TOSHIBA

e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A

MULTIFUNCTIONAL DIGITAL SYSTEMS
Security Target

Version 0.11

TOSHIBA e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A MULTIFUCTINAL DIGITAL SYSTEMS security target reprinted with permission from IEEE, 445 Hoes Lane, Piscataway, New Jersey 08855, from IEEE 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A, and Copyright© 2009 IEEE. All rights reserved.

— Table of Contents —

1. ST INTRODUCTION 1

1.1. Security Target Reference 1

1.2. TOE Reference 1

1.3. TOE Overview 1

1.3.1. Usage and Major Security Features of the TOE 1

1.3.2. TOE Type 2

1.3.3. Environment Assumptions 2

1.3.4. Required Non-TOE Hardware and Software 2

1.4. TOE Description 3

1.4.1. Physical Boundary 3

1.4.2. Guidance 5

1.4.3. Logical Boundary 6

1.4.3.1. General Functions 6

1.4.3.2. Security Functions 7

1.5. Entity Definitions 8

1.5.1. Users 8

1.5.2. Objects (Assets) 8

1.5.2.1. User Data 8

1.5.2.2. TSF Data 9

1.5.2.3. Functions 9

1.5.3. Operations 9

1.5.4. Channels 9

1.5.5. Terminology 10

1.6. Trademarks 11

2. CONFORMANCE CLAIM 12

2.1. CC Conformance Claim 12

2.2. PP conformance Claim, Package conformance Claim 12

2.2.1. PP conformance Claim 12

2.2.2. Package conformance Claim 12

2.3. Conformance Rationale 12

2.3.1. TOE type 12

2.3.2. ST Conformance 12

2.3.2.1. Security Problem Definition 13

2.3.2.2. Security Objectives 13

2.3.2.3. Extended Components Definitions 13

2.3.2.4. SFR Components Definitions 13

2.3.2.5. SFR Components in SFR Package Definitions 13

2.3.2.6. Conformance claim rationale 14
3. SECURITY PROBLEM DEFINITION 15
3.1. Threats agents 15
3.2. Threats to TOE Assets 15
3.3. Organizational Security Policies for the TOE 15
3.4. Assumptions 16
4. SECURITY OBJECTIVES 17
4.1. Security Objectives for the TOE 17
4.2. Security Objectives for the Operational environment 17
4.3. Security Objectives rationale 18
5. EXTENDED COMPONENTS DEFINITION 21
6. SECURITY REQUIREMENTS 23
6.1. Security Functional Requirements 23
6.1.1. Class FAU: Security audit 23
6.1.2. Class FDP: User data protection 26
6.1.3. Class FIA: Identification and authentication 30
6.1.4. Class FMT: Security management 33
6.1.5. Class FPT: Protection of the TSF 41
6.1.6. Class FTA: TOE access 42
6.2. SFR Package functions 42
6.3. SFR Package attributes 42
6.4. 2600.1-PRT SFR Package for Hardcopy Device Print Functions, Operational Environment A 42
6.5. 2600.1-SCN SFR Package for Hardcopy Device Scan Functions, Operational Environment A 43
6.6. 2600.1-CPY SFR Package for Hardcopy Device Copy Functions, Operational Environment A 43
6.7. 2600.1-DSR SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment A 43
6.8. 2600.1-SMI SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A 43
6.8.1. Class FTP: Trusted paths/channels 43
6.8.2. Class FPT: Protection of the TSF 43
6.9. Security assurance requirements 44
6.10. Security requirements rationale 45
6.10.1. Security requirements rationale 45
6.10.2. Traceability rationale 46
6.10.3. Dependencies of Security Functional Requirements 49
6.10.4. Security Assurance Requirements Rationale 50
7. TOE SUMMARY SPECIFICATION 51
Annex - Acronyms 58

－ List of Tables －

Table 1 English Guidance 5
Table 2 Japanese Guidance 5
Table 3 Users 8
Table 4 User Data 8
Table 5 TSF Data 9
Table 6 Terminology 10
Table 7 Definition of the SFR Package 13
Table 8 Relationship of SFR defined in the ST and the PP 14
Table 9 Threat to User Data for the TOE 15
Table 10 Threats to TSF Data for the TOE 15
Table 11 Organizational Security Policies for the TOE 15
Table 12 Assumptions for the TOE 16
Table 13 Security Objectives for the TOE 17
Table 14 Security Objectives for Operational environment 17
Table 15 Completeness of Security Objectives 18
Table 16 Sufficiency of Security Objectives 19
Table 17 Audit Data Requirements 23
Table 18 List of Audit Information 25
Table 19 Common Access Control SFP 27
Table 20 CPY Access Control SFP 27
Table 21 PRT Access Control SFP 27
Table 22 SCN Access Control SFP 28
Table 23 DSR Access Control SFP 28
Table 24 The TOE Function Access Control SFP 28
Table 25 Protected Authentication Feedback 31
Table 26 User Password Policy 32
Table 27 Management of Object Security Attributes 33
Table 28 Management of Subject Security Attributes 33
Table 29 Management of Subject Attributes 34
Table 30 Management of Object Attributes 34
Table 31 Characteristics Static Attribute Initialisation 35
Table 32 Static Attribute Initialisation 35
Table 33 Operation of TSF Data 36
Table 34 TSF Data 37
Table 35 Management Functions 38
Table 36 Administrative Functions 41
Table 37 SFR Package Functions 42

Table 38 SFR Package Attributes 42
Table 39 IEEE Std 2600.1 Security Assurance Requirements 44
Table 40 Completeness of Security Requirements 45
Table 41 Dependencies of Security Functional Requirements 49
Table 42 Correspondences between SFRs and TOE Security Functions 51
Table 43 Logged Event and Audit Log 52
Table 44 List of Acronyms 58

－ List of Figures －

Figure 1 Environment for the usage of the MFP 2
Figure 2 Physical Boundary 4
Figure 3 Logical Boundary 6

1. ST INTRODUCTION

The Security Target (ST) applies to complete Multifunction Peripheral (MFP) that includes the entire hardware and software components that provide the functionality for printing and scanning documents over the network, through email and on the MFP;and document storage and retrieval. The ST complies with IEEE Std 2600.1 Protection Profile for Operation Environment A.

1.1. Security Target Reference

The details are as follows:

Title	TOSHIBA e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A MULTIFUNCTIONAL DIGITAL SYSTEMS Security Target
Version	0.11
Author	TOSHIBA TEC CORPORATION
Publication Date	June 29, 2016

1.2. TOE Reference

Following are the details of the TOE Reference:

TOE Name	TOSHIBA e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A MULTIFUNCTIONAL DIGITAL SYSTEMS
TOE Version Number	SYS V1.0
Developer Name	TOSHIBA TEC CORPORATION

1.3. TOE Overview

The Security Target provides the requirements for the TOSHIBA e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A MULTIFUCTINAL DIGITAL SYSTEMS Target of Evaluation (TOE) for IEEE Std 2600.1 Protection Profile for Operational Environment A.
Operational Environment A is generally characterized as a restrictive commercial information processing environment in which a relatively high level of document security, operational accountability, and information assurance, are required. Typical information processed in this environment is trade secret, mission-critical, or subject to legal and regulatory considerations such as for privacy or governance. This environment is not intended to support life-critical or national security applications.
The Security Target provides the requirements for the Toshiba MFP Target of Evaluation (TOE) for IEEE Std2600.1 Protection Profile for Operational Environment A.

1.3.1. Usage and Major Security Features of the TOE

The TOE is mainly used to perform the following functions:

- Copy function
- Print function
- Scan function
- Internet Fax function
- e-Filing function

The TOE provides the following security features:

- User Authentication
- User Access Control
- Audit Data Generation and Review
- Secure Erase
- Secure Channel
- TSF Self Protection
- TSF Data Protection

The TOE is the MFP and implements the TOE Security Functions of User Authentication for MFP, and Device Configuration Protection. It provides Role Based Access Control (RBAC) where users can be assigned various roles and thus restricted to specific permissions on TOE assets. The TOE provides residual data protection using secure erase of user documents. In addition, it provides support for network security protocols such as TLS, IPPs and maintains an audit log where the key events are recorded and whose integrity and confidentiality are assured. The TOE also executes the integrity test and restricts TSF data management to the permitted roles.

1.3.2. TOE Type

The TOE is a Multifunction Systems that works in a network environment and provides capabilities of print, copy, and scan.

1.3.3. Environment Assumptions

The TOE is assumed to be used as an IT product at general office, user clients, and the internal network protected from threats on the external network by firewall etc.
Necessary security functions work by setting it in a high security mode at the time of setup of TOE.
For executing Secure Erase, an optional kit, GP-1070(Data Overwrite kit), is required to be purchased.

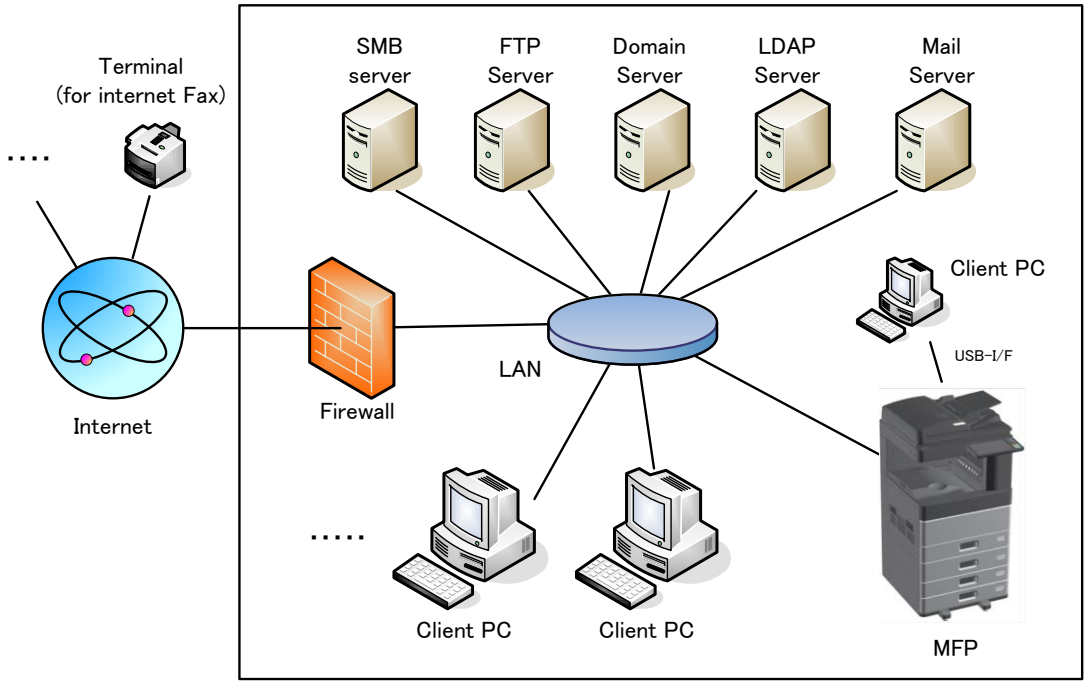


Figure 1 Environment for the usage of the MFP

1.3.4. Required Non-TOE Hardware and Software

Hardware other than the TOE and its operational environment are described below.

(1) Client PC

The Client PC can execute the following.
The U.NORMAL can request printing of document data through LAN or USB interface to the TOE, and saving and retrieving document data in e-Filing Box by which the U.NORMAL registered. The U.ADMINISTRATOR can refer to or change the setting data in the MFP using the Web browser.
The configuration of browser and Client Utility Software is as follows:

- Browsers:
  - Internet Explorer 9
- Client Utility Software:
  - TOSHIBA Universal Printer 2 (Version 7.170.3811.0)

(2) Mail Sever

The Mail Server is a server which transmits/receives email using POP/SMTP. The TOE and the Mail Server is connected with TLS communication.

(3) LDAP Server

When a TOE user is registered to and managed with the LDAP Server, user authentication is executed through the LDAP Server. Connection between the TOE and the LDAP Server must be secure by using TLS. In this document, only internal authentication is supported, and external authentication with the LDAP Server is not supported.

(4) Domain Server

It is possible to execute user authentication using the Domain Server on the network which manages the TOE user with the Windows domain. Connection between the TOE and the Domain Server must be secure by using TLS. In this document, only internal authentication is supported, and external authentication with the Domain Server is not supported.

(5) SMB Sever

The SMB Server is a server which transmits and receives files between the TOE and the Client PC using the Server Message Block Protocol. It is not guaranteed if the files are managed by being saved in the SMB server.

