Sindoh MF2000, MF3000, MF4000, N610, N410 Series

Security Target Lite V 1.0

Unmistakable

Document history

Version	Date	Description of change	Remarks
V1.0	2017. 04. 03	Publication version	

Table of Contents

List of Tables

1. ST Introduction

This document describes Security Target of Sindoh MF2000, MF3000, MF4000, N610, N410 Series (hereafter "TOE”). This security target describes the basic information on the identification and operational environment of TOE and the security requirements and assurance requirements provided by TOE. The purpose of this security target is to protect the hardcopy device in the commercial information processing environment, which requires mid-level document security, network security and security assurance.

1.1 Security Target References

This security target can be uniquely identified by the following reference information.

Title	Sindoh MF2000, MF3000, MF4000, N610, N410 Series Security Target Lite
Version	V1.0
Date	April 3, 2017
Author	Sindoh SW Development Department

1.2 TOE References

This security target can uniquely identify TOE using the following reference information. TOE identification can be uniquely identified using the TOE name and SW Package.

TOE name	Sindoh MF2000, MF3000, MF4000, N610, N410 Series	
Date	March 27, 2017	
Developer	Sindoh Co., Ltd.	
SW Package	JUNIPER_Pkg_170327_2 (JUNIPER_Pkg_170327_2.zip)	
Components	JUNIPER_CTL	: JUNIPER_170327_2
	JUNIPER_S_EGB	: 02.06.41
	JUNIPER_S_UICC	: 0.0.8
	JUNIPER_S_DFC	: 01.59
	JUNIPER_BANK	: 1.02
	JUNIPER_C_EGB	: 02.06.40
	JUNIPER_C_UICC	: 0.0.8
	JUNIPER_C_DFC	: 01.45
MFP model	MF2083, MF3033, MF4041, MF4091, N610, N611, N612, N613, N410, N411	

1.3 TOE Overview

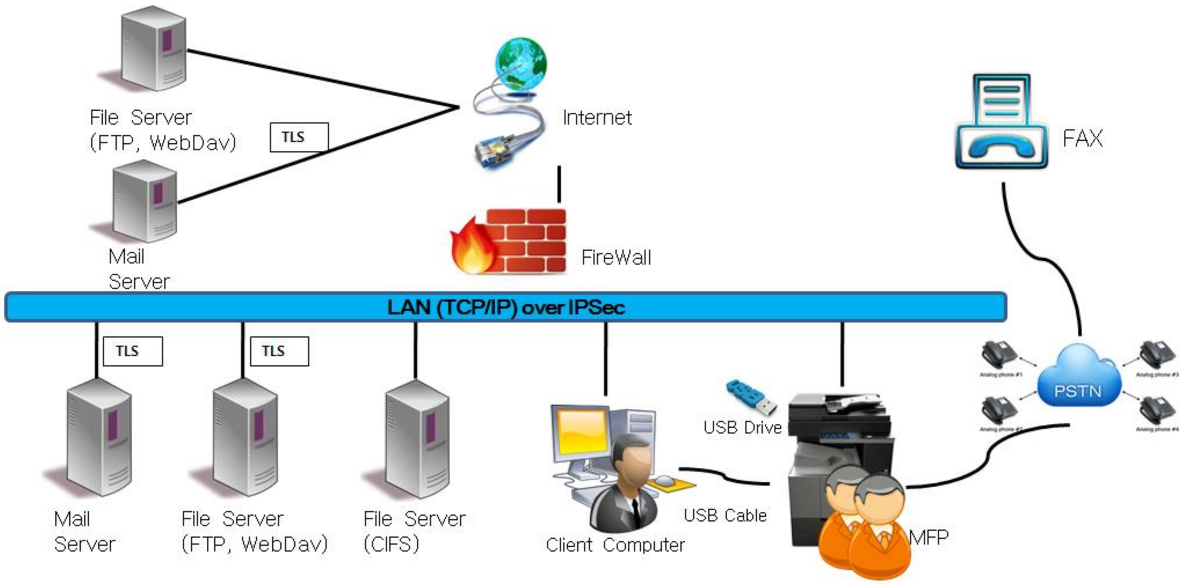
This section defines TOE Type, TOE Usage and Major Security Features of TOE.

1.3.1 TOE Type

TOE is IT products that control the functions of all MFPs (Multi-Function Peripherals[1]) including the copy, print, scan, and fax functions.

1.3.2 Purposes of TOE

The operational environment of the TOE is illustrated below and the usage of TOE is described in this section.



[Figure 1] TOE operational environment

The TOE is used by connecting to the local area network (hereafter "LAN") as shown in [Figure 1]. Users can operate the TOE from the Operation Panel of the TOE or through LAN communications. TOE (MFP) and hardware and software other than TOE will be described below.

[1] MFP: A hardcopy device that fulfills multiple purposes by using multiple functions in different combinations to replace several, single function devices.

The purpose of TOE (MFPs) and the specifications by MFP model are as follows.

- MFPs: The TOE is the MFP. The MFP is connected to LAN, and users can perform the following operations from the Operation Panel of the MFP:
  - Various settings for the MFP
  - Copy: duplicating a hardcopy document
  - Print: producing a hardcopy document from its electronic form
  - Scan: producing an electronic document from its hardcopy form
  - Fax: scanning documents in hardcopy form and transmitting them in electronic form over PSTN(Public Switched Telephone Network) and receiving documents in electronic form over PSTN and printing them in hardcopy form

TOE provides the following 10 MFP models and the detailed specifications of each model are shown in the table below.

[Table 1] General Specifications of MFP

MFP Model		N410	N411	N610	N611	N612	N613	MF2083	MF3033	MF4041	MF4091
		Specification									
Copy speed (unit: ppm)		26	30	26	30	40	45	26	30	40	45
Memory(RAM)		1GB		2GB							
Scanner Type		CIS		CCDM							
Duplex		Standard									
OP Type		5 inch Color TFT LCD		9 inch Color TFT LCD							
CPU		Quad Core (800MHz Dual Core + 533MHz Dual Core)									
FAX module		Standard									
Storage	SD Card	(None) or 32GB		(None) or 64GB				32GB			
	SSD	(None) or 256GB		(None) or 256GB				(None) or 256GB			
	Nand Flash	512MB		512MB				512MB			
PS/PCL Control		Standard (PCL 6, PCL5e, PS3)									

* The options listed in [Table 1] are provided as a standard.

* SD Card and SSD are optional products provided at the user's request, and are used for storing user data.

The external IT entities and software that are not included in TOE but needed for TOE operation are as follows:

- Web browser: Provides communication function between the Client Computer and the MFP.
- Printer driver: The software installed in the computer to use the TOE Print function.

- Scanner driver: The software installed in the computer to use the TOE Scan function.
- Client Computer: A computer that performs as a client of the TOE if it is connected to the LAN, and users can remotely operate the MFP from the client computer. The possible remote operations from the client computer are as follows:
  - Various settings for the MFP using a Web browser installed on the client computer
  - Storage and/or printing of documents using the printer driver installed on the client computer
  - Storage image and/or sending scan command using the scan driver installed on the client computer.
- Firewall: A device to prevent the office environment from network attacks via the Internet.
- File Server (FTP, WebDAV, and CIFS): A server used by the TOE for folder transmission of the stored documents in the TOE to its folders.
- Mail Server: A server used by the TOE for e-mail transmission.

