times by using the TOE's function.
OE.OPERATE	Those in charge of the organisation shall understand the role of the administrator and select a suitable person with the utmost care.

4.3 Security Objectives Rationale

Table 4-3 demonstrates that the policies indicated in the security objectives are effective for the threats, organisational security policies and assumptions indicated in the security problem definitions. Table 4-3 shows the sections of this document that provide the rationale for the correspondences of threats, organisational security policies and the assumptions.

Table 4-3: Security Objectives Rationale

Security problem / Security objective	T.RECOVER	P.RESIDUAL	A.OPERATOR
O.MANAGE		4.3.2	
O.REMOVE	4.3.1		
O.RESIDUAL		4.3.2	
OE.ERASEALL		4.3.2	
OE.OPERATE			4.3.3

Table 4-3 shows that all the threats are countered, that all the organisational security policies are implemented and that all the assumptions are satisfied when the security objectives are achieved. The followings show rationale for each concretely.

4.3.1 T.RECOVER

To counter T.RECOVER, the TOE encrypts image data of jobs using a cryptographic key unique to the MFD as defined in O.REMOVE, before spooling it to the Flash memory. Therefore, the attacker

possessing the basic attack potential cannot make out the data that is stored or remained after deleting in the Flash memory even if the attacker could read it out.

The cryptographic key used to encrypt the image data shall be stored in the memory (volatile memory) in the MFD so that the attacker with the basic attack potential cannot read it. This enables the TOE to prevent information of image data remaining in the Flash memory from leaking.

The possibility that the cryptographic key and the image data in MFD are read is supplemented as follows:

- If the memory in the MFD is removed, power supply to the memory is cut off. When the power is cut off, the data in the volatile memory is lost. The data in the Flash memory is not lost.
- There is no interface to read the data in the memory directly from MFD in operation. High level of technology is required to specify the data area and the data which is during transferring and to read the data from the MFD by attaching probes directly to the terminals or harness of MFD. Therefore, it is impossible for attacker possessing the basic attack potential.

In a word, regarding the possibility that an attacker with the basic attack potential will read the data from the memory in the MFD, this ST considers only the attempts to remove the Flash memory as a threat.

4.3.2 P.RESIDUAL

P.RESIDUAL can be achieved by the following objective below.

- According to O.RESIDUAL, the TOE overwrites the user data area which is spooled in the MSD one or more times upon completion or interruption of a job.
- When the MFD is disposed of or its ownership is changed, the administrator overwrites all user data areas in the MSD one or more times by using the function of the TOE according to OE.ERASEALL. This requires the support of the TOE and the function described in next paragraph is available.
- The TOE provides the function to overwrite all spool areas in the MSD one or more times by the administrator's operation according to O.RESIDUAL.
- According to O.MANAGE, the TOE provides the function to identify and to authenticate the administrator who configures the settings indispensable to the operation, as a support for the previous paragraph.

These objectives above can achieve P.RESIDUAL.

4.3.3 A.OPERATOR

The assumption A.OPERATOR requires that the administrator is a trustworthy person. OE.OPERATE is achieved in strictly choosing the manager, by the person in charge of organization. The person in charge of the organization that owns MFD equipped with TOE shall understand the manager's role, and choose the suitable person.

Therefore, A.OPERATOR can be achieved.

5 Extended Components Definition

This ST does not define any extended components.

6 Security Requirements

This chapter describes the security requirements.

6.1 Requirement Operations

This section defines the operations of CC functional and assurance components.

- Iteration operation: used to cover different aspects of the same requirements.
  - This is not used in this ST.
- Assignment operation: used to assign specified values to undetermined parameters such as the length of a password in the components.
  - A value assigned to a parameter is shown in brackets. Values, even if they are a part of a list of all, are comma-delimited or itemized.
  - Information in parentheses identifying each value such as its parameter name is added to the value as necessary.
- Selection operation: used to select one or more items from those given in the components.
  - Selected items are shown in brackets, with being underlined and in italics.
- Refinement operation: used to further refine the TOE by adding details to the components.
  - Additional text is shown in **bold**.
  - If a part of the original text is deleted, the part is shown in parentheses.
  - If a part of the original text is replaced with new text, the new text in **bold** is shown immediately before the original text in parentheses.
- *Simple Italics* do not indicate requirement operations. They are only used to emphasize text throughout the ST.