(6) Fire Wall

When internal network accesses the external network, the connection must be made via Fire Wall so as to prevent unauthorized access from the external network.

(7) FTP Server

The FTP Server is a server which activates the File Transfer Protocol Server Software.

(8) NTP Server

The TOE internal clock has a function to synchronize with the NTP server which is opened to the public.
It is not guaranteed if the clock in the TOE is managed by synchronizing with the NTP server.

(9) Printer Driver(Universal Printer 2)

The Printer Driver is a software which is installed to the computer to enable printing from an application. Advanced print functionalities, such as document layout and page formatting, that cannot be set with an application are supplied.

1.4. TOE Description

This section describes the physical boundary, logical boundary, and functions regarding the e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A.

1.4.1. Physical Boundary

The TOE consists of the following:

- Multifunctional Digital System

The TOE does not consist of the following:

- Client side driver modules
- External Authentication Server

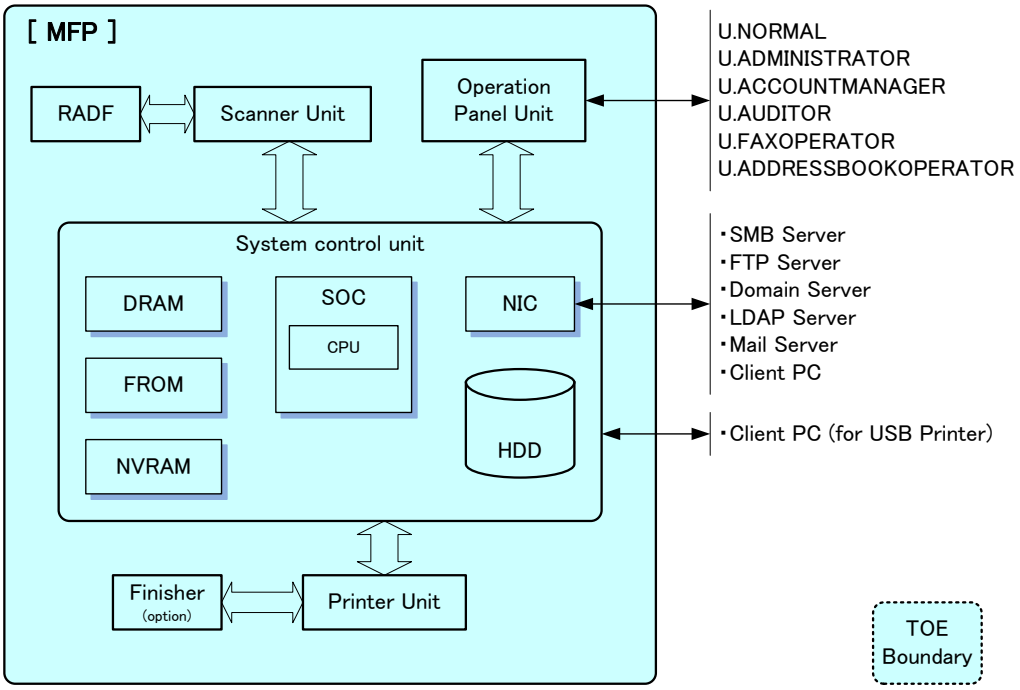


Figure 2 Physical Boundary

(1) Control Panel Unit

The Control Panel Unit is a user interface by which a U.USER operates the MFP. Hardware construction is operation buttons, LEDs, and LCD with a touch panel. Information from the MFP is displayed on the LCD and each operation such as copy start is executed by communicating with the System Control Unit.

(2) Scanner Unit

The Scanner Unit is an input device which scans paper original and transmits the image data to the System Control Unit.

(3) RADF (Reverse Auto Document Feeder)

The RADF makes the MFP scan document per page automatically or makes the MFP scan both sides of the original depending on the setting.

(4) System Control Unit

The System Control Unit is a unit which achieves each function by controlling the entire MFP.

(5) Printer Unit

The Printer Unit is a unit which receives a print request from the System Controller Unit and prints the print data on the paper.

(6) Finisher

The Finisher is a paper exit device which automatically sorts or groups papers which are printed and exited from the MFP.

(7) HDD (Hard Disk Drive)

The HDD is a general hard disk drive. Not only a part of software that controls the MFP, but also image data and document data is stored.

(8) FROM (Flash ROM)

The FROM is a nonvolatile memory. A part of software that controls the MFP is stored.

(9) NVRAM (NonVolatile RAM)

The NVRAM is a nonvolatile memory. This is a memory device which saves setup values required for controlling the MFP.

(10) SoC (System on a Chip)

SoC is a LSI in which a device controller circuit is integrated with a microprocessor at the core.

(11) DRAM (Dynamic Random Access Memory)

The DRAM is a volatile memory. This is a memory which loads and executes a program which controls the MFP.

(12) NIC (Network Interface Card)

The NIC is a device for network-connection interface. It supports 10Base-T/100Base-TX/Gigabit Ethernet.

1.4.2. Guidance

The following are the guidance documents for this TOE. However, the guidance is written in both English and Japanese.

Table 1 English Guidance

Title	Version
Quick Start Guide	OME15003700
Safety Information	OME150045A0
Copying Guide	OME150047A0
Scanning Guide	OME150053A0
e-Filing Guide	OME150055A0
MFP Management Guide	OME150061A0
Software Installation Guide	OME150059A0
Printing Guide	OME150057A0
TopAccess Guide	OME150063A0
Software Troubleshooting Guide	OME150049A0
Hardware Troubleshooting Guide	OME15004100
High Security Mode Management Guide	OME150065B0
Paper Preparation Guide	OME15003900
Specifications Guide	OME150043A0
Fax Guide	OME150067A0

Table 2 Japanese Guidance

Title	Version
かんたん操作ガイド	OMJ15003600
安全にお使いいただくために	OMJ150044A0
コピーガイド	OMJ150046A0
スキャンガイド	OMJ150052A0
ファイリングボックスガイド	OMJ150054A0
設定管理ガイド	OMJ150060A0
インストールガイド	OMJ150058A0
印刷ガイド	OMJ150056A0
TopAccessガイド	OMJ150062A0
トラブルシューティングガイド［ソフトウェア編］	OMJ150048A0
トラブルシューティングガイド[ハードウェア編]	OMJ15004000
ハイセキュリティモード管理ガイド	OMJ150064B0
用紙準備ガイド	OMJ15003800
仕様ガイド	OMJ150042A0
ファクスガイド	OMJ150066A0

1.4.3. Logical Boundary

The logical boundary of TOE is defined by the TOE security function and a general function which are described by the following section.

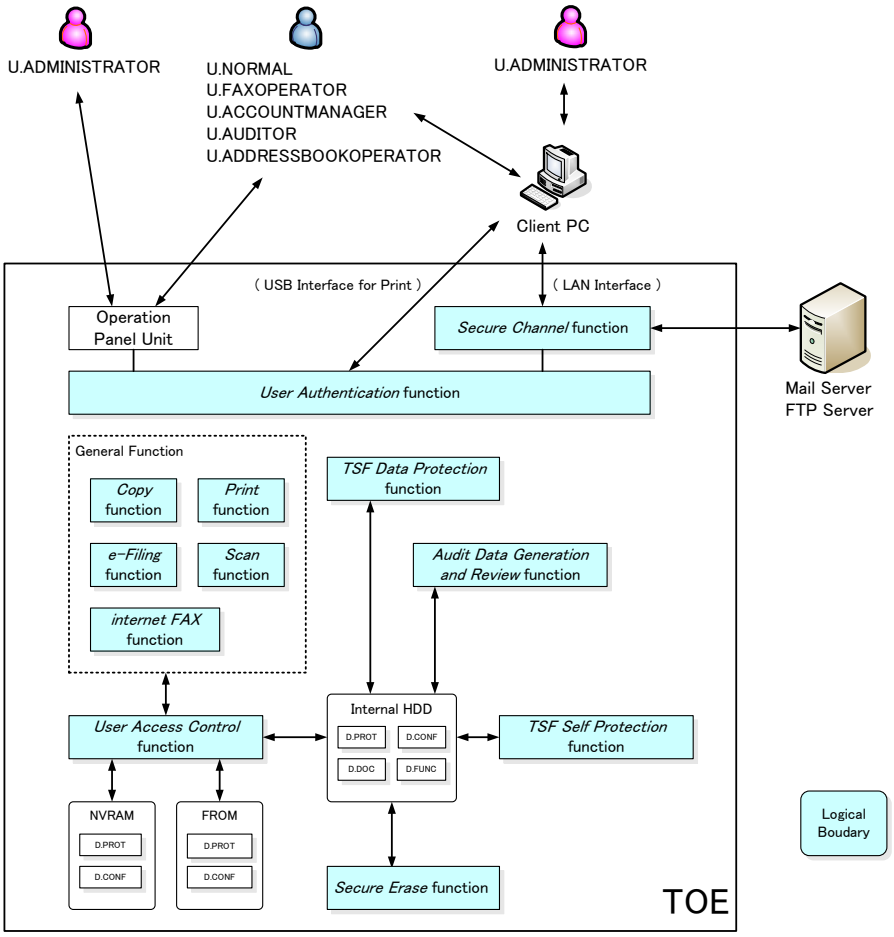


Figure 3 Logical Boundary

1.4.3.1. General Functions

In MFP, a series of function for the office work concerning the image such as copy, print and scan exists as a general function, and TOE performs the core control in the operation of these functions.

(1) Copy function

A Copy function is a function to read the original with the scanner and print it out from the printer according to the general user's operation from the control panel.

(2) Print function

A print function is a function which prints the data from the client PC through the LAN or the USB interface, and the data in the e-filing Box on a paper. In addition, the TOE prints the data which is received by the e-mail or Internet fax.

(3) Scan function

A scan function is to preserve scan data in internal HDD and to read the preserved data from HDD, and to tell it to a mail server or a FTP server automatically according to information set to MFP reading original data from the scanner unit by the general user's instruction. A general user can demand this function from the control panel.

(4) e-Filing function

The user box is an e-Filing that each user can create. It is suitable for specific users or U.ADMINISTRATOR to store confidential documents. In addition user can operate various functions to the document such as print/edit/manage, etc.

(5) Internet Fax function

Internet Fax function is a function that transmits and receives an e-mail with a file in a given format between the TOE and the other internet Fax devices or client computers through the mail server. The document data which was scanned by the TOE is attached to the e-mail and the e-mail is transmitted to the destination e-mail address. The TOE accesses the mail server so as to receive a new e-mail and a document which is attached to the e-mail.

1.4.3.2. Security Functions

The security functions provided by the TOE are as follows:

(1) User Authentication

The TOE has a protected feedback function at password entry and a lockout function for a user who failed the authentication. The TOE prompts the user to enter the User ID and password from the control panel or client PC to execute identity authentication.

(2) User Access Control

The TOE controls access to the user data and functions that are secured assets to the allowed users.

(3) Audit Data Generation and Review

The TOE generates audit logs for tracking the state of the TOE at any given instance of time. This is done by logging device events (e.g., print/scan job submission; user authentication; authorization etc.) and mapping them to users (based on local or network login) and a reliable timestamp. All logs are available for viewing only to TOE U.AUDITOR and U.ADMINISTRATOR role. The logs can be transferred in network with TLS for viewing and analysis.

(4) Secure Erase

The TOE removes residual data with DoD secure-erase mechanism before releasing resources from HDD of TOE.

(5) Secure Channel

The TOE provides support for TLS and is allowed to secure different protocols such as https. The TLS functionality also permits the TOE to be securely administered from the Web UI, as well as, being used to secure the connection between the TOE and any other external server. The TOE uses TLS to transfer the print job from the client. IPPs is an IPP print service from the printer driver using TLS. The TOE also prevents data inputted from an external interface from being directly transferred to the shared medium interface without TSF processing.

(6) TSF Self Protection

The TOE performs integrity tests on its static executables and configuration files using verification of their digital signatures against the known TOSHIBA signatures. This allows the TOE to detect any tampering of its trusted state.

(7) TSF Data Protection

Only an administrator role user has the capability to manage the configuration and enable/disable available services and protocols. U.ADMINISTRATOR can modify the TSF data.

1.5. Entity Definitions

1.5.1. Users

Users are entities that interact with the TOE and are external to the TOE. There are six types of Users: Normal Administrator, Accout manager, Auditor, Internet Fax operator, and Addressbook operator. U.ADMINISTRATOR, U.ACCOUNTMANAGER U.AUDITOR, U.FAXOPERATOR, and U.ADDRESSBOOKOPERATOR that are the users to whom management operation was permitted specially, there is reliability equivalent to "administrators" described by A.ADMIN.TRAINING and A.ADMIN.TRUST.