1.3.3 Major Security Features of TOE

The TOE stores documents in it, and sends and receives documents to and from the IT devices connected to the LAN. To ensure provision of confidentiality and integrity for those documents, the TOE has the following security features:

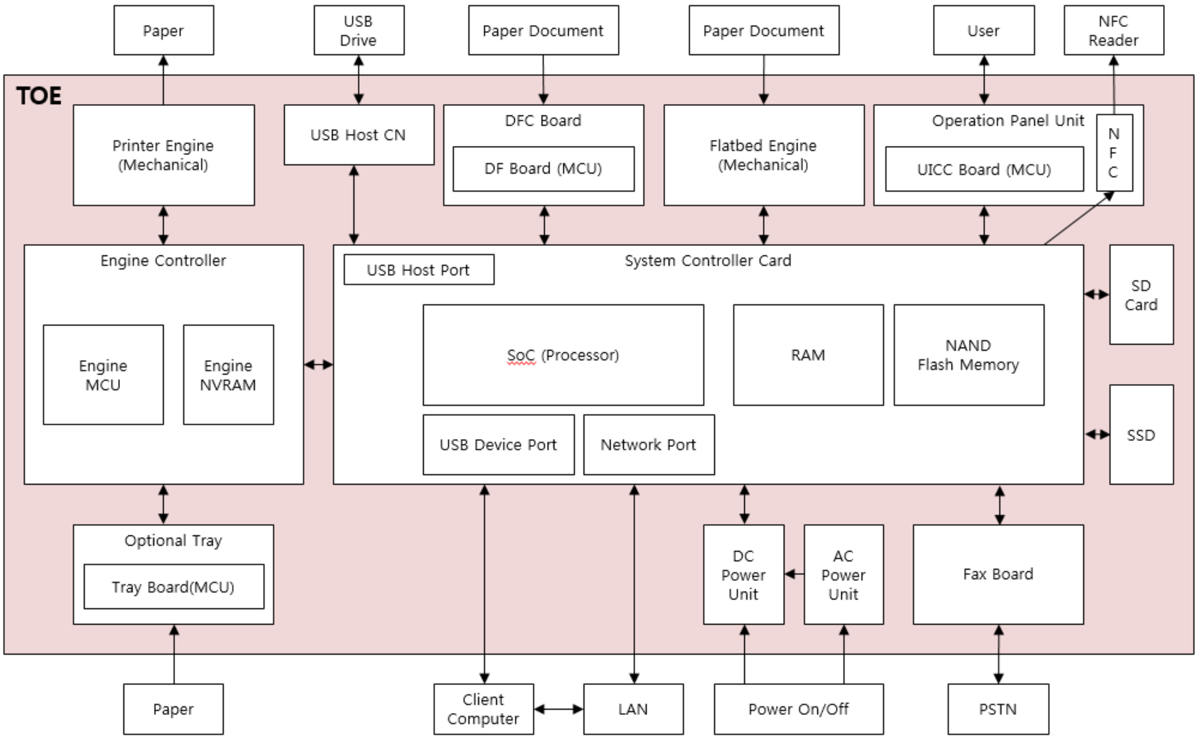
- Identification and Authentication
- Access Control
- Stored Data Protection
- Audit
- Secure Communication
- Security Management
- Self-Testing
- Fax Data Control

1.4 TOE Description

This section describes Physical Boundary of TOE, Guidance Documents, Definition of Users, Logical Boundary of TOE, and Protected Assets.

1.4.1 Physical Boundary of TOE

The physical boundary of the TOE is the MFP, which consists of the following hardware components: DFC Board, Operation Panel Unit, Engine Controller, System Controller Card, Optional Tray, Printer Engine, USB Host CN, Flatbed Engine, SD Card, SSD, DC Power Unit, AC Power Unit, Fax Board



[Figure 2] Hardware configuration of the TOE

- Printer Engine: Prints an electronic document as a hardcopy document
- USB Host CN: The connection device for USB flash drive
- DFC Board: The board for controlling the document feeder
- Flatbed Engine: Flatbed scanner device
- Operation Panel Unit: UI touch pad device provided to user so that he/she can use the TOE
- Engine Controller: Control board for controlling the Printer Engine
- System Controller Card: Control card for controlling the overall functions of the MFP

- SD Card: User data storage device
- SSD (Solid State Disk): User data storage device
- Optional Tray: Additional paper feeder
- DC Power Unit: Power button on the Operation Panel Unit
- AC Power Unit: Power switch connected to the power supply
- Fax Board: Fax modem for sending and receiving facsimile
- Near Field Communication (NFC): The near field communication device to provide the IP information to the NFC terminal

The firmware and software included in the TOE are as follows:

[Table 2] Firmware and software included in the TOE

Classification	N410, N411	N610, N611, N612, N613, MF2083, MF3033, MF4041, MF4091
Controller S/W	JUNIPER_CTL :JUNIPER_170327_2	
Engine Control F/W	JUNIPER_C_EGB :02.06.40	JUNIPER_S_EGB :02.06.41
UICC Control F/W	JUNIPER_C_UICC :0.0.8	JUNIPER_S_UICC :0.0.8
DFC Control F/W	JUNIPER_C_DFC :01.45	JUNIPER_S_DFC :01.59
Tray Control F/W	JUNIPER_BANK :1.02	

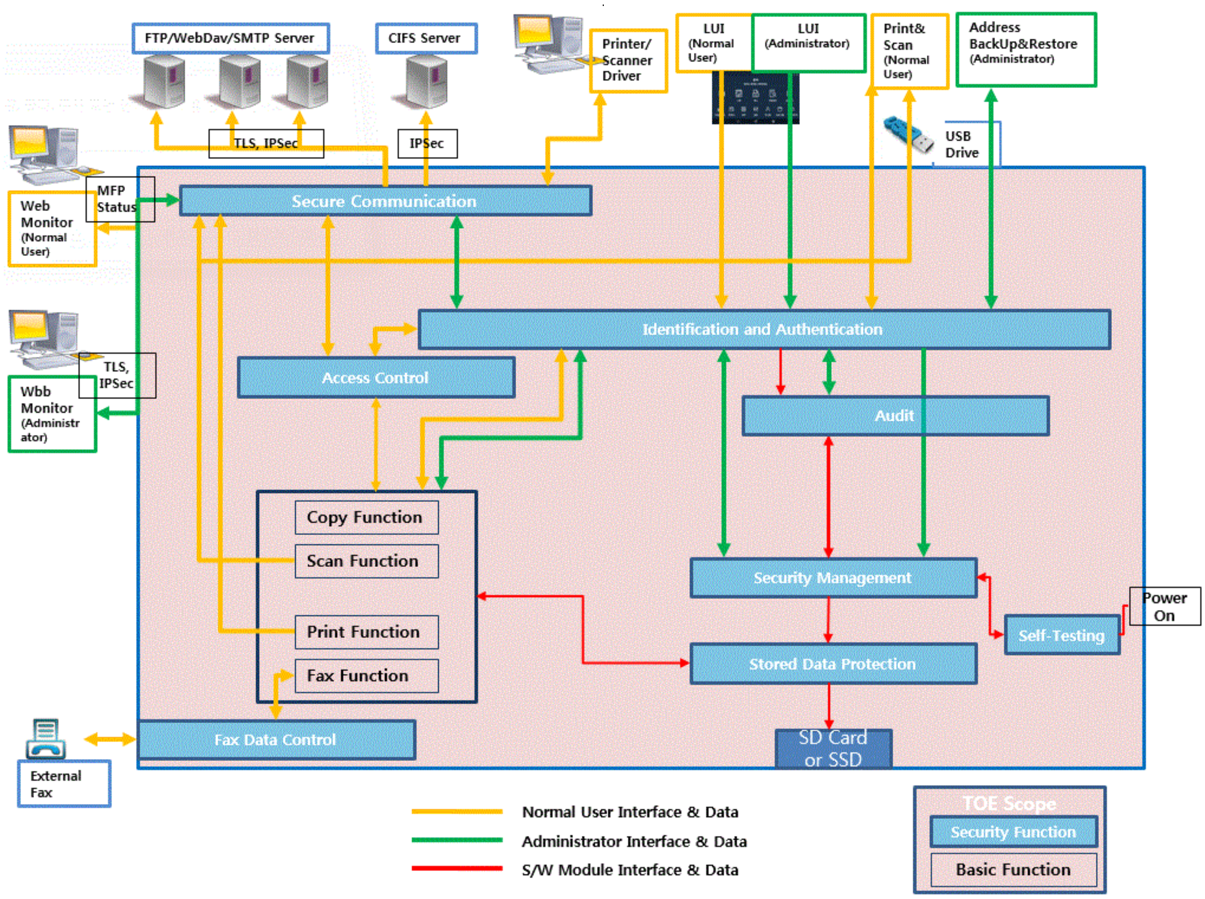
The Guidance Documents for using the TOE are as follows:

- Sindoh MF2000, MF3000, MF4000, N610, N410 Series User Manual V1.8 (N410/MF Series)

  Sindoh MF2000, MF3000, MF4000, N610, N410 Series User Manual V1.8 (N610/MF Series)

1.4.2 Logical Boundary of TOE

The basic functions and security functions are described as follows:



[Figure 3] TOE logical scope

1.4.2.1 Basic Functions

The basic functions are described as follows:

- **Print function**

  producing a hardcopy document from its electronic form

- **Scan function**

  producing an electronic document from its hardcopy form.