6.2 Security Functional Requirements

This section describes the Security Functional Requirements that the TOE shall satisfy, based on the classes of CC Part 2.

6.2.1 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [MSN-R2 expansion algorithm] and specified cryptographic key sizes [128 bits] that meet the following: [Data Security Kit Encryption Standard].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [

- Encrypting the user data that will be written to the Flash memory
- Decrypting the user data that was read from the Flash memory

] in accordance with a specified cryptographic algorithm [Rijndael Algorithm] and cryptographic key sizes [128 bits] that meet the following: [FIPS PUB 197].

6.2.2 Class FDP: User Data Protection

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting one or more times** upon the *[deallocation of the resource from]* the following objects: [image data files spooled to the MSD].

6.2.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *[met]*, the TSF shall [

- Unsuccessful authentication reached three times: Authentication trial receptionist stop for five minutes
- Five minutes pass from stopping: the unsuccessful authentication number of times is cleared, and it is return automatically

].

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that **the administrator password** (secrets) **meets** (meet) [5 to 32 alphanumeric and/or symbol characters, i.e., all the 95 characters of No. 32 through No.126 specified by ISO/IEC 646 coded character set for information interchange].

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [the number of characters that are provided] to the **administrator** (user) while the authentication **of the administrator** is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each **administrator** (user) to be successfully identified before allowing any other TSF-mediated actions on behalf of that **administrator** (user).

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

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

FMT_MOF.1.1 The TSF shall restrict the ability to *[enable, disable]* the functions [Clear All Memory] to [administrator].

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

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

FMT_MTD.1.1 The TSF shall restrict the ability to *[modify]* the [administrator password] to [administrator].

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [
- Enable and Disable: “Clear All Memory”
- Modify: “the administrator password”

].

Note: Consideration for management requirement is described in Section 6.4.1.5.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [administrator].

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

6.3 Security Assurance Requirements

The EAL3 security assurance requirements to which this ST claims conformance are shown by assurance class of CC Part 3. This ST uses the security assurance components defined in CC Part 3 without changes as the security assurance requirements.

Class ADV: Development

ADV_ARC.1	Security architecture description
ADV_FSP.3	Functional specification with complete summary
ADV_TDS.2	Architectural design

Class AGD: Guidance documents

AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures

Class ASE: Security Target evaluation

ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.2	Security objectives
ASE_REQ.2	Derived security requirements
ASE_SPD.1	Security problem definition
ASE_TSS.1	TOE summary specification

Class ALC: Life-cycle support

ALC_CMC.3	Authorisation controls
ALC_CMS.3	Implementation representation CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model

Class ATE: Tests

ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample

Class AVA: Vulnerability assessment

AVA_VAN.2	Vulnerability analysis

6.4 Security Requirements Rationale

This section demonstrates that the security requirements are effective to meet the security objectives.

6.4.1 Security Functional Requirements Rationale

The correspondence between security functional requirements and security objectives is shown in Table 6-1. Table 6-1 shows the section that provides the rationale for the correspondence between the security functional requirements and the security objectives.

Table 6-1: Security Functional Requirements Rationale

Objective / Requirement	O. MANAGE	O. REMOVE	O. RESIDUAL
FCS_CKM.1		6.4.1.2	
FCS_COP.1		6.4.1.2	
FDP_RIP.1			6.4.1.3
FIA_AFL.1	6.4.1.1		
FIA_SOS.1	6.4.1.1		
FIA_UAU.2	6.4.1.1		
FIA_UAU.7	6.4.1.1		
FIA_UID.2	6.4.1.1		
FMT_MOF.1			6.4.1.3
FMT_MTD.1	6.4.1.1		
FMT_SMF.1	6.4.1.1		6.4.1.3
FMT_SMR.1	6.4.1.1		

6.4.1.1 O.MANAGE

O.MANAGE can be met by the combination of the following functional requirements.

a) The administrator is identified by FIA_UID.2 and authenticated by FIA_AFL.1, FIA_UAU.2 and FIA_UAU.7.

b) The TOE provides the capability of performing the modification of the administrator password that is required for operating of authentication of the administrator described above according to FMT_SMF.1.

c) It is ensured that the administrator password meets 5 to 32 alphanumerical and/or symbol characters when the administrator password is modified according to FIA_SOS.1.

d) The ability to modify the administrator password that is the TSF data to implement O.MANAGE is restricted to the administrator by FMT_MTD.1.

e) The roles of administrator are maintained and the administrator is associated with those roles by FMT_SMR.1.

