TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASKalfa 3553ci Series with FAX System

Security Target

Version 1.07

November 8, 2019

KYOCERA Document Solutions Inc.

- History of Revisions-

Date	Version	Detail
2018-09-28	0.95	First release
2018-10-17	0.96	Modified for corresponding ORs.
2018-10-26	0.961	Modified for corresponding ORs.
2018-10-31	0.962	Modified for corresponding ORs.
2018-12-13	0.97	Modified for corresponding ORs.
2019-01-25	0.98	Modified to clarify statements.
2019-03-19	0.99	Update of TOE version.
2019-07-29	1.00	Modified for corresponding ORs.
2019-09-03	1.01	Modified for corresponding ORs.
2019-09-20	1.02	Modified for corresponding ORs.
2019-10-15	1.03	Modified for corresponding ORs.
2019-10-24	1.04	Modified for corresponding ORs.
2019-10-25	1.05	Modified for corresponding ORs.
2019-11-06	1.06	Modified for corresponding ORs.
2019-11-08	1.07	Modified for corresponding ORs.

Table of Contents

List of Figures

List of Tables

1. ST Introduction

1.1. ST Reference

ST Title	TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASKalfa 3553ci Series with FAX System Security Target
ST Version	1.07
Date	November 8, 2019
Author	KYOCERA Document Solutions Inc.

1.2. TOE Reference

TOE Title :	TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASKalfa 3553ci, TASKalfa 6053ciG, TASKalfa 5053ciG, TASKalfa 4053ciG(KYOCERA), CS 6053ci, CS 5053ci, CS 4053ci, CS 3553ci(Copystar), 6007ci, 5007ci, 4007ci(TA Triumph-Adler/UTAX), with FAX System Remarks : This TOE configures the following additional options to TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASKalfa 3553ci, TASKalfa 6053ciG, TASKalfa 5053ciG, TASKalfa 4053ciG, CS 6053ci, CS 5053ci, CS 4053ci, CS 3553ci, 6007ci, 5007ci, and 4007ci: - FAX Option (FAX System 12)
TOE Version：	System Firmware : 2V8_S0IS.C01.013 FAX Firmware : 3R2_5100.003.012
Developer :	KYOCERA Document Solutions Inc.
Applicable MFP :	KYOCERA TASKalfa 6053ci, KYOCERA TASKalfa 5053ci, KYOCERA TASKalfa 4053ci, KYOCERA TASKalfa 3553ci, KYOCERA TASKalfa 6053ciG, KYOCERA TASKalfa 5053ciG, KYOCERA TASKalfa 4053ciG, Copystar CS 6053ci, Copystar CS 5053ci, Copystar CS 4053ci, Copystar CS 3553ci, TA Triumph-Adler 6007ci, TA Triumph-Adler 5007ci, TA Triumph-Adler 4007ci UTAX 6007ci, UTAX 5007ci, UTAX 4007ci

This TOE is identified by a combination of the respective MFP product names as listed in the TOE title and each version of the two kinds of firmwares as listed in the TOE version. There are multiple MFP product names as listed above, however the MFP components are all the same. The only differences are print speed and sales destinations.

1.3. TOE Overview

1.3.1. TOE Type

The TOE defined in this ST is a Multi-Function Printer (MFP) manufactured by KYOCERA Document Solutions Inc., namely, "TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASKalfa 3553ci, TASKalfa 6053ciG, TASKalfa 5053ciG, TASKalfa 4053ciG, CS 6053ci, CS 5053ci, CS 4053ci, CS 3553ci, 6007ci, 5007ci, 4007ci", each of which includes mainly Copy function, Scan function, Print function, FAX function and Box function. As for the FAX function, the optional FAX System 12 must be installed on the device to be available.

1.3.2. TOE Usage

This TOE can perform copying (duplication), printing (paper output), sending (electronization) and storing (accumulation) of various documents handled by users. The TOE is located in a common office environment and is not only used as a standalone but also connected to LAN for the use in the network environment. In the network environment, the TOE is assumed to be used by connecting to a server and a client PC on the internal network protected from unauthorized access on the external network by firewall. And, the TOE is assumed to be used by connecting to a Local Port (USB Port). In this user environment, the above-mentioned operational functions can be performed through operations on the operation panel or from the client PCs on the network and of the local connection.

Figure 1-1 shows a normal user environment.

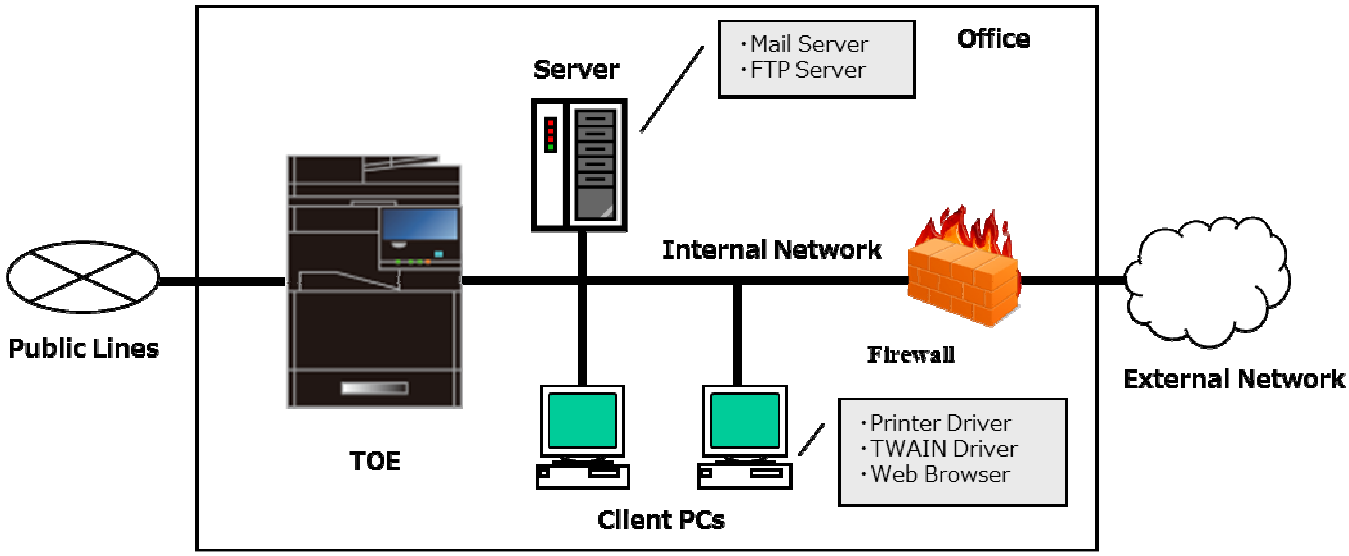


Figure 1-1 Common usage in the offices

The environment to use the common functions of the TOE is illustrated as follows.

- Internal Network :
  The network environment inside the office protected from unauthorized access on the external network by firewall.

- Client PC:
  It is connected to the MFP via the internal network or a Local Port (USB Port). The common functions of the MFP can be available upon receipt of a user instruction.
  Client PC needs the following:
  - Printer Driver
  - TWAIN Driver
  - Web Browser

- Server:
  It is used when sending the documents in the MFP. The following servers are needed.
  - Mail Server
  - FTP Server

- Public Line:
  A public line is needed when sending and receiving the documents in the MFP by the FAX.

1.3.3. Required Non-TOE Hardware, Software and Firmware

Required Non-TOE Hardware, Software and Firmware name is as follows.

- Client PCs:
  - Printer Driver : KX Driver
  - TWAIN Driver : Kyocera TWAIN Driver
  - Web Browser : Microsoft Internet Explorer 11.0
- Mail Server : IPsec(IKEv1) should be available.
- FTP Server : IPsec(IKEv1) should be available.

1.3.4. Major Security Features of TOE

The TOE can perform copying, printing, sending scanned data, FAX (send/receive) and Box storage of various documents handled by users. To prevent alteration and leaks of these documents, the TOE has functions to identify and to authenticate users, to control access to image data or functions, to encrypt image data, to overwrite-erase the residual image data, to generate and to refer audit logs, to allow only authorized users to make security function related settings, to perform the TOE self-test, and to protect the network.

1.4. TOE Description

1.4.1. TOE user

User roles related to the use of the TOE are defined as follows.

Table 1-1 TOE User

Designation	Explanation
U.USER User	A person who is authorized to use the TOE.
U.NORMAL Normal User	A person who uses the TOE. A normal user can use Copy function, Print function, Scan to Send function, Fax (Send/Receive) function and Box function.

	U.ADMINISTRATOR Device Administrator	A person who manages the TOE. A device administrator has privilege to manage device configuration, installation and operation for the TOE correct behavior. This ST includes both a user (Device Administrator) who has administration privilege that has been registered in advance when setting the factory default and a user (Administrator) who has administrator privilege that enable this administrator to make additional registration as needed during operation.

1.4.2. Physical Configuration of TOE

The conceptual figure of physical configuration of the TOE is shown in Figure 1-2.

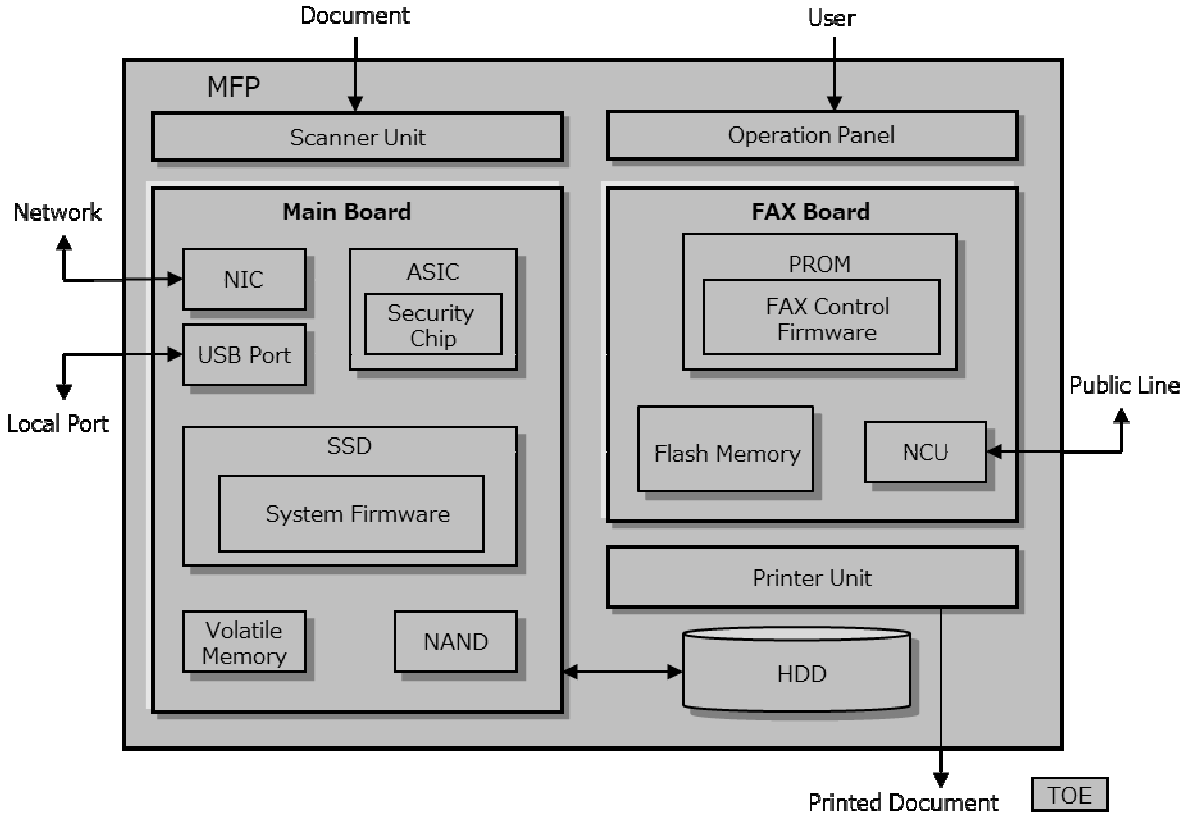


Figure 1-2 Physical Configuration of TOE

The TOE consists of an Operation Panel, a Scanner Unit, a Printer Unit, a Main Board, a FAX Board, HDD and SSD hardware, and firmwares.
The Operation Panel is the hardware that displays status and results upon receipt of input by the TOE user. The Scanner Unit and the Printer Unit are the hardware that input document into MFP and output as printed material.

A Main Board is the circuit board to control entire TOE. A system firmware is installed on a SSD, which is positioned on the Main Board. The Main Board has a Network Interface (NIC) and a Local Interface (USB Port).
ASIC that is also on the Main Board includes a Security Chip, which shares installation of some of the security functions. The Security Chip realizes security arithmetic processing for HDD encryption function and HDD Overwrite-Erase function (See below).
A FAX control firmware that controls FAX communication is installed on the PROM, which is positioned on the FAX Board. Additionally, a FAX Board has a NCU as an interface.