- **Copy function**

  duplicating a hardcopy document.

- **Fax function**

  scanning documents in hardcopy form and transmitting them in electronic form over PSTN and receiving documents in electronic form over PSTN and printing them in hardcopy form

1.4.2.2 Security Functions

The security functions are described as follows:

- **Identification and Authentication**

  To be able to access the TOE (using LUI or RUI) and use its functions, users must be identified and authenticated using their ID/password. The identification and authentication data of a user is stored in the database inside the TOE. When a user makes authentication errors for the number of consecutive times pre-defined by the administrator, the authentication will be limited according to the following authentication policies.

  Administrator: Authentication is delayed for a specified amount of time
  Normal user: Authentication is prevented until it is re-allowed by the administrator

  Normal users can be identified and authenticated only through LUI, and the administrator can be identified and authenticated through both LUI and RUI.

- **Access Control**

  The TOE controls users who can access the document data generated by the print, scan, fax and copy function based on the user ID, and denies all accesses except for document owners. According to the basic function access right set by the administrator, the execution rights are controlled based on user ID and user role. All accesses of normal users except the ones explicitly permitted by the administrator are denied. The TOE provides the function to deny all accesses except for the IPs allowed by the administrator.

- **Audit**

  The TOE stores and manages internal history of actions occurring in the TOE, such as the MFP job log, fax log, and audit log. These logs can be viewed and managed only by the administrator through the operation panel. The job log (Print, Scan and Copy) and the fax log can be viewed by the administrator and normal users.

- **Security management**

  The TOE provides Security Management functions for managing TSF data and security attributes (e.g. management of audit records, user management, IP filtering function management, and user data repository management) necessary for safely managing the TOE. Security management functions can be performed only by the administrator through LUI or RUI.

- **Stored Data Protection**

  Temporal save data for printing/fax transmission and permanent archive data are stored in the user data repository (SD Card or SSD) installed in the TOE. To protect the user data stored in the data repository, the function to encrypt the data repository is provided. Also, the function to delete the data stored in the data repository is provided to prevent user data in the data repository from leaking out.

- **Self-Testing**

  To demonstrate correct operation of the TSF, the TOE conducts self-tests at start-up, at a regular intervals, and at the request of authorized users. It also provides the function to verify the integrity of TSF data and TSF to authorized users to assure that the TSF is operating correctly.

- **Fax data control**

  Unless explicitly permitted by the authorized administrative role, the forwarding of inbound fax data through PSTN to external interfaces is limited by the TOE. Except for the fax data, the forwarding of the data received from all external interfaces to all other external interfaces is also limited.

- **Secure Communication**

  The TOE provides an encrypted communication channel for the communication between TOE and external IT entity to protect user data or TSF data transmitted.

[Table 3] Secure Communication Protocol

External IT Entity	Encrypted Communication Protocol
Client Computer	IPSec, TLS
FTP server	IPSec, TLS
WebDAV server	IPSec, TLS
Mail server	IPSec, TLS
CIFS server	IPSec

1.5 Terms and Definitions

- LUI (Local User Interface): The interface for general users and administrators who directly access, use, and manage the MFP by using the operation panel

- RUI (Remote User Interface): The interface for general users and administrators who remotely access, use, and manage the MFP over the web

- Operation Panel: The MFP's panel that provides LUI for interacting with users to perform functions including security management and viewing the audit log

- Print: Print a hardcopy document from a document source in electronic form

- Scan: Produce an electronic document from a document source in hardcopy form

- Copy: Duplicate a hardcopy document

- Fax: Transmit and receive facsimiles of hardcopy documents over PSTN

- User data repository: The SD card or SSD (Solid-state disk) for storing user data

- TLI (Top Level Index): The identifier for classifying finished products

- User: Authorized users including normal users and administrators who have full or limited access permission to MFP functions.

- Normal User: The users who are authorized by the administrator to perform actions on the user document data by using the TOE.

- Administrator: Users with special privilege to manage the whole or parts of TOE and thus influencing the TOE security policy.

- MFP Controller Software: A software component installed in the TOE. This component is stored in NAND Flash Memory.

2. Conformance Claim

This section describes Conformance Claim.

2.1 Conformance to Common Criteria

□ **Common Criteria Identification**

- Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1r4, 2012. 9, CCMB-2012-09-001
- Common Criteria for Information Technology Security Evaluation, Part 2: SFR (Security Functional Requirement), version 3.1r4, 2012. 9, CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation, Part 3: SAR (Security Assurance Requirement), version 3.1r4, 2012. 9, CCMB-2012-09-003

□ **Common Criteria Conformance**

- Common Criteria for Information Technology Security Evaluation, Part 2 extended
- Common Criteria for Information Technology Security Evaluation, Part 3 conformant

2.2 Conformance to Protection Profiles

This security target does not conform to the protection profile.

2.3 Conformance to Packages

This security target conforms to the following assurance package:

□ **Assurance Package: EAL2**

2.4 Conformance Claim Rationale

As this security target does not conform to the protection profile, no conformance claim rationale is provided.

3. Security Problem Definition

This section describes threats, security policies of the organization, and assumptions.

The assets are as follows:

1) User data

   User Data are data created by and for Users and do not affect the operation of the TOE Security Functionality (TSF). This type of data is composed of two objects: User Document Data and User Function Data.

   User Document Data (D.DOC) consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually-stored data created by the hardcopy device while processing an original document and printed hardcopy output.

   User Function Data (D.FUNC) are the information about a user's document or job to be processed by the TOE.

2) TSF data

   TSF Data are data (D.PROT) created by and for the TOE and that might affect the operation of the TOE. This type of data is composed of two objects: TSF Protected Data and TSF Confidential Data.

   TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.

   TSF Confidential Data (D.CONF) are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

3) TOE functions

   Functions perform processing, storage, and transmission of data that may be present in TOE.

3.1 Threats

This security problem definition addresses threats posed by four categories of threats:

- Persons who are not permitted to use the TOE who may attempt to use the TOE.

- Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.

- Persons who are authorized to use the TOE who may attempt to access data in ways for which they are not authorized.

- Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats

[Table 4] Threats to TOE

Threat	Affected asset	Description
T.DOC.DIS	D.DOC	User document data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User document data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User function data may be altered unauthorized persons
T.PROT.ALT	D.PROT	TSF protection data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF confidential data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF confidential data may be altered by unauthorized persons

3.2 Organizational Security Policies

[Table 5] Organizational Security Policies

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

3.3 Assumptions

[Table 6] Assumptions for the TOE

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer’s guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4. Security Objectives

This section describes Security Objectives for TOE, Security Objectives of Operational Environment and Security Objectives Rationale.

4.1 Security Objectives for the TOE

[Table 7] Security Objectives for the TOE

Objectives	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events and prevent its unauthorized disclosure or alteration.

4.2 Security Objectives for Operational Environment

[Table 8] Security Objectives for operational environment

Objectives	Definition
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons.
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization; have the training, competence, and time to follow the manufacturer’s guidance and documentation; and correctly configure and operate the TOE in accordance with those policies and procedures.

OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.

4.3 Security Objective Rationale

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those Security Objectives counter the threats, enforce the policies, and uphold the assumptions.