Table 3 Users

Designation	Definition
U.USER	Any authorized User.
U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE. A user who has the roles for CopyOperator, Print, PrintOperator, ScanOperator, Fax, e-FilingOperator, and User out of the Allocation Roles.
U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP. A user who has the Administrator Role out of the Allocation Roles or has the Built-in Administrator Account.
U.ACCOUNTMANAGER	A specially-authorized user who can control the user information. A user who has the AccountManager Role out of the Allocation Roles.
U.AUDITOR	A Special user entitled to view and data mine all MFP logs (job, event, etc.). A user who has the Auditor Role out of the Allocation Role.
U.FAXOPERATOR	A specially-authorized user who can send user documents and print received data using the Internet Fax functions. A user who has the FaxOperator Role out of the Allocation Roles.
U.ADDRESSBOOKOPERATOR	A specially-authorized user who can edit the Address Book. A user who has the AddressBookRemoteOperator Role out of the Allocation Roles.

1.5.2. Objects (Assets)

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

1.5.2.1. User Data

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

Table 4 User Data

Designation	Definition	Details
D.DOC	User Document Data consist of the information contained in a user's document. This includes the original document itself in any of hardcopy, electronic form, image data, or residually stored data created by the hardcopy device while processing an original document and printed hardcopy output.	Copy Documents data
		Print Documents data
		Scan Documents data
		e-Filing Documents data except stored in Public Folder
		Residual data after deleting Jobs
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.	Print Hold Queues
		Address Book data

1.5.2.2. TSF Data

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

Table 5 TSF Data

Designation	Definition	Details
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.	ACL Information
		Device Security Setting for system
		Hash value-acquiring code
D.CONF	TSF Confidential Data are an asset 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.	Job Log
		Message Log
		User Password

1.5.2.3. Functions

Functions perform processing, storage, and transmission of data that may be present in TOE. These functions are used by SFR Packages and are identified and defined in Chapter 6.2.

1.5.3. Operations

Operations are a specific type of actions performed by a Subject on an Object. In this Security Target, six types of operations are considered: those that result in disclosure of information (**Read**), those that result in alteration of information (**Create**, **Modify**, **Delete**), those that invoke a function (**Execute**), those that result in transfers to outside (**Export**).

1.5.4. Channels

Channels are the mechanisms through which data can be transferred into and out of the TOE. In this Security Target, four types of Channels are allowed.

(1) Private-medium Interface

The TOE has control panel and USB interfaces.

(2) Shared-medium Interface

The TOE is connected with the internal network accessed by multiple Users.

(3) Original Document Handler

Mechanisms for transferring User Document Data into the TOE in hardcopy form. It is an input channel.

(4) Hardcopy Output Handler

Mechanisms for transferring User Document Data out of the TOE in hardcopy form. It is an output channel.
In practice, at least one input channel and one output channel would be present in any TOE configuration, and at least one of those channels would be either an Original Document Handler or a Hardcopy Output Handler.

1.5.5. Terminology

Table 6 defines the meaning of certain terms.

Table 6 Terminology

Terminology	Definition
User ID	It has been given to the user identifier. TOE is used to identify the person by that identifier.
User Password	User's password to log into the TOE.
User Token	The User Token is required to use the security function (SSDK), and is generated and managed within the SSDK. The User Token is used to check access to objects.
ACL information	ACL information defines the MFP functions that are permitted for use per Permission Role.
Job Log	The job information such as Print Job, Transmission Journals, Reception Journals and Scan Job.
Hash value-acquiring code	The code which is used to acquire the Hash value from the digital signature of TSF excutable code. This data is stored in the FROM.
Message Log	Log regarding MFP's device information or operations executed by users.
Device Security Setting for system	Security settings and network settings.
TopAccess	A web-based job and device control tool. The MFP information can be retrieved by using this tool through network. e-Filing Box operation can be also performed through network.
e-Filing	The location where users save user document data. After saving data, users can refer to, print, or edit them with the control panel or the TopAccess.
e-Filing Box Password	A password to access e-Filing.
Print Hold Queue	A queue to which a print job waiting for printing is saved temporarily.
Permission	An access right to each operation which is given to the Role.
Address Book	A function which controls the email address information.
Auto logout time	Time to log out when the logged in user does not operate the MFP for a certain period of time.
Count Clear Time	Time to clear the counted number of authentication trials which fails when failed number of authentication trials does not reach the set number of times. Specified period of time is set for the count-clear time.
Allowable Number of entry for Login Password	Number of login trials permitted for failure in the specified period of time.
Locked-out Account Status	Locked-out status failing in user authentication.
Lockout Time	Time until the locked out account is released.
Date and Time Information	Time information for log management. Year/moth/day/hour/min/sec
User Password (U.ADMINISTRATOR)	Password information for U.ADMINISTRATOR authentication.
User Password (U.ACCOUNTMANAGER)	Password information for U.ACCOUNTMANAGER authentication.
User Password (U.AUDITOR)	A login password for U.AUDITOR authentication.
User Password (U.FAXOPERATOR)	A login password for U.FAXOPERATOR authentication.
User Password (U.NORMAL)	A login password for U.NORMAL authentication.
User Password (U.ADDRESSBOOKOPERATOR)	A login password for U.ADDRESSBOOKOPERATOR authentication.
Role	Shows roles of U.USER. Ex. U.NORMAL, U.ADMINISTRATOR, U.AUDITOR, and U.FAXOPERATOR.
Permission Role	Permission Role is attached to the MFP functions, such as F.PRT or F.SCN, and used as a security attribute that shows a role which allows the use of the MFP functions.

Terminology	Definition
Allocation Role	Allocation Role is attached to the user, and used as a security attribute that shows a role which shows the use of the MFP function.
Administrator Role	The Administrator Role has the following authority. · Authority to use e-Filing Box function. · Authority to manage the MFP device setting. · Authority to perform the User and Department management setting. · Authority to execute query, export and clear in the audit log.
AccountManager Role	A role which has an authority to perform User management setting.
Auditor Role	A role which has an authority to browse the audit log.
CopyOperator Role	A role which has an authority to use Copy.
ScanOperator Role	A role which has an authority to scan a document to a mail server, a FTP server, or to send a document in a e-filing Box to a mail server.
Print Role	A role which has an authority to use the function to print.
PrintOperator Role	A role which has an authority to print/delete a Print JOB in the Print Hold Queue.
e-FilingOperator Role	A role which has an authority to use e-Filing function.
Fax Role	A role which has an authority to use the transmission functions of Internet Fax.
FaxOperator Role	A role which has an authority to use the transmission function of Internet Fax and to print the data automatically received via Internet Fax in the Print Hold Queue.
Built-in Administrator Account	An Administrator account which is registered to the MFP beforehand.
User Role	A general user role which can use Print, Scan, Copy, e-Filing, and Internet fax transmission functions.
AddressBookRemoteOperator Role	A role which has an authority to edit the Address Book.

1.6. Trademarks

- Microsoft, Windows and the brand names and product names of other Microsoft products are trademarks of Microsoft Corporation in the US and other countries.
- TopAccess is a trademark of Toshiba Tec Corporation.
- Other company and product names given in this manual or displayed in this software may be the trademarks of their respective companies.

2. CONFORMANCE CLAIM

2.1. CC Conformance Claim

The ST and TOE are conformant to the following CC specifications:

Common Criteria version: Version 3.1 Release 4

Part 1: Introduction and general model September 2012 Version 3.1 Revision 4
Part 2: Security functional components September 2012 Version 3.1 Revision 4
Part 3: Security assurance components September 2012 Version 3.1 Revision 4

ST conformance for CC part2: CC part2 Extend

ST conformance for CC part3: CC part3 Conformant

2.2. PP conformance Claim, Package conformance Claim

2.2.1. PP conformance Claim

The ST conforms to following PP.

PP Identification: IEEE Std 2600.1-2009

PP Registration: CCEVS-VR-VID10340-2009

PP Version: 1.0

Date: June 2009

2.2.2. Package conformance Claim

This ST conforms to Common Criteria Evaluation Assurance Level (EAL) 3 augmented by ALC_FLR.2.
SFR Packages conform to PP are as follows.

2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A (Package Version 1.0, dated June 2009)

2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A (Package Version 1.0, dated June 2009)

2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A (Package Version 1.0, dated June 2009)

2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment A (Package Version 1.0, dated June 2009)

2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A (Package Version 1.0, dated June 2009)

2.3. Conformance Rationale

2.3.1. TOE type

TOE is Multifunction Peripheral (MFP) that includes the entire hardware and software components. The TOE provides the printing, scanning, copying, is intended to be used for the Operation Environment A defined in IEEE Std 2600.1. These are described in Chapter 1, 1.3.2 and 1.4 in the ST. Therefore TOE type is equivalent as that of defined in IEEE Std 2600.1.

2.3.2. ST Conformance

The ST conforms to IEEE Std 2600.1 with demonstrate that it is equivalent or more restrictive than the PP which is claiming demonstrable conformance.
This TOE states the SAR which conforms to EAL3 augmented by ALC_FLR.2 in the ST as requested by PP as for the SAR which is prescribed by PP.

This is explained in more detail as follows:

2.3.2.1. Security Problem Definition

Threat Agents and Threats, Assumptions, and Organizational Security Policies (OSPs) in the ST's environment are equivalent to those defined in the IEEE Std 2600.1.

2.3.2.2. Security Objectives

Security Objectives for the TOE and its environment in the ST are more restrictive than those defined in the IEEE Std 2600.1. Because the ST's security objectives for the TOE include all PP's security objectives for the TOE, O.AUDIT_STORAGE_PROTECTED, and O.AUDIT_ACCESS_AUTHORIZED in the ST's security objectives fot the TOE described in Chapter 4, the TOE described in the ST satisfies PP's security objectives for the TOE. Because the security objectives for the operational environment in PP includes all objectives of the operational environments in the ST, OE.AUDIT_STRAGE.PROTECTED, and OE.AUDIT_ACCESS.AUTHORIZED, all operational environments which satisfy the security objectives for the operational environment in PP satisfy the security objectives for the operational environment in this ST. Thus, ST's security objectives are more restrictive than PP's.

2.3.2.3. Extended Components Definitions

The extension component definition of the ST is the same as the extension component definition of PP because the extension component definition of the ST described in Chapter 5 refers to the definition of PP as it is.

2.3.2.4. SFR Components Definitions

This TOE selects the SFR described in "10.Common Security Functional Requirements (APE_REQ)" of PP and 2600.1-PRT, 2600.1-SCN, 2600.1-CPY, 2600.1-DSR, 2600.1-SMI as the SFR Package.
Some SFRs are added to the statement of ST on account of restricting the capability of the TOE to address the Objectives. These SFRs do not weaken the SFRs which defined in the IEEE Std 2600.1.
Also, because additional SFRs to PP are described as stated in 2.3.2.6, it is more restrictive.

2.3.2.5. SFR Components in SFR Package Definitions

All SFRs components defined in SFR package are described in the ST as shown below, therefore the ST conform with SFR package.

Table 7 Definition of the SFR Package

SFR Package	Definition
PRT **SCN** **CPY** **DSR**	PRT, CPY, SCN, DSR access control SFP are represented as TOE access control SFP at FDP_ACC.1(a) and FDP_ACF.1(a).
SMI	FPT_FDI_EXP.1 and FTP_ITC.1 which required in IEEE Std 2600.1 are represented in the ST and these SFRs relevant auditable events are generated by FAU_GEN.1 in the ST.

2.3.2.6. Conformance claim rationale

Table 8 shows the relationship of SFR defined in the ST and the PP.

Table 8 Relationship of SFR defined in the ST and the PP

SFRs of this ST	PP's request
FAU_SAR.1	
FAU_SAR.2	
FAU_STG.1	
FAU_STG.4	
FAU_GEN.1	✓
FAU_GEN.2	✓
FDP_ACC.1(a)	✓
FDP_ACC.1(b)	✓
FDP_ACF.1(a)	✓
FDP_ACF.1(b)	✓
FDP_RIP.1	✓
FIA_ATD.1	✓
FIA_UAU.1	✓
FIA_UAU.7	
FIA_UID.1	✓
FIA_AFL.1	
FIA_USB.1	✓
FMT_MSA.1(a)	✓
FMT_MSA.1(b)	✓
FMT_MSA.3(a)	✓
FMT_MSA.3(b)	✓
FMT_MTD.1	✓
FMT_SMF.1	✓
FMT_SMR.1	✓
FMT_MOF.1	
FPT_STM.1	✓
FPT_TST.1	✓
FTA_SSL.3	✓
FIA_SOS.1	
FPT_FDI_EXP.1	✓
FTP_ITC.1	✓

In this ST, an SFR is added based on the PP APPICATION NOTE as shown below upon applying all SFRs required in the PP.
FAU_STG.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2 are added according to PP APPLICATION NOTE7 so that the TOE maintains and manages the audit log. FIA_AFL.1, FIA_UAU.7, and FIA_SOS.1 are added according to PP APPLICATION NOTE36 so that the TOE performs authentication. Although FMT_MOF.1 is added in order to control behavior of the security function, this addition does not damage the SFR requirements prescribed in PP.