Among above, a) is relevant related to the event of the identification and authentication of the administrator. b), c) and d) are relevant to the event of the modification of the administrator password. These two events occur independently, and do not conflict with each other. The four functional requirements in a) do not conflict, because they interact mutually and supplementary to execute the identification and authentication of the administrator. The three functional requirements in b), c) and d) do not conflict because they interact mutually and supplementary to execute the modification of the administrator password. Since the functional requirement of e) is for the dependency of d) and it is supported by a), these functional requirements do not conflict. Thus, no conflict between functional requirements occurs to meet O.MANAGE as above.

6.4.1.2 O.REMOVE

The intent of O.REMOVE is to counter T.RECOVER; in other words to make the user data stored in the MSD not to be regenerated even if the Flash memory is removed from the MFD and accessed using other devices (other than the MFD which originally spooled to the Flash memory). This can be met by the combination of the following functional requirements.

- FCS_COP.1 encrypts image data to be spooled to the Flash memory. Therefore, even if the Flash memory is connected to MFD other than MFD that executes preservation to the Flash memory and the reproduction of the image data is tried, it is obstructed.
- FCS_CKM.1 generates the cryptographic key to achieve FCS_COP.1.

FCS_COP.1 and FCS_CKM.1 are interdependences. Thus, no conflict between functional requirements occurs to achieve O.REMOVE as above.

6.4.1.3 O.RESIDUAL

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

- FDP_RIP.1 overwrites object areas one or more times upon the deallocation of the resource from the objects. The target object is the spooled image data files in the volatile memory or Flash memory. The

deallocation of the resource from these objects is occurred when the jobs are finished or cancelled and when the Clear All Memory is invoked by the administrator's operation.

- FMT_SMF.1 provides management functions relating to FDP_RIP.1 such as the ability to activate and cancel the Clear All Memory.
- FMT_MOF.1 allows the ability to enable and disable the Clear All memory that is a TSF relating to FDP_RIP.1 only to the administrator.

FMT_SMF.1 and FMT_MOF.1 define the management of FDP_RIP.1 in a mutually complementary manner, and they do not compete against each other. Therefore, no conflict between functional requirements occurs to achieve O.RESIDUAL as above.

6.4.1.4 Rationale for Consistence of the Whole Security Functional Requirements

O.REMOVE and O.RESIDUAL which are part of the TOE security objectives do not compete against each other. They counter attempts to steal image data stored in the MFD independently, mutually and complementary. O.MANAGE supports O.RESIDUAL.

As described in Sections 6.4.1.1 through 6.4.1.3, for each TOE security objective, the security function requirements that realize it do not occur any conflicts and they are consistent.

Thus, no conflict occurs among the whole security functional requirements which realize the TOE security objectives and the entire security functional requirements are consistent.

6.4.1.5 Rationale for Consistence of TOE Security Management Functions

Some of TOE security functional requirements require the security management function. CC Part 2 suggests the management activities foreseen to each functional component as the management requirements of each component.

The management functions required by all TOE security functional requirement components are shown in Table 6-2 with the consideration for management requirement. The management functions specified by FMT_SMF.1 is corresponding to the management functions required shown in the table.

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

Table 6-2: Management Functions of the TOE

Management Function / Origin	Management Function required	Consideration for management requirement
FCS_CKM.1	—	(no management requirements)
FCS_COP.1	—	(no management requirements)
FDP_RIP.1	• Enable or Disable "Clear All Memory"	The timing to perform protection is fixed to the release of allocation.
FIA_AFL.1	—	The threshold and action are fixed.
FIA_SOS.1	—	The quality metric is fixed.
FIA_UAU.2	• Modify "the administrator password"	Management Function required agrees with management requirement.
FIA_UAU.7	—	(no management requirements)
FIA_UID.2	—	Identification of the administrator is fixed.
FMT_MOF.1	—	No role groups
FMT_MTD.1	—	No role groups
FMT_SMF.1	—	(no management requirements)
FMT_SMR.1	—	No user groups

6.4.1.6 Rationale for Security Functional Requirement Dependencies

Table 6-3 shows the dependencies that the security functional requirements must satisfy according to the CC, the dependencies that the TOE satisfies and the dependencies that the TOE does not satisfy. The dependency that is marked with "#" in the table is satisfied with the hierarchically upper component. Table 6-4 shows the justification for the TOE not to satisfy certain dependencies. Correspondences between the following two tables are indicated by common identifiers (such as J1).