As for memory mediums, a NAND that stores device settings, a Volatile Memory that is used as working area and a SSD for the system firmware installation are positioned on the Main Board. A Flash Memory that stores FAX receive/send image, and a PROM for the FAX control firmware installation are positioned on the FAX Board. A HDD that stores image data and job data, is connected to the Main Board. Any of the above memory mediums are not removable. Only the FAX receive/send image is stored in the Flash Memory. Image data handled by other basic functions is stored in the HDD. However, image data is not stored in the SSD.

The delivery method for each TOE components is as follows. Guidance is also a part of TOE.

Table 1-2 Delivery method for each TOE components

TOE Configuration	Form	Delivery Method	Identification Information
MFP Device	MFP Device	Courier	MFP product name and firmware version information described in TOE Reference + Mass storage device: HDD 320GB
Fax	FAX Board	Courier	FAX System 12
Guidance	Paper document, PDF format file in DVD	Included in the box of the MFP device.	Name and version described in Table 1-3

* Firmware is preinstalled in the MFP

1.4.3. Logical Configuration of TOE

The conceptual figure of logical configuration of the TOE is shown in Figure 1-3.

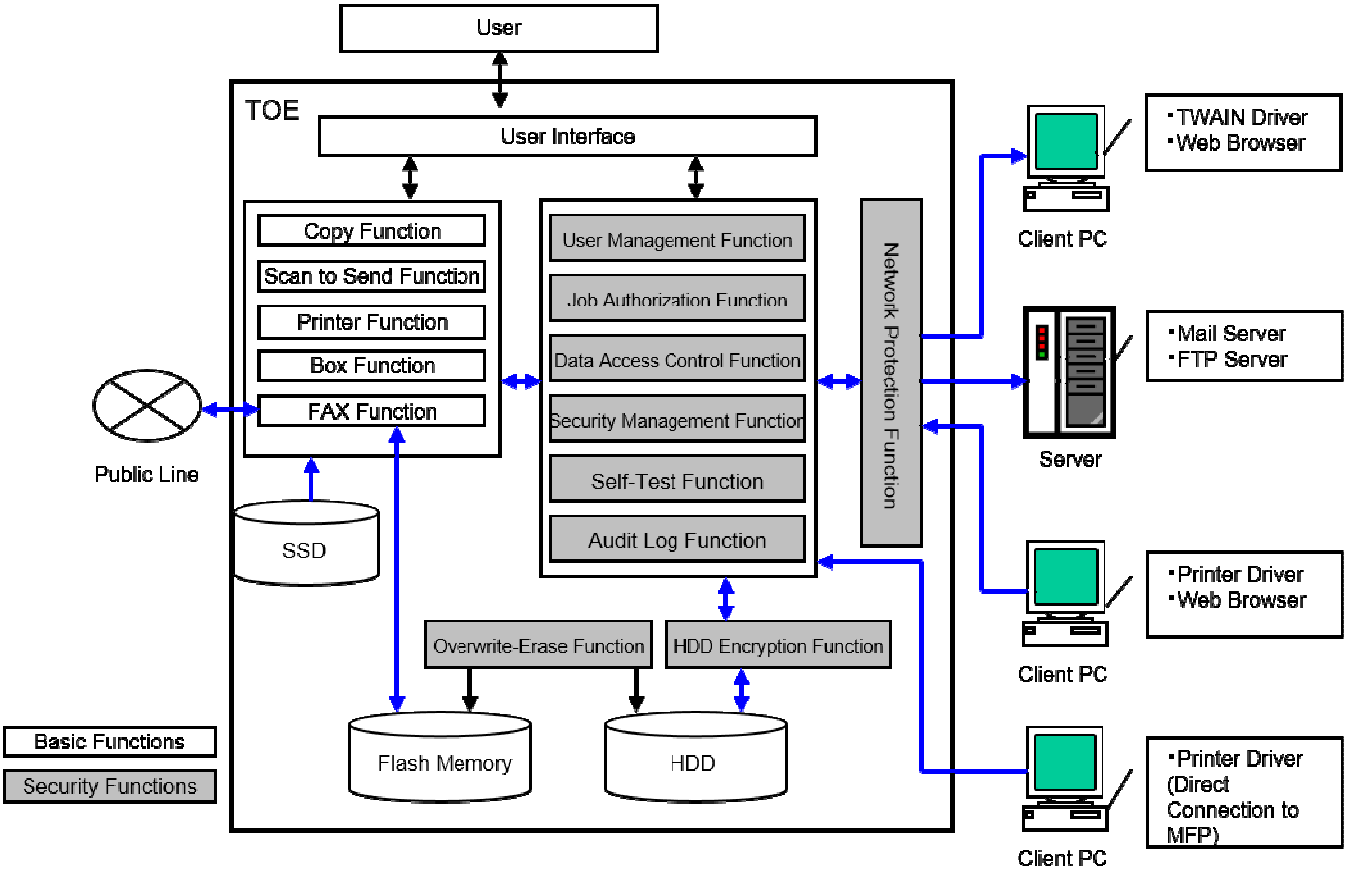


Figure 1-3 Logical Configuration of TOE

1.4.3.1. Basic Functions provided by TOE

The TOE provides the following basic functions.

- Copy Function

  A function that reads image data from the Scanner of the TOE and outputs from the Printer Unit of the TOE by inputting or operating from the Operation Panel by normal users. (Execute a Copy job)

- Scan to Send Function

  A function that sends image data to client PCs or servers connected via LAN by inputting or operating from the Operation Panel and the TWAIN Driver of Client PCs by general users. The following types of send functions are available. (Execute a Scan to Send job)

  - FTP send (FTP Server)
  - E-mail send (Mail Server)
  - TWAIN send (TWAIN Driver)

- Print Function

  A function that outputs received image data from the Printer Unit of the TOE by printing instructions from Client PCs connected over LAN or a local port to MFP by normal users. The printing instructions are given from the printer driver installed on Client PCs. The function also supports printing from a USB Memory connected to the local port. The printing instructions are given from the Operation Panel. (Execute a Print job)

- Fax Function

  A function that sends and receives documents by FAX via public line. As for FAX Send, the scanned image data will be sent by FAX to outside. Whereas for FAX Reception, the received image data will be outputted from the Print Unit of the TOE, and then forwarded to outside. (Execute a FAX Send job)

- Box Function

  A function that stores image data in the HDD, reads image data from the HDD and then sends it or print it by normal users. Image data can also be moved or joined inside the box. However, image data sent or received by the FAX function can be stored in a Flash Memory. (Execute a Box Storage job, a Box Send job and a Box Print job)

  Inputted image data is stored in the HDD by inputting/operating by normal users from the Operation Panel or the Client PCs connected over LAN or directly connected with MFP. In addition, image data transmitted/received by using the FAX function is stored in the Flash Memory. Stored image data can be outputted from the Print Unit of the TOE or sent to a server such as a Client PC, a mail server and other faxes over public line. Stored image data can also be deleted. When inputting from Client PCs, printer driver is used, and when operating from Client PCs, web browser is used. The following types of send functions are available.

  - FTP send (FTP Server)
  - E-mail send (Mail Server)
  - TWAIN send (TWAIN Driver)
  - FAX send (Other faxes)
  - USB Memory send (USB Memory)

1.4.3.2. Security Functions provided by TOE

TOE provides the following security functions.

- User Management Function

  A function that identifies and authenticates users so that only authorized users can use the TOE. When using the TOE from the Operation Panel and Client PCs, a user will be required to enter his/her login user name and login user password for identification and

authentication. The User Management Function includes a User Account Lockout Function, which prohibits the users access for a certain period of time if the number of identification and authentication attempts consecutively result in failure, a function, which protects feedback on input of login user password when performing identification and authentication and a function, which automatically logouts in case no operation has been done for a certain period of time.

- Data Access Control Function

A function that restricts access to protected assets so that only authorized users can access to the protected assets inside the TOE.
The following types of Access Control Functions are available.

- Access Control Function to control access to image data
- Access Control Function to control access to job data

- Job Authorization Function

A function that restricts usage of the function so that only authorized persons can use basic functions of the TOE .
The following types of Job Authorization are available.

- Copy Job (Copy Function)
- Print Job (Print Function)
- Send Job (Scan to Send Function)
- FAX Send Job (FAX Function)
- FAX Reception Job (FAX Function)
- Storing Job (Box Function)
- Network Job (Network Protection Function)

- HDD Encryption Function

A function that encrypts information assets stored in the HDD in order to prevent leakage of data stored in the HDD inside the TOE.

- Overwrite-Erase Function

A function that does not only logically delete the management information of the image data, but also entirely overwrites and erases the actual data area so that it disables re-usage of the data where image data that was created on the HDD or the Flash Memory during usage of the basic functions of the TOE.

- Audit Log Function

A function that records and stores the audit logs of user operations and security-relevant events on the HDD. This function provides the audit trails of TOE use and security-relevant events. Stored audit logs can be accessed only by a device administrator. The stored

audit logs will be sent by email to the destination set by the device administrator.

- Security Management Function
  A function that sets security functions of the TOE. This function can be used only by authorized users. This function can be utilized from an Operation Panel and a Client PC. Operations from a Client PC use a web browser.

- Self-Test Function
  A function that verifies the integrity of TSF executable code and TSF data to detect unauthorized alteration of the executable code of the TOE security functions.

- Network Protection Function
  A function that protects communication paths to prevent leaking and altering of data by eavesdropping of data in transition over the internal network connected to TOE.
  This function verifies the propriety of the destination to connect to and protects targeted information assets by encryption, when using a Scan to Send Function, a Print Function, a Box Function and a BOX Function from a Client PC (web browser), or a Security Management Function from a Client PC (web browser). However, usage of a Print Function directly connected to a MFP is exception.
  This function also provides a feature to prevent forwarding of information from an external interface to an internal network through TOE without permission.

1.4.4. Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Maintenance Interface

1.4.5. Guidance

The guidance comprising the TOE is shown below.

Table 1-3 Guidance that comprises TOE

Name	Version
Notice	302VK5641004
FAX System 12 Installation Guide	303RK5671006
TASKalfa 6053ci / TASKalfa 5053ci / TASKalfa 4053ci / TASKalfa 3253ci / TASKalfa 2553ci First Steps Quick Guide	302V85602001
TASKalfa 6053ci / TASKalfa 5053ci / TASKalfa 4053ci / TASKalfa 3253ci / TASKalfa 2553ci Operation Guide	2V8KDEN000

TASKalfa 2553ci / TASKalfa 3253ci / TASKalfa 4053ci / TASKalfa 5003i / TASKalfa 5053ci / TASKalfa 6003i / TASKalfa6053ci Safety Guide	302V85622001
FAX System 12 Operation Guide	First edition 2015.7 3R2KDEN000
Data Encryption/Overwrite Operation Guide	3MS2V8GEEN3
Command Center RX User Guide	CCRXKDEN17
TASKalfa 6053ci / TASKalfa 5053ci / TASKalfa 4053ci / TASKalfa 3553ci / TASKalfa 3253ci / TASKalfa 2553ci Printer Driver User Guide	2V8CLKTEN730.2018.09
KYOCERA Net Direct Print User Guide	DirectPrintKDEN1.2016.02

1.4.6. Protected Assets of TOE

Protected Assets of TOE are User Data, TSF Data and Functions.

1.4.6.1. User Data

User Data is created by a user, and have no effect on the TOE Security Functions (TSF). The User Data is classified into the following two types.

Table 1-4 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 is the information about a user's document or job to be processed by the TOE.

User Data to be targeted by the TOE is shown in Table 1-5.

Table 1-5 User Data to be targeted by the TOE

Designation	User Data	Explanation
D.DOC	Image Data	Image Data that have attributes of +PRT、+SCN、+CPY、+FAXIN、+FAXOUT、+DSR、+SMI shown in Table 2-2.

	Residual Data	After processing the above image data, unneccesary image data is deleted but only management data is deleted, and so actual data still remain.
D.FUNC	Job Data	Job Data that is processed when executing basic functions.

1.4.6.2. TSF Data

TSF Data is created by the TOE, and could have an effect on the TOE. The TSF Data is classified into the following two types.

Table 1-6 TSF Data

Designation	Definition
D.PROT	TSF Protected Data is 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 is 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.

TSF Data to be targeted by the TOE is shown in Table 1-7.

Table 1-7 TSF Data to be targeted by the TOE

Designation	TSF Data	Explanation
D.PROT	Login User Name	User's identification information that is used for the User Management Function.
	User Authorization	User's authorization information that is used for the User Management Function. There are authorization such as U. ADMINISTRATOR and U.NORMAL with respect to the TOE.
	Job Authorization Settings	This is to set whether or not the TOE attribute-based execution is authorized. Job authorization settings for the user management function are assigned to each user.
	Executable Attributes	Attributes that show Copy Function, Print Function, Scan to Send Function, FAX Function and Box Function of the TOE are excutable.