[Table 9] Completeness of Security Objectives

Definition of security problems Security Objectives	T.DOC.DIS	T.DOC.ALT	T.FUNC.ALT	T.PROT.ALT	T.CONF.DIS	T.CONF.ALT	P.USER.AUTHORIZATION	P.SOFTWARE.VERIFICATION	P.AUDIT.LOGGING	P.INTERFACE.MANAGEMENT	A.ACCESS.MANAGED	A.USER.TRAINING	A.ADMIN.TRAINING	A.ADMIN.TRUST
O.DOC.NO_DIS	O													
O.DOC.NO_ALT		O												
O.FUNC.NO_ALT			O											
O.PROT.NO_ALT				O										
O.CONF.NO_DIS					O									
O.CONF.NO_ALT						O								
O.USER.AUTHORIZED	O	O	O	O	O	O	O							
O.INTERFACE.MANAGED										O				
O.SOFTWARE.VERIFIED								O						
O.AUDIT.LOGGED									O					
OE.AUDIT_STORAGE.PROTECTED									O					
OE.AUDIT_ACCESS.AUTHORIZED									O					
OE.INTERFACE.MANAGED										O				
OE.PHYSICAL.MANAGED											O			
OE.USER.TRAINED												O		
OE.ADMIN.TRAINED													O	
OE.ADMIN.TRUSTED														O
OE.AUDIT.REVIEWED									O					
OE.USER.AUTHORIZED	O	O	O	O	O	O	O							

[Table 10] Sufficiency of Security Objectives

Threats, policies, and assumptions	Summary	Objectives and rationale
T.DOC.DIS	User document data may be disclosed to unauthorized persons.	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure.
		O.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC.ALT	User document data may be altered by unauthorized persons.	O.DOC.NO_ALT protects D.DOC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.

T.FUNC.ALT	User Function data may be altered by unauthorized persons.	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	TSF protection data may be altered by unauthorized persons.	O.PROT.NO_ALT protects D.PROT from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.DIS	TSF confidential data may be disclosed to unauthorized persons.	O.CONF.NO_DIS prevents D.CONF from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.ALT	TSF confidential data may be altered by unauthorized persons.	O.CONF.NO_ALT protects D.CONF from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
P.USER.AUTHORIZATION	Users will be authorized to use the TOE.	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF.	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF.
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events and prevents unauthorized disclosure or alteration.
		OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion, and modifications.
		OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records.
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed.
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies.
		OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces.
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE.

A.USER.TRAINING	Administrators are aware of and trained to follow security policies and procedures.	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.
A.ADMIN.TRAINING	TOE Users are aware of and trained to follow security policies and procedures.	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.

5. Extended Components Definition

FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behavior

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:

FPT_FDI_EXP Restricted forwarding of data to external interfaces

1

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

The following actions could be considered for the management functions in FMT:

a) Definition of the role(s) that are allowed to perform the management activities

b) Management of the conditions under which direct forwarding can be allowed by an administrative role

c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

There are no auditable events foreseen.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components

Dependencies: FMT SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: list of external interfaces] from being forwarded without further processing by the TSF to [assignment: list of external interfaces].

Rationale

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. That is, direct forwarding of such data between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this ST, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It is considered inappropriate to use FDP_IFF and FDP_IFC by applying refinement for this purpose. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or the FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this led the authors to define a new family with just one member.

6. Security Requirements

This section describes Security Functional Requirements, Security Assurance Requirements and Security Requirements Rationale. The operations (creation rule) applied to security function requirements are as follows:

- **Iteration**

Iterated functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, for example, FIA_AFL.1 (1) and FIA_AFL.1 (2).

- **Assignment**

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

- **Selection**

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*

- **Refinement**

The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinement of security requirements is denoted by **bold text.**

This ST defines all subjects, objects, operations, security attributes, and external entities used in security requirements, as follows:

Subject (User)

Users are entities that are external to the TOE and which interact with the TOE. There may be two types of Users: Normal and Administrator.

[Table 11] Definitions of subjects

Designation		Definition
U.USER		Any authorized User.
	U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE
	U.ADMINISTRATOR	A User who has been specifically granted the authority to manage all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Objects

Objects are passive entities in the TOE, that contain or receive information, and upon which Subjects perform Operations. In this Protection Profile, Objects are equivalent to TOE Assets. There are three types of Objects: User Data, TSF Data, and Functions.

User data

User Data are data created by and for Users and do not affect the operation of the TOE Security Functionality (TSF). This type of data is composed of two objects: User Document Data and User Function Data.

[Table 12] User data

Designation	Definition
D.DOC	User Document Data consist of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

TSF data

TSF Data are data created by and for the TOE and that might affect the operation of the TOE. This type of data is composed of two objects: TSF Protected Data and TSF Confidential Data.

[Table 13] TSF data

Designation	Definition
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

The TSF data used in the TOE is as follows:

[Table 14] TSF data

TSF data list	TSF confidential data	TSF protection data
Address book		O
Job log, fax log		O
Audit log	O	
User ID	O	
User password	O	
User roles (basic function)	O	
Security fax setting	O	
Network setting	O	
Security warning mail setting	O	
Mail server setting	O	
SD Card setting (LUI)	O	
SSD setting (LUI)	O	
Service port	O	
IPSec setting	O	
SNMP setting	O	
Login limit time	O	
Number of login attempts	O	
IP filtering setting	O	
Administrator connection IP setting	O	
Output authentication setting	O	
Fax data control setting	O	
MFP time setting	O	

TOE functions

TOE functions process, store, and send the data in the TOE.

[Table 15] Basic Functions provided by the TOE

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output

Attributes

It refers to an identification of the functions related to certain data (e.g. security attributes) when data is processed, stored, and sent. With the attributes of the TOE, it is possible to discriminate the functions that are being executed from the related SFRs.

[Table 16] Attributes

Designation	Description
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.

Operations

Operations are specific types of actions performed by a subject on an Object. This security target includes 6 types of operations (read, modify, delete, register, backup/restoring the data, and execute).

External entities

[Table 17] Definitions of external entities

External entities	Description
File server (FTP, WebDAV, CIFS)	A server used by the TOE for folder transmission of the stored documents in the TOE to its folders
Mail server	A server used by the TOE for e-mail transmission.

6.1 Security Functional Requirements

The security function requirements defined in this security target are the related security function components selected from Common Criteria Part 2 to meet the Security Objectives identified in Chapter 4.

6.1.1 Security Audit Class

FAU_ARP.1 Security alarms

Hierarchical to: No other components

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [send a warning mail to the administrator (U.ADMINISTRATOR)] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events.
a) Start-up and shut-down of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [See the auditable events in [Table 18]]

[Table 18] Auditable events

SFR-related Auditable Events	History of Auditable Events	Related SFR
Audit log repository fill-up	Details of audit log repository fill-up	FAU_STG.4
Administrator/user authentication failure	History of responses to authentication failures	FIA_AFL.1
Administrator/user authorization	Authentication success/failure history	FIA_UAU.1
Data access control setting change	History of data access control setting change	FMT_MSA.1(1)
Basic function access control setting change	History of basic function access control setting change	FMT_MSA.1(2)
Network information flow control setting change	History of network information flow control setting change	FMT_MSA.1(3)
Data access control setting change	History of data access control setting change	FMT_MSA.3(1)
Basic function access control setting change	History of basic function access control setting change	FMT_MSA.3(2)
Network information flow control setting change	History of network information flow control setting change	FMT_MSA.3(3)
Security management result	History of administrator's security management	FMT_MTD.1
Self-test result	Self-test result(success/failure)	FPT_TST.1
Session end result	Session end details	FTA_SSL.3

Auditable event related to basic functions	**History of auditable event**	**Remark**
Copy	Copy record	Auditable events of basic functions that are not related to SFR
Scan	Scan record	
Fax	Fax send/receive record	
Print	Print record	

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [None].

FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [continuous failures of user authorization (the failure count follows the administrator’s setting)] known to indicate a potential security violation;

b) [in case of the audit records repository fill-up, and a self-test result error]

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [U.ADMINISTRATOR] with the capability to read [all audit records] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [Select] of audit data based on [User ID].

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *protect* unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [send a warning email to the administrator] if the audit trail is full.

6.1.2 Cryptographic Support Class

FCS_CKM.1(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 the cryptographic key generation algorithm [Sindoh user data repository cryptographic key generation algorithm] and specified cryptographic key sizes [256-bits] that meet the following [None].