Table 6-3: Security Functional Requirement Dependencies

Dependencies / Requirement	Stipulated	Satisfied	Unsatisfied	Justification
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1	FCS_CKM.4	J1
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1	FCS_CKM.4	J1
FDP_RIP.1	—	—	—	—
FIA_AFL.1	FIA_UAU.1 #	FIA_UAU.2	—	—
FIA_SOS.1	—	—	—	—
FIA_UAU.2	FIA_UID.1 #	FIA_UID.2	—	—
FIA_UAU.7	FIA_UAU.1 #	FIA_UAU.2	—	—
FIA_UID.2	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1	FIA_UID.1 #	FIA_UID.2	—	—

Table 6-4: Justification of Unsatisfied SFR Dependencies

	Unsatisfied	Justification Rationale
J1	FCS_CKM.4	The cryptographic key is stored in volatile memory. When the power is off, electrical charge of volatile memory in which the cryptographic key is stored disappears and the cryptographic key is destroyed. Therefore, there is no necessity to implement the TSF that performs the standard key destruction method, and FCS_CKM.4 is not required to specify standards.

6.4.2 Security Assurance Requirements Rationale

The TOE is an optional product for the MFD that is sold separately; in other words commercial product. The major threat is that an attacker with the basic attack potential read out and leak the information in the Flash memory in the MFD by physically removing the Flash memory from the MFD and installing it on other devices. For this reason, the TOE claims conformance to the evaluation assurance level 3 (EAL3) since it is sufficient for commercial products.

Since the assurance requirements conform to EAL3, all assurance requirements meet the dependencies.

7 TOE Summary Specification

By describing a summary specification of the TOE security function (TSF), this chapter shows that the security functional requirements are satisfied. Table 7-1 shows the correspondences between the TOE security functional requirements and the TOE security functions. The section number where each correspondence is described is shown in the table.

Table 7-1: Security Functional Requirements and TOE Security Specifications

Function / Requirement	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT
FCS_CKM.1	7.1			
FCS_COP.1		7.2		
FDP_RIP.1			7.3	
FIA_AFL.1			7.3	7.4
FIA_SOS.1				7.4
FIA_UAU.2			7.3	7.4
FIA_UAU.7			7.3	7.4
FIA_UID.2			7.3	7.4
FMT_MOF.1			7.3	
FMT_MTD.1				7.4
FMT_SMF.1			7.3	7.4
FMT_SMR.1				7.4

7.1 Cryptographic Key Generation (TSF_FKG)

This TOE generates a cryptographic key (common key) to support the cryptographic operation function (TSF_FDE) described in the next section. When the MFD is powered on, a cryptographic key (common key) is always generated.

The TOE generates a 128-bit secure key using the MSN-R2 expansion algorithm and stores the key in the volatile memory to use it for the AES Rijndael, a cryptographic algorithm. The MSN-R2 expansion algorithm is an algorithm to generate cryptographic keys which conforms to the Sharp Corporation Encryption Standards for MFD Data Security Kits. Therefore, the TOE satisfies FCS_CKM.1.

7.2 Cryptographic Operation (TSF_FDE)

During job processing, this TSF always encrypts image data of jobs when it is necessity to write them to the Flash memory. It also reads them from the Flash memory and decrypts when the data is required.

For encryption and decryption of the image data in the Flash memory, the AES Rijndael algorithm based on FIPS PUBS 197 and the 128-bit cryptographic keys generated by the cryptographic key generation function (TSF_FKG) are used.

Therefore, this TOE satisfies FCS_COP.1.

7.3 Data Clear (TSF_FDC)

In the following, first the TSF overview and then each component are described.

7.3.1 Overview of the Data Clear Function

The whole picture of this TSF and its correspondences between the SFR are described.