	Owner Information	Owner Information that targeted assets hold. Login user name is assigned to the owner information.
	Number of Retries until Locked (User Account Lockout Policy Settings)	Number of retries until user account is locked out. This information is used for the user management function.
	Lockout Duration (User Account Lockout Policy Settings)	Time duration of rejection before user account is unlocked. This information is used for the user management function.
	Lockout List	User list that shows users with their user names who are locked out for user management function. Release of lockout on per user account basis from the list can be instructed by a device administrator.
	Auto Logout Time Setting	Time information about automatic termination of login session.
	Password Policy Settings	Information that is used for setting Password Policy such as password length, complexity and validity period.
	Box Owner	Setting for showing the box owner. Login user name is assigned to the owner information.
	Box Permission	Setting for sharing documents inside a box with all users. When box permission is enabled , all the users can access to the box.
	Date and Time Settings	Setting information for date and time
	Network Encryption Setting	Setting information for TLS and IPsec encryption communication, which is used for Network Protection function.
	FAX Forward Setting	Setting for forwarding of received fax data.
	Send destination information for forwarding Audit Log Report	Destination information when sending audit log report to an administrator.
D.CONF	Login User Password	Authentication information of users that is required for user management function.
	Audit Log	Log data that are generated by an audit log function.
	Encryption Key	Encryption key that is used for HDD encryption function.

1.4.6.3. Functions

Functions are shown in Table 2-1 SFR Package functions.

2. Conformance Claim

2.1. CC Conformance Claim

The CC conformance claim of this ST and TOE is as follows.

CC version for which this ST and TOE claim conformance:

Common Criteria for Information Technology Security Evaluation
Part1: Introduction and general model Version 3.1 Revision 5
Part2: Security functional components Version 3.1 Revision 5
Part3: Security assurance components Version 3.1 Revision 5

Common Criteria conformance: CC Part2 extended and CC Part3 conformant

2.2. PP Claims

This ST claims demonstrable conformance to the following PP.

PP Name/Identification :	IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B" (with NIAP CCEVS Policy Letter #20) ([PP2600.2])
Version :	1.0

Notes: In this Security Target, [PP2600.2] has been modified to conform with the NIAP CCEVS Policy Letter #20 ([CCEVS-PL20]).

2.3. Package Claims

The ST and TOE claim the package: EAL2 augmented by ALC_FLR.2.

The ST conforms to the following SFR Packages.

2600.2-PRT SFR Package for Hardcopy Device Print Functions, Operational Environment B Conformant
2600.2SCN SFR Package for Hardcopy Device Scan Functions, Operational Environment B Conformant
2600.2-CPY SFR Package for Hardcopy Device Copy Functions, Operational Environment B Conformant
2600.2-FAX SFR Package for Hardcopy Device Fax Functions, Operational Environment B Conformant

2600.2-DSR SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B Conformant
2600.2-SMI SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B Conformant

2.4. SFR Packages

2.4.1. SFR Packages functions

Functions perform processing, storage, and send of data that may be present in HCD products. The functions that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 2-1.

Table 2-1 SFR Package functions

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) send, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

2.4.2. SFR Packages attributes

When a function is performing processing, storage, or send of data, the identity of the function is associated with that particular data as a security attribute. This attribute in the TOE model makes it possible to distinguish differences in Security Functional Requirements that depend on the

function being performed. The attributes that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 2-2 SFR Package attributes.

Table 2-2 SFR Package attributes

Designation	Definition
+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.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

2.5. Conformance Rationale

The rationale that the ST conforms to PP is as follows.

The TOE type is the MFP, which has mainly the Copy Function, Scan to Send Function, Print Function, FAX Function and Box Function. This MFP is consistent with the TOE type, which is the Hardcopy Devices described in the PP (i.e. 2600.2, Protection Profile for Hardcopy Devices, Operational Environment B). The MFP also has the network function that connects to an internal network. Whereas, the MFP has the NAND, Volatile Memory, Flash Memory, HDD, SSD as storage medium, and PROM to install firmware, however None of which are removable storage medium. Therefore, the MFP conforms to six out of seven SFR Packages, which are defined by the PP, except for 2600.2-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment B.

Next, described below are the security problem definitions, security objectives and security requirements that conform to the PP.

Regarding security problem definitions, P.HDD. ENCRYPTION is augmented to the security problem definitions, covering all the contents of the PP. P.HDD.ENCRYPTION is not OSP that restricts an operational environment. Therefore, the operational environment, which conforms to the security problem definitions in the PP, still confirms to the security problem definitions of the ST. Thus the ST is more restrictive than all the security problem definitions in the PP.

Regarding security objectives, O.HDD.ENCRYPTION is augmented to the security objectives, which includes all the contents of the PP, except for OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED. O.HDD.ENCRYPTION is not the objective that restricts an operational environment. Therefore, the operational environment, which conforms to the security objectives in the PP, still conforms to the security objectives of the ST. Thus the ST is more restrictive than all the security objectives in the PP.
With the security objectives defined in the PP, the security objectives to P.AUDIT.LOGGING such as OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED are replaced by O.AUDIT_STORAGE.PROTECTED and O.AUDIT_ACCESS.AUTHORIZED. Internal functions that enforce O.AUDIT_STORAGE.PROTECTED and O.AUDIT_ACCESS.AUTHORIZED have the equivalent capability to the capability of the operational environment security objectives that are requested from OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED.

Regarding security requirements, relation between SFR defined in the ST and SFR defined in the PP is shown in .

Table 2-3 Relation between SFR of the ST and SFR of the PP

SFR of the ST	PP requirements	
FAU_GEN.1	✓	
FAU_GEN.2	✓	
FAU_SAR.1		
FAU_SAR.2		
FAU_STG.1		
FAU_STG.4		
FCS_CKM.1(a)		
FCS_CKM.1(b)		
FCS_CKM.1(c)		
FCS_COP.1(a)		
FCS_COP.1(b)		
FDP_ACC.1(a)	✓	
FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	✓	
FDP_ACF.1(b)	✓	
FDP_RIP.1	✓	
FIA_AFL.1		
FIA_ATD.1	✓	

SFR of the ST	PP requirements	
FIA_SOS.1		
FIA_UAU.1	✓	
FIA_UAU.7		
FIA_UID.1	✓	
FIA_USB.1	✓	
FMT_MSA.1(a)	✓	
FMT_MSA.3(a)	✓	
FMT_MSA.1(b)	✓	
FMT_MSA.3(b)	✓	
FMT_MTD.1(a)	✓	
FMT_MTD.1(b)	✓	
FMT_SMF.1	✓	
FMT_SMR.1	✓	
FPT_STM.1	✓	
FPT_TST.1	✓	
FPT_FDI_EXP.1	✓	
FTA_SSL.3	✓	
FTP_ITC.1	✓	

The ST covers all the SFRs required from the PP. In addition, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.1(c), FCS_COP.1(a), FCS_COP.1(b), FIA_AFL.1, FIA_SOS.1 and FIA_UAU.7 are augmented to the ST. In the operation of assignment of FTA_SSL.3, the time interval of user inactivity of operation panel and web browser is specified. However, this TOE does not have any interfaces that support an interactive session with the exception of operation panel and web browser. The operation of assignment of the rule of explicit authorization for U.ADMINISTRATOR is eliminated in FDP_ACF.1.3(b). However, it is more strict comparing to the original PP requirement that it does not have rules to have additional authorization.
All of the TOE that satisfy the ST, fulfill the PP security requirements, but more restrictive.

Finally, SAR defined in the PP and SAR defined in the ST are equivalent to each other.

Because the ST provides the PP with the resolution for common security problem definitions described in the PP in the equivalent and more restrictive manner, therefore conformance to the PP is demonstrated.

3. Security Problem Definitions

This section describes Threats, Organizational Security Policies and Assumptions.

3.1. Threats agents

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

a) Persons who are not permitted to use the TOE who may attempt to use the TOE
b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.
c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they not authorized.
d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in the Protection Profile address the threats posed by these threat agents.

3.2. Threats to TOE Assets

This section describes threats to assets described in clause 1.4.6.

Table 3-1 Threats to User Data for the 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 by unauthorized persons

Table 3-2 Threats to TSF Data for the TOE

Threat	Affected asset	Description
T.PROT.ALT	D.PROT	TSF Protected 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

3.3. Organizational Security Policies for the TOE

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for Security Objectives that are commonly desired by TOE Owners in this operational environment but for which it is not practical to universally define the assets being protected or the threats to those assets.

Table 3-3 Organizational Security Policies for the TOE

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.

P.HDD.ENCRYPTION	To improve the confidentiality of the documents, User Data and TSF Data stored in HDD will be encrypted by the TOE.

3.4. Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of the Protection Profile are based on the condition that all of the assumptions described in this section are satisfied.

Table 3-4 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

This section describes the security objectives that the TOE shall fulfill.

Table 4-1 Security objectives for the TOE

Objective	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.
O.AUDIT_STORAGE.PROTECTED	The TOE shall ensure that audit records are protected from unauthorized access, deletion and modifications.

Objective	Definition
O.AUDIT_ACCESS.AUTHORIZED	The TOE shall ensure that audit records can be accessed in order to detect potential security violations, and only by authorized persons.
O.HDD.ENCRYPTION	The TOE shall encrypt User Data and TSF Data, when the TOE stores them in HDD.

4.2. Security Objectives for the operational environment

This section describes the security objectives that must be fulfilled by operational environment of the TOE.

Table 4-2 Security objectives for the operational environment

Objective	Definition
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.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.
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.

Objective	Definition
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.

4.3. Security Objectives 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 4-3 Completeness of security objectives

Threats, Policies and Assumptions	Objectives																			
	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	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED	O.HDD.ENCRYPTION
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.ADMIN.TRAINING																	✓			
A.ADMIN.TRUST																		✓		

Threats, Policies and Assumptions	Objectives																		
	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	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED	O.HDD.ENCRYPTION
A.USER.TRAINING																			✓	
P.HDD.ENCRYPTION																				✓

Table 4-4 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 user identification and authentication as the basis for 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	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration

	persons	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 Protected 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 protects 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 to use the TOE
		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 by the TOE and its IT environment.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration
		O.AUDIT_STORAGE.PROTECTED protects audit records from unauthorized access, deletion and modifications
		O.AUDIT_ACCESS.AUTHORIZED provides appropriate access to audit records only by authorized persons.
		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
P.HDD.ENCRYPTION	User Data and TSF Data stored in HDD will be encrypted by the TOE.	O.HDD.ENCRYPTION encrypts User Data and TSF Data stored in HDD by TOE
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.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.TRUSTED establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
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.

5. Extended Components Definition

This ST defines components that are extensions to Common Criteria 3.1 Release 3, Part 2. These extended components are defined in the ST but are used in SFR Packages, and therefore, are employed only in TOEs whose STs conform to those SFR Packages.

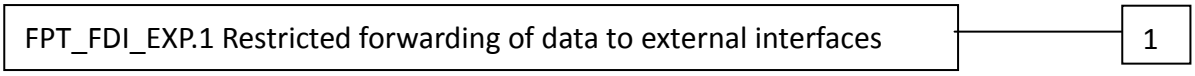
5.1. FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

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.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 this data is 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**

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

There are no auditable events foreseen.

Rationale:

Quite often a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data is allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i. e. without processing the data first) 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 the Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and could therefore be placed in either the FDP or 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 lead the authors to define a new family with just one member.

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*].

6. Security Requirements

This section describes the TOE Security Functional Requirements.

6.1. TOE Security Functional Requirements.

6.1.1. Class FAU: Security Audit

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:

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
- all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 6-1; [assignment: other specifically defined auditable events].

[selection, choose one of: *minimum, basic, detailed, not specified*]

- not specified

[assignment: *other specifically defined auditable events*]

- None

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, for each Relevant SFR listed in Table 6-1: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required); [assignment: other audit relevant information].

[assignment: *other audit relevant information*]

- None

Table 6-1 Auditable data requirements

Relevant SFR	Auditable event	Additional information	Actions to be audited (defined by CC or PP)
FAU_GEN.1	-	-	There are no auditable events foreseen.
FAU_GEN.2	-	-	There are no auditable events foreseen.
FAU_SAR.1	[Not specified] -	-	a) Basic: Reading of information from the audit records.
FAU_SAR.2	[Not specified] -	-	a) Basic: Unsuccessful attempts to read information from the audit records.
FAU_STG.1	-	-	There are no auditable events foreseen.
FAU_STG.4	[Not specified] -	-	a) Basic: Actions taken due to the audit storage failure.
FCS_CKM.1(a)	[Not specified] -	-	a) Minimum: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
FCS_CKM.1(b)	[Not specified] -	-	a) Minimum: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
FCS_CKM.1(c)	[Not specified] -	-	a) Minimum: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any

			sensitive information (e.g. secret or private keys).
FCS_COP.1(a)	[Not specified] -	-	a) Minimum: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FCS_COP.1(b)	[Not specified] -	-	a) Minimum: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FCS_COP.1(c)	[Not specified] -	-	a) Minimum: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FDP_ACC.1(a)	-	-	There are no auditable events foreseen.
FDP_ACF.1(a)	[Not specified] Successful requests to perform an operation on an object as the following: ・ D.DOC: Read ・ D.DOC: Delete ・ D.FUNC: Read	Type of job	a) Minimum: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.