Thus, the TOE which satisfies the ST may be more restricted while satisfying the security requirement of the PP.

3. SECURITY PROBLEM DEFINITION

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 are not authorized.
d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this ST address the threats posed by these threat agents.

3.2. Threats to TOE Assets

The threats identified in the following Table sections are addressed by the TOE and/or Operating Environment.

Table 9 Threat 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 10 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 11 Organizational Security Policies for the TOE

Name	Description
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 malfunction of the TOE, procedures will exist to self-verify executable code in the TOE.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

3.4. Assumptions

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

Table 12 Assumptions for the TOE

Assumption	Description
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 the security objectives that the TOE shall fulfill.

4.1. Security Objectives for the TOE

Table 13 shows the security objectives which include all security objectives for the TOE described in PP and in which O.AUDIT_STORAGE.PROTECTED and O.AUDIT_ACCESS.AUTHORIZED are added to.

Table 13 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.
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.

4.2. Security Objectives for the Operational environment

This section describes the security objectives that must be fulfilled by the methods in the operational environment for the TOE. Refer to the objectives for the operational environment in IEEE Std 2600.1.

Table 14 Security Objectives for 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.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.
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.

Objective	Definition
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.

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 (Refer to the Completeness of security objectives) and that those security objectives counter the threats, enforce the policies, and uphold the assumptions. (Refer to the Sufficiency of security objectives). Table 15 shows the completeness of Security Objectives and Table 16 shows the Sufficiency of the objectives.

Table 15 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
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																		✓	
A.USER.TRAINING																			✓

Table 16 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 persons.	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	TSF 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.

Threats. Policies, and assumptions	Summary	Objectives and rationale
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF.	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF.
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration.
		O.AUDIT_STORAGE.PROTECTED protects audit records from unauthorized access, deletion and modifications.
		O.AUDIT_ACCESS.AUTHORIZED provides audit records accessed in order to detect potential security violation, and 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.
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 Revision 4, Part 2. This ST defines the extended component quoting a description of the Protection Profile.

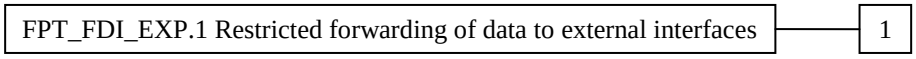
FPT_FDI_EXP Restricted forwarding of data to external interfaces

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 these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

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

a) Definition of the role(s) that are allowed to perform the management activities
b) Management of the conditions under which direct forwarding can be allowed by an administrative role
c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

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

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

6.1. Security Functional Requirements

The security functional requirements are given in detail in the following subsections. These requirements are verbatim from IEEE Std 2600.1 Protection Profile A with appropriate selection or assignments provided.
The following Table summarizes the security functional requirements claimed.

6.1.1. Class FAU: Security audit

(1) 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; and
- 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 17; [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 17:(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 17 Audit Data Requirements

Auditable event	Relevant SFR	Audit level	Additional information	Details (Actual event names)
None	**FAU_SAR.1**	Minimum	None required	None
None	**FAU_SAR.2**	Minimum	None required	None
None	**FAU_STG.1**	Minimum	None required	None
None	**FAU_STG.4**	Minimum	None required	None
None	**FAU_GEN.1**	Minimum	None required	None
None	**FAU_GEN.2**	Minimum	None required	None
None	**FDP_ACC.1(a)**	Minimum	None required	None
None	**FDP_ACC.1(b)**	Minimum	None required	None

Auditable event	Relevant SFR	Audit level	Additional information	Details (Actual event names)
Job completion	**FDP_ACF.1(a)**	Not specified	Type of job	・Success of the reading demand of D.DOC ・Success of the deletion demand of D.DOC ・Success of the modify demand of D.FUNC ・Success of the deletion demand of D.FUNC ・Termination of job ・Success of the modify demand of D.DOC
	FDP_ACF.1(b)			・Success of the Print function demand ・Success of the Scan function demand ・Success of the Copy function demand ・Success of e-Filing function demand ・Termination of job
None	**FDP_RIP.1**	Minimum	None required	None
Both successful and unsuccessful use of the user authentication mechanism	**FIA_UAU.1**	Basic	None required	・Failure of login (Failure of the password verification) ・Success of login (Success of password verification)
None	**FIA_UAU.7**	Minimum	None required	None
Both successful and unsuccessful use of the identification mechanism	**FIA_UID.1**	Basic	Attempted user identity, if available	・Success of login (Success of the User ID verification) ・Failure of login (Failure of the User ID verification)
The reaching of the threshold for the unsuccessful user 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_AFL.1**	Minimum	None required	・Login refusal by the certification trial number of times over ・Release of login denied
None	**FIA_ATD.1**	Minimum	None required	None
Rejection by the TSF of any tested secret	**FIA_SOS.1**	Minimum	None required	Failure of the login password modify
Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).	**FIA_USB.1**	Minimum	None required	Failure of binding User Token
None	**FMT_MTD.1**	Minimum	None required	None

Auditable event	Relevant SFR	Audit level	Additional information	Details (Actual event names)
Use of the management functions	**FMT_SMF.1**	Minimum	None required	Use of the management functions
Modifications to the group of users that are part of a role	**FMT_SMR.1**	Minimum	None required	None (They will not be modified.)
None	**FMT_MSA.1(a)**	Minimum	None required	None
None	**FMT_MSA.1(b)**	Minimum	None required	None
None	**FMT_MSA.3(a)**	Minimum	None required	None
None	**FMT_MSA.3(b)**	Minimum	None required	None
None	**FMT_MOF.1**	Minimum	None required	None
Changes to the time	**FPT_STM.1**	Minimum	None required	Modify the time
None	**FPT_TST.1**	Minimum	None required	None
None	**FPT_FDI_EXP.1**	Minimum	None required	None
Termination of an interactive session by the session locking mechanism	**FTA_SSL.3**	Minimum	None required	Termination of session due to time limit
a) Failure of the trusted channel functions **b)** Identification of the initiator and target of failed trusted channel functions	**FTP_ITC.1**	Minimum	None required	・Failure of TLS comunication ・Identification of the initiator and target of failed TLS communication

(2) FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

(3) 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*]

- refer to Table 18

[assignment: *list of audit information*]

- refer to Table 18

Table 18 List of Audit Information

Authorised Users	Audit Information
U.NORMAL	Job log information which is generated by own job
U.ADMINISTRATOR	All log information
U.ACCOUNTMANAGER	None
U.AUDITOR	All log information
U.FAXOPERATOR	Job log information which is generated by own Internet Fax transmission job
U.ADDRESSBOOKOPERATOR	None

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

(4) 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.

(5) 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 unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

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

- prevent

(6) 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 FDP: User data protection

The Security Function Policy (SFP) described in Table 19 is referenced by the Class FDP SFRs in this clause.

(1) 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 Access Control SFP in Table 19, Table 20, Table 21, Table 22, and Table 23 on the list of users as subjects, objects, and operations among subjects and objects covered by the Access Control SFP in Table 19, Table 20, Table 21, Table 22, and Table 23.

Table 19 Common Access Control SFP

Object	Function Attribute	Object Attribute	Operation(s)	Subject	Subject Attribute	Access Control Rule
D.DOC	+CPY +PRT +SCN	User ID	Delete	U.NORMAL	User ID	If the User ID matchs, the U.NORMAL is permitted to delete the D.DOC except Internet Fax reception D.DOC.
		None	Delete	U.ADMINISTRATOR	Role	If the Subject is U.ADMINISTRATOR, operation except deleting Internet Fax reception D.DOC is permitted.
D.FUNC (Address Book)	+SCN +DSR	None	Delete, Modify	U.ADMINISTRATOR, U.ADDRESSBOOKOPERATOR	Role	If the Subject is U.ADMINISTRATOR or U.ADDRESSBOOKOPERATOR, operation is permitted.

Table 20 CPY Access Control SFP

Object	Function Attribute	Object Attribute	Operation(s)	Subject	Subject Attribute	Access Control Rule
D.DOC	+CPY	None	Read	U.NORMAL	None	None

Table 21 PRT Access Control SFP

Object	Function Attribute	Object Attribute	Operation(s)	Subject	Subject Attribute	Access Control Rule
D.DOC	＋PRT	User ID	Read	U.NORMAL	User ID	If the User ID does not match, operation is denied.
		None	Read	U.FAXOPERATOR	Role	If the Subject is U.FAXOPERATOR, operation to D.DOC which is received by the Internet Fax is permitted.
D.FUNC (Print job in Print Hold Queue)		User ID	Delete	U.NORMAL	User ID	If the User ID does not match, operation is denied.
		None	Delete	U.ADMINISTRATOR	Role	If the Subject is U.ADMINISTRATOR, operation is permitted.
		None	Modify	U.USER	None	Operation of U.USER is denied.
D.FUNC (Internet Fax reception job in Print Hold Queue)		None	Modify, Delete	U.USER	None	Operation of U.USER is denied.

Table 22 SCN Access Control SFP

Object	Function Attribute	Object Attribute	Operation(s)	Subject	Subject Attribute	Access Control Rule
D.DOC	+SCN	User ID	Read, Modify	U.NORMAL, U.FAXOPERATOR	User ID	If the User ID does not match, operation is denied.

Table 23 DSR Access Control SFP

Object	Function Attribute	Object Attribute	Operation(s)	Subject	Subject Attribute	Access Control Rule
D.DOC	+DSR	e-Filing Box Password	Read, Delete, Modify	U.NORMAL, U.ADMINISTRATOR	e-Filing Box Password	If e-Filing Box Password does not match, operation is denied. If the entered e-Filing Box Password is that of the Built-in Administrator Account, operation is permitted.
		None	Delete	U.ADMINISTRATOR	Role	If the Subject is U.ADMINISTRATOR, operation is permitted.

(2) 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 on users as subjects, TOE functions as objects, and the right to use the functions as operations as specified in Table 24.

Table 24 The TOE Function Access Control SFP

Object (TOE Function)	Object Attribute	Subject	Subject Attribute	Access Control Rule
F.PRT	Permission Role	U.NORMAL, U.FAXOPERATOR	Allocation Role	If an Allocation Role is included in the Permission Role of F.PRT, U.NORMAL or U.FAXOPERATOR is permitted to execute F.PRT.
F.SCN	Permission Role	U.NORMAL, U.FAXOPERATOR	Allocation Role	If an Allocation Role is included in the Permission Role of F.SCN, U.NORMAL or U.FAXOPERATOR is permitted to execute F.SCN.
F.CPY	Permission Role	U.NORMAL	Allocation Role	If an Allocation Role is included in the Permission Role of F.CPY, U.NORMAL is permitted to execute F.CPY.
F.DSR	Permission Role	U.NORMAL	Allocation Role	If an Allocation Role is included in the Permission Role of F.DSR, U.NORMAL is permitted to execute F.DSR.

(3) 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 Access Control SFP in Table 19, Table 20, Table 21, Table 22, and Table 23 to objects based on the following: the list of users as subjects and objects controlled under the Access Control SFP in Table 19, Table 20, Table 21, Table 22, and Table 23, and for each, the indicated security attributes in Table 19, Table 20, Table 21, Table 22, and Table 23.

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 Access Control SFP in Table 19, Table 20, Table 21, Table 22, and Table 23 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 authorize access of subjects to objects*].

[*assig*nment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

- refer to Table 19, Table 20, Table 21, Table 22, and Table 23

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

(4) 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*]

- refer to Table 24

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.ADMINISTRATOR 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.ADMINISTRATOR 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*]]

- the user is explicitly authorized by U.ADMINISTRATOR to use a function

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: the user acts in the role U.ADMINISTRATOR: [assignment: *other rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: *other 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

(5) 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

6.1.3. Class FIA: Identification and authentication

(1) 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*]

- User ID
- Allocation Role
- Role

(2) 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***]

- storing the document data from printer driver
- storing the document data from mail Server

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.

(3) 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*]

- refer to Table 25

Table 25 Protected Authentication Feedback

Action	Feedback
Input of the password	Display dummy characters

(4) 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***]

- storing the document data from mail Server

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.