The TSF clears image data that are spooled. Each of the following functions is included in this TSF:

a) Auto Clear at Job End

b) Clear All Memory

The above-mentioned each function composes this TSF. The functions correspond to the SFR as follows.

- Each function overwrites the volatile memory one or more times with a random value, and the Flash memory once with a fixed value. Each function overwrites deallocated objects (image data files) to disable regeneration of the information stored in the objects (image data). Thus, the TOE satisfies FDP_RIP.1.
- This TSF allows the administrator who is identified and authenticated according to TSF_AUT to invoke the above b) according to FMT_SMF.1 and FMT_MOF.1.
- The above b) has the cancel operation (Section 7.3.3) to stop in accordance with FMT_SMF.1 and satisfy FIA_AFL.1, FIA_UAU.2, FIA_UAU.7 and FIA_UID.2 in cooperation with TSF_AUT which is later discussed. The cancel operation requires the administrator to be identified and authenticated according to FIA_UID.2 and FIA_UAU.2. For authentication, the feedback protection by FIA_UAU.7

and the safeguard by FIA_AFL.1 are provided. This allows only the administrator to stop the data clear function in process as defined in FMT_MOF.1.

The following sections elaborate each function:

7.3.2 Auto Clear at Job End

This function overwrites image data spooled in the volatile memory or the Flash memory in order to process a job, when the job ends. The TOE always invokes this function at the specified timing. No method to disable this function is provided.

7.3.3 Clear All Memory

This function is invoked from the operation panel by the administrator who is identified and authenticated by TSF_AUT and overwrites all spooled image data in the volatile memory or the Flash memory.

This function accepts the cancel operation. Before allowing cancelling this function while running, this TSF always requires the administrator who calls this function to enter the administrator password whenever a cancel operation is taken. The cancel operation serves as identification of the administrator defined in FIA_UID.2 and entering the administrator password serves as authentication of the administrator defined in FIA_UAU.2.

While entering for authentication, the TOE shows as many asterisk "＊" characters as characters entered according to FIA_UAU.7, however does not show the characters entered. The clearing operation is only cancelled if entering for authentication is successful.

If an incorrect administrator password is entered three times in a row while entering for authentication of cancel operation, this program stops accepting further authentication attempts as defined in FIA_AFL.1; that is to lock the administrator password. When five minutes passed from locking, this program unlocks automatically; that is to clear the unsuccessful authentication number of times and return from locking state automatically.

7.4 Authentication (TSF_AUT)

This TSF enforces the identification and authentication of the administrator by the administrator password. According to FMT_SMF.1 and FMT_MTD.1, the TSF allows only the administrator who is identified and authenticated by the TSF to modify the administrator password. According to FIA_SOS.1, the TSF only accepts a password which is 5 to 32 characters consisting of any of the 95 characters of No. 32 through No.126 specified by ISO/IEC 646 coded character set for information interchange. An example is as follows. Note that the shape of each character depends on the environment:

- 52 alphabetic characters: `A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z`
- 10 numerical characters: `0 1 2 3 4 5 6 7 8 9`
- 33 symbolic characters: `! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ¥ ] ^ _ ` { | }` ~ and space.

The functions not for the administrator are available without identification and authentication of the administrator.

In cooperation with TSF_FDC, this TSF satisfies FIA_AFL.1, FIA_UAU.2, FIA_UAU.7 and FIA_UID.2.

This function provides the interfaces of the function for the administrator only when the administrator is identified by the running operation of the management functions according to FIA_UID.2, and when the authentication of the administrator is successful by the correct administrator password according to FIA_UAU.2.

When the administrator password is entered from the operation panel, this TSF, according to FIA_UAU.7, shows as many asterisk "＊" characters as characters entered, however does not show the characters entered.

If an incorrect administrator password is entered three times in a row while entering for authentication of the administrator password, this program stops accepting further authentication attempts according to FIA_AFL.1; that is to lock the administrator password. When five minutes passed from locking, this program unlocks automatically; that is to clear the unsuccessful authentication number of times and return from locking state automatically.

The TSF identifies the administrator by the authentication function and relates him/her to the role. By providing only the administrator with the management function to change (modify) the administrator password, the secure maintenance of the role is achieved. Thus, the TOE satisfies FMT_SMR.1.

8 Appendix

This chapter describes the definitions of terms.

8.1 Terminology

Terminology used in this ST is defined in Table 8-1.