Application Note: This component describes that generate of cryptographic keys used to encrypt the user data repository.

FCS_CKM.1(2) 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 [Password Based Key Derivation Function (PBKDF1)] and specified cryptographic key sizes [256-bits] that meet the following [RFC2898].

Application Note: This component describes that generate of cryptographic keys used for the address book backup/restore function.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes or

FDP_ITC.2 Import of user data including security attributes or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [initialized to 0(zero)] that meets the following: [None].

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 including security attributes or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform the [Cryptographic operations in Table 19] in accordance with a specified cryptographic algorithm [Algorithm in Table 19] and the cryptographic key sizes [Cryptographic key sizes in [Table 19] that meet the following: [None].

[Table 19] Cryptographic operation

Cryptographic operation	Algorithm	Cryptographic key size
User data repository encryption User data repository decryption	AES-CBC	256
Address book backup data encryption Address book backup data decryption	AES-CBC	256

6.1.3 User Data Protection Class

FDP_ACC.1(1) Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF must enforce the [data access control SFP] on [Table 20].

FDP_ACC.1(2) Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [basic function access control SFP] on [Table 21].

FDP_ACF.1(1) Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [data access control SFP] to objects based on the following: [subjects, objects and the security attributes and operations of subjects and objects in Table 20].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the following list: Table 20].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [None].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [None].

[Table 20] Data access control SFP

SFP name	Object	Attribute(s)	Operation	Subject	Security attributes	Access control rule
Data access control SFP	D.DOC	+PRT	Delete	U.NORMAL	User ID	Denied, except for his/her own documents
	D.DOC	+PRT	Read	U.NORMAL	User ID	Denied, except for his/her own documents
	D.DOC	+SCN	Delete	U.NORMAL	User ID	Denied, except for his/her own documents
	D.DOC	+SCN	Read	U.NORMAL	User ID	Denied, except for his/her own documents
	D.DOC	+FAXIN +FAXOUT	Delete	U.NORMAL	User ID	Denied, except for his/her own documents
	D.DOC	+FAXIN +FAXOUT	Read	U.NORMAL	User ID	Denied, except for his/her own documents
	D.DOC	+CPY	Read	No restriction on access		
	D.FUNC	+PRT +SCN +FAXIN +FAXOUT	Delete	U.NORMAL	User ID	Denied, except for his/her own function data

Application Note: If fax documents are received, the fax job owner is regarded as the administrator.

Application Note: The operation "Read" is described as follows according to the attributes of objects.

Operation(s)	Attributes	Description
Read	+PRT	Forward the hardcopy target to the hardcopy output handler
	+SCN	User document data is delivered through the interface selected by the user.
	+CPY	Forward the hardcopy target to the hardcopy output handler
	+FAXIN +FAXOUT	Uses the hardcopy output handler to deliver the hardcopy target in order to receive fax (+FAXIN), and uses the fax interface to send and receive user document data (+FAXOUT or +FAXIN)

FDP_ACF.1(2) Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF must enforce the [basic function access control SFP] based on [Table 21].

FDP_ACF.1.2 The TSF must enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Table 211]

FDP_ACF.1.3 The TSF must explicitly authorize access of subjects to objects based on the following additional rules: [None]

FDP_ACF.1.4 The TSF must explicitly deny access of subjects to objects based on the following additional rules: [None]

[Table 21] Basic function access control SFP

SFP name	Object	Attribute	Operation(s)	Subject	Security	Control policy

					attribute	
Basic function access control SFP	F.PRT	Permission	Execute	U.NORMAL	User ID, user role	Denied, except for the U.NORMAL explicitly authorized by U.ADMINISTRATOR to use a function
	F.SCN					
	F.CPY					
	F.FAX					

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [network information flow control security policy] on [subject (external IT entities), information (network packet)] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [network information flow control security policy] based on the following types of subject and information security attributes: [list of subjects and information controlled by the following SFP, and the security attributes of subjects and information.

Subject: External IT

Information: Network Packet

Attributes of Subject: IP

Attributes of Information: IP]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [If the subject’s IP is the IP registered as Allowed in the IP filtering policy set up by U.ADMINISTRATOR].

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [None].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [None].

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 upon the *recovering resources from* the following objects: [SD card and SSD].

Application Note: User data stored in the SD card and SSD is encrypted print data and fax data.

6.1.4 Identification and Authentication Class

FIA_AFL.1(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 *ranging between [3 and 10], which is configurable by the administrator* unsuccessful authentication attempts occur related to [administrator authentication failures].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met,* the TSF shall [delay authentication by 5~30 minutes].

Application Note: The default number of authentication failures is 5 times during initial installation.

FIA_AFL.1(2) Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *ranging between [3 and 10], which is configurable by the administrator* unsuccessful authentication attempts occur related to [general user authentication failures].

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

Application Note: The default number of authentication failures is 5 times during initial installation, and authentication of general users must be prevented until the administrator changes authentication of the users.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User ID and users' job authority].

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [receiving fax data and using menus unrelated to security (product information, address book, job status, and product status information)] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that 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 [*] to user while authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [using menus unrelated to security (product information, address book, job status and product status information)] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

Hierarchical to: No other components

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [User ID and user role]

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [Allocating the security attributes of U.USER to subjects acting on behalf of the user].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [The security attributes of the connected session are not changed].

6.1.5 Security Management Class

FMT_MSA.1(1) Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specifications of management functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [data access control SFP] to restrict the ability to *query, modify, delete, [add]* the [Table 20] to [U.ADMINISTRATOR].

FMT_MSA.1(2) Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specifications of management functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [basic function access control SFP] to restrict the ability to *query, modify* the security attributes on the [Table 20] to [U.ADMINISTRATOR].

FMT_MSA.1(3) Management of security attributes

Hierarchical to: None

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specifications of management functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [network information flow control security policy] to restrict the ability to *query, modify, delete, [add]* the security attributes of the [IP address] to [U.ADMINISTRATOR].

FMT_MSA.3(1) Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [data access control SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(2) Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [basic function access control SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(3) Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [network information flow control security policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

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 *query, modify, delete, [add, backup/restore]* the [the following list: Table 22] to [U.ADMINISTRATOR].

[Table 22] Managing of TSF data

TSF data list	Query	Modify	Delete	Add	Backup/ restore	User roles
Address book	O	O	O	O	O	U.USER (* U.NORMAL can modify, delete and register his/her own address book.)
job log, fax log	O	-	-	-	-	U.USER
Audit log	O	-	-	-	-	U.ADMINISTRATOR
User ID	O	O	-	-	-	
User password	-	O	-	-	-	
User roles(basic function)	O	O	-	-	-	
Security fax setting	O	O	-	-	-	
network setting	O	O	-	-	-	
Security warning mail setting	O	O	O	O	-	
Mail server setting	O	O	O	O	-	
SD Card setting(LUI)	O	O	-	-	-	
SSD setting(LUI)	O	O	-	-	-	
Service port	O	O	-	-	-	
IPSec setting	O	O	O	O	-	
SNMP setting	O	O	-	-	-	
Login limit time	O	O	-	-	-	
Login attempts	O	O	-	-	-	
IP filtering setting	O	O	O	O	-	
Administrator connection IP setting	O	O	O	O	-	
Output authentication setting	O	O	-	-	-	
Fax data control setting	O	O	-	-	-	
MFP time setting	O	O	-	-	-	

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: [the following list: Table 23].

[Table 23] Management functions

Management functions	Related SFR
Viewing audit log	FAU_SAR.1 FAU_SAR.2 FAU_SAR.3

Management of security attributes	FMT_MSA.1(1)
	FMT_MSA.1(2)
	FMT_MSA.1(3)
	FMT_MSA.3(1)
	FMT_MSA.3(2)
	FMT_MSA.3(3)

Managing TSF data	FMT_MTD.1

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 [U.ADMINISTRATOR, U.NORMAL].

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

6.1.6 TSF Protection Class

FPT_FDI_EXP.1Restricted forwarding of data to external interfaces

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [any external interface] from being forwarded without further processing by the TSF to [any Shared-medium interface].