(5) FIA_USB.1 User-subject binding

Hierarchical to: No other components
Dependencies: FIA_ATD.1 User attributes 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*]

- User ID
- Allocation Role
- Role
- e-Filing Box Password

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on 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 with the subjects acting on behalf of users: [assignment: *rules for the changing of attributes*].

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

- none

(6) 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 ~ 30

[assignment: *list of authentication events*]

- user authentication

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*]

- lockout each account in lockout time
- only an administrator can release a lockout account

(7) 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*]

- refer to Table 26

Table 26 User Password Policy

User Password	Available Characters	Password Length	Rule
User Password (U.NORMAL) (U.FAXOPERATOR) (U.ADDRESSBOOKOPERATOR)	**Numbers :** 0-9 **Alphabet :** A-Z, a-z **Punctuation :** ! # ( ) * + , - . / : ; = ? @ ¥ ^ _ ` { | } ~ $ Space **European special characters**(Note1)	Min:8 Max:64	・User name is not allowed to be used as a password. ・Same password cannot be used successively. ・User Password is not allowed to use same characters more than 3 times successively in one password. ・Don't accept the prohibited character string that he/she can set from the TopAccess. (the plural settings are possible).
User Password (U.ADMINISTRATOR) (U.ACCOUNTMANAGER) (U.AUDITOR)			・User name is not allowed to be used as a password. ・Same password cannot be used successively. ・User Password is not allowed to use same characters more than 3 times successively in one password. ・Don't accept the prohibited character string that he/she can set from the TopAccess. (the plural settings are possible). ・A password has to include at least one alphanumeric character.

Note1: Character with Germanic umlaut and French cedilla

6.1.4. Class FMT: Security management

(1) 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 Access Control SFP in Table 19, Table 20, Table 21, Table 22, and Table 23 [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]*]

- refer to Table 27, Table 28

[assignment: *other operations*]

- none

[assignment: *list of security attributes*]

- refer to Table 27, Table 28

[assignment: *the authorised identified roles*]

- refer to Table 27, Table 28

Table 27 Management of Object Security Attributes

Access Control SFP	Object Security Attribute	Authorised Identified Roles	Operations
Common Access Control PRT Access Control SCN Access Control	User ID	Nobody	Any operation
DSR Access Control	e-Filing Box Password	U.NORMAL, U.ADMINISTRATOR	Modify

Table 28 Management of Subject Security Attributes

Access Control SFP	Subject Security Attribute	Authorised Identified Roles	Operations
Common Access Control PRT Access Control SCN Access Control	User ID	U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify
	Role	U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify
DSR Access Control	Role	U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify

(2) 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]*]

- refer to Table 29, Table 30

[assignment: *other operations*]

- refer to Table 29, Table 30

[assignment: *list of security attributes*]

- refer to Table 29, Table 30

[assignment: *the authorised identified roles*]

- refer to Table 29, Table 30

Table 29 Management of Subject Attributes

Subject Attribute	Authorised Identified Roles	Operations
Allocation Role	U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify

Table 30 Management of Object Attributes

Object Attribute	Authorised Identified Roles	Operations
Permission Role	U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify

(3) 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 Access Control SFP in Table 19, Table 20, Table 21, Table 22, and Table 23, [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]*]

- [assignment: other property]

[assignment: *other property*]

- refer to Table 31

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

Table 31 Characteristics Static Attribute Initialisation

Access Control SFP	Object	Function Attribute	Object Security Attribute	Default value for Object Security Attribute
Common Access Control SFP	D.DOC	+CPY +PRT +SCN +DSR	User ID	User ID of U.NORMAL who created the left Object.
	D.FUNC (Print job in Print Hold Queue)	+CPY +PRT +SCN +DSR	User ID	User ID of U.NORMAL who created the left Object.
PRT Access Control SFP	D.DOC	+PRT	User ID	User ID of U.NORMAL who created the left Object.
DSR Access Control SFP	D.DOC	+DSR	e-Filing Box Password	e-Filing Box Password which was entered when the left object was created.

(4) 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]*]

- [assignment: other property]

[assignment: *other property*]

- refer to Table 32

Table 32 Static Attribute Initialisation

Object (TOE Function)	Security Attribute	Characteristics which restricts access only to Subject with any of the following attributes
F.PRT	Permission Role	Print Role, PrintOperator Role, FaxOperator Role, User Role
F.SCN	Permission Role	ScanOperator Role, FaxOperator Role, User Role, Fax Role
F.CPY	Permission Role	CopyOperator Role, User Role
F.DSR	Permission Role	ScanOperator Role, Administrator Role, e-FilingOperator Role, User Role

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

(5) FMT_MTD.1 Management of TSF data

Hierarchical to: **No other components.**
Dependencies: **FMT_SMR.1 Security roles**
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1(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]*]

- refer to Table 33

[assig*nment: other operations*]

- refer to Table 33

[assignment: list of TSF data]

- refer to Table 33

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

- [selection: U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]]

[selection: *U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]*]

- [assignment: the authorized identified roles except U.NORMAL]

[assignment: *the authorized identified roles except U.NORMAL*]

- refer to Table 33

Table 33 Operation of TSF Data

Classification	TSF Data	Authorized Identified Roles	Operations
Confidential Data	All Job Logs	U.ADMINISTRATOR	Query, Delete, Export
		U.AUDITOR	Query
	Job Logs (Only Internet Fax transmission own job log)	U.FAXOPERATOR	Query
	Message Logs	U.ADMINISTRATOR	Query, Delete, Export
		U.AUDITOR	Query
	User Password (U.ADMINISTRATOR)	U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify, Export
	User Password (U.ACCOUNTMANAGER)	U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify, Export
	User Password (U.AUDITOR)	U.AUDITOR who relates to this TSF Data.	Modify,
		U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify, Export
	User Password (U.FAXOPERATOR)	U.FAXOPERATOR who relates to this TSF Data.	Modify
		U.ADMINISTRATOR, U.ACCOUNTMANGER	Modify, Export
	User Password (U.ADDRESSBOOKOPERATOR)	U.ADDRESSBOOKOPERATOR who relates to this TSF Data.	Modify
		U.ADMINISTRATOR, U.ACCOUNTMANGER	Modify, Export

Classification	TSF Data	Authorized Identified Roles	Operations
Protected Data	ACL Information	U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify
	Allowable number of entry for Login Password	U.ADMINISTRATOR	Modify
	Lockout Time	U.ADMINISTRATOR	Modify
	Locked-out Account Status	U.ADMINISTRATOR, U.ACCOUNTMANGER	Clear
	Auto Logout Time	U.ADMINISTRATOR	Modify
	Date and Time Information	U.ADMINISTRATOR	Modify
	User Password Policy Information	U.ADMINISTRATOR	Modify
	Hash value-acquiring code	Nobody	Any operation

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 are associated]*].

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

- refer to Table 34

[assignment: *other operations*]

- refer to Table 34

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

- refer to Table 34

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

- [selection: U.ADMINISTRATOR, the U.NORMAL to whom such TSF data are associated]

[selection: *U.ADMINISTRATOR, the U.NORMAL to whom such TSF data are associated*]

- refer to Table 34

Table 34 TSF Data

Classification	TSF Data	Authorized Identified Roles	Operations
Confidential Data	User Password (U.NORMAL)	U.NORMAL who relates to this TSF Data.	Modify
		U.ADMINISTRATOR, U.ACCOUNTMANAGER	Modify, Export
	Own print log, scan log, and internet Fax transmission log	U.NORMAL	Query

(6) 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*]

- refer to Table 35

Table 35 Management Functions

SFR	Management	Management Function	Reason
FAU_GEN.1	There are no management activities foreseen.	None	-
FAU_GEN.2	There are no management activities foreseen.	None	-
FAU_SAR.1	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.	None	Action is fixed and not managed.
	-	Management of Audit records	-
FAU_SAR.2	There are no management activities foreseen.	None	-
FAU_STG.1	There are no management activities foreseen.	None	-
FAU_STG.4	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	None	Action is fixed.
FDP_ACC.1(a)	There are no management activities foreseen.	None	-
FDP_ACC.1(b)	There are no management activities foreseen.	None	-
FDP_ACF.1(a)	Managing the attributes used to make explicit access or denial based decisions.	Management of Built-in Administrator Account Password	-
FDP_ACF.1(b)	Managing the attributes used to make explicit access or denial based decisions.	None	The attribute is fixed.
	-	Management of Allocation Role Management of Permission Role	-
FDP_RIP.1	a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.	None	The timing of overwriting for the residual information protection is fixed and cannot be changed.
FPT_FDI_EXP.1	a) Definition of the role(s) that are allowed to perform the management activities	None	There is no role.
	b) Management of the conditions under which direct forwarding can be allowed by an administrative role	None	Direct forwarding is permitted nobody and not managed.
	c) Revocation of such an allowance	None	Direct forwarding is permitted nobody and not managed.
FPT_TST.1	a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions	None	Action is fixed and not managed.
	b) management of the time interval if appropriate	None	Action is fixed and not managed.
FPT_STM.1	a) management of the time.	Management of time stamp setting.	-
FIA_UID.1	a) the management of the user identities;	Management of the User ID	-
	b) if an authorised administrator can change the actions allowed before identification, the managing of the action lists.	None	Action is fixed and not managed.
FIA_UAU.1	a) management of the authentication data by an administrator;	・Management of the User Password	-

SFR	Management	Management Function	Reason
		(U.ACCOUNTMANAGER/ U.ADMINISTRATOR/U.NORMAL/U.AUDITOR/U.FAXOPERATOR/ U.ADDRESSBOOKOPERATOR) by U.ADMINISTRATOR. ・Management of the User Password (U.ACCOUNTMANAGER/U.ADMINISTRATOR/ U.NORMAL/U.AUDITOR/U.FAXOPERATOR/ U.ADDRESSBOOKOPERATOR) by U.ACCOUNTMANAGER	
	b) management of the authentication data by the associated user;	・Management of the own User Password (U.NORMAL) by U.NORMAL. ・Management of the own User Password (U.AUDITOR) by U.AUDITOR. ・Management of the User Password (U.FAXOPERATOR) by U.FAXOPERATOR. ・Management of the User Password (U.ADDRESSBOOKOPERATOR) by U.ADDRESSBOOKOPERATOR.	-
	c) managing the list of actions that can be taken before the user is authenticated.	None	Action is fixed and not managed.
FIA_UAU.7	There are no management activities foreseen.	None	-
FIA_ATD.1	a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.	None	This function is not provided.
FIA_USB.1	a) an authorised administrator can define default subject security attributes.	None	There is no permitted role.
	b) an authorised administrator can change subject security attributes.	None	There is no permitted role.
FIA_AFL.1	a) management of the threshold for unsuccessful authentication attempts;	Management of user authentication failure handling	-
	b) management of actions to be taken in the event of an authentication failure.	None	Action is fixed and not managed.
FIA_SOS.1	a) the management of the metric used to verify the secrets.	Management of user password policy	-
FTA_SSL.3	a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user;	None	It is not possible to set it to each individual user.
	b) specification of the default time of user inactivity after which termination of the interactive session occurs.	Specification of the default time of user inactivity after which termination of the interactive session occurs.	-
FTP_ITC.1	a) Configuring the actions that require trusted	Management of Network	-

SFR	Management	Management Function	Reason
	channel, if supported.	settings	
FMT_SMR.1	a) managing the group of users that are part of a role.	None	Action is fixed and not managed.
FMT_MOF.1	a) managing the group of roles that can interact with the functions in the TSF;	None	Action is fixed and not managed.
FMT_MTD.1	a) managing the group of roles that can interact with the TSF data.	None	Action is fixed and not managed.
FMT_MSA.1(a)	a) managing the group of roles that can interact with the security attributes;	None	Action is fixed and not managed.
	b) management of rules by which security attributes inherit specified values.	None	Action is fixed and not managed.
FMT_MSA.1(b)	a) managing the group of roles that can interact with the security attributes;	None	Action is fixed and not managed.
	b) management of rules by which security attributes inherit specified values.	None	Action is fixed and not managed.
FMT_MSA.3(a)	a) managing the group of roles that can specify initial values;	None	There is no role that can specify initial value.
	b) managing the permissive or restrictive setting of default values for a given access control SFP;	None	The initial value is fixed and can not be changed.
	c) management of rules by which security attributes inherit specified values.	None	Nobody can change the rule
FMT_MSA.3(b)	a) managing the group of roles that can specify initial values;	None	There is no role that can specify initial value.
	b) managing the permissive or restrictive setting of default values for a given access control SFP;	None	The initial value is fixed and can not be changed.
	c) management of rules by which security attributes inherit specified values.	None	Nobody can change the rule.
FMT_SMF.1	There are no management activities foreseen.	None	-

(7) 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]*]

- [assignment: the authorised identified roles]

[assignment: *the authorised identified roles*]

- refer to Table 3

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.**

(8) FMT_MOF.1 Management of security functions behavior

Hierarchical to: **No other components.**
Dependencies: **FMT_SMR.1 Security roles**
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

[selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

- refer to Table 36

[assignment: *list of functions*]

- refer to Table 36

[assignment: *the authorised identified roles*]

- refer to Table 36

Table 36 Administrative Functions

Security Function	Behaviour	Role
Secure Channel	Enable/Disable	U.ADMINISTRATOR

6.1.5. Class FPT: Protection of the TSF

(1) 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.