Table 8-1: Terminology

Term	Definition
Administrator password	A password to protect special functions for the administrator including the security management functions which are important in operation and management of the TOE and MFD from being used by those other than the administrator.
Auto Clear at Job End	The function that clears (by overwriting) image data of each job stored in some MSD of the MFD, invoked when a job is finished or cancelled.
Board	A printed circuit board on which components are mounted by soldering.
Clear All Memory	The function to overwrite the all image data that is stored to the MSD in the MFD. This function is invoked by the operation of the administrator.
Controller board	The board that controls the whole MFD. This contains the microprocessor to execute firmware of the TOE, volatile memory and others.
Controller firmware	The firmware that controls the controller board of the MFD. This is contained in the ROM board on the controller board.
Data file	In this document, objects consisting of allocated MSD resources to store information (including image data).
Engine	A device that forms print images on receiver papers, with mechanism of paper feeding/ejection. Also called as “print engine” or “engine unit”.
Firmware	The software that is embedded to the machines to control the machine’s hardware. In this document, firmware especially indicates the controller firmware.
Flash memory	A type of non-volatile memory that allows the entire memory to be erased at once and also allows rewriting to any part of memory.
Image data	Digital data, especially in this document, of two-dimensional image that each function of the MFD manages.
Job	The sequence from beginning to end of the use of an MFD function (copier, printer, scanner send, fax reception, fax transmission, or PC-Fax). In addition, the instruction for a functional operation is sometimes called a job.
Lock	The function to stop accepting passwords if incorrect passwords are entered in a row.
Memory	A memory device; in particular a semiconductor memory device.
MSN-R2 expansion algorithm	A Sharp Corporation’s original cryptographic key generation algorithm defined in the Sharp Corporation Encryption Standards for MFD Data Security Kits.
Non-volatile memory	The memory device that retains its contents even when the power is turned off.
Operation panel	The user interface unit in front of the MFD. This contains the start key, numerical key, function key and liquid crystal display with touch operation system.
Scanner unit	The device that scans the original and gets the image data. This is used for copier, scanner or fax transmission.
Sharp Corporation Encryption Standards for MFD Data Security Kits	A document created by Sharp Corporation defines the standards for the cryptographic operation algorithm used in the Data Security Kits for the MFD and for generation of cryptographic keys to be used for the cryptographic operation.
Spool	Storing the job’s image data to the MSD temporary to increase the input and output efficiency.
Standard firmware	The controller firmware that is installed to the MFD that TOE is not installed to. TOE contains the controller firmware and standard firmware is replaced with the TOE’s controller firmware when TOE is installed.
Tandem copy	Tandem print in the MFD’s copier function.
Tandem print	The function to print a large job twice faster than usually by halving that job among two MFDs.

Term	Definition
Unit	A substance provided standard that can be attached to or detached from a printed circuit board; or an option that is installed and is ready for operation. This can also be a system that includes a mechanism and is ready for operation.
Volatile memory	A memory device, the contents of which vanish when the power is turned off.

8.2 Acronyms

Acronyms used in this ST are indicated in Table 8-2 and Table 8-3.

Table 8-2: Acronyms in the CC

Acronym	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Table 8-3: Other Acronyms

Acronym	Definition
AES	Advanced Encryption Standard, established by NIST (National Institute of Standards and Technology, United States of America)
DSK	Data Security Kit MX-FR15, an optional product sold separately for the MFD, by which the TOE is provided.
EEPROM	Electrically Erasable Programmable ROM, a type of non-volatile memory that allows low frequency of electrical rewriting at any address.
I/F	Interface
IP	An internet protocol dividing data in packets to deliver it to the destination.
IT	Information Technology
MFD	Multi Function Device, a digital multifunctional device which is an office machine mainly equipped with copier, printer, scanner and fax functions. In this document, only models listed in Section 1.3.2.
MSD	Mass Storage Device, in this document, this especially indicates part of the volatile memory and the Flash memory in MFD.
NIC	Network Interface Card, or, Network Interface Controller
OS	Operating System
PC	Personal Computer
ROM	Read Only Memory
UI	User Interface
USB	Universal Serial Bus, a serial bus standard to connect between IT equipments.
SMTP	Simple Mail Transfer Protocol, a communication protocol to transfer E-mails.