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF testing

Hierarchical to: No other components

Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial startup, periodically during normal operations and at the request of authorized users* to demonstrate the correct operation of [MFP Controller Software].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *[Encryption Key Data]*.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *[Stored TSF executable code].*

6.1.7 TOE Access Class

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after [between 60 seconds, specified by the administrator, and 600 seconds. The default value is 60 seconds].

6.1.8 Trusted Path/Channel Class

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF and another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [communication with trusted IT products].

6.2 Assurance Requirements

The assurance requirements of this security target consist of the assurance components of Common Criteria Part 3 (CCMB-2012-09-003), and the evaluation assurance level is EAL2.

6.2.1 Security Target Class

ASE_INT.1 ST introduction

Dependencies: No dependencies

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview, and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview must identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical boundary of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview and the TOE description are consistent with each other.

ASE_CCL.1 Conformance Claims

Dependencies: ASE_INT.1 Introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The Conformance Claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended..

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 Conformant or CC Part 3 Extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

ASE_CCL.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies: No dependencies

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

ASE_SPD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.2 Security Objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

ASE_ECD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator *shall confirm* that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFR and the SAR.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE Summary Specifications

Dependencies: ASE_INT.1 introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specifications

Developer action elements:

ASE_TSS.1.1D The developer shall provide TOE Summary Specifications.

Content and presentation elements:

ASE_TSS.1.1C The TOE Summary Specifications shall describe how the TOE meets each SFR.

Evaluator action elements:

ASE_TSS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.2 Development Class

ADV_ARC.1 Security Architecture Description

Dependencies: ADV_FSP.1 Basic functional specifications

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 Security-enforcing functional specifications

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

Evaluator action elements:

ADV_TDS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator must determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3 Guidance Document Class

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specifications

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparation procedures

Dependencies: No dependencies

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operations.

6.2.4 Lifecycle Support Class

ALC_CMC.2 Use of the configuration management system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ALC_CMC.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Distribution procedure

Dependencies: No dependencies

Developer action elements:

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

6.2.5 Test Class

ATE_COV.1 Evidence of test coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specifications
ATE_FUN.1 Functional testing

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios must include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs of a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specifications

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of test coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer must provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample test for the test items in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability Assessment Class

AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specifications

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator *shall perform* an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

[Table 24] Completeness of security requirements

Security objective Security functional requirements	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED
FAU_ARP.1										O
FAU_GEN.1										O
FAU_GEN.2										O
FAU_SAA.1										O
FAU_SAR.1										O
FAU_SAR.2										O
FAU_SAR.3										O
FAU_STG.1										O
FAU_STG.4										O
FCS_CKM.1(1)	O	O	O							
FCS_CKM.1(2)				O	O	O				
FCS_CKM.4	O	O	O							
FCS_COP.1	O	O	O							
FDP_ACC.1(1)	O	O	O							
FDP_ACC.1(2)							O			
FDP_ACF.1(1)	O	O	O							
FDP_ACF.1(2)							O			
FDP_IFC.2								O		
FDP_IFF.1								O		
FDP_RIP.1	O									
FIA_AFL.1(1)							O			
FIA_AFL.1(2)							O			
FIA_ATD.1							O			
FIA_UAU.1							O	O		
FIA_UAU.7							O			
FIA_UID.1	O	O	O	O	O	O	O	O		O
FIA_USB.1							O			
FMT_MSA.1(1)	O	O	O							
FMT_MSA.1(2)							O			
FMT_MSA.1(3)								O		
FMT_MSA.3(1)	O	O	O							
FMT_MSA.3(2)							O			
FMT_MSA.3(3)								O		
FMT_MTD.1				O	O	O				
FMT_SMF.1	O	O	O	O	O	O				
FMT_SMR.1	O	O	O	O	O	O	O			
FPT_FDI_EXP.1								O		
FPT_STM.1										O
FPT_TST.1									O	
FTA_SSL.3								O		
FTP_ITC.1	O	O	O	O	O	O				

[Table 25] Security Functional Requirements Rationale

Security Objectives	SFR	Rationale
O.DOC.NO_DIS	FCS_CKM.1(1)	Supports cryptographic operations when it is requested that the key for encrypting the user data repository should be generated
	FCS_CKM.4	Supports cryptographic operations when it is required that the key for the user data repository encryption should be destroyed
	FCS_COP.1	Enforces protection when cryptographic operations for the user data repository encryption is required
	FDP_ACC.1(1)	Enforces protection for establishing the access control policy
	FDP_ACF.1(1)	Supports the access control policy by providing the access control function
	FDP_RIP.1	Enforces protection by making residual data unavailable
	FIA_UID.1	Supports the access control and security role when user identification is required
	FMT_MSA.1(1)	Supports the access control function by controlling security attributes
	FMT_MSA.3(1)	Supports the access control function by controlling the default values of security attributes
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting the use of trusted channels for data communication through the SMI
O.DOC.NO_ALT	FCS_CKM.1(1)	Supports cryptographic operations when it is required that the key for the user data repository encryption should be generated
	FCS_CKM.4	Supports cryptographic operations when it is required that the key for the user data repository encryption should be destroyed
	FCS_COP.1	Enforces protection when cryptographic operations are required for the user data repository encryption
	FDP_ACC.1(1)	Enforces protection by establishing the access control policy
	FDP_ACF.1(1)	Supports the access control policy by providing the access control function
	FIA_UID.1	Supports the access control and security roles when user identification is required
	FMT_MSA.1(1)	Supports the access control function by controlling security attributes
	FMT_MSA.3(1)	Supports the access control function by controlling the default values of security attributes
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting the use of trusted channels for data communication through SMI
O.FUNC.NO_ALT	FCS_CKM.1(1)	Supports cryptographic operations when it is required that the key for encryption of the user data repository should be generated

	FCS_CKM.4	Supports cryptographic operations when it is required that the key for encrypting the user data repository should be destroyed
	FCS_COP.1	Enforces protection when cryptographic operations for encrypting the user data repository is required
	FDP_ACC.1(1)	Enforces protection by establishing the access control policy
	FDP_ACF.1(1)	Supports the access control policy by providing the access control function
	FIA_UID.1	Supports the access control and security roles when user identification is required
	FMT_MSA.1(1)	Supports the access control function by controlling security attributes
	FMT_MSA.3(1)	Supports the access control function by controlling the default values of security attributes
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting the use of trusted channels for data communication through SMI
O.PROT.NO_ALT	FCS_CKM.1(2)	Supports cryptographic operations when it is required that the key for encrypting the address book backup/restore function should be generated
	FIA_UID.1	Supports the access control and security roles when user identification is required
	FMT_MTD.1	Enforces the protection function by restricting access
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting the use of trusted channels for data communication through SMI
O.CONF.NO_DIS	FCS_CKM.1(2)	Supports cryptographic operations when it is required that the key for encrypting the address book backup/restore function should be generated
	FIA_UID.1	Supports the access control and security roles when user identification is required
	FMT_MTD.1	Enforces the protection function by restricting access
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting the use of trusted channels for data communication through SMI
O.CONF.NO_ALT	FCS_CKM.1(2)	Supports cryptographic operations when it is required that the key for encrypting the address book backup/restore function should be generated
	FIA_UID.1	Supports the access control and security roles when user identification is required
	FMT_MTD.1	Enforces the protection function by restricting access
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting that the use of trusted channels for data communication through the SMI