(2) 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]*]

- at the request of the authorised user

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

- the TSF

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*]

- Hash value-acquiring code

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]

- stored TSF executable code

6.1.6. 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*]

- Control Panel: Auto logout time (15 - 150 sec)
- Web brosers or Client Utilities: Auto logout time (5 - 999 min)

6.2. SFR Package functions

The TOE provides the functions which perform processing, storage, and transmission of data. These functions are listed in Table 37.

Table 37 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.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 is or can be shared by other users, such as wired network media.

6.3. SFR Package attributes

When a function is performing processing, storage, or transmission 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. These attributes in the TOE are listed in Table 38.

Table 38 SFR Package Attributes

Designation	Definition
+PRT	Indicates data that is associated with a print job.
+SCN	Indicates data that is associated with a scan job.
+CPY	Indicates data that is associated with a copy job.
+DSR	Indicates data that is associated with a document storage and retrieval job.
+SMI	Indicates data that is transmitted or received over a shared-medium interface.

6.4. 2600.1-PRT SFR Package for Hardcopy Device Print Functions, Operational Environment A

This SFR package, as a minimum, provides access controls for releasing pending hardcopy output to a Hardcopy Output Handler. In this ST, the SFRs of PRT-SFR Package are included in the description of 6.1.2.

6.5. 2600.1-SCN SFR Package for Hardcopy Device Scan Functions, Operational Environment A

This SFR package, as a minimum, provides access controls for transmitting scanned documents to another IT device. In this ST, the SFRs of SCN-SFR Package are included in the description of 6.1.2.

6.6. 2600.1-CPY SFR Package for Hardcopy Device Copy Functions, Operational Environment A

This SFR package, as a minimum, provides access controls for releasing pending copies of documents to a Hardcopy Output Handler. In this ST, the SFRs of CPY-SFR Package are included in the description of 6.1.2.

6.7. 2600.1-DSR SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment A

This SFR package, as a minimum provides access controls for storing and retrieving documents. In this ST, the SFRs of DSR-SFR Package are included in the description of 6.1.2. It is also used to specify additional rules for modifying stored documents.

6.8. 2600.1-SMI SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

This SFR package, as a minimum, provides protection for User Data or TSF Data that are transmitted or received over shared-medium interfaces and management control of data transmission involving shared-medium interfaces. In this ST, FAU_GEN.1 in SMI SFR package is included in the description of 6.1.1 (1).

6.8.1. Class FTP: Trusted paths/channels

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.

6.8.2. Class FPT: Protection of the TSF

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.

6.9. Security assurance requirements

The Table below lists the security assurance requirements for IEEE Std 2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A, and related SFR packages, EAL 3 augmented by ALC_FLR.2.
In this ST, these SAR are used.

Table 39 IEEE Std 2600.1 Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorization controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL3)
	ALC_LCD.1 Developer defined life-cycle model
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.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.10. Security requirements rationale

6.10.1. Security requirements rationale

Table 40 demonstrates the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 40 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_ACCESS.AUTHORIZED	O.AUDIT_STORAGE.PROTECTED
FAU_SAR.1											**P**	
FAU_SAR.2											**P**	
FAU_STG.1												**P**
FAU_STG.4												**P**
FAU_GEN.1										**P**		
FAU_GEN.2										**P**		
FDP_ACC.1(a)	**P**	**P**	**P**									
FDP_ACC.1(b)							**P**					
FDP_ACF.1(a)	S	S	S									
FDP_ACF.1(b)							S					
FDP_RIP.1	**P**											
FIA_ATD.1							**S**					
FIA_UAU.1							**P**	**P**				
FIA_UAU.7							S	S				
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S		
FIA_AFL.1							**P**					
FIA_USB.1							**P**					
FMT_MSA.1(a)	S	S	S									
FMT_MSA.1(b)							S					
FMT_MSA.3(a)	S	S	S									
FMT_MSA.3(b)							S					
FMT_MTD.1				**P**	**P**	**P**						
FMT_SMF.1	S	S	S	S	S	S						
FMT_SMR.1	S	S	S	S	S	S	S					
FMT_MOF.1	S	S	S	S	S	S		S				
FPT_STM.1										S		
FPT_TST.1									**P**			
FTA_SSL.3							**P**	**P**				
FIA_SOS.1							S	S				
FPT_FDI_EXP.1								**P**				
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**						

6.10.2. Traceability rationale

O.DOC.NO_DIS Protection of document disclosure

O.DOC.NO_DIS is a security objective to prevent D.DOC from any unauthorized disclosure.
In order to implement this security objective, the following counter measures need to be taken.

- In D.DOC, the access is controlled using the User ID and Role of the user who generated that particular D.DOC. Therefore, FDP_ACC.1(a) and FDP_ACF.1(a) help in preventing any kind of unauthorized disclosure.
- The user is identified using FIA_UID.1 and the Role that is assigned to the User is maintained through FMT_SMR.1.
- The residual information of the deleted D.DOC is completely erased using FDP_RIP.1 and so it cannot be read again.
- The control of secutity attributes like User ID, e-Filing Box Password, and Role is restricted only to the specified User through FMT_MSA.1(a). Also, through FMT_MSA.3(a) , the User ID of the user who created the D.DOC and the e-Filing Box Password are assigned to the security attribute when D.DOC is generated.
- The behaviour of the security function is maintained through FMT_MOF.1 for only the U.ADMINISTRATOR.
- The D.DOC that is transmitted and received by the TOE via LAN is protected using FTP_ITC.1.
- These security function controls are provided through FMT_SMF.1.

O.DOC.NO_ALT Protection of document alteration

O.DOC.NO_ALT is a security objective to protect the D.DOC from any form of unauthorized tampering. In order to implement this security objective, the following counter measures need to be taken:

- In D.DOC, the access is controlled by User ID and Role of the user who generated that particular D.DOC. Therefore,FDP_ACC.1(a) and FDP_ACF.1(a) are used to prevent any unauthorized modification.
- The user is identified by FIA_UID.1, and the Role that is assigned to the User is maintained through FMT_SMR.1.
- The control of secutity attributes like User ID, e-Filing Box Password, and Role is restricted only to the specified User through FMT_MSA.1(a). Also, through FMT_MSA.3(a) , the User ID and e-Filing Box Password of the user who created the D.DOC is assigned to the security attribute when the D.DOC is generated.
- Through FMT_MOF.1, management of the behavior of security function is restricted to the U.ADMINISTRATOR.
- The D.DOC that is transmitted and received by the TOE via LAN is protected using FTP_ITC.1.
- These security function controls are provided through FMT_SMF.1.

O.FUNC.NO_ALT Protection of user job alteration

O.FUNC.NO_ALT is a security objective to protect D.FUNC from any kind of unauthorized tampering. In order to implement this security objective, the following countermeasures need to be taken:

- Through FDP_ACC.1(a) and FDP_ACF.1(a), the control related to Addressbook is permitted for the U.ADMINISTRATOR and the U.ADDRESSBOOKOPERATOR.
- Through FDP_ACC.1(a) and FDP_ACF.1(a), the control related to the print job is permitted for the U.ADMINISTRATOR and the U.NORMAL associated with the print job.
- The user is identified by FIA_UID.1, and the Role that is assigned to the User is maintained through FMT_SMR.1.
- The control of the security attributes like User ID, and Role is restricted only to the specified User through FMT_MSA.1(a). Also, through FMT_MSA.3(a), the User ID of the user who created the D.FUNC is assigned to the D.FUNC security attribute when D.FUNC is generated.
- Through FMT_MOF.1, management of the behavior of security function is restricted to the U.ADMINISTRATOR.
- The D.FUNC that is transmitted and received by TOE via LAN, is protected using FTP_ITC.1.
- These security function controls are provided through FMT_SMF.1.

O.PROT.NO_ALT Protection of TSF protected data alteration

O.PROT.NO_ALT is a security objective to protect D.PROT from unauthorized data tampering. In order to implement this security objective, the following countermeasures need to be taken.:

- The user is identified by FIA_UID.1 and the Role that is assigned to the user is maintained using MT_SMR.1.
- Through FMT_MTD.1, the U.ADMINISTRATOR and U.ACCOUNTMANAGER are allowed to operate the ACL Information and Locked-out Account Status, and the U.ADMINISTRATOR is allowed to operate the allowable number of entry for Login Password, Lockout Time, Auto Logout Time, Date and Time Information, and User Password Policy Information.
- The behaviour of security function is maintained only for the U.ADMINISTRATOR through FMT_MOF.1.

・The D.PROT that is transmitted and received by TOE via LAN, is protected through FTP_ITC.1.
・These security function controls are provided using FMT_SMF.1.
・Through FMT_MTD.1, the permission for cotrolling the Hash value-acquiring code is not given to anyone.

O.CONF.NO_DIS Protection of TSF confidential data disclosure

O.CONF.NO_DIS is a security objective to protect unauthorized data disclosure of D.CONF. In order to implement this security objective, the following countermeasures need to be taken:

・The User is identifed by FIA_UID.1 and the Role that is assigned to the User is maintained through FMT_SMR.1.
・Through FMT_MTD.1, the operation of All Job Logs and Message Logs is permitted for the U.ADMINISTRATOR and the U.AUDITOR, and the operation of Job Logs is permitted only to the Internet Faxed U.FAXOPERATOR.
・Through FMT_MTD.1, control of the User Password for the U.ADMISISTRATOR, U.ACCOUNT MANAGER, U.AUDITOR, U.FAXOPERATOR, and U.ADDRESSBOOKOPERATOR is permitted for the U.ADMINISTRATOR and U.ACCOUNTMANGER.
・Through FMT_MTD.1, the control of the U.NORAMAL User Password is permitted for the U.ADMINISTRATOR and U.ACCOUNTMANAGER. Also, the operation of the own U.NORMAL Print Log, Scan Log, and Internet Fax transmission Log is permitted only for the U.NORMAL alone.
・Through FMT_MOF.1, management of the behavior of security function is restricted to the U.ADMINISTRATOR.
・The D.CONF that is transmitted and received by the TOE via LAN is protected using FTP_ITC.1.
・These security function controls are provided through FMT_SMF.1.

O.CONF.NO_ALT Protection of TSF confidential data alteration

O.CONF.NO_ALT is a security objective to protect D.CONF from unauthorized data tampering. In order to implement this security objective, the following countermeasures need to be taken:

・The User is identified by FIA_UID.1 and the Role that is assigned to the User is maintained through FMT_SMR.1.
・Through FMT_MTD.1, the control of All Job Logs and Message Logs is permitted to the U.ADMINISTRATOR.
・Through FMT_MTD.1, the control of User Password of the U.ADMINISTRATOR and the U.ACCOUNTMANAGER is permitted to the U.ADMINISTRATOR and the U.ACCOUNTMANAGER.
・Through FMT_MTD.1, the control of the U.AUDITOR User Password is permitted to the U.ADMINISTRATOR, U.ACCOUNTMANAGER, and the U.AUDITOR associated with TSF data.
・Through FMT_MTD.1, the control of the U.FAXOPERATOR User Password is permitted to the U.ADMINISTRATOR , U.ACCOUNTMANAGER, and the U.FAXOPERATOR associated with TSF data.
・Through FMT_MTD.1, the control of the U.ADDRESSBOOKOPERATOR User Password is permitted to the U.ADMINISTRATOR, U.ACCOUNTMANAGER, and the U.ADDRESSBOOKOPERATOR associated with TSF data.
・Through FMT_MTD.1, the control of the U.NORAMAL User Password is permitted to the U.NORMAL associated with TSF data, U.ADMINISTRATOR and the U.ACCOUNTMANAGER.
・The D.CONF that is transmitted and received by the TOE via LAN is protected by FTP_ITC.1.
・The behaviour of the security function is maintained using FMT_MOF.1 for only the U.ADMINISTRATOR
・These security function controls are provided through FMT_SMF.1.