	・ D.FUNC: Modify ・ D.FUNC: Delete		
FDP_ACC.1(b)	-		There are no auditable events foreseen.
FDP_ACF.1(b)	[Not specified]	-	a) Minimum: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.
FDP_RIP.1	-	-	There are no auditable events foreseen.
FIA_AFL.1	[Minimum] The following actions taken, when reaching of the threshold for the unsuccessful authentication attempts since the last successful authentication. ・ Perform user account lockout, and the following action taken to restore to the normal state. ・ Release the lockout state by a device administrator.	-	a) Minimum: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_ATD.1	-	-	There are no auditable events foreseen.
FIA_SOS.1	[Minimum] Rejection by the tested secrete as shown below:		a) Minimum: Rejection by the TSF of any tested secret;

	・ Rejection by quality check of the login user password, which was imputed when initially creating the user information. ・ Rejection by quality check of the login user password, which was changed when editing the user information.		b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.
FIA_UAU.1	[Basic] Both successful and unsuccessful use of the authentication mechanism	None required	Defined by PP: Both successful and unsuccessful use of the authentication mechanism
FIA_UAU.7	-	-	There are no auditable events foreseen.
FIA_UID.1	[Basic] Both successful and unsuccessful use of the identification mechanism	Attempted user identity	Defined by PP: Both successful and unsuccessful use of the identification mechanism
FIA_USB.1	[Not specified] -	-	a) Minimum: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).
FMT_MSA.1(a)	[Not specified] -	-	a) Basic: All modifications of the values of security attributes.
FMT_MSA.3(a)	[Not specified] -	-	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of

			the initial values of security attributes.
FMT_MSA.1(b)	[Not specified] -	-	a) Basic: All modifications of the values of security attributes.
FMT_MSA.3(b)	[Not specified] -	-	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.
FMT_MTD.1(a)	[Not specified] -	-	a) Basic: All modifications to the values of TSF data.
FMT_MTD.1(b)	[Not specified] -	-	a) Basic: All modifications to the values of TSF data.
FMT_SMF.1	[Minimum] Use of the management functions	None required	Defined by PP: Use of the management functions
FMT_SMR.1	[Minimum] Modifications to the group of users that are part of a role	None required	Defined by PP: Modifications to the group of users that are part of a role
FPT_STM.1	[Minimum] Changes to the time	None required	Defined by PP: Changes to the time
FPT_TST.1	[Not specified] -	-	a) Basic: Execution of the TSF self tests and the results of the tests.
FPT_FDI_EXP.1	-	-	There are no auditable events foreseen.
FTA_SSL.3	[Minimum] Termination of an interactive session by the session locking mechanism	None required	Minimal: Termination of an interactive session by the session locking mechanism.
FTP_ITC.1	[Minimum] Failure of the trusted channel functions	The destination IP address of failure of the trusted channel functions. (No need to obtain the sender's IP	Defined by PP: Failure of the trusted channel functions a) Identification of the initiator and target of failed trusted channel

		address, because the sender is TOE itself and so the sender's IP address has been fixed already.)	functions.

FAU_GEN.2 User identify 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_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

[assignment: *authorised users*]

- U.ADMINISTRATOR

[assignment: *list of audit information*]

- Information as shown in the "Auditable event" column and "Additional information" column of "Table 6-1 Auditable data requirements".

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_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 [selection, choose one of: prevent, detect] unauthorized modifications to the stored audit records in the audit trail.

[selection: *choose one of: prevent, detect*]
- prevent

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 [selection, *choose one of: "ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment*: other actions to be taken in case of audit storage failure*] if the audit trail is full.

[selection: *choose one of: "ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]
- "overwrite the oldest stored audit records"

[assignment: *other actions to be taken in case of audit storage failure*]

- None

6.1.2. Class FCS: Cryptographic Support

FCS_CKM.1(a) Cryptographic key generation (Storage Encryption)

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(a) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: cryptographic key generation algorithm]

- SHA-256

[assignment: cryptographic key sizes]

- 256 bits

[assignment: list of standards]

- FIPS PUB 180-4, FIPS 197

FCS_CKM.1(b) Cryptographic key generation (TLS)

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(b) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [multiple key generation algorithms described below] and specified cryptographic key sizes [as described below] that meet the following: [multiple standards as described below].

Table 6-2 Key Generation

Algorithm	Key sizes	Standards
RSA	2048 bits	FIPS 186-4, Appendix B
AES	128, 256 bits	FIPS 197

FCS_CKM.1(c) Cryptographic key generation (IPSec)

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(c) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] implement [assignment: Diffie-Hellman Groups] that meet the following: [assignment: list of standards].

[assignment: cryptographic key generation algorithm]

- IKEv1KDF

[assignment: Diffie-Hellman Groups]

- Diffie-Hellman Group 14, 16, 17, 18, 19, 20, 21, 22, 23, 24

[assignment: list of standards]

- SP 800-135 Rev.1, RFC 2409, RFC 5114

FCS_COP.1(a) Cryptographic operation (Storage Encryption)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(a) The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: list of cryptographic operations]

- Encryption of D.DOC, D.FUNC, D.PROT and D.CONF when writing into the HDD
- Decryption of D.DOC, D.FUNC, D.PROT and D.CONF when reading out from the HDD

[assignment: cryptographic algorithm]

- AES

[assignment: cryptographic key sizes]

- 256 bits

[assignment: list of standards]

- FIPS PUB 197

FCS_COP.1(b) Cryptographic operation (TLS)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(b) The TSF shall perform [the operations listed in the table below] in accordance with a specified cryptographic algorithm [multiple algorithms described below] and cryptographic key sizes [as described below] that meet the following: [multiple standards as described below].

Table 6-3 Cryptographic Operations

Operations	Algorithm	Key/Hash Size in Bits	Standards
Encryption, decryption	AES (CBC mode)	128, 256 bits	FIPS 197 SP800-38A SP800-38D
	AES (GCM mode)		
Cryptographic Signature Services	RSA Digital Signature Algorithm (RSASSA-PKCS1-v1_5)	2048 bits	PKCS #1 v2.2 FIPS 186-4
Hashing	SHA-1	160 bits	FIPS 180-4
	SHA-256, SHA-384	256, 384 bits	FIPS 180-4
Keyed Hash Message Authentication Code	HMAC-SHA-1	160 bits	RFC 2104
	HMAC-SHA-256, HMAC-SHA-384	256, 384 bits	

FCS_COP.1(c) Cryptographic operation (IPSec)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(c) The TSF shall perform [the operations listed in the table below] in accordance with a specified cryptographic algorithm [multiple algorithms described below] and cryptographic key sizes [as described below] that meet the following: [multiple standards as described below].

Table 6-4 Cryptographic Operations

Operations	Algorithm	Key/Hash Size in Bits	Standards
Hashing	SHA-256, SHA-384, SHA-512	256, 384, 512 bits	FIPS 180-4
Data	HMAC-SHA256-128	256 bits	RFC2104

authentication	HMAC-SHA384-192	384 bits	RFC 4868
	HMAC-SHA512-256	512 bits	
Encryption, decryption	3DES	168 bits	FIPS 46-3 SP 800-67 Rev.2
	AES (CBC mode)	128, 192, 256 bits	FIPS 197 SP800-38A

6.1.3. Class FDP: User Data Protection

FDP_ACC.1 (a) Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (a) The TSF shall enforce the **User Data Access Control SFP in Table 6-5** on **the list of users as subjects, objects, and operations among subjects and objects covered by the User Data Access Control SFP in Table 6-5**.

FDP_ACF.1 (a) Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ ACF.1.1 (a) The TSF shall enforce the **User Data Access Control SFP in Table 6-5** to objects based on the following: **the list of users as subjects and objects controlled under the User Data Access Control SFP in Table 6-5, and for each, the indicated security attribute in Table 6-5**.

FDP_ ACF.1.2 (a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the User Data Access Control SFP in Table 6-5 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects**.

FDP_ ACF.1.3 (a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

- Explicitly authorize access control rule as shown in Table 6-6

FDP_ ACF.1.4 (a) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

- None

Table 6-5 User Data Access Control SFP

Object (Security attribute)	Attribute	Operation(s)	Subject (Security attribute)	Access control rule
D.DOC (Owner Information)	+PRT,+SCN,+CPY ,+FAXOUT	Read, Delete	U.NORMAL (Login User Name)	Denied, except for his/her own documents. When “Owner Information” of D.DOC matches “Login User Name” of U. NORNAL, operation is permitted.
D.DOC (Box Owner, Box Permission)	+DSR	Read, Delete	U.NORMAL (Login User Name)	Denied, except (1) for his/her own documents, or (2) if authorized by another role or mechanism if such functions are provided by a conforming TOE. (1) When “Owner Information” of D.DOC matches “Login User Name” of U. NORNAL, operation is permitted. (2)When “Box Permission” storing D.DOC is enabled, operation is permitted.
D.DOC (Owner Information)	+FAXIN	[assignment: other operations] Any Operations	U.NORMAL (Login User Name)	Denied. Any Operations by U.NORMAL is denied.
D.FUNC (Owner Information)	N/A	Read, Modify, Delete	U.NORMAL (Login User Name)	Denied, except for his/her own function data. When “Owner Information “of D.FUNC matches “Login User Name” of U. NORNAL, operation is permitted.

Table 6-6 User Data Access Control SFP for U.ADMINISTRATOR

Object (Security attribute)	Attribute	Operation(s)	Subject (Security attribute)	Explicitly authorize access control rule
D.DOC (Owner Information)	+PRT	Delete	U.ADMINISTRATOR (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
D.DOC (Owner Information)	+SCN	Delete	U.ADMINISTRATOR (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
D.DOC (Owner Information)	+CPY	Delete	U.ADMINISTRATOR (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
D.DOC (Owner Information)	+FAXOUT	Delete	U.ADMINISTRATOR (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
D.DOC (Box Owner)	+DSR	Read, Delete	U.ADMINISTRATOR (User Authorization)	Regardless of "Box Owner" value, operation is permitted.
D.DOC (Owner Information)	+FAXIN	Read, Delete	U.ADMINISTRATOR (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
D.FUNC (Owner Information)	N/A	Read, Modify, Delete	U.ADMINISTRATOR (User Authorization)	Regardless of "Owner Information" value, operation is permitted.

FDP_ACC.1 (b)Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (b) The TSF shall enforce the **TOE Function Access Control SFP** in Table 6-7 on **users as subjects, TOE functions as objects, and the right to use the functions as operations**.

FDP_ACF.1 (b) Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ ACF.1.1 (b) The TSF shall enforce the **TOE Function Access Control SFP** to objects based on the following: **users and [assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]**.

[assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]

- Function(s) listed in "Object "column and security attributes listed in "security attribute", respectively as shown in Table 6-7.

FDP_ ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[selection: *the user is explicitly authorized by U.ADMINISTATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]**.

[selection: *the user is explicitly authorized by U.ADMINISTATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]

- [assignment: other conditions]

[assignment: *other conditions*]

- Rules as shown in Table 6-7

FDP_ ACF.1.3 (b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

- None

FDP_ ACF.1.4 (b) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

- None

Table 6-7 TOE Function Access Control SFP

Object (Security attribute)	Operation	Subject (Security attribute)	Access control rule
F.CPY (Executable Attribute)	Job Execution	U.ADMINISTRATOR U.NORMAL (Job Authorization Settings)	When the executable attribute of Object is included in job authorization settings that Subject have, operation is permitted.
F.PRT (Executable Attribute)	Job Execution	U.ADMINISTRATOR U.NORMAL (Job Authorization Settings)	When the executable attribute of Object is included in job authorization settings that Subject have, operation is permitted.
F.SCN (Executable Attribute)	Job Execution	U.ADMINISTRATOR U.NORMAL (Job Authorization Settings)	When the executable attribute of Object is included in job authorization settings that Subject have, operation is permitted.
F.FAX (Executable Attribute)	Job Execution	U.ADMINISTRATOR U.NORMAL (Job Authorization Settings)	When the executable attribute of Object is included in job authorization settings that Subject have, operation is permitted.
F.DSR (Executable Attribute)	Job Execution	U.ADMINISTRATOR U.NORMAL (Job Authorization Settings)	When the executable attribute of Object is included in job authorization settings that Subject have, operation is permitted.

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 [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: **D.DOC,** [assignment: *list of objects*].

[selection: *allocation of the resource to, deallocation of the resource from*]
- deallocation of the resource from

[assignment: *list of objects*]
- None

6.1.4. Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
- an administrator configurable positive integer within [assignment: range of acceptable values]

[assignment: range of acceptable values]
- 1 to 10

[assignment: *list of authentication events*]
- Consecutive unsuccessful authentication attempts since the last successful authentication occur related to login user name designated by login from an operational panel.
- Consecutive unsuccessful authentication attempts since the last successful authentication occur related to login user name designated by login from a client PC.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

[selection: *met, surpassed*]

- met

[assignment: *list of actions*]

- Login from the account is locked out between 1 and 60 minutes and until the time designated by a device administrator that elapse, or until a device administrator releases lock status.