O.USER.AUTHORIZED	FDP_ACC.1(2)	Enforces authentication by establishing the access control policy
	FDP_ACF.1(2)	Supports the access control policy by providing the access control function
	FIA_AFL.1(1)	Delays authentication when authentication fails (U.ADMINISTRATOR)
	FIA_AFL.1(2)	Prevents authentication when authentication fails (U.NORMALAD)
	FIA_ATD.1	Supports authentication in connection with user security attributes
	FIA_UAU.1	Enforces authentication with user authentication
	FIA_UAU.7	Supports authentication by protecting authentication information feedback
	FIA_UID.1	Enforces authentication when user identification is required
	FIA_USB.1	Enforces authentication by classifying subject security attributes linked to user roles
	FMT_MSA.1(2)	Supports the access control function by controlling security attributes
	FMT_MSA.3(2)	Supports the access control function by controlling the default values of security attributes
	FMT_SMR.1	Supports control of security attributes when security roles are required
O.INTERFACE.MANAGED	FDP_IFC.2	Manages by establishing the network information flow control policy
	FDP_IFF.1	Supports the network information flow control policy by providing the information flow control function
	FIA_UAU.1	Enforces authentication with user authentication
	FIA_UID.1	Enforces authentication when user identification is required
	FMT_MSA.1(3)	Supports the information flow control function by controlling security attributes
	FMT_MSA.3(3)	Supports the information flow control function by controlling the default values of security attributes
	FPT_FDI_EXP.1	Enforces the function to restrict the direct forwarding of data from one external interface to another
	FTA_SSL.3	Enforces authentication when the termination of an inactive session is required
O.SOFTWARE.VERIFIED	FPT_TST.1	Enforces software verification when self-test is required
O.AUDIT.LOGGED	FAU_ARP.1	Enforces a security warning in case of security breaches
	FAU_GEN.1	Enforces the audit record policy when audit logs are required in relation to MFP functions
	FAU_GEN.2	Supports the security audit policy when the audit logs of information linked to logged events are generated
	FAU_SAA.1	Provides support when analysis of logged security audits is required
	FAU_SAR.1	Enforces restriction of the viewing of stored audit records to U.ADMINISTRATOR
	FAU_SAR.2	Prohibits all users from reading audit records except for those users who are clearly allowed to read
	FAU_SAR.3	Enforces application when the viewing of stored audit records according to the standard of logical relationship is required
	FAU_STG.1	Enforces protection of the audit records repository by preventing unauthorized alteration of stored audit records

	FAU_STG.4	Enforces protection of audit data from loss by overwriting oldest audit records
	FIA_UID.1	Enforces authentication when user identification is required
	FPT_STM.1	Supports the security audit policy by providing a correct time stamp when audit records are created

6.3.2 Security Assurance Requirements Rationale

This security target was developed in consideration of the assumption that it is operated in a limited environment where the level of document security and operational responsibilities require a relatively high level of assurance. The TOE was developed in consideration of the fact that it is operated in a physically secure environment and unauthorized access over the network is limited. User data is encrypted and stored in the SD card or SSD inside the MFP. The SD and SSD are inaccessible unless they are physically separated from the MFP. So user data is safe from the physical disclosure. Also, the self-verification function for executable codes is provided so that the malfunctions of the MFP can be detected. Accordingly, the Evaluation Assurance Level 2 is appropriate.

6.3.3 Dependency Rationale

[Table 26] Dependencies on the TOE Security Functional Components

No.	Security Functional Requirements	Claimed Dependencies	Dependencies Satisfaction in ST (No.)
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	35
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	1 24
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.2	FAU_SAR.1	5
7	FAU_SAR.3	FAU_SAR.1	5
8	FAU_STG.1	FAU_GEN.1	2
9	FAU_STG.4	FAU_STG.1	8
10	FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	12 11
11	FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Not satisfied (As the cryptographic key for the address book backup/restore function is generated by user input during every backup or restore, but is not stored in the system, key destruction is not necessary.)
12	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	10
13	FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	10 12
14	FDP_ACC.1(1)	FDP_ACF.1(1)	14
15	FDP_ACC.1(2)	FDP_ACF.1(2)	15

16	FDP_ACF.1(1)	FDP_ACC.1(1)
		FMT_MSA.3(1)
			14
			31

17	FDP_ACF.1(2)	FDP_ACC.1(2)
		FMT_MSA.3(2)
			15
			32

18	FDP_IFC.2	FDP_IFF.1	19
19	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3(3)	18 33
20	FDP_RIP.1	-	-
21	FIA_AFL.1(1)	FIA_UAU.1	24
22	FIA_AFL.1(2)	FIA_UAU.1	24
23	FIA_ATD.1	-	-
24	FIA_UAU.1	FIA_UID.1	26
25	FIA_UAU.7	FIA_UAU.1	24
26	FIA_UID.1	-	-
27	FIA_USB.1	FIA_ATD.1	23
28	FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	14 35 36
29	FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	15 35 36
30	FMT_MSA.1(3)	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	18 35 36
31	FMT_MSA.3(1)	FMT_MSA.1(1) FMT_SMR.1	28 36
32	FMT_MSA.3(2)	FMT_MSA.1(2) FMT_SMR.1	29 36
33	FMT_MSA.3(3)	FMT_MSA.1(3) FMT_SMR.1	39 36
34	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	35 36
35	FMT_SMF.1	-	-
36	FMT_SMR.1	FIA_UID.1	26
37	FPT_STM.1	-	-
38	FPT_TST.1	-	-
39	FTA_SSL.3	-	-
40	FTP_ITC.1	-	-
41	FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	35 36

[Table 27] Dependencies on the Assurance Requirements

No.	Security Assurance Requirements	Claimed Dependencies	Dependencies Satisfaction in ST (No.)
1	ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	2 3
2	ADV_FSP.2	ADV_TDS.1	3
3	ADV_TDS.1	ADV_FSP.2	2
4	AGD_OPE.1	ADV_FSP.1	2
5	AGD_PRE.1	-	
6	ALC_CMC.2	ALC_CMS.1	7
7	ALC_CMS.2	-	
8	ALC_DEL.1	-	
9	ASE_INT.1	-	
10	ASE_CCL.1	ASE_INT.1 ASE_ECD.1 ASE_REQ.1	9 11 13
11	ASE_ECD.1		
12	ASE_OBJ.2	ASE_SPD.1	14
13	ASE_REQ.2	ASE_OBJ.2 ASE_ECD.1	12 11
14	ASE_SPD.1	-	
15	ASE_TSS.1	ASE_INT.1 ASE_REQ.1	9 13

		ADV_FSP.1	2
16	ATE_COV.1	ADV_FSP.2 ATE_FUN.1	2 17
17	ATE_FUN.1	ATE_COV.1	16
18	ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	2 4 5 16 17
19	AVA_VAN.2	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1	1 2 3 4 5

7. TOE Summary Specification

7.1 TOE Security Functions

This section describes the security functions performed by the TOE to meet the security function requirements described in Section 6.1.

7.1.1 Identification and Authentication

The TSF provides the function for identifying and authenticating users (U.USER). The administrator (U.ADMISTRATOR) uses the browser installed on the client computer through network connection to perform TOE security management, or uses the operation panel of the TOE to perform security management. General users (U.NORMAL) can use the operation panel of the TOE to use the functions provided by the TOE. If the administrator accesses the TOE for security management, the TOE identifies and authenticates the administrator so that the authorized administrator can perform security management. If the user accesses the TOE, the TOE identifies and authenticates the user so that the functions of the TOE are provided to the authorized user. The user identification and authentication mechanism is provided using the general ID/password method. If a user fails to be authenticated as often as the number of times specified by the administrator, authentication will be restricted according to the following authentication failure policies.

> Administrator: Authentication is delayed for a certain amount of time specified by administrator.
> Normal user: Authentication is prevented until the administrator allows it.

By default, up to five user failures are allowed, and the administrator may define the number of failures with an integer between 3 and 10.

When accessing the TOE through the RUI, users may use such functions as using menus unrelated to security (viewing product information, address book, job status, and product status information) before identification and authentication.

While users are entering identification and authentication information, authentication information will be masked with * so that authentication feedback information can be protected.

7.1.2 Access Control

The TSF protects user data by controlling access to user data while users are using the MFP. For the user data created by print, scan, and fax functions, the TOE denies accesses of all users excluding the document owner based on the user ID. When logged in to the TOE through LUI, normal users can view or print the list of the print data they own and they also can forward scan data of their choice to external entities (USB, email address, CIFS, WebDAV, FTP). When logged in to the TOE through LUI, administrators can view or print the list of fax data. The deletion of user data or jobs are only allowed to the owner of print, scan, fax functions. There is no access restriction on copy function.

The TSF controls access based on user ID and user's role with regard to using the basic functions of the MFP. When logged in to the TOE through LUI, normal users can only execute the functions that are allowed by the administrator (print, scan, copy, and fax).

The TSF provides the information flow control function based on the IP of the external IT entity. For external IT entities accessing the TOE over the network, the administrator can control them based on information flow control security policy setting.

7.1.3 Audit

The TSF generates audit logs for all jobs performed by the TSF and all actions performed by users. Audit logs are generated and stored when the MFP boots up and shuts down, and when related events listed in [Table 28] below occur.

[Table 28] Audit events

SFR-related Auditable events	History of auditable events	Related SFR
Audit log repository fill-up	Details of audit log repository fill-up	FAU_STG.4
Administrator/user authentication failure	History of responses to authentication failures	FIA_AFL.1
Administrator/user authentication	Authentication success/failure history	FIA_UAU.1
Data access control setting change	History of data access control setting change	FMT_MSA.1(1)
Basic function access control setting change	History of basic function access control setting change	FMT_MSA.1(2)
Network information flow control setting change	History of network information flow control setting change	FMT_MSA.1(3)
Data access control setting change	History of data access control setting change	FMT_MSA.3(1)
Basic function access control setting change	History of basic function access control setting change	FMT_MSA.3(2)
Network information flow control setting change	History of network information flow control setting change	FMT_MSA.3(3)
Security Management result	History of administrator’s security management	FMT_MTD.1
Self-test result	Self-test result (success/failure)	FPT_TST.1
Session end result	Session termination result	FTA_SSL.3
Default function related auditable events	**History of auditable events**	**Remark**
Copy	Copy record	Auditable events of default functions that are not related to SFR
Scan	Scan record	
Fax	Fax send/receive record	
Print	Print record	

The TSF records event dates using the time stamp provided by the MFP when generating audit logs, and records information on event type, subject’s identity and event result (success or failure).

The TSF provides the capability to detect potential violations, such as the administrator's consecutive authentication failures, audit log repository fill-up, and errors during self-tests based on the stored audit data. If there are potential errors, the TSF uses e-mail to send a warning to help the administrator operate TSF stably.

The audit log created by TSF can be viewed and managed only by the administrator through the operation panel. The job log (Print, Scan and Copy) and fax log can be viewed by the administrator and the user through the operation panel. When looking up the created audit data, the TSF can look up the auditable events by user ID.

If the audit data repository is full, the TSF continuously stores the latest audit history by overwriting oldest audit data first.

7.1.4 Security Management

The TSF provides management functions for TSF data defined in the [Table 30]. These functions are used in access control policy for the administrator whose identification and authentication have been completed.

[Table 29] Managing of TSF Data

TSF data list	Query	Modify	Delete	Add	Backup /restore	User roles
Address book	O	O	O	O	O	U.USER (* U.NORMAL can modify, delete and register his/her own address book.)
job log, fax log	O	-	-	-	-	U.USER
Audit log	O	-	-	-	-	U.ADMINISTRATOR
User ID	O	O	-	-	-	
User password	-	O	-	-	-	
User roles(basic function)	O	O	-	-	-	
Security fax setting	O	O	-	-	-	
network setting	O	O	-	-	-	
Security warning mail setting	O	O	O	O	-	
Mail server setting	O	O	O	O	-	
SD Card setting(LUI)	O	O	-	-	-	
SSD setting(LUI)	O	O	-	-	-	
Service port	O	O	-	-	-	
IPSec setting	O	O	O	O	-	
SNMP setting	O	O	-	-	-	
Login limit time	O	O	-	-	-	
Login attempts	O	O	-	-	-	
IP filtering setting	O	O	O	O	-	
Administrator connection IP setting	O	O	O	O	-	
Output authentication setting	O	O	-	-	-	
Fax data control setting	O	O	-	-	-	
MFP time setting	O	O	-	-	-	

The administrator can perform security management on the web through the operation panel of the MFP. The administrator must check the details of the security warning sent by the TSF via e-mail, and perform security management so that the TSF is always secure. To protect the address book data when performing the address book backup/restore functions, the TSF provides the function to encrypt the address book. The cryptographic algorithm used for encryption is the AES block cryptographic algorithm, and 256-bit cryptographic keys are used. The TSF uses the Password Based Key Derivation Function (PBKDF1) to generate the cryptographic key when generating the cryptographic keys used for encrypting the address book. The cryptographic key for the address book backup/restore functions is generated by user input at every backup or restore, and it is not stored in the system.

If the administrator manages the TOE via web (RUI) or operation panel (LUI), the TSF controls the session. If the administrator does not do anything after login, the TSF provides the capability to terminate the session. By default, the session is terminated after 60 seconds, and the value can be any number between 60 seconds and 600 seconds depending on the setting made by the administrator.

7.1.5 Stored data protection

The TSF provides the capability to protect user data stored in the TOE. The image data generated by the fax / scan jobs and the documents in the form of electronic files stored by the normal user for printing will be stored in the user data repository installed in the TOE (SD Card or SSD).

The TSF provides the capability to encrypt the data repository to protect stored user data. The cryptographic algorithm used for encryption is the AES block cryptographic algorithm. The AES cryptographic algorithm uses 256-bit cryptographic keys.

The TSF uses the Shindoh data repository cryptographic key generation algorithm to generate cryptographic keys when generating the cryptographic keys used for encryption. The generated cryptographic keys will be stored in the secure repository of the device. When destroying cryptographic key, it is overwritten with ‘0’.

The TSF provides the function to delete the data stored in the user data repository. As the user data repository is installed physically inside the TOE, it is impossible to take the data repository out without permission. If the product is replaced or put into disuse, however, the data in the data repository must be deleted. At this time, the TSF deletes all domains of the data repository (overwriting them with ‘0’). Also, the TSF destroys the cryptographic keys used for encryption by overwriting them with ‘0’ when deleting all domains of the user data repository.

7.1.6 Self-Testing

The TOE performs self-test on a subset of the TSF to demonstrate correct operations of the TSF. The self-test is done at TOE start-up and regularly during the operation by the administrator. TOE conducts self-tests when it starts periodically during regular operations and at the request of the administrator. The MFP Controller Software is subject to self-test.

Also, the TSF provides the capability to check the integrity of a subset of the TSF data (Encryption Key Data) and stored TSF executable code. To check integrity, SHA256 hash algorithm is used. The hash values from the data saved at initial installation and the data saved by an on-demand integrity check are compared for integrity check. If the integrity of the TSF data is found compromised, the issue is reported to the administrator by an email and an audit result is logged.

7.1.7 Fax Data Control

The TOE restricts data forwarding to external interfaces. The TOE restricts the forwarding of inbound fax data over PSTN to external interfaces. Direct data forwarding from PSTN to other interfaces is possible only in case where it is explicitly allowed by authorized administrative roles. Excluding the fax data, all inbound data from external interfaces are not allowed to be forwarded to any external interface.

7.1.8 Secure Communication

The TSF provides encrypted communication listed in the [Table 31] below to ensure the security of the transmitted data during communication between the TOE and external IT entities (Client Computer, FTP server, WebDAV server, CIFS server and Mail server).

[Table 30] Encrypted Communication Provided by TOE

External IT Entity	Encrypted Communication Provided by TOE	
	Protocol	Encryption algorithm
Client Computer	IPSec	AES (128bits), 3DES (168bits)
	TLS 1.0, TLS 1.1, TLS1.2	AES(128bits, 192bits, 256bits), 3DES (168bits)
FTP server	IPSec	AES (128bits), 3DES (168bits)
	TLS 1.0, TLS 1.1, TLS1.2	AES (128bits, 192bits, 256bits), 3DES (168bits)
WebDAV server	IPSec	AES (128bits), 3DES (168bits)
	TLS 1.0, TLS 1.1, TLS1.2	AES (128bits, 192bit, 256bits), 3DES (168bits)
CIFS server	IPSec	AES (128bits), 3DES (168bits)
Mail server	IPSec	AES (128bits), 3DES (168bits)
	TLS 1.0, TLS 1.1, TLS1.2	AES (128bits, 192bits, 256bits), 3DES (168bits)