O.USER.AUTHORIZED User identification and authentication

O.USER.AUTHORIZED is a security objective to identify and authenticate the User for using the TOE. In order to implement this security objective, the following countermeasures need to be taken.:

・FDP_ACC.1(b) and FDP_ACF.1(b) are used to perform access control based on the authority/privileges that have been given to execute the TOE function, for the user whose identification and authentication is successful.
・Through FIA_UAU.1, FIA_UID.1, the user who uses the TOE is identified and authenticated from the control panel and client PC.
・Through FIA_UAU.7, the disclosure of the login password is prevented by displaying dummy characters in the authentication feedback.
・Through FTA_SSL.3, auto logout is done from the logged-in Control Panel or the Client PC.
・Through FIA_SOS.1, the user password that will be authenticated by the TOE is set as per the Password policy, so that it becomes difficult for an outsider to guess the password.
・Through FIA_AFL.1, access to the TOE will not be permitted for a specified period of time if the authentication fails more than the permitted number of times while attempting login.
・Through FIA_ATD.1, the User ID, Allocation Role and Role are defined and maintained as the user security attribute.

・Through FIA_USB.1, the User ID, Allocation Role, Role and e-Filing Box Password which are the user security attribute can be bound to the security attribute of the subject.
・Through FMT_MSA.3(b), the initial value of the security attribute is set, and through FMT_MSA.1(b), the Modify operation of the security attribute is permitted for the U.ADMINISTRATOR and the U.ACCOUNTMANGER.
・Through FMT_SMR.1, the User Role is specified and maintained.

O.INTERFACE.MANAGED Management of external interfaces by TOE

O.INTERFACE.MANAGED is a security objective to ensure that the TOE controls the operation of external interfaces. In order to implement this security objective, the following countermeasures need to be taken:

・Through FIA_UAU.1,FIA_UID.1, the User who uses the TOE is identified and authenticated from the Control Panel and Client PC.
・Through FIA_UAU.7, the disclosure of the login password is prevented by displaying dummy characters in the authentication feedback
・FPT_FDI_EXP.1 is used to prevent the data received in the Control Panel, and LAN interface from being transmitted from the LAN without any additional TSF processing.
・Through FIA_SOS.1, the user password that will be authenticated by TOE is set as per the Password policy, so that it becomes difficult for an outsider to guess the password.
・Through FTA_SSL.3, the session is automatically terminated in certain instances where the Control Panel, Web browser or the Client Utility are not used for a specified period of time.
・The behaviour of security functions is maintained only for the U.ADMINISTRATOR using FMT_MOF.1.

O.SOFTWARE.VERIFIED Software verification

O.SOFTWARE.VERIFIED is a security objective to ensure that the TOE software is legitimate. In order to implement this security objective, the following countermeasures need to be taken:

・Through FPT_TST.1, a function to validate if the Hash value-acquiring code and the TSF execution code are legitimate is provided.

O.AUDIT.LOGGED Management of audit log records

O.AUDIT.LOGGED is a security objective where the audit log is recorded and controlled using the authenticated access. In order to implement these security objective, the following countermeasures need to be taken:

・Through FAU_GEN.2 and FIA_UID.1, the user identification information which triggers each audit event is assocaited to the event.
・Through FAU_GEN.1 and FAU_GEN.2, the event that needs to be audited is recorded.
・Through FPT_STM.1, an accurate timestamp is provided in the audit log in order to record the time of the audit event accurately.

O.AUDIT_ACCESS.AUTHORIZED

O.AUDIT_ACCESS.AUTHORIZED is a security objective to ensure that the audit log is distributed to the people for whom access has been permitted so that potential security attacks are detected. In order to implement this security objective, the following countermeasures need to be taken:

・Through FAU_SAR.1 and FAU_SAR.2, U.NORMAL reads its own job log information, the U.ADMINISTRATOR and U.AUDITOR reads all the job logs while the U.FAXOPERATOR reads its own internet transmitted job log information in a format in where it can be interpreted. Also, the U.ACCOUNTMANAGER does not permit the reading of the audit log.

O.AUDIT_STORAGE.PROTECTED

O.AUDIT_STORAGE.PROTECTED is a security objective to protect the audit log data from unauthorized access, deletion and modifications. In order to implement this objective, the following countermeasures need to be taken:

・Through FAU_STG.1, the audit log is protected from unauthorized deletion and modifications.
・When audit log becomes full, FAU_STG.4 overwrites the oldest stored audit record by new audit log data.

6.10.3. Dependencies of Security Functional Requirements

Table 41 describes the functional requirements that are depended on by security functional requirements.

Table 41 Dependencies of Security Functional Requirements

SFRs	Required Dependence	Fulfilled Dependence in ST	Un-fulfilled Dependence in ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1, FIA_UID.1	None
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	None
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	FAU_STG.1	None
FDP_ACC.1(a)	FDP_ACF.1	FDP_ACF.1(a)	None
FDP_ACC.1(b)	FDP_ACF.1	FDP_ACF.1(b)	None
FDP_ACF.1(a)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(a), FMT_MSA.3(a)	None
FDP_ACF.1(b)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(b), FMT_MSA.3(b)	None
FDP_RIP.1	None	None	None
FIA_ATD.1	None	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	None
FIA_UID.1	None	None	None
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	The user security attribute is associated with the subject every time the user enters the value to the e-Filing Box Password. Thus the user attribute definition relevant to the e-Filing Box Password is not required.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	None
FIA_SOS.1	None	None	None
FMT_MSA.1(a)	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(a), FMT_SMR.1, FMT_SMF.1	None
FMT_MSA.1(b)	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(b), FMT_SMR.1, FMT_SMF.1	None
FMT_MSA.3(a)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(a), FMT_SMR.1	None
FMT_MSA.3(b)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(b), FMT_SMR.1	None
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1	None
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None
FPT_STM.1	None	None	None
FPT_TST.1	None	None	None
FTA_SSL.3	None	None	None
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	None
FTP_ITC.1	None	None	None

6.10.4. Security Assurance Requirements Rationale

This TOE is a digital multi functional peripheral which is commercially available. Because this TOE is supposed to be used in a general office, chance of an attack will be restricted. Thus, threat agents which have basic attack ability is assumed for this TOE. In order to counter the threat agents, it is decided to evaluate the range covered by analysis of the security policies for the TOE development (organized analysis and test of the design, and safety development environment). Failure report procedure for failure found after the operation starts is structured so that the TOE operates continuously and securely. Therefore, EAL3+ALC_FLR.2 warranty package is applicable for the evaluation warranty level to this TOE. In addition, because SAR is the same as PP in this ST, dependency property is satisfied.

7. TOE SUMMARY SPECIFICATION

This section provides the mapping between the TOE Security Functional Requirements (SFRs) and the security functions implemented in the TOSHIBA e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A Multifunctional Digital Systems product. Table 42 shows the correspondences between SFRs and TOE security functions.

Table 42 Correspondences between SFRs and TOE Security Functions

SFRs	Security Function						
	User Authentication	User Access Control	Audit Data Generation and Review	Secure Erase	Secure Channel	TSF Self Protection	TSF Data Protection
FAU_GEN.1			✓				
FAU_GEN.2			✓				
FAU_SAR.1			✓				
FAU_SAR.2			✓				
FAU_STG.1			✓				
FAU_STG.4			✓				
FDP_ACC.1(a)		✓					
FDP_ACC.1(b)		✓					
FDP_ACF.1(a)		✓					
FDP_ACF.1(b)		✓					
FDP_RIP.1				✓			
FPT_FDI_EXP.1					✓		
FPT_TST.1						✓	
FPT_STM.1			✓				
FIA_UID.1	✓						
FIA_UAU.1	✓						
FIA_UAU.7	✓						
FIA_ATD.1		✓					
FIA_USB.1		✓					
FIA_AFL.1	✓						
FIA_SOS.1	✓						✓
FTA_SSL.3	✓						
FTP_ITC.1					✓		
FMT_SMR.1							✓
FMT_MOF.1							✓
FMT_MTD.1							✓
FMT_SMF.1							✓
FMT_MSA.1(a)							✓
FMT_MSA.1(b)							✓
FMT_MSA.3(a)							✓
FMT_MSA.3(b)							✓

FAU_GEN.1 is realized by the following:

The TOE creates the audit log when an audit event occurs, and records it in the audit log file as shown in Table 43.

Table 43 Logged Event and Audit Log

Logged Events	Audit Log
Start-up/finish of the audit function	・ Date/Time ・ Error Level ・ Message ・ Error Code ・ User Name
Success/Failure of Login (Based on verification of User ID or Password)	
Release of login denied	
Login refusal by the certification trial number of times over	
Failure of login password modify	
Success of Modify/Reading/Deletion demand of User documents	
Success of Modify/Deletion demand of Address Book	
Reading/Modify/Deletion demand of Queue	
Success of Print function demand	
Success of Scan function demand	
Success of Copy function demand	
Success of e-Filing function demand	
Termination of JOB	
Modify the time	
Termination of session due to time limit	
Failure of TLS comunication	
Identification of the initiator and target of failed TLS communication	
Failure of binding User Token	
Use of the management functions	

The TOE appends the following data to the event to be audited.
- Date/Time: A time when error/event occurred
- Error Level: Event category and degree of importance
- Message: A sentence which explains the contents of the event
- Error Code: An event is defined as a code and expressed as 4-digit hexadecimal.
- User Name: Logged in User Name

FAU_GEN.2 is realized by following:

When each event to be audited occurs, the TOE appends the User ID of a user who caused the event to the audit log.

FAU_SAR.1 is realized by following:

- The TOE provides a function by which U.NORMAL can refer to only the Job Log which is executed by the U.NORMAL on the control panel and TopAccess in the text format.
- The TOE provides a function by which U.ADMINISTRATOR or U.AUDITOR can refer to all log informations on TopAccess in the text format.
- The TOE provides a function by which U.ADMINISTRATOR or U.AUDITOR can refer to all Job logs on the control panel in the text format.
- The TOE provides a function by which U.ADMINISTRATOR can refer to all log informations by exporting in the format of XML or CSV.
- The TOE provides a function by which U.FAXOPERATOR can refer to the Internet Fax Transmission Log which is executed by the U.FAXOPERATOR on the control panel and TopAccess in the text format.

FAU_SAR.2 is realized by following:

- The TOE denies a read operation of the Job log which is not executed by himself to the U.NORMAL.
- The TOE denies a read operation of the Internet Fax transmission log which is not executed by himself to the U.FAXOPERATOR.
- The TOE prohibits U.ACCOUNTMANAGER or U.ADDRESSBOOKOPERATOR from accessing all Job logs and all Message logs.
- The TOE permits U.ADMINISTRATOR or U.AUDITOR to execute read operation for all Job logs and all Message logs.

FAU_STG.1 is realized by following:

- The TOE provides only U.ADMINISTRATOR with an operation function to delete all Job logs and Message logs.
- The TOE does not provide an interface which executes modification operation to all Job logs and all Message logs.

FAU_STG.4 is realized by following:

The TOE can record a new audit log data without any damage by overwriting the oldest audit log data when the audit log becomes full.

FDP_ACC.1(a), FDP_ACF.1(a) are realized by using a combination of the following:

Common Access Control SFP

- The TOE permits the U.NORMAL who has a user ID for executing a D.DOC job operation to delete the target D.DOC. The D.DOC job operations include Copy, Print (except internet Fax reception), and Scan (including Internet Fax transmission).
- The TOE permits deletion operation of target D.DOC regarding Copy, Print (except Internet Fax reception) and Scan (including Internet Fax transmission) to the U.ADMINISTRATOR.
- The TOE permits deletion operation and modification operation of Address Book which is used for Scanning and e-Filing to the U.ADMINISTRATOR and the U.ADDRESSBOOKOPERATOR.

CPY Access Control SFP

- The TOE does not execute access restriction for D.DOC by which the U.NORMAL executes Copy operation.

PRT Access Control SFP

- The TOE denies Print operation of targeted D.DOC for the U.NORMAL who does not have the User ID which stores the D.DOC to be printed to the TOE.
- The TOE permits Print operation of Internet Fax-received document for the U.FAXOPERATOR.
- The TOE denies an operation to delete a print job from the Print Hold Queue for the U.NORMAL who does not have the User ID which saved the targeted D.DOC to the TOE.
- The TOE permits an operation to delete a print job in the Print Hold Queue for the U.ADMINISTRATOR.
- The TOE denies modification operation of the Print Job in the Print Hold Queue by any U.USER.
- The TOE denies modification operation and deletion operation of the Internet Fax reception Print Job in the Print Hold Queue by any U.USER.