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: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]

- Login User Name, User Authorization, Job Authorization Setting

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]

- Password Length ： At least 8 characters
- Character Type ： Alphanumeric or special characters

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 [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is authenticated.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]

- Obtain a device status
- Display a list of job information
- Display counter information
- Receive FAX data

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 [assignment: *list of feedback*] to the user while the authentication is in progress.

[assignment: *list of feedback*]

- dummy characters（*：asterisk）

FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is identified.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]

- Obtain a device status
- Display a list of job information
- Display counter information
- Receive FAX data

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 the behalf of that user: [assignment: *list of user security attributes*].

[assignment: *list of user security attributes*]

- Login User Name, User Authorization, Job Authorization Setting

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: [assignment: *rules for the initial association of attributes*].

[assignment: *rules for the initial association of attributes*]

- None

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: [assignment: *rules for the changing of attributes*].

[assignment: *rules for the changing of attributes*]

- None

6.1.5. Class FMT: Security Management

FMT_MSA.1 (a) 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_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (a) The TSF shall enforce the **User Data Access Control SFP in Table 6-5,** [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]

- None

[selection: *change_default, query, modify, delete, [assignment: other operations]*]

- Operation(s) as listed in Table 6-8

[assignment: *list of security attributes*]

- Security Attributes as listed in Table 6-8

[assignment: *the authorised identified roles*]

- Role as listed in Table 6-8

Table 6-8 Management of security attributes

Security Attributes	Operation(s)	Role
Box Owner	modify	U.ADMINISTRATOR
Box Permission	modify	U.ADMINISTRATOR
		U.NORMAL that matches a Box Owner.
Owner Information	modify	U.ADMINISTRATOR

FMT_MSA.3 (a) Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (a) The TSF shall enforce the **User Data Access Control SFP in Table 6-5,** [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]

- None

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]

- restrictive

FMT_MSA.3.2 (a) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]

- nobody

FMT_MSA.1 (b) 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_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (b) The TSF shall enforce the **TOE Function Access Control SFP,** [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]
- None

[selection: *change_default, query, modify, delete, [assignment: other operations]*]
- [assignment: other operations]

[assignment: *other operations*]
- Any Operations

[assignment: *list of security attributes*]
- Executable Attributes

[assignment: *the authorised identified roles*]
- Nobody

FMT_MSA.3 (b) Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (b) The TSF shall enforce the **TOE Function Access Control Policy**, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security

attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]

- None

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]

- permissive

FMT_MSA.3.2 (b) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]

- Nobody

FMT_MTD.1 (a) 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 (a) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to **[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*,** [assignment: *the authorized identified roles* ***except U.NORMAL***]**]]**.

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

- Operation as listed in Table 6-9

[assignment: *list of TSF data*]

- TSF data as listed in Table 6-9

[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*, [assignment: *the authorized identified roles* ***except U.NORMAL***]**]]**

- Roles as listed in Table 6-9

Table 6-9 Operation of TSF data

TSF data	Roles	Operation
Login User Name	U.ADMINISTRATOR	modify, delete, create
Login User Password	U.ADMINISTRATOR	modify, delete, create
User Authorization	U.ADMINISTRATOR	modify, delete, create
Job Authorization Settings	U.ADMINISTRATOR	modify, delete, create
Number of Retries until locked (User Account Lockout Policy Settings)	U.ADMINISTRATOR	modify
Lockout Duration (User Account Lockout Policy Settings)	U.ADMINISTRATOR	modify
Lockout List	U.ADMINISTRATOR	modify
Auto Logout Time Setting	U.ADMINISTRATOR	modify
Password Policy Settings	U.ADMINISTRATOR	modify
Date and Time Settings	U.ADMINISTRATOR	modify
Network Encryption Setting	U.ADMINISTRATOR	modify
FAX Forward Setting	U.ADMINISTRATOR	modify
Send Destination Information for Forwarding Audit Log Report	U.ADMINISTRATOR	modify
Encryption Key	Nobody	*[assignment: other operations]* ・Any Operations

FMT_MTD.1 (b) 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 (b) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data* ***associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***] to **[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR, the U.NORMAL to whom such TSF data is associated*]]**.

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

- Operation as listed in Table 6-10

[assignment: *list of TSF data* ***associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***]

- TSF data as listed in Table 6-10

[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR, the U.NORMAL to whom such TSF data is associated*]]

- Role as listed in Table 6-10

Table 6-10 Operation of TSF data

TSF data	Roles	Operation
Login User Password associated with U.NORMAL	U.NORMAL	modify

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: [assignment: *list of management functions to be provided by the TSF*].

[assignment: *list of management functions to be provided by the TSF*]

- Functions that manage security attributes (i.e. Box Owner, Box Permission and Owner Information) related to a Box function.
- Functions that manage TSF Data (i.e. Login User Name, Login User Password, User Authorization, Job Authorization Settings, Number of Retries until Locked, Lockout Duration, Auto Logout Time Setting, Password Policy Settings, Date and Time Settings, Network encryption Setting, Fax Forward Setting, Send Destination Information for forwarding Audit Log Report)

Table 6-11 Management Functions

Relevant SFR	Management Functions	Management Items (defined by CC or PP)
FAU_GEN.1	-	There are no management activities foreseen.
FAU_GEN.2	-	There are no management activities foreseen.
FAU_SAR.1	U.ADMINISTRATOR Management of Authorization	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_SAR.2	-	There are no management activities foreseen.
FAU_STG.1	-	There are no management activities foreseen.
FAU_STG.4	None (Action is fixed and is not managed.)	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
FCS_CKM.1(a)	-	There are no management activities foreseen.
FCS_CKM.1(b)	-	There are no management activities foreseen.
FCS_CKM.1(c)	-	There are no management activities foreseen.
FCS_COP.1(a)	-	There are no management activities foreseen.
FCS_COP.1(b)	-	There are no management activities foreseen.
FCS_COP.1(c)	-	There are no management activities foreseen.
FDP_ACC.1(a)	-	There are no management activities foreseen.
FDP_ACF.1(a)	None (The role group is fixed as U. ADMINISTRATOR and is not managed.)	a) Managing the attributes used to make explicit access or denial based decisions.
FDP_ACC.1(b)	-	There are no management activities foreseen.

FDP_ACF.1(b)	None (The role group is fixed as U.ADMINISTRATOR and is not managed.)	a) Managing the attributes used to make explicit access or denial based decisions.
FDP_RIP.1	None (When only deallocating the resource, residual information protection is enforced. Therefore, the timing of residual information protection is not managed.	a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.
FIA_AFL.1	Management of unsuccessful authentication attempts.	a) management of the threshold for unsuccessful authentication attempts; b) management of actions to be taken in the event of an authentication failure.
FIA_ATD.1	None (There are no additional security attributes and there are no additional security attributes to be managed.)	a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.
FIA_SOS.1	Management of Login User Password Policy	a) the management of the metric used to verify the secrets.
FIA_UAU.1	Management of login user password by U.ADMINISTRATOR. Management of U.NORMAL (him/her) login user password by U.NORMAL.	a) management of the authentication data by an administrator; b) management of the authentication data by the associated user; c) managing the list of actions that can be taken before the user is authenticated.
FIA_UAU.7	-	There are no management activities

		foreseen.
FIA_UID.1	Management of the user identities	Defined by PP: Management of the user identities
FIA_USB.1	None (Subject security attributes are fixed and are not managed.	a) an authorised administrator can define default subject security attributes. b) an authorised administrator can change subject security attributes.
FMT_MSA.1(a)	None (The role group is fixed as U.ADMINISTRATOR and is not managed.)	a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values.
FMT_MSA.3(a)	None (The role group is fixed as U.ADMINISTRATOR and is not managed.)	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.
FMT_MSA.1(b)	None (The role group is fixed as U.ADMINISTRATOR and is not managed.)	a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values.
FMT_MSA.3(b)	None (The role group is fixed as U.ADMINISTRATOR and is not managed.)	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.
FMT_MTD.1(a)	None (The role group is fixed as U.ADMINISTRATOR and is not managed.)	a) managing the group of roles that can interact with the TSF data.

FMT_MTD.1(b)	None (The role group is fixed as U.ADMINISTRATOR and is not managed.)	a) managing the group of roles that can interact with the TSF data.
FMT_SMF.1	-	There are no management activities foreseen.
FMT_SMR.1	Manage the group of users that are user authorization.	a) managing the group of users that are part of a role.
FPT_STM.1	Management of system time	Defined by PP: Management of system time
FPT_TST.1	None (Self test executable condition is fixed and is not managed.)	a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; b) management of the time interval if appropriate.
FPT_FDI_EXP.1	Management of FAX forward condition.	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.
FTA_SSL.3	Management of auto-logout time.	a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user; b) specification of the default time of user inactivity after which termination of the interactive session occurs.
FTP_ITC.1	Management of Network Encryption Setting.	a) Configuring the actions that require trusted channel, if supported.

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, [selection: *Nobody*,** [assignment: *the authorised identified roles*]].

[selection: *Nobody*, [assignment: *the authorised identified roles*]]

- Nobody

FMT_SMR.1.2 The TSF shall be able to associate users with roles**, except for the role "Nobody" to which no user shall be associated**.

6.1.6. Class FPT: TSF Protection

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 [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

[selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]

- during initial start-up

[selection: [assignment: *parts of TSF*], *the TSF*]
- [assignment: *parts of TSF*]

[assignment: *parts of TSF*]
- HDD Encryption Function

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF data*], *TSF data*].

[selection: [assignment: *parts of TSF data*], *TSF data*]
- [assignment: *parts of TSF data*]

[assignment: *parts of TSF data*]
- Encryption Key

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF*].

[selection: [assignment: *parts of TSF*], *TSF*]
- [assignment: *parts of TSF*]

[assignment: *parts of TSF*]
- TSF executable module

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 **any external Interface** from being forwarded without further processing by the TSF to **any Shared-medium Interface**.

6.1.7. Class FTA: TOE Access

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 a [assignment: *time interval of user inactivity*].

[assignment: *time interval of user inactivity*]

- Operation Panel : No operation after time set by a device administrator elapsed (between 5 seconds and 495 seconds)
- Web browser : No operation after 10 minutes elapsed.

*There are no interactive session exists with the exception of an operation panel and a web browser.

6.1.8. Class FTP: High Trusted Path/Channel

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 communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF, 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 of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface**.

6.2. TOE Security Assurance Requirement

Security assurance requirements are described in **Table 6-12 2600.2 Security Assurance Requirements**. The evaluation assurance level of this TOE is EAL2. The security assurance component, ALC_FLR.2 is added to the assurance components as shown in the Table 6-12.

Table 6-12 2600.2 Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Functional specification with complete summary
	ADV_TDS.1 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Authorisation controls
	ALC_CMS.2 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL2)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

Table 6-13 shows the TOE security functional requirements and the corresponding security objectives.

Bold typeface items provide principal (P) fulfillment of the security objectives, and normal

typeface items provide supporting (S) fulfillment.

Table 6-13 Completeness of Security Requirements

SFRs	Objectives												
	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	O.AUDIT_STORAGE.PROTE	O.AUDIT_ACCESS.AUTHORI	O.HDD.ENCRYPTION
FAU_GEN.1										**P**			
FAU_GEN.2										**P**			
FAU_SAR.1					**P**							**P**	
FAU_SAR.2					**P**							**P**	
FAU_STG.1						**P**					**P**		
FAU_STG.4						**P**					**P**		
FCS_CKM.1(a)													**P**
FCS_CKM.1(b)	S	S	S	S	S	S							
FCS_CKM.1(c)	S	S	S	S	S	S							
FCS_COP.1(a)													**P**
FCS_COP.1(b)	S	S	S	S	S	S							
FCS_COP.1(c)	S	S	S	S	S	S							
FDP_ACC.1(a)	**P**	**P**	**P**										
FDP_ACF.1(a)	S	S	S										
FDP_ACC.1(b)							**P**						
FDP_ACF.1(b)							S						
FDP_RIP.1	**P**												
FIA_AFL.1							S	S					
FIA_ATD.1							S						

SFRs	Objectives												
	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	O.AUDIT_STORAGE.PROTE	O.AUDIT_ACCESS.AUTHORI	O.HDD.ENCRYPTION
FIA_SOS.1							S	S					
FIA_UAU.1							**P**	**P**					
FIA_UAU.7							S	S					
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S			
FIA_USB.1							**P**						
FMT_MSA.1(a)	S	S	S	**P**									
FMT_MSA.3(a)	S	S	S										
FMT_MSA.1(b)				**P**			S						
FMT_MSA.3(b)							S						
FMT_MTD.1(a)				**P**	**P**	**P**							
FMT_MTD.1(b)					**P**	**P**							
FMT_SMF.1	S	S	S	S	S	S							
FMT_SMR.1	S	S	S	S	S	S	S						
FPT_STM.1										S			
FPT_TST.1									**P**				
FPT_FDI_EXP.1								**P**					
FTA_SSL.3							**P**	**P**					
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**							

The rationale for “Table 6-13 Completeness of Security Requirements” demonstrates below.

O.DOC.NO_DIS

O.DOC.NO_DIS is the security objective to protect D.DOC from unauthorized disclosure.

FCS_CKM.1(b), FCS_CKM.1(c), FCS_COP.1(b), and FCS_COP.1(c) support the objective by requiring the TOE to provide key management and cryptographic functions to protect management interactions during network transmission.

FIA_UID.1 identifies users. FDP_ACC.1 (a) and FDP_ACF.1 (a) allow the authorized users only to operate D.DOC.

Regarding D.DOC as residual data, any previous information cannot be used by FDP_RIP.1.
FMT_MSA.1 (a) manages operations on the security attributes.
FMT_MSA.3 (a) surely sets owner information of D.DOC, an owner of a box storing D.DOC, or appropriate default value for a box permission, when D.DOC is generated.
FMT_SMR.1 assigns and maintains user authorization of U.ADMINISTRATOR and U.NORMAL.
FMT_SMF.1 provides U.NORMAL who are owners of U.ADMINISTRATOR and D.DOC with the security management functions.
By FTP_ITC.1, D.DOC in transit over the network between the TOE and other trusted IT products are protected from alteration and disclosure.
Therefore, O.DOC.NO_DIS ensures the protection of D.DOC from unauthorized disclosure.

O.DOC.NO_ALT
O.DOC.NO_ALT is the security objective to protect D.DOC from unauthorized alteration.
FCS_CKM.1(b), FCS_CKM.1(c), FCS_COP.1(b), and FCS_COP.1(c) support the objective by requiring the TOE to provide key management and cryptographic functions to protect management interactions during network transmission.
FIA_UID.1 identifies users. FDP_ACC.1 (a) and FDP_ACF.1 (a) allow the authorized users only to perform operations on D.DOC.
FMT_MSA.1 (a) manages operations on the security attributes.
FMT_MSA.3 (a) surely sets owner information of D.DOC, an owner of a box storing D.DOC, or appropriate default value for a box permission, when D.DOC is generated.
FMT_SMR.1 assigns and maintains user authorization of U.ADMINISTRATOR and U.NORMAL.
FMT_SMF.1 provides U.NORMAL who are owners of U.ADMINISTRATOR and D.DOC with the security management functions.
By FTP_ITC.1, D.DOC in transit over the network between the TOE and other trusted IT products are protected from alteration and disclosure.
Therefore, O.DOC.NO_ALT ensures the protection of D.DOC from unauthorized alteration.

O.FUNC.NO_ALT
O.FUNC.NO_ALT is the security objective to protect D.FUNC from unauthorized alteration.
FCS_CKM.1(b), FCS_CKM.1(c), FCS_COP.1(b), and FCS_COP.1(c) support the objective by requiring the TOE to provide key management and cryptographic functions to protect management interactions during network transmission.
FIA_UID.1 identifies users. FDP_ACC.1 (a) and FDP_ACF.1 (a) allow the authorized users only to operate D.FUNC.
FMT_MSA.1 (a) manages operations on the security attributes.
FMT_MSA.3 (a) ensures that owner information of D.FUNC have appropriate default value, when D.FUNC is generated.
FMT_SMR.1 assigns and maintains user authorization of U.ADMINISTRATOR and U.NORMAL.
FMT_SMF.1 provides U.NORMAL who are owners of U.ADMINISTRATOR and D.FUNC with the

security management functions.

D.FUNC in transit over the network between the TOE and other trusted IT products are protected from alteration and disclosure by FTP_ITC.1.

Therefore, O.FUNC.NO_ALT ensures the protection of D.FUNC from unauthorized alteration.

O.PROT.NO_ALT

O.PROT.NO_ALT is the security objective to protect D.PROT from unauthorized alteration.

FCS_CKM.1(b), FCS_CKM.1(c), FCS_COP.1(b), and FCS_COP.1(c) support the objective by requiring the TOE to provide key management and cryptographic functions to protect management interactions during network transmission.

FIA_UID.1 identifies users and allows the authorized users only to operate D.PROT.

FMT_MTD.1(a), FMT_MSA.1(a) and FMT_MSA.1(b) restricts U.ADMINISTRATOR to perform operations of the TSF data.

FMT_SMR.1 assigns and maintains user authorization of U.ADMINISTRATOR and U.NORMAL.

FMT_SMF.1 provides U.NORMAL who are owners of U.ADMINISTRATOR and D.FUNC with the security management functions.

By FTP_ITC.1, D.PROT in transit over the network between the TOE and other trusted IT products are protected from alteration and disclosure by FTP_ITC.1.

Therefore, O.PROT.NO_ALT ensures the protection of D.PROT from unauthorized alteration.

O.CONF.NO_DIS and O.CONF.NO_ALT

O.CONF.NO.DIS and O.CONF.NO_ALT are the security objectives to protect D.CONF from unauthorized disclosure and alteration.

FCS_CKM.1(b), FCS_CKM.1(c), FCS_COP.1(b), and FCS_COP.1(c) support the objective by requiring the TOE to provide key management and cryptographic functions to protect management interactions during network transmission.

FAU_SAR.1 and FAU_SAR.2 restricts performing read operation of the TSF Data(Audit logs) to U.ADMINISTRATOR.

FAU_STG.1 protects TSF Data(Audit logs) from unauthorized deletion and alteration.

FAU_STG.4 protects TSF Data(Audit logs) from possible loss if the audit log is full.

FIA_UID.1 identifies users and allows the authorized users only to operate D.PROT.

FMT_MTD.1 (a) restricts U.ADMINISTRATOR and Nobody to operate the TSF data.

FMT_MTD.1 (b) restricts U.NORMAL who are owners of D.CONF to operate the TSF data.

FMT_SMR.1 maintains user authorization of U.ADMINISTRATOR, U.NORMAL and Nobody, and assigns user authorization of U.ADMINISTRATOR and U.NORMAL to the users.

FMT_SMF.1 provides U.NORMAL who are owners of U.ADMINISTRATOR and D.CONF with the security management functions.

FTP_ITC.1 protects D.CONF in transit over the network between the TOE and other trusted IT product from modification and disclosure.

Therefore, O.CONF.NO.DIS and O.CONF.NO_ALT ensure protection of D.CONF from

unauthorized disclosure and alteration.

O.USER.AUTHORIZED

O.USER.AUTHORIZED is the security objective to ensure that the TOE requires identification and authentication of users, and access privilege is given to users before the users are allowed to use the TOE.

FIA_UID.1 and FIA_UAU.1 implement identification and authentication of users.

FIA_UAU.7 protects authentication feedback to users.

FIA_AFL.1 lockouts user login when users consecutively fail their authentication.

FIA_ATD.1 maintains user attributes of login user name, user authorization and job authorization setting.

FIA_SOS.1 verifies if the secret of user authentication meet the defined quality metrics.

FIA_USB.1 binds user attributes of login user name, user authorization and job authorization setting to the subject security attributes.

FTA_SSL.3 manages user session and terminates out of session.

FDP_ACC.1 (b) and FDP_ACF (b) allow authorized users only to operate basic functions.

FMT_MSA.1 (b) manages operation on the security attributes.

FMT_MSA.3 (b) ensures that executable attributes that are the security attributes have appropriate default values.

FMT_SMR.1 maintains that user authorization of U.ADMINISTRATION and U.NORMAL are assigned to the users.

Therefore, O.USER.AUTHORIZED ensures that the TOE requires identification and authentication of users, and access privilege is given to users before users are allowed to user the TOE.

O.INTERFACE.MANAGED

O.INTERFACE.MANAGED is the security objective to ensure that the TOE manages the operation of external interfaces according to the security policies.

FIA_UID.1 and FIA_UAU.1 implement identification and authentication of users.

FIA_UAU.7 protects authentication feedback to users.

FIA_AFL.1 lockouts user login when users consecutively fail their authentication.

FIA_SOS.1 verifies if the secrete of user authentication meet the defined quality metrics.

FTA_SSL3 manages user session and terminates out of session.

FPT_FDI_EXP.1 protects forwarding of data to internal network.

Therefore, O.INTERFACE.MANAGED can manage the operation of external interfaces.

O.SOFTWARE.VERIFIED

O.SOFTWARE.VERIFIED is the security objective to provide self-verification of the TSF executable code.

FPT_TST.1 runs a suite of self-test during the TOE start-up, and verifies the integrity of parts of

TSF data and verifies the integrity of parts of TSF by operating at arbitrary timing after the start-up.
Therefore, O.SOFTWARE.VERIFIED can provide authorized users with the procedure for self-verification of the TSF executable code.

O.AUDIT.LOGGED
O.AUDIT.LOGGED is the security objective to record and manage usage of the TOE and the security events, and prevent unauthorized disclosure and alteration.
FAU_GEN.1 records the audit log of the events, which should be auditable.
By associating FAU_GEN.2 with FIA_UID.1, the auditable events are associated with identification information of users.
FPT_STM.1 provides a trusted time stamp function inside the TOE, and records the times when auditable events occurred.
Therefore, O.AUDIT.LOGGED records and manages usage of the TOE and the security auditable events, and ensures the prevention of unauthorized disclosure and alteration.

O.AUDIT_STORAGE.PROTECTED
O.AUDIT_STORAGE.PROTECTED is the security objective to protect the audit logs from unauthorized access, deletion and alteration.
FAU_STG.1 protects the stored audit logs from unauthorized deletion and alteration.
FAU_STG.4 overwrites the oldest stored audit logs, and stores new audit logs when the number of audit logs reach threshold.
Therefore, O.AUDIT_STORAGE.PROTECTED ensures the protection of the audit logs from unauthorized access, deletion and alteration.

O.AUDIT_ACCESS.AUTHORIZED
O.AUDIT_ACCESS.AUTHORIZED is the security objective to allow the authorized users only to access the audit log to detect potential security violation.
FAU_SAR.1 provides U.ADMINISTRATOR with the capability to read information from the audit logs.
FAU_SAR.2 restricts access to the audit logs, except U.ADMINISTRATOR.
Therefore, O.AUDIT_ACCESS.AUTHORIZED ensures that authorized users only access the audit logs to detect potential security violation.

O.HDD.ENCRYPTION
O.HDD.ENCRYPTION is the security objective to encrypt User Data and TSF Data stored in HDD inside the TOE.
FCS_CKM.1(a) generates encryption keys in accordance with a specified encryption algorithm.
FCS_COP.1(a) encrypts D.DOC, D.FUNC, D.PROT and D.CONF when storing in the HDD using a specified encryption algorithm and encryption key length, and decrypts D.DOC, D.FUNC,

D.PROT and D.CONF when reading out from the HDD.
Therefore, O.HDD.ENCRYPTION ensures the encryption of User Data and TSF Data when storing in HDD.

6.3.2. Dependency Relationship of the TOE Security Functional Requirements

Table 6-14 shows the dependency relationship of the TOE security functional requirements.

Table 6-14 Dependency Relationship of the TOE Security Functional Requirements

Functional Requirements	Dependency Relationship	Dependencies Not Satisfied
FAU_GEN.1	FPT_STM.1	_
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	_
FAU_SAR.1	FAU_GEN.1	_
FAU_SAR.2	FAU_SAR.1	_
FAU_STG.1	FAU_GEN.1	_
FAU_STG.4	FAU_STG.1	_
FCS_CKM.1(a)	FCS_COP.1(a) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_CKM.1(b)	FCS_COP.1(b) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_CKM.1(c)	FCS_COP.1(c) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_COP.1(a)	FCS_CKM.1(a) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_COP.1(b)	FCS_CKM.1(b) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_COP.1(c)	FCS_CKM.1(c) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1

FDP_ACC.1(a)	FDP_ACF.1(a)	_
FDP_ACF.1(a)	FDP_ACC.1(a) FMT_MSA.3(a)	_
FDP_ACC.1(b)	FDP_ACF.1(b)	_
FDP_ACF.1(b)	FDP_ACC.1(b) FMT_MSA.3(b)	_
FDP_RIP.1	No dependencies.	_
FIA_AFL.1	FIA_UAU.1	_
FIA_ATD.1	No dependencies.	_
FIA_SOS.1	No dependencies.	_
FIA_UAU.1	FIA_UID.1	_
FIA_UAU.7	FIA_UAU.1	_
FIA_UID.1	No dependencies.	_
FIA_USB.1	FIA_ATD.1	_
FMT_MSA.1(a)	FDP_ACC.1(a) FMT_SMF.1 FMT_SMR.1	_
FMT_MSA.3(a)	FMT_MSA.1(a) FMT_SMR.1	_
FMT_MSA.1(b)	FDP_ACC.1(b) FMT_SMF.1 FMT_SMR.1	_
FMT_MSA.3(b)	FMT_MSA.1(b) FMT_SMR.1	_
FMT_MTD.1(a)	FMT_SMF.1 FMT_SMR.1	_
FMT_MTD.1(b)	FMT_SMF.1 FMT_SMR.1	_

FMT_SMF.1	No dependencies.	_
FMT_SMR.1	FIA_UID.1	_
FPT_STM.1	No dependencies.	_
FPT_TST.1	No dependencies.	_
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	_
FTA_SSL.3	No dependencies.	_
FTP_ITC.1	No dependencies.	_

6.3.2.1. Rationale for why dependency on FCS_CKM.4 is not needed.

The encryption key to encrypt HDD is generated with a unique value only per device every time main power is turned on, and is stored in the volatile memory. However, the TOE is physically protected by security objectives in operational environment, that is OE.PHYSICAL.MANAGED, even when the main power is turn off. Therefore the requirement for the encryption key destruction is not needed.

The symmetric session key generated during the handshake by the client, used to encrypt application data exchanged in the TLS session, is not persistently stored by either the client or the server. This session key is held in memory and is only valid for that given session. Once the session is terminated the key cannot be used to decrypt subsequent sessions. The attack potential required attempting to extract the key from the client memory following session termination to decrypt traffic captured between the client and server is significantly beyond the attack potential of EAL2. Therefore the requirement for the encryption key destruction is not needed.

The pre-shared key authentication method is used for the authentication of the IP-Sec peer. The pre-shared key is set by Device Administrator and not generated and destructed by the device. The symmetric encryption communication key obtained by DH IKEv1 Key Derivation Function is not persistently stored by each peers. This key is held in memory and is only valid with the corresponding Security Association. Once the SA is terminated the key cannot be used. Therefore the requirement for the encryption key destruction is not needed.

6.3.3. Security Assurance Requirements Rationale

This TOE is Hardcopy Devices used in commercial information processing environments that require a moderate level of document security, network security, and security assurance. The TOE will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE. Agents have limited or no means of infiltrating the TOE with code to effect a change and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.

EAL 2 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

7. TOE Summary Specification

This section describes the summary specification for the security functions that are provided by the TOE.

Table 7-1 shows the relations between the TOE security functions and security functional requirements

Table 7-1 TOE security functions and security functional requirements

Security Functions / Functional Requirements	TSF.USER_AUTHENTICATION	TSF.DATA_ACCESS	TSF.JOB_AUTHORIZED	TSF.HDD_ENCRYPTION	TSF.DOC_OVERWRITE	TSF.AUDIT_LOGGED	TSF.SECURITY_MANAGEMENT	TSF.SELF_TEST	TSF.NETWORK_PROTECTION
FAU_GEN.1						✓			
FAU_GEN.2						✓			
FAU_SAR.1						✓			
FAU_SAR.2						✓			
FAU_STG.1						✓			
FAU_STG.4						✓			
FCS_CKM.1(a)				✓					
FCS_CKM.1(b)									✓
FCS_CKM.1(c)									✓
FCS_COP.1(a)				✓					
FCS_COP.1(b)									✓
FCS_COP.1(c)									✓
FDP_ACC.1(a)		✓							
FDP_ACF.1(a)		✓							
FDP_ACC.1(b)			✓						
FDP_ACF.1(b)			✓						
FDP_RIP.1					✓				
FIA_AFL.1	✓								
FIA_ATD.1	✓								

FIA_SOS.1	✓								
FIA_UAU.1	✓								
FIA_UAU.7	✓								
FIA_UID.1	✓								
FIA_USB.1	✓								
FMT_MSA.1(a)							✓		
FMT_MSA.3(a)		✓							
FMT_MSA.1(b)							✓		
FMT_MSA.3(b)			✓						
FMT_MTD.1(a)							✓		
FMT_MTD.1(b)							✓		
FMT_SMF.1							✓		
FMT_SMR.1							✓		
FPT_STM.1						✓			
FPT_TST.1								✓	
FPT_FDI_EXP.1									✓
FTA_SSL.3	✓								
FTP_ITC.1									✓

7.1. User Management Function

TSF.USER_AUTHENTICATION

User management function is a function that identifies and authenticates whether persons are authorized users when users intend to operate the TOE from the operation panel or the client PCs.

When the TOE is used from the Operation Panel or a Web browser, the login screen is displayed and a user is required to enter his or her login user name and login password.

When the TOE is accessed from the printer driver or TWAIN driver, the TOE identifies and authenticates if the person is authorized by referring to the login user name and login user password obtained from a user job.

(1) FIA_UID.1 Timing of identification

When a user intends to login to the TOE, the TOE verifies if the entered login user name exists in the user information pre-registered in the TOE.

With reception of the device status, the TOE provides information before the user is identified. With a list of user jobs and counter information, the TOE displays the information before the user is identified. With fax data reception, the TOE receives fax data before the user is identified.

(2) FIA_UAU.1 Timing of authentication

When the user is successfully identified by FIA_UID.1, the TOE verifies if the entered login user password matches with one pre-registered in the TOE.

With reception of the device status, the TOE provides information before the user is authenticated. With a list of user jobs and counter information, the TOE displays the information before the user is authenticated. With fax data reception, the TOE receives fax data, before the user is authenticated.

(3) FIA_UAU.7 Protected authentication feedback

The TOE displays login user password entered from the operation panel or a client PC on the login screen, which is masked by dummy characters (*: asterisk).

(4) FIA_ATD.1 User attribute definition

The TOE defines and maintains user attributes such as login user name, user authorization and job authorization setting.

(5) FIA_SOS.1 Verification of secrets

The TOE verifies that a login user password meets specified quality metrics such as password length: no fewer than the minimum number of characters (8 characters), character and types: Alphanumeric or special characters.

(6) FIA_USB.1 User-subject biding

The TOE associates user attributes such as login user name, user authorization and job authorization setting with subjects.

(7) FIA_AFL.1 Authentication failure handling

When the number of consecutive unsuccessful login attempts from the operation panel or a client PC since the last successful authentication, reaches the threshold, the TOE does not allow the users to access to the accounts (i.e. state changes to lockout condition).

The number of unsuccessful authentication attempts set by the device administrator can be within 1 to 10 times.

After changing to lockout state, If time between 1 and 60 minutes and until the lockout time designated by a device administrator that elapse, or until a device administrator releases lockout state, the TOE is then back to the normal state.

(8) FTA_SSL.3 TSF-initiated termination

The auto-logout is activated if no operation is performed from the operation panel or a web browser for certain period of time.

*There are no interactive session exists with the exception of an operation panel and a web browser.

- Operation Panel
  After the user logs on to the TOE and if no operation is performed while the auto-logout time set by the device administrator elapses, the auto-logout is activated. The time can be set to 5 to 495 seconds by the device administrator.
- Web browser
  After the user logs on to the TOE and if no operation is performed for 10 minutes, the auto-logout is activated.

7.2. Data Access Control Function

TSF.DATA_ACCESS

The data access control function is a function that allows authorized users only to access to image data and job data stored in the TOE using each of the TOE basic function such as copy, scan to send, print, fax and box function.

(1) FDP_ACC.1(a) Subset access control
FDP_ACF.1(a) Security attribute based access control

The TOE allows authorized users only to access to image data and job data handled by respective basic functions in accordance with the access control rules for users as shown in Table 7-2.

In Table 7-2 Access Control Rules, login user names and owner information of targeted assets need to be matched in order to determine if the jobs are executed by themselves.

Table 7-2 Access Control Rules for Data Access Control Functions

Targeted Assets	Operations	Users	Access Control Rules
Image Data (Print Function)	Box Print (Job after print request from a printer driver), Print from a USB memory, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
	Delete	Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Scan to Send Function)	FTP Send, E-mail Send, TWAIN Send, Preview send image, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
	Delete	Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Copy Function)	Copy Print, Copy preview image, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
	Delete	Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Fax Send Function)	FAX Send, Send preview image, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
	Delete	Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Box Function)	Box print, Box preview, Box Send, Move, Join and Delete documents inside a box	Normal User	It is allowed for a normal user to access to image data stored in their own box set as an owner or a box permission to be enabled.
		Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Fax Reception Function)	Print FAX reception, FAX forward, Delete	Device Administrator	It is allowed for a device administrator to access to image data stored in FAX box.

Job Data	Job status confirmation, Edit, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
		Device Administrator	It is allowed for a device administrator to access to all job image data.

(2) FMT_MSA.3(a) Static attribute initialization

The TOE sets default values for image data that is initially generated, and a box. Owner information is created using a login user name of the user who initially creates the image data. Box owner is a device administrator who initially creates the box, and the box permission is disabled.

7.3. Job Authorization Function

TSF.JOB_AUTHORIZED

The job authorization function is a function that allows authorized users only to use the TOE basic function such as copy, scan to send, print, fax and box function.

(1) FDP_ACC.1(b) Subset access control

FDP_ACF.1(b) Security attribute-based access control

Table 7-3 shows that the TOE confirms job authorization setting included in user information of a user who is identified and authenticated by user management function, and allows the user to execute a job by using the authorized basic functions only.

Table 7-3 Access Control Rules for Job Authorization Function

Targeted Function	Users	Access Control Rules
Copy Function	Normal User Device Administrator	When executable attributes of targeted functions are included in job authorization setting of a user, TOE allows the user to execute a job.
Print Function	Normal User Device Administrator	When executable attributes of targeted functions are included in job authorization setting of a user, TOE allows the user to execute a job.
Scan to Send Function	Normal User Device Administrator	When executable attributes of targeted functions are included in job authorization setting of a user, TOE allows the user to execute a job.
FAX Function	Normal User Device Administrator	When executable attributes of targeted functions are included in job authorization setting of a user, TOE allows the user to execute a job.
Box Function	Normal User Device Administrator	When executable attributes of targeted functions are included in job authorization setting of a user, TOE allows the user to execute a job.

(2) FMT_MSA.3(b) Static attribute initialization

Table 7-3 shows that the TOE sets default values for job executable attributes that are targeted functions of job authorization setting on a per user basis. When a user is newly added, default values for executable attributes that are included in job authorization setting, have been set for all jobs.

7.4. HDD Encryption Function

TSF.HDD_ENCRYPTION

Once the basic function of the TOE is executed, image data, job data and TSF data is stored on the HDD. The HDD encryption function is a function that encrypts data and then stores the data on the HDD when storing these data on the HDD.

(1) FCS_CKM.1(a) Cryptographic key generation (Storage Encryption)

The TOE generates a 256 bits encryption key to be used in the AES algorithm by using the encryption key generation algorithm in accordance with FIPS PUB 180-4. This encryption key is generated from multiple information including the encryption code which users register and a unique value on a per device basis, every time each TOE is powered on, and this encryption key is stored in a volatile memory. The encryption code is set only at the

activation of Data Encryption/Overwrite function and is not changed during the operation.

(2) FCS_COP.1(a) Cryptographic operation (Storage Encryption)
When storing data on the HDD, the TOE encrypts the data, using the 256 bits encryption key generated at the time of booting (FCS_CKM.1(a)) and the AES encryption algorithm based on FIPS PUB 197, and write into the HDD. When reading out the stored data from the HDD, the TOE decrypts the data, similarly using the 256 bits encryption key generated at the time of booting and the AES encryption algorithm.

7.5. Overwrite-Erase Function

TSF.DOC_OVERWRITE

After process of the respective basic functions is complete, the TOE instructs to delete used image data on the HDD or flash memory. The overwrite-erase function is a function that overwrites the actual image data with meaningless character strings so that it disables re-usage of the data when receiving an instruction for deletion of the stored image data on the HDD.

(1) FDP_RIP.1 Subset residual information protection
The TOE stores the used image data to be overwritten and erased in the specific area on the HDD and flash memory, and then conducts to overwrite and erase by the process of auditing of the specific area. When receiving an instruction for operation of another basic function and so when waiting for the overwrite-erase function to be performed, or when the existence of the used image data is found because of turning off the power during overwrite-erase processing, the overwrite-erase is conducted by the audit process at the time of coming out of the waiting status or at the time of turning on the power.

7.6. Audit Log Function

TSF.AUDIT_LOGGED

The audit log function is a function that generates, records and manages audit logs when occurring auditable events.

(1) FAU_GEN.1 Audit data generation
The TOE records audit data as listed in Table 7-4, and generates audit logs when auditable events shown in Table 7-4 occur.

Table 7-4 Auditable Events and Audit Data

Auditable Events	Audit Data	Additional Audit Data
Power-on*1	Date and time of the event, Type of event, Identification information of the user (Including the identification information of the user who attempted to login), The outcome of the event (success or failure)	–
Power-off*1		–
Completion of a job		Identification information of the event
Operation of job data (read, modify, delete)		Identification information of the event
Success and failure of the user identification and authentication		–
Execution of user lockout and release of lockout status by a device administrator when the number of consecutive unsuccessful authentication attempts since the last successful authentication, reaches the threshold.		–
Session termination by auto-logout		–
Operation of image data (read, delete)		Identification information of the event
Edit of user management information (Modify user authorization)		–
When registration of login user password is made, deny by quality check (create, edit)		
Use of security management function		–
Change of time		–
Communication failure of TLS or IPsec communication		Recipient's communication IP address

*1 Start-up and shutdown of the audit functions synchronize power-on and power-off of the TOE, and thus power-on and power-off of the TOE of the event can be substituted.

(2) FAU_GEN.2 User identity association
For each auditable event, the TOE associates the user identity information that is a cause, with the audit log.

(3) FAU_SAR.1 Audit review
FAU_SAR.2 Restricted audit review
The TOE provides device administrators only with the capability to read information from the audit records. Read-access to the audit records is sent (by email) to the email destination set by a device administrator.

(4) FAU_STG.1 Protected audit trail storage
The TOE provides device administrators only with capability to read and delete information from the audit records, and does not provide normal users other than device administrators with a function to access to the audit records.

(5) FAU_STG.4 Prevention of audit data loss
The TOE overwrites the oldest stored audit records and records new auditable events if the audit log files are full.

(6) FPT_STM.1 Reliable time stamps
The TOE has a system clock inside itself. The TOE records a date and time of the event with the system clock when auditable events occur. The TOE provides a highly reliable time stamp by recording the time stamps on audit records without delay when the time is recorded by the system clock inside the TOE.

7.7. Security Management Function

TSF.SECURITY_MANAGEMENT

Security management function is a function that allows authorized users only to edit user information, set the TOE security functions and manage. The Security management function can be performed from the Operation Panel and Client PCs. Web browser is used for operation from Client PCs.

(1) FMT_MSA.1(a) Management of security attributes
The TOE allows device administrators only to use box functions for all boxes as shown below.

- Read and modify a box owner
- Read and modify a box permission

Whereas, the TOE allows device administrators only to use box functions for documents as shown below.

- Read and modify document owner information

Normal users are allowed to perform the following operation on the self owner boxes.

- Read and modify a box permission

(2) FMT_MSA.1(b) Management of security attributes
No roles of executable attributes as shown in Table 7-3 are available for the TOE.

(3) FMT_MTD.1(a) Management of TSF Data
The TOE provides device administrators only with the operation listed in Table 7-5 on TSF data listed in Table 7-5.

Table 7-5 Operation of TSF Data by Device Administrators

TSF Data	Authorized Operation
Register user information (Login user name, login user password, user authorization, job authorization settings)	Edit, Delete, Newly create
User account lockout policy settings (number of retries until locked, lockout duration)	Modify
Lockout list	Modify
Auto logout time setting	Modify
Password policy settings	Modify
Date and time settings	Modify
Network Encryption Setting	Modify
FAX forward setting	Modify
Send destination information for forwarding audit log report	Modify

(4) FMT_MTD.1(b) Management of TSF Data
The TOE provides normal users with the operation listed in Table 7-6 on TSF data listed in Table 7-6.

Table 7-6 Operation of TSF Data by Normal Users

TSF Data	Authorized Operation
Edit user information (Login user password associated to the users)	Edit

(5) FMT_SMR.1 Security roles
The TOE maintains the user authorizations of device administrators and normal users, and associates users to the user authorizations.

(6) FMT_SMF.1 Specification of management function
The TOE provides management function of security attributes for box functions as mentioned in (1), and security management function shown in Table 7-5 and Table 7-6 on TSF data shown in Table 7-5 and Table 7-6.

7.8. Self-Test Function

TSF.SELF_TEST

The self-test function is a function that performs the following self-test.

(1) FPT_TST.1 TSF test
The TOE performs the following self-test.

- Check if HDD encryption function is correctly performed.
- Check the integrity of the encryption key
- Check the integrity of executable module of the security function

At the TOE start-up, the TOE simultaneously checks if HDD encryption function is correctly performed and the integrity of the encryption key is verified by confirming encryption and decryption operations using the encryption key. Also, the TOE checks the integrity of executable module of the security functions when receiving an instruction from a device administrator.

In case abnormal operation is found by check at the TOE start-up, the users are notified of this abnormal status by displaying it on the Operation Panel of the TOE. If no abnormal item is found on the Operation Panel, the users assume the TOE correctly operates and so the users can use the TOE.

7.9. Network Protection Function

TSF.NETWORK_PROTECT

The network protection function is a function that encrypts all data in transit over the network

between the TOE and trusted IT product and prevents unauthorized alteration and disclosure. This function also provides a feature to prevent forwarding of information from an external interface to an internal network through TOE without permission.

(1) FTP_ITC.1 Trusted channel between TSF

When the TOE communicates with each type of server or a Client PC that are trusted IT products, communication starts between them via a trusted channel. This communication can start from either of the TOE or the trusted IT product. The following functions are provided.

- Scan to send function
- Print function
- Box function (Send Function)
- Operation of a box function from a client PC (web browser)
- Operation of security management function from a client PC (web browser)

However, use of print function for a direct connection with the TOE is exception.

The TOE provides trusted channel communications listed below.

Table 7-7 Trusted channel communications provided by the TOE

Destination	Protocols	Encryption algorithm
Client PC	TLSv1.2	AES(128 bits, 256 bits)
Mail Server	IPsec with ESP	3DES(168 bits), AES(128 bits, 192 bits, 256 bits)
FTP Server	IPsec with ESP	3DES(168 bits), AES(128 bits, 192 bits, 256 bits)

(2) FCS_CKM.1(b) Cryptographic key generation (TLS)

Secure Communications requires generation of a certificate with an RSA public-private key pair.

The TOE creates session keys following the TLS protocol specification and using the DRBG implemented in OpenSSL.

(3) FCS_CKM.1(c) Cryptographic key generation (IPSec)

ISAKMP and IKEv1 are used to establish the Security Association (SA) and keys for the IPSec exchanges.

(4) FCS_COP.1(b) Cryptographic operation (TLS)

TLS 1.2 (RFC5246) is used to establish secure channel between client PCs and TOE. The TOE sends the server certificate chain to the client. The client performs certificate path validation of the server certificate during the TLS handshake. If the certificate cannot be

successfully validated (e.g. it has expired or has been revoked) the TLS session is not established.

The TOE only allows the establishment of a TLS secure channel using TLSv1.2. The TOE denies any attempt by a TLS client to establish communication using the following versions of the SSL or TLS protocols: SSLv1.0, SSLv2.0, SSLv3.0, TLSv1.0 or TLSv1.1. The TOE creates session keys following the TLS protocol specification and using the DRBG implemented in OpenSSL. This session key is held in memory and is only valid for that given session. Once the session is terminated the key cannot be used to decrypt subsequent sessions. The TOE supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (RFC5289)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (RFC5289)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (RFC5289)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (RFC5289)
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (RFC5288)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (RFC5288)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (RFC5288)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (RFC5288)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (RFC5246)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (RFC5246)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (RFC5246)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (RFC5246)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (RFC5246)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (RFC5246)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (RFC5246)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (RFC5246)
- TLS_RSA_WITH_AES_256_CBC_SHA (RFC5246)
- TLS_RSA_WITH_AES_128_CBC_SHA (RFC5246)

(5) FCS_COP.1(c) Cryptographic operation (IPSec)

IPSec with ESP is required for network datagram exchanges with Mail Server/FTP Server. IPSec provide confidentiality, integrity and authentication of the endpoints. Supported encryption options for ESP are 3DES and AES. HMAC-SHA256-128, HMAC-SHA384-192, and HMAC-SHA512-256 are supported for Data authentication.

ISAKMP and IKEv1 are used to establish the Security Association (SA) and keys for the IPSec exchanges. Diffie-Hellman is used for IKEv1 Key Derivation Function as specified in RFC2409, using Oakley Groups 14, 16, 17, 18, 19, 20, 21, 22, 23, or 24. In the ISAKMP exchange, a pre-shared keys is configured by administrators and validated between endpoints.

The key size specified in the SA exchange is 128, 192, or 256 bits and the encryption algorithm is 3DES or AES-CBC and the Hash Authentication Algorithm may be SHA-256,

SHA-384, or SHA-512 (as configured by administrators).
Keys generated for the IKEv1 exchanges are performed per RFC2409. If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded. All keys are held in memory and is only valid with the corresponding SA. Once the SA is terminated the key cannot be used.

(6) FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces
The TOE does not have a structure that forwards information entered and data received from all external interfaces to a server or a client PC directly on an internal network, and controls not to be able to forward the information and data without permission.
Also, data received via a telephone line is limited to use fax function only. The TOE has a structure that receives data via fax communication protocol only. Thus forwarding of data to an internal network without permissions cannot be done.

7.10. Deviations From Allowed Cryptographic Standards
The following deviations from the Allowed Cryptographic Standards in 188 Scheme Crypto Policy are noted:

1. Hashing: SHA-1 is supported for backward compatibility with remote systems.

8. Acronyms and Terminology

8.1. Definition of terms

The definitions of the terms used in this ST are indicated in Table 8-1.

Table 8-1 Definitions of terms used in this ST

Terms	Definitions
FAX System 12	This is provided as an optional product of MFP to use fax function. FAX function can be used by installing FAX board separately on MFP.
TWAIN	This function is to read image from scanner and send the image to a client PC. The term, “TWAIN” indicates the API specification.
FAX Data Reception	It indicates an action that includes reception of incoming FAX data to TOE. (the process such as printing and forwarding of data is not included.)
Job	This is the operation processing unit to perform copy function, print function, scan to send function, fax function and document box function of TOE.
Job Data	This data is generated when normal users use copy function, scan to send function, print function, FAX function and box function to execute jobs. The job data is waiting in a job queue for execution. This data is deleted, once job is complete.
Job Information	It indicates information that job holds. It mainly indicates jobs in operation. However, it also indicates histories of execution results.
A list of Job Information	One that list job information.
Job Status Confirmation	This is to confirm on detailed information about job data.
Box Information	Information that is stored in an area, called “box” when using box function. For example, box name, box number, box size etc. Security attributes such as box owner and box permission are also included in this information.
Edit	An operation that modifies data registered by users, such as user information and box information.
Move	It is to move document stored in a box to another box.

Join	It is to join multiple documents stored in a box, and create a new joined document. Original documents remain.
Preview Send Image	This is one of scan to send function and FAX function operation. A function that displays image preview read from a scanner of TOE for sending on the operation panel.
Preview Copy Image	This is one of copy function operation. A function that displays image preview read from a scanner of TOE for copying on the operation panel.
Box Preview	This is one of box function operation. It is to display the preview of the document stored in a box on the operation screen.
Device Status	Information that shows TOE status. Remaining toner volume, papers and mechanical errors are displayed.
Counter Information	Information about counting jobs performed by TOE. When print function performs, print counter increases. When scan to send function performs, send counter increases.
Image Data	It indicates the image information that is processed inside the MFP when TOE normal users use copy function, scan to send function, print function, FAX function and box function.
Client PC	It indicates the computers that connect to the network, and utilize the TOE services (functions) of the TOEs that are connected to the network.
FIPS PUB 180-4	This is an algorithm about a hash function, which is standardized by the NIST, U.S.(National Institute of Standards and Technology).
FIPS PUB 197	This is an algorithm about the common cryptographic key, which is standardized by the NIST, U.S. (National Institute of Standards and Technology). Also, this is called “AES”.
Management Area	An area within the image data where management information for that data is recorded. A logical deletion of image data means making this area unrecognizable.
Actual Data Area	An area within the image data where data composing the actual image is recorded. When image data is logically deleted, this area will remain. This remaining area will be called “residue area”.

Overwrite-Erase	This is to overwrite on the actual image data area with meaningless character strings when receiving an instruction for deletion of the stored image data in the HDD, and to delete the management information of the image data after the actual data area is completely erased. Thus it disables re-usage of the data.
Operation Panel	This is installed on the uppermost part of the MFP, and is constituted by a liquid crystal panel. It is an external interface, and users can utilize the TOE via this operation panel.

8.2. Definition of acronyms

The definitions of the acronyms used in this ST are indicated in Table 8-2.

Table 8-2 Definitions of acronyms used in this ST

Acronyms	Definitions
A.	assumption (when used in hierarchical naming)
ADMIN.	administrator (when used in hierarchical naming)
AES	Advanced Encryption Standard
ALT	alteration
CC	Common Criteria
CONF.	confidential (when used in hierarchical naming)
CPY	copy
D.	data (when used in hierarchical naming)
DIS	disclosure
DOC.	document (when used in hierarchical naming)
DSR	document storage and retrieval
EAL	Evaluation Assurance Level
F.	Function (when used in hierarchical naming)
FAX	facsimile
FUNC.	function (when used in hierarchical naming)
HCD	Hardcopy Device
HDD	Hard Disk Drive
IT	information technology
MFP	Multi Functional Printer
NCU	Network Control Unit
NVS	nonvolatile storage

O.	Security Objective (of the TOE) (when used in hierarchical naming)
OE.	Security Objective (of the operational environment) (when used in hierarchical naming)
OSP	organizational security policy
P.	organizational security policy (when used in hierarchical naming)
PP	Protection Profile
PROT.	protected (when used in hierarchical naming)
PRT	print
SAR	Security Assurance Requirement
SCN	scan
SFP	Security Function Policy
SFR	Security Functional Requirement
SMI	Shared-medium Interface
SSD	Solid State Drive
ST	Security target
T.	threat (when used in hierarchical naming)
TOE	Target of Evaluation
TSF	TOE security functionality
U.	user (when used in hierarchical naming)
USB	Universal Serial Bus

(The final page)