SCN Access Control SFP

- The TOE permits an operation to transfer target D.DOC to the FTP server for the U.NORMAL who has the User ID which executed scanning job operation by copying.
- The TOE permits an operation to preview and transfer target D.DOC to the mail server, the FTP server for the U.NORMAL who has the User ID which executed scanning job operation except by copying.
- The TOE permits an operation to preview and transfer target D.DOC of Internet Fax to the mail server for the U.FAXOPERATOR who has the User ID which executed scanning job operation by Internet Fax transmission operation.
- The TOE permits a modification operation per page of D.DOC for the U.NORMAL who has the User ID which executed scanning operation or U.FAXOPERATOR who has the User ID which executed scanning operation by Internet Fax transmission operation.

DSR Access Control SFP

- The TOE permits preview operation, print operation, deletion operation, modification operation, and export operation to the client PC of D.DOC for the U.NORMAL or U.ADMINISTRATOR when the e-Filing Box Password entered by the U.NORMAL or U.ADMINISTRATOR matches the e-Filing Box Password of the D.DOC or the password of the Built-in Administrator Account.
- The TOE permits deletion operation of D.DOC regarding e-Filing for the U.ADMINISTRATOR.

FDP_ACC.1(b), FDP_ACF.1(b) are realized by using a combination of the following:

The TOE controls the access to F.PRT, F.SCN, F.CPY, and F.DSR. These functions will be available to a user when U.ADMINISTRATOR allocates the Role expressly.

- The TOE permits to execute printing for the U.NORMAL or U.FAXOPERATOR if the Allocation Role of the U.NORMAL or U.FAXOPERATOR is included in the Permission Role of F.PRT.
- The TOE permits to execute scanning for the U.NORMAL or U.FAXOPERATOR if the Allocation Role of the U.NORMAL or U.FAXOPERATOR is included in the Permission Role of F.SCN.
- The TOE permits to execute copying functions for the U.NORMAL if the Allocation Role of the U.NORMAL is included in the Permission Role of F.CPY.
- The TOE permits to execute document storage and retrieval for the U.NORMAL if the Allocation Role of the U.NORMAL is included in the Permission Role of F.DSR.
- The TOE permits access to F.PRT, F.SCN, F.CPY, and F.DSR for U.ADMINISTRATOR of Built-in Administrator Account explicitly.

FDP_RIP.1 is realized by the following:

The TOE frees assignment of the storage area on the HDD after overwriting 00h, FFh and random data on a deleted D.DOC in order. The TOE provides a function which deletes remaining information of the deleted D.DOC so as to prevent it from being restored and decrypted by this overwriting method.

FPT_FDI_EXP.1 is realized using the following:

The TOE controls not to permit to relay data entered from an external interface to the TOE to the Shared medium interface. This function prevents direct access to the Shared medium interface from an external interface of the TOE.

FPT_TST.1 is realized by the following:

The TOE executes TSF self-test upon U.ADMINISTRATOR's request, verify integrity of all TSF execution codes and also verify integrity of the Hash value-acquiring code which is TSF data, in order to verify TSF normal operation. In the case that abnormality is found on the test, an error message appears on the control panel and all functions other than the control panel are disabled so that the user cannot use the TOE. Also, TOE validates the integrity of the Hash value-acquiring code and TSF executable code by comparing the computed file hash value with the correct value at the time of execution.

FPT_STM.1 is realized by the following:

The TOE provides a time stamp (year, month, day, hour, minute, and second) for recording to the audit log.

FIA_UID.1, FIA_UAU.1 are realized using the following mechanism:

The TOE requires a user to be identified and authenticated. The user identification and authentication is performed against an internal user accounts' database, in case an internal user management function is used. If User ID and Password do not match the internally stored credentials then access is denied and the user is prompted again. However, when print data from the printer driver is stored in the TOE, identification by the entered user ID is required to succeed before the storage. When storing emails from the mail server to the TOE, the TOE stores them without the identification and the authentication.

FIA_UAU.7 is realized using the following:

The TOE displays dummy characters (e.g. "*") in place of the input characters on the operation screen when the user inputs the password.

FIA_ATD.1 is realized using the following:

- The TOE associates the User ID, the Allocation Role, and the Role to the User as the security attribute, registers and retains it.
- The TOE recognizes the Allocation Role and Role from the User ID of a user whose identity is authenticated, and allows only U.ADMINISTRATOR and U.ACCOUNTMANAGER to modify the Allocation Role and modify and delete the Role.

FIA_USB.1 is realized using the following:

- The TOE associates the User ID, the Allocation Role, and the Role with the user who has succeeded in identity authentication.
- The TOE associates the e-Filing Box Password which is entered when accessing the e-Filing Box.

FIA_AFL.1 is realized using the following:

- The TOE provides a function that locks a user out when the user fails in authentication.
- The TOE counts the number of failures during the specified period of time set by the U.ADMINISTRATOR per each User ID that tries to log in, and resets the number of failures to 0 when the user succeeds in login. When the number of failures of successive user authentication meets the allowable number of times set by U.ADMINISTRATOR (1 through 30 times), the TOE locks the User ID out for a certain period of time.
- The TOE provides a function to unlock the lockout of the User ID which is locked out.
  Automatic unlocking:
  The lockout is automatically unlocked when the time reaches the unlock time set by U.ADMINISTRATOR per each User ID.

  Unlocking by U.ADMINISTRATOR:
  Unlocking of lockout by specifying the User ID which is under account lockout state by U.ADMINISTRATOR.

FIA_SOS.1 is realized using the following:

The TOE provides a function to inspect User Password at the time of registration/change of User Password or login of the user as shown in Table 26.

FTA_SSL.3 is realized using the following:

If a user does not operate on the control panel on the TOE for the set period of times, the TOE forcibly logs out. The set period is settable from 15 through 150 seconds. In addition, the TOE forcibly terminates the network session and logs out when the set period of time has passed after the final operation of the TOE using browsers or Client Utilities. The set period is settable from 5 through 999 minutes.

FTP_ITC.1 is realized by the following:

The TOE executes TLS communication so as to protect data during communication with the Client PC and among each types of server. For Scan job, e-mail reception, and Internet Fax transmission, TSF requests to start TLS communication when accessing the email server or saving a file to the filing box of the FTP server, and TSF starts communication after receiving the request to start TLS communication from the Client PC when accessing from the Client PC using Client Utility Software or the web browser.

FMT_SMR.1 is realized using the following:

The TOE retains Role associated with U.ADMINISTRATOR, U.ACCOUNTMANAGER, U.NORMAL, U.AUDITOR, U.FAXOPERATOR, and U.ADDRESSBOOKOPERATOR and associates the Role to the appropriate user when registering a user.

FMT_MOF.1 is realized using the following:

The TOE provides a function to refer to Secure Channel function setting and to switch Enable/Disable setting only for U.ADMINISTRATOR.

FMT_MTD.1 is realized using the following:

The TOE provides U.ADMINISTRATOR with the following operation functions.
- Query, Deletion and Export of all Job Logs
- Query, Deletion and Export of all Message Logs
- Modification and Export of U.ADMINISTRATOR's User Password
- Modification and Export of U.ACCOUNTMANAGER's User Password
- Modification and Export of U.AUDITOR's User Password
- Modification and Export of U.FAXOPERATOR's User Password
- Modification and Export of U.ADDRESSBOOKOPERATOR's User Password
- Modification and Export of U.NORMAL's User Password
- Modification of ACL information
- Modification of the allowable number of entry of Login Password
- Modification of Lockout Time
- Status Clear for Locked-out Account
- Modification of Auto Logout Time
- Modification of Date and Time Information
- Modification of User Password Policy Information

The TOE provides U.AUDITOR with the following operation functions.
- Query of all Job Logs
- Query of all Message Logs
- Modification of the own User Password

The TOE provides U.FAXOPERATOR with the following operation functions.
- Query of Internet Fax transmission own job log
- Modification of the own User Password

The TOE provides U.ACCOUNTMANAGER with the following operation functions.
- Modification and Expot of the U.ADMINISTRATOR's User Password
- Modification and Export of the U.ACCOUNTMANAGER's User Password
- Modification and Export of U.AUDITOR's User Password
- Modification and Export of U.FAXOPERATOR's User Password
- Modification and Export of U.ADDRESSBOOKOPERATOR's User Password
- Modification and Export of U.U.NORMAL's User Password
- Modification of ACL Information
- Status Clear for Locked-out Account

The TOE provides U.NORMAL with the following operation functions.
- Query operation of own print log, scan log, and internet Fax transmission log.
- Modification of the own User Password

The TOE provides U.ADDRESSBOOKOPERATOR to following operation functions.
- Modification of the own User Password

The TOE does not provide a function to operate the Hash value-acquiring code.

FMT_SMF.1 is realized using the following:

The TOE realizes FMT_SMF.1 by providing the following security management functions.

Management of Audit records:
- Query, Delete and Export operations for all Job logs and all Message logs by the U.ADMINISTRATOR.
- Query operation for all Job logs and all Message logs by the U.AUDITOR.
- Query operation for Job logs (Only Internet Fax transmission own job log) by the U.FAXOPERATOR.
- Query operation for own print log, scan log, and Internet Fax transmission log by the U.NORMAL.

Management of Built-in Administrator Account's Password:
- Modification and Export operations for Built-in Administrator Account's Password by U.ADMINISTRATOR or U.ACCOUNTMANAGER.

Management of Allocation Role and Permission Role:
- Modification operation for the Allocation Role by the U.ADMINISTRATOR or U.ACCOUNTMANAGER.
- Modification operation for the Permission Role by the U.ADMINISTRATOR or U.ACCOUNTMANAGER.
- Modification operation for the ACL information by the U.ADMINISTRATOR or U.ACCOUNTMANAGER.

Management of time stamp setting:
- Modification operation for Date and Time Information by the U.ADMINISTRATOR.

Management of the User ID:
- Modification operation for the User ID by the U.ADMINISTRATOR or U.ACCOUNTMANAGER.

Management of User Password:
- Modification and Export operations for User Passwords for the U.ACCOUNTMANAGER, U.NORMAL, U.AUDITOR, U.FAXOPERATOR, U.ADMINISTRATOR, and U.ADDRESSBOOKOPERATOR by the U.ADMINISTRATOR and U.ACCOUNTMANAGER.
- Modification operation for own User Password by the U.NORMAL.
- Modification operation for own User Password by the U.AUDITOR.
- Modification operation for own User Password by the U.FAXOPERATOR.
- Modification operation for own User Password by the U.ADDRESSBOOKOPERATOR.

Management of user authentication failure handling:
- Modification operation for Allowable number of entry for Login Password by the U.ADMINISTRATOR.
- Modification operation for Lockout Time by the U.ADMINISTRATOR.
- Clear operation for Locked-out Account Status by the U.ADMINISTRATOR or U.ACCOUNTMANAGER.

Management of user password policy:
- Modification operation for the User Password policy Information by the U.ADMINISTRATOR.

Specification of the default time of user inactivity after which termination of the interactive session occurs:
- Modification operation for Auto Logout Time by the U.ADMINISTRATOR.

Management of Network settings:
- Enable/Disable operation for the Secure Channel by the U.ADMINISTRATOR.

FMT_MSA.1(a) is realized using the following:

- The TOE denies any operation regarding the User ID as the Object attribute.
- The TOE permits U.NORMAL and U.ADMINISTRATOR to modify the e-Filing Box Password as the object attribute.
- The TOE permits U.ADMINISTRATOR and U.ACCOUNTMANAGER to modify the User ID as the subject attribute.
- The TOE permits U.ADMINISTRATOR and U.ACCOUNTMANAGER to modify the Role as the subject attribute.

FMT_MSA.1(b) is realized using the following:

The TOE permits U.ADMINISTRATOR and U.ACCOUNTMANAGER to modify the Allocation Role which is the subject object attribute and Permission Role which is the object security attribute.

FMT_MSA.3(a) is realized using the following:

The TOE performs access control to give the default value of the security attribute when D.DOC or D.FUNC which is related to +CPY, +PRT, +SCN, and +DSR is created as shown in Table 31. The TOE does not provide a function to specify the alternative initial value which overwrites the default value when these objects are created.

FMT_MSA.3(b) is realized using the following:

The TOE performs access control to give the default value of the security attribute when CPY, PRT, SCN, and DSR functions are created as shown in Table 32. The TOE does not provide a function to specify the alternative initial value which overwrites the default value when these functions are created.

Annex - Acronyms

Table 44 List of Acronyms

Acronym	Definition
CC	Common Criteria for Information Technology Security Evaluation
DoD	United States Department of Defense
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy