Canon imageRUNNER ADVANCE C5200 Series 2600.1 model

Security Target

Version 1.08
2014/08/07

Canon Inc.

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

Table of Contents

1 ST introduction

1.1 ST reference

This section provides the Security Target (ST) identification information.

ST name:	Canon imageRUNNER ADVANCE C5200 Series 2600.1 model Security Target
Version:	1.08
Issued by:	Canon Inc.
Date of Issue:	2014/08/07
Keywords:	IEEE 2600, Canon, imageRUNNER, iR, Advance, digital MFP, multifunction product (MFP), copy, print, fax, send, facsimile, identification, authentication, access control, log, encryption, Secured Print, BOX, security kit

1.2 TOE reference

This section provides the TOE identification information.

TOE name:	Canon imageRUNNER ADVANCE C5200 Series 2600.1 model
Version:	1.3

The TOE is comprised of the following software, hardware, and licenses.

iR-ADV Security Kit-C1 for IEEE 2600.1 Common Criteria Ver 1.03
HDD Data Encryption & Mirroring Kit-C
(Canon MFP Security Chip 2.01)
Canon imageRUNNER ADVANCE C5200 Series

*Japanese Name
iR-ADV Security Kit-C1 for IEEE 2600.1 Ver 1.03
HDD Data Encryption / Mirroring Kit-C
(Canon MFP Security Chip 2.01)
Canon imageRUNNER ADVANCE C5200 Series

1.3 TOE overview

The TOE is a digital multi-function product (MFP) known as < Canon imageRUNNER ADVANCE C5200 Series 2600.1 model >. This is a version of the standard model < Canon imageRUNNER ADVANCE C5200 Series > which by installing/attaching the following 2 products and making the proper settings, makes up the < Canon imageRUNNER ADVANCE C5200 Series 2600.1 model > or TOE.

- iR-ADV Security Kit-C1 for IEEE 2600.1 Common Criteria
- HDD Data Encryption & Mirroring Kit

< iR-ADV Security Kit-C1 for IEEE 2600.1 Common Criteria > contains the < Canon imageRUNNER ADVANCE C5200 Series > control software and security kit license.
HDD Data Encryption & Mirroring Board is the hardware which encrypts all data stored in the HDD (including software). The HDD of the TOE may be a removable drive.

< Canon imageRUNNER ADVANCE C5200 Series 2600.1 model > is capable of fully implementing the Protection Profile (PP) for Multi-Function Products indicated below, as well as the security functions required by the 7 SFR Packages defined in the PP.

Protection Profile

- :2600.1, Protection Profile for Hardcopy Devices, Operational Environment A

SFR Packages

- 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
- 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
- 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
- 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
- 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
- 2600.1-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A
- 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

1.4 Terms and Abbreviations

The following terms and abbreviations are used throughout this ST.

Table 1 —Terms and Abbreviations

Terms/Abbreviations	Description
Multi-Function Product (MFP)	A machine which incorporates the functionality of multiple devices in one, such as copier, fax, printer, and Universal Send, and containing a large capacity HDD to facilitate such capabilities.
Control software	Software that runs on the hardware of the device, and controls security functions.
Control panel	One of the hardware elements of the MFP, consisting of a touch panel and operation keys, which provides the interface for operation of the MFP.
Remote UI	An interface that provides access to the MFP from a Web browser via the LAN, to allow the acquisition of operating status, perform job operations or BOX operations, and making various settings.
HDD	Hard disk drive mounted on the MFP, where control software and assets are stored.
I-Fax	Short for Internet Fax. Uses the Internet to receive and send faxes.
Image file	Image data generated within the MFP, from operations such as scan, print, and receive.
Temporary image file	Image files generated during jobs such as Copy and Print, which are needed only until the job completes.
Roles	Used by access restriction functions to restrict the functions that each user can use. One role is associated with each user. In addition to pre-defined default roles, default roles may be modified to create custom roles. The default roles are: Administrator, Power User, General User, Limited User, and Guest User. A user assigned the Administrator role is capable of using management operations (administrative privileges).
Administrator	User assigned the Administrator role and has administrative privileges. Equivalent to U.ADMINISTRATOR defined in the PP.

Terms/Abbreviations	Description
Job	When a user uses the functions of the TOE to execute an operation on a document, a Job is the intended document data combined with the user instructions for processing those data. The operations that can be performed on a document are: Scan, Print, Copy, Fax TX, Save, and Delete. The processing phases for a Job issued by the user are: generation, execution, and completion.
Document data	User data processed within the MFP, consisting of image files and attribute information.
Memory RX (Reception)	Allows data received by fax/I-fax to be stored in the Memory RX Inbox for later processing.
Box	Collective name for Mail Boxes, Fax Inboxes, or the Memory RX Inbox wherein data from operations such as scan, print, and received faxes are stored in the MFP. *Use of Fax Inboxes is not included in this TOE.
Mail Box	Whether a general user feeds data to the MFP directly, or specifies a document for printing from a PC, data can be stored here to be printed or sent later.
Memory RX Inbox	When memory reception is set, documents received by fax/I-fax are stored in the Memory RX Inbox. Stored documents can be printed or sent later.
Mail server	Server that facilitates I-fax transmission or email transmission of document data in the MFP.
User authentication server	Server that maintains user information such as user ID and password, for user authentication over the network.
Firewall	Device or system designed to protect the internal LAN against threats from the Internet.
Time server	Server that uses the Network Time Protocol to provide the accurate time over the Internet.
[Secured Print]	A button on the control panel that activates the Secured Print function (print jobs with a PIN).
[Copy]	A button on the control panel that activates the Copy function.
[Scan]	Indicates the [Scan and Store] and [Scan and Send] buttons on the control panel, that allow the user to scan paper documents to be stored as files, or scanned documents to be sent to some location such as to an email address or a shared folder in a PC, respectively.
[Access Stored Files]	A button on the control panel that allows the user to access files stored in a Mail Box/Inbox.
Remote UI [Access Stored Files]	A button on the remote UI that allows the user to access files stored in a Mail Box/Inbox.

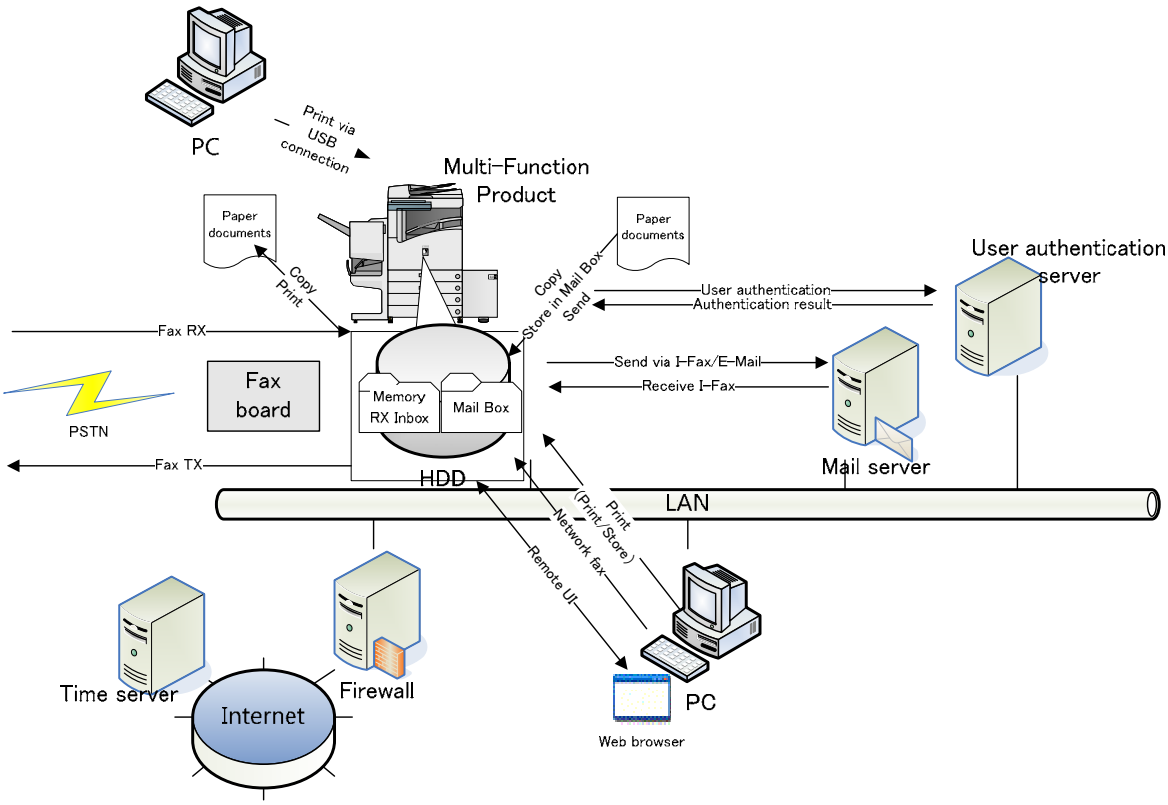
1.5 TOE description

The TOE is a MFP that offers Copy, Print, Universal Send, Fax, I-Fax RX, and Mail Box capabilities. The TOE, which conforms to ":2600.1, Protection Profile for Hardcopy Devices, Operational Environment A" is designed to operate in an environment such as the one shown below (as excerpted from ":2600.1, Protection Profile for Hardcopy Devices, Operational Environment A" clause "1.1 Scope").

This standard is for a Protection Profile for Hardcopy Devices in a restrictive commercial information processing environment in which a relatively high level of document security, operational accountability, and information assurance are required. The 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. This environment will be known as "Operational Environment A."

Figure 1 shows the environment for which the TOE or < Canon imageRUNNER ADVANCE C5200 Series 2600.1 model > has been designed, with options included. Since not all of these features may be required, the actual operational environment is expected to differ than what is shown here.

Figure 1 The assumed operational environment of the MFP
< Canon imageRUNNER ADVANCE C5200 Series **>**



In Figure 1, the MFP is connected by an internal LAN, to all of the other major components, namely the Mail Server, User Authentication Server, PC, and Firewall. Furthermore, the internal LAN is protected by Firewall from threats from the Internet. To send (via I-Fax or email) a previously scanned document or when receiving a document by I-Fax for example, the MFP connects to the Mail Server. By using a PC with a Web browser[1], functions such as printing, storing, or I-Fax can also be executed remotely. However, in order to print from a PC, the appropriate printer driver needs to be installed in the PC. Alternatively, a USB could be used to connect the PC directly, and print or store document data from the PC. In this case, some

[1] This evaluation was performed using Microsoft Internet Explorer 8 as the Web browser.

configuration is required initially, in order to protect against data being taken out of the MFP and stored in a PC or USB device. Additionally, by attaching a fax board to the TOE, faxes can be sent and received over phone lines via the fax board.

The TOE also obtains accurate time from the Time server for time synchronization, and supports user authentication through the External Authentication Server. The functions available to the MFP in such an environment are listed below:

- Copy function

  Produces duplicates of the hardcopy document by scanning and printing.

- Print function

  Produces a hardcopy document from its electronic form (contained in the MFP or sent from a PC).

- I-Fax RX (receive) function

  Uses the Internet to receive faxes. Data received by I-fax is not printed immediately; rather it is stored for processing at a later time. Stored documents can be printed or sent later.

- Fax RX (receive) function

  Uses a fax line to receive faxes. Data received by fax is not printed immediately; rather it is stored for processing at a later time. Stored documents can be printed or sent later.

- Fax TX (send) function

  Scanned document data or electronic documents stored in a Mail Box or in Memory RX Inbox can be retrieved for transmission by fax.

- Universal Send function

  Scanned document data or electronic documents stored in a Mail Box or in Memory RX Inbox can be transmitted by email or I-fax, or sent to a shared folder on a PC, in TIFF or PDF file format.

- Box

  Refers to the storage of image files into a Mail Box or in Memory RX Inbox, or to functions that utilize the Mail Box/inbox functionality.

  - Image files Stored in Mail Box or Memory RX Inbox

    Scanned document data or electronic data specified for storage from a PC, are stored in a Mail Box, or documents received by fax/I-fax are stored in a Fax Inbox or in Memory RX Inbox.

  - Functions that utilize Box functionality

    The following functions can be executed on data stored in a Mail Box.

    - Edit
    - Print
    - Send
    - Delete

    The following functions can be executed on data stored in the Memory RX Inbox.

    - Print
    - Send

- Delete

1.6 Scope of the TOE

The TOE conforms to ":2600.1, Protection Profile for Hardcopy Devices, Operational Environment A" and is designed to meet the requirements specified therein, as described below.

The physical and logical scopes of the TOE are described below.

1.6.1 Physical Scope of the TOE

The TOE is a MFP consisting of hardware and software components. The physical scope of the TOE is illustrated in Figure 2.

Figure 2 Hardware and software components of the TOE

<table>
<tr><td colspan="2">Control Software</td></tr>
<tr><td>Canon imageRUNNER ADVANCE C5200 Series
MFP Main Unit
(TOE: Hardware)</td><td>HDD Data Encryption & Mirroring Board
(TOE: Hardware)</td></tr>
</table>

In Figure 2, "Control Software" refers to the < iR-ADV Security Kit-C1 for IEEE 2600.1 Common Criteria >.
Note also that the "MFP Main Unit" together with the < iR-ADV Security Kit-C1 for IEEE 2600.1 Common Criteria > make up the MFP main unit.

The TOE or < Canon imageRUNNER ADVANCE C5200 Series 2600.1 model > consists of the MFP main unit combined with the HDD Data Encryption & Mirroring Board. Note that, use of the fax function requires attachment of a fax board (which is outside the scope of the TOE).

< Canon imageRUNNER ADVANCE C5200 Series >, or the hardware making up the TOE, refers to the following product lineup.

Table 2 —Line of Products

Products
iR-ADV C5255 / iR-ADV C5250 / iR-ADV C5240 / iR-ADV C5235

The documentation for the TOE are listed below.

(English Name)
- imageRUNNER ADVANCE C5255/ C5250/ C5240/ C5235 e-Manual
- iR-ADV Security Kit-C1 for IEEE 2600.1 Common Criteria Certification Administrator Guide
- ACCESS MANAGEMENT SYSTEM Individual Management Configuration Administrator Guide
- HDD Data Encryption & Mirroring Kit-C Series User Documentation
- Before Using iR-ADV Security Kit-C1 for IEEE 2600.1 Common Criteria Certification

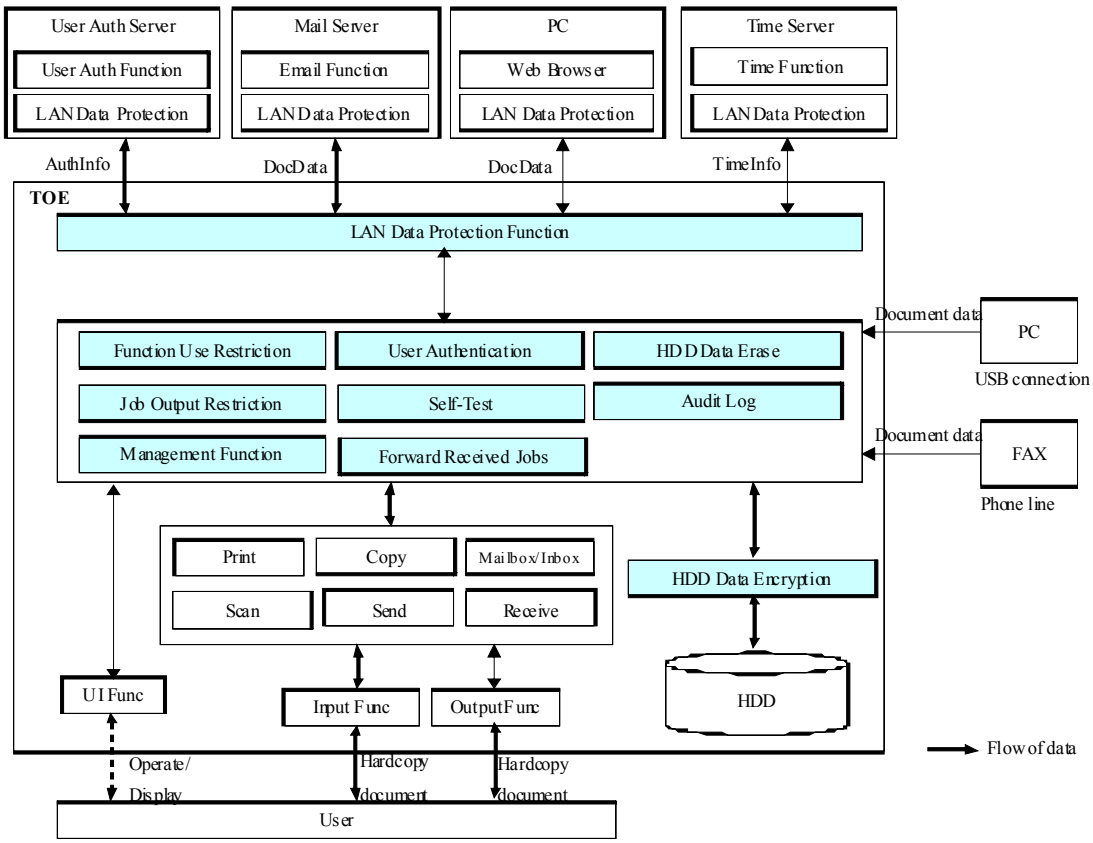
(Japanese Name)
- imageRUNNER ADVANCE C5255/ C5255F/ C5250/ C5250F/ C5240/ C5240F/ C5235/ C5235F e-Manual
- iR-ADV Security Kit-C1 for IEEE 2600.1 Administrator Guide

- ACCESS MANAGEMENT SYSTEM Kit-B1 Individual Management Configuration Administrator Guide
- HDD Data Encryption Kit User's Guide
- To Read Before Using iR-ADV Security Kit-C1 for IEEE 2600.1

1.6.2 Logical Scope of the TOE

The logical scope of the TOE is illustrated in Figure 3 (excluding: User, User Authentication Server, Mail Server, PC, and Time Server). In the table, the security functions of the TOE are shown in blue.

Figure 3 Functional configuration of the TOE



In addition to the capabilities described in Section 1.5, the TOE embodies the following basic functionality.

- UI Functionality

  Enables the user to operate the TOE from the control panel, and the TOE to display information on the control panel.

- Output Functionality

  Enables the TOE to output hardcopy documents.

- Input Functionality

  Enables the TOE to input hardcopy documents.

The TOE embodies the following security functions.

- User Authentication Function

  Performs authentication on the user, to prevent any unauthorized access to the TOE.

  Two types of user authentication are supported: Internal Authentication wherein authentication takes place internally within the TOE, and External Authentication which uses an external user authentication server. External authentication uses Kerberos or LDAP authentication[2].

- Function Use Restriction Function

  Uses role management to restrict the functions that each authenticated user can use.

- Job Output Restriction Function

  This function restricts access to print, cancel, and other job operations, to the user that executed the job.

- Forward Received Jobs Function

  This function restricts the machine from forwarding received data directly to the LAN. It is provided as a countermeasure against threats arising from misuse of the fax line.

- HDD Data Erase Function

  Function for erasing unnecessary data from the hard disk by overwriting the data, in order to prevent unauthorized use of previously generated image data.

- HDD Data Encryption Function

  Because the HDD (alone or together with the HDD Data Encryption & Mirroring Board) could potentially be removed for unauthorized access to its contents, the HDD Data Encryption & Mirroring Board addresses this threat by identifying the MFP at startup, so that it may only be used with the correct MFP. Additionally, all data stored in the HDD are encrypted to protect the confidentiality of the HDD data.

- LAN Data Protection Function

  To protect LAN data from IP packet sniffing, IP packets are encrypted using IPSec.

- Self-Test Function

  When the machine starts, this function checks to see that the primary security functions are running properly.

- Audit Log Function

  Allows auditing of user operations by generating logs which are stored in the HDD. Stored audit logs are protected and can be viewed.

  The date/time recorded on the audit log is provided by the TOE. The TOE's date/time information is set by the Management Function, or is set by time synchronization when the accurate time is obtained from the Time Server.

- Management Function

  Consists of user management functions such as user registration and role management, and device management functions which enable proper operation of various security functions, which can only be specified by Administrators.

[2] This evaluation was performed using eDirectory 8.8 SP7 as the authentication server software for LDAP authentication.

1.7 Users of the TOE

The TOE has two types of users (U.USER): U.NORMAL and U.ADMINISTRATOR

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.
	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.

1.8 Assets

There are three types of assets: user data, TSF data, and functions.

1.8.1 User Data

User data are created by the user, and have no effect on TOE security functions. There are two types of user data: D.DOC and D.FUNC.

Table 4 — User Data

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

1.8.2 TSF Data

TSF Data are data that have an effect on TOE security functions. There are two types of TSF data: D.PROT and D.CONF.

Table 5 — TSF Data

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

A list of the TSF data used in this TOE is given in Table 6.

Table 6 — List of TSF data

Type	TSF data	Description	Stored in
D.PROT	User name	User identification information used by the user identification and authentication function.	HDD
	Role	Used by access restriction functions to restrict the functions that each user can use.	HDD
	Lockout policy settings	Settings for the lockout function, such as number of attempts before lockout and the lockout time.	HDD
	Password policy settings	Policy for the password for user authentication, such as minimum password length, allowed characters, and combination of character types.	HDD
	Auto Reset Time setting	Settings for session timeout in the control panel.	Non-volatile memory
	Date/Time setting	Specifies the date and time that is set.	RTC
	HDD Data Erase setting	Settings for the HDD Data Erase function, including the settings to enable or disable the HDD Data Erase function.	Non-volatile memory
	IPSec settings	Settings for the LAN Data Protection function, including the settings to enable or disable the LAN Data Protection function.	Non-volatile memory
D.CONF	Password	Password used to authenticate the user in the User Identification and Authentication function.	HDD
	Audit logs	Logs generated by the Audit Log function.	HDD
	Box PIN	PIN used for access control to the Mail Box or the Memory RX Inbox where the data is stored, for Job Output Restriction functions.	HDD

1.8.3 Functions

Refer to the functions listed in Table 7.

2 Conformance claims

2.1 CC Conformance claim

This ST conforms to the following Common Criteria (CC).

- Common Criteria version: Version 3.1 Release 4
- Common Criteria conformance: Part 2 extended and Part 3 conformant
- Assurance level: EAL3 augmented by ALC_FLR.2

2.2 PP claim, Package claim

This ST conforms to the following Protection Profile (PP).

- Title :2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
  - Version:1.0, dated June 2009

This ST is package-conformant to and package-augmented by the following SFR packages:

- 2600.1-PRT conformant
- 2600.1-SCN conformant
- 2600.1-CPY conformant
- 2600.1-FAX conformant
- 2600.1-DSR conformant
- 2600.1-NVS augmented
- 2600.1-SMI augmented

2.3 SFR Packages

2.3.1 SFR Packages reference

Title: 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as printers, paper-based fax machines, and MFPs) that perform a printing function in which electronic document input is converted to physical document output.

Title: 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as scanners, paper-based fax machines, and MFPs) that perform a scanning function in which physical document input is converted to electronic document output.

Title: 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This Protection Profile shall be used for HCD products (such as copiers and MFPs) that perform a copy function in which physical document input is duplicated to physical document output.

Title: 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as fax machines and MFPs) that perform a scanning function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a printing function in which a telephone-based document facsimile (fax) reception is converted to physical document output.

Title: 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as MFPs) that perform a document storage and retrieval feature in which a document is stored during one job and retrieved during one or more subsequent jobs.

Title: 2600.1-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 extended and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for products that provide storage of User Data or TSF Data in a nonvolatile storage device (NVS) that is part of the evaluated TOE but is designed to be removed from the TOE by authorized personnel. This package applies for TOEs that provide the ability to protect data stored on Removable Nonvolatile Storage devices from unauthorized disclosure and modification. If such protection is supplied only by the TOE environment, then this package cannot be claimed.

Title: 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 extended and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products that transmit or receive User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio frequency wireless media. This package applies for TOEs that provide a trusted channel function allowing for secure and authenticated communication with other IT systems. If such protection is supplied by only the TOE environment, then this package cannot be claimed.

2.3.2 SFR Package functions

Functions perform processing, storage, and transmission of data that may be present in HCD products. The functions that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 7:

Table 7 —SFR Package functions

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.NVS	Nonvolatile storage: a function that stores User Data or TSF Data on a nonvolatile storage device that is part of the evaluated TOE but is designed to be removed from the TOE by authorized personnel
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

2.3.3 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. The attributes that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 8:

Table 8 —SFR Package attributes

Designation	Definition
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+NVS	Indicates data that are stored on a nonvolatile storage device.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

2.4 PP Conformance rationale

In addition to the primary functionality of the MFP (Copy, Print, Scan, and Fax), the TOE implements the document storage function, HDD encryption function, and the LAN data encryption function. As such, it is appropriate to conform to all of the SFR Packages defined in the PP.

In the following, the ST is compared against the PP containing all seven of the aforementioned SFR Packages.

In terms of the Security Problem Definition, the ST is equivalent to the PP except for the addition of one other OSP:

P.HDD.ACCESS.AUTHORIZATION

This OSP is a restriction on the TOE, rather than a restriction on the operational environment.

As such:

- All TOEs that would meet the security problem definition in the ST also meet the security problem definition in the PP.

- All operational environments that would meet the security problem definition in the PP would also meet the security problem definition in the ST.

In terms of Objectives, the ST is equivalent to the PP except for the addition of one other objective:

O.HDD.ACCESS.AUTHORISED

This objective is a restriction on the TOE.

As such:

- All TOEs that would meet the security objectives for the TOE in the ST also meet the security objectives for the TOE in the PP.
- All operational environments that would meet the security objectives for the operational environment in the PP would also meet the security objectives for the operational environment in the ST.

In terms of the functional requirements, the ST compared with the PP contains all functional requirements of the PP including the seven SFR Packages, as well as additional functional requirements, as shown in Table 9.

Table 9 — Functional requirements specified in the PP and the ST

PP_Package	PP functional requirement	ST functional requirement
Common	FAU_GEN.1	FAU_GEN.1
Common	FAU_GEN.2	FAU_GEN.2
Common	FAU_SAR.1	FAU_SAR.1
Common	FAU_SAR.2	FAU_SAR.2
Common	FAU_STG.1	FAU_STG.1
Common	FAU_STG.4	FAU_STG.4
Common	FDP_ACC.1(a)	FDP_ACC.1(delete-job)
Common	FDP_ACC.1(b)	FDP_ACC.1(exec-job)
Common	FDP_ACF.1(a)	FDP_ACF.1(delete-job)
Common	FDP_ACF.1(b)	FDP_ACF.1(exec-job)
Common	FDP_RIP.1	FDP_RIP.1
Common	FIA_ATD.1	FIA_ATD.1
Common	FIA_UAU.1	FIA_UAU.1
Common	FIA_UID.1	FIA_UID.1
Common	FIA_USB.1	FIA_USB.1
Common	FMT_MSA.1(a)	FMT_MSA.1(delete-job)
Common	FMT_MSA.3(a)	FMT_MSA.3(delete-job)
Common	FMT_MSA.1(b)	FMT_MSA.1(exec-job)
Common	FMT_MSA.3(b)	FMT_MSA.3(exec-job)
Common	FMT_MTD.1(FMT_MTD.1.1(a))	FMT_MTD.1(device-mgt)
Common	FMT_MTD.1(FMT_MTD.1.1(b))	FMT_MTD.1(user-mgt)
Common	FMT_SMF.1	FMT_SMF.1
Common	FMT_SMR.1	FMT_SMR.1
Common	FPT_STM.1	FPT_STM.1
Common	FPT_TST.1	FPT_TST.1
Common	FTA_SSL.3	FTA_SSL.3(lui), FTA_SSL.3(rui)
PRT	FDP_ACC.1	FDP_ACC.1(prt)
PRT	FDP_ACF.1	FDP_ACF.1(prt)
SCN	FDP_ACC.1	FDP_ACC.1(box)
SCN	FDP_ACF.1	FDP_ACF.1(box)
CPY	FDP_ACC.1	FDP_ACC.1(box)
CPY	FDP_ACF.1	FDP_ACF.1(box)
FAX	FDP_ACC.1	FDP_ACC.1(box)
FAX	FDP_ACF.1	FDP_ACF.1(box)
DSR	FDP_ACC.1	FDP_ACC.1(box)
DSR	FDP_ACF.1	FDP_ACF.1(box)
NVS	FPT_CIP_EXP.1	FPT_CIP_EXP.1
SMI	FAU_GEN.1	FAU_GEN.1

PP_Package	PP functional requirement	ST functional requirement
SMI	FPT_FDI_EXP.1	FPT_FDI_EXP.1
SMI	FTP_ITC.1	FTP_ITC.1
Common	-	FIA_AFL.1
Common	-	FIA_SOS.1
Common	-	FIA_UAU.7
NVS	-	FCS_COP.1(h)
NVS･SMI	-	FCS_CKM.1
SMI	-	FCS_COP.1(n)
SMI	-	FCS_CKM.2
NVS	-	FPT_PHP.1

Note the following:

For FDP_ACF.1(a) in the PP, the Subject for a Delete of +FAXIN D.DOC, and Delete of +FAXIN D.FUNC is specified as U.NORMAL.

For FDP_ACF.1(delete-job) in the ST, the Subject is specified as U.ADMINISTRATOR, with Access Control rule for U.NORMAL specified as "Denied".

For FDP_ACC.1 in the PP, the Subject for a Read of +FAXIN D.DOC is specified as U.NORMAL.

For FDP_ACC.1(box) in the ST, the Subject is specified as U.ADMINISTRATOR, with Access Control rule for U.NORMAL specified as "Denied".

The ST functional requirements as mentioned above, are restrictive in the scope of Subjects allowed to Delete or Read, and restrains U.NORMAL from having access to any Object. As such, the ST functional requirements specify greater restrictions than the corresponding PP functional requirements.

For FDP_ACF.1(a) in the PP, the Subject for a Modify of +FAXIN D.FUNC is specified as U.NORMAL.

For FDP_ACF.1(delete-job) in the ST, the Subject is specified as U.User, with Access Control rule specified as "Denied".

The ST functional requirement as mentioned above, does not allow use of the function to any Subject. As such, the ST functional requirement specifies greater restriction than the corresponding PP functional requirement.

Consequently, the SFRs of the ST are equivalent or more restrictive than SFRs of the PP.

As such:

- All TOEs that would meet the SFRs in the ST would also meet the SFRs in the PP.

In terms of the Security Assurance Requirements, the ST and PP are equivalent.

As such, this ST compared with the PP, specifies equal or greater restrictions on the TOE, and at most equal restrictions on the operational environment of the TOE.

Therefore, this ST claims demonstrable conformance to the PP.

3 Security Problem Definition

3.1 Notational conventions

- Defined terms in full form are set in title case (for example, "Document Storage and Retrieval").
- Defined terms in abbreviated form are set in all caps (for example, "DSR").
- In tables that describe Security Objectives rationale, a checkmark ("✓") place at the intersection of a row and column indicates that the threat identified in that row is wholly or partially mitigated by the objective in that column.
- In tables that describe completeness of security requirements, a **bold** typeface letter "P" placed at the intersection of a row and column indicates that the requirement identified in that row performs a principal fulfillment of the objective indicated in that column. A letter "S" in such an intersection indicates that it performs a supporting fulfillment.
- In tables that describe the sufficiency of security requirements, a **bold** typeface requirement name and purpose indicates that the requirement performs a principal fulfillment of the objective in the same row. Requirement names and purposes set in normal typeface indicate that those requirements perform supporting fulfillments.In specifications of Security Functional Requirements (SFRs):

o **Bold typef**ace indicates the portion of an SFR that has been completed or refined in this Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition.

o *Italic* typeface indicates the portion of an SFR that must be completed by the ST Author in a conforming Security Target.

o ***Bold italic*** typeface indicates the portion of an SFR that has been partially completed or refined in this Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition, but which also must be completed by the ST Author in a conforming Security Target.

- The following prefixes are used to indicate different entity types:

Table 10— Notational prefix conventions

Prefix	Type of entity
U.	User
D.	Data
F.	Function
T.	Threat
P.	Policy
A.	Assumption
O.	Objective
OE.	Environmental objective
+	Security attribute

3.2 Threats agents

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

a) Persons who are not permitted to use the TOE who may attempt to use the TOE

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

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

d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

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

3.3 Threats to TOE Assets

This section describes threats to assets described in clause 1.8.

Table 11—Threats to User Data for the TOE

Threat	Affected asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons

Table 12—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

3.4 Organizational Security Policies

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 13—Organizational Security Policies

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

3.5 Assumptions

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

Table 14—Assumptions

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

4 Security Objectives

4.1 Security Objectives for the TOE

This section describes the Security Objectives that are satisfied by the TOE.

Table 15— 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.HDD.ACCESS.AUTHORISED	The TOE shall protect TOE assets in the HDD from accessing without the TOE authorization.

4.2 Security Objectives for the IT environment

This section describes the Security Objectives for the IT environment.

Table 16— Security Objectives for the IT environment

Objective	Definition
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.

4.3 Security Objectives for the non-IT environment

This section describes the Security Objectives for non-IT environments.

Table 17— Security Objectives for the non-IT environment

Objective	Definition
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization, and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization, have the training, competence, and time to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.4 Security Objectives rationale

This section describes the rationale for the Security Objectives.

Table 18—Completeness of Security Objectives

	Objectives																		
Threats. Policies, and Assumptions	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.HDD.ACCESS.AUTHORISED	OE.AUDIT_STORAGE.PROTECTED	OE.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															✓		✓			
P.HDD.ACCESS.AUTHORIZATION											✓									
A.ACCESS.MANAGED																✓				
A.ADMIN.TRAINING																		✓		
A.ADMIN.TRUST																			✓	

Threats. Policies, and Assumptions	Objectives																		
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.HDD.ACCESS.AUTHORISED	OE.AUDIT_STORAGE.PROTECTED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
A.USER.TRAINING																			✓

Table 19—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
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration
		OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion and modifications
		OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed
P.HDD.ACCESS.AUTHORIZATION	To prevent access TOE assets in the HDD with connecting the other HCDs, TOE will have authorized access the HDD data.	O.HDD.ACCESS.AUTHORISED protects TOE assets in the HDD from accessing without the TOE authorization.
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.TRUST 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 (APE_ECD)

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

5.1 FPT_CIP_EXP Confidentiality and integrity of stored data

Family behaviour:

This family defines requirements for the TSF to protect the confidentiality and integrity of both TSF and user data.

Confidentiality and integrity of stored data is important security functionality in the case where the storage container is not, or not always, in a protected environment. Confidentiality and integrity of stored data is often provided by functionality that the TSF uses for both TSF and user data in the same way. Examples are full disk encryption functions, where the TSF stores its own data as well as user data on the same disk. Especially when a disk is intended to be removable and therefore may be transported into an unprotected environment, this becomes a very important functionality to achieve the Security Objectives of protection against unauthorized access to information.

Component leveling:

FPT_CIP_EXP.1 Confidentiality andintegrity of stored data	1

FPT_CIP_EXP.1 Confidentiality and integrity of stored data, provides for the protection of user and TSF data stored on a storage container that cannot be assumed to be protected by the TOE environment.

Management: FPT_CIP_EXP.1

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

a) Management of the conditions under which the protection function is activated or used;

b) Management of potential restrictions on the allowance to use this function.

Audit: FPT_CIP_EXP.1

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

a) Basic: failure condition that prohibits the function to work properly, detected attempts to bypass this functionality (e. g. detected modifications).

FPT_CIP_EXP.1 Confidentiality and integrity of stored data

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_CIP_EXP.1.1 The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data when either is written to [assignment: *media used to store the data*].

FPT_CIP_EXP.1.2 The TSF shall provide a function that detects and performs [assignment: *list of actions*] when it detects alteration of user and TSF data when

either is written to [assignment: *media used to store the data*].

Rationale:

The Common Criteria defines the protection of user data in its FDP class and the protection of TSF data in its FPT class. Although both classes contain components that define confidentiality protection and integrity protection, those components are defined differently for user data and TSF data and therefore are difficult to use in cases where a TOE provides functionality for the confidentiality and integrity for both types of data in an identical way.

This Protection Profile defines an extended component that combines the confidentiality and integrity protection for both types of data in a single component. The authors of this Protection Profile view this as an approach that simplifies the statement of security functional requirements significantly and therefore enhances the readability and applicability of this Protection Profile. 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 FPT class. Since it is intended to protect data that are exported to storage media, and in particular, storage media that might be removable from the TOE, 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.

5.2 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	1

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

Management: FPT_FDI_EXP.1

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

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

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

c) Revocation of such an allowance.

Audit: FPT_FDI_EXP.1

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 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

This section describes the security requirements for the TOE.

6.1 Security functional requirements

This section describes the security functional requirements for the TOE.
The text in brackets following the component identifier or element name denotes iteration operations.

6.1.1 User Authentication Function

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 1 to 10

[assignment: *list of authentication events*]
- Login attempts from the control panel or remote UIs.

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

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 name, role

FIA_UAU.1 Timing of authentication

Hierarchical to: **No other components.**

Dependencies: **No dependencies.**

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***]
- Submission of print jobs, fax jobs, I-fax jobs

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

FIA_UAU.7 Protected authentication feedback

Hierarchical to: **No other components.**

Dependencies: **FIA_UAU.1 Timing of authentication**

FIA_UAU .7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

[assignment: *list of feedback*]
- *

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***]
- Submission of print jobs, fax jobs, I-fax jobs

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

FIA_USB.1 User-subject binding

Hierarchical to: **No other components.**

Dependencies: **FIA_ATD.1 User attribute definition**

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

[assignment: *list of user security attributes*]
- User name, role

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

FTA_SSL.3(lui) TSF-initiated termination

Hierarchical to: **No other components.**

Dependencies: **No dependencies.**

FTA_SSL.3.1(lui) The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

[assignment: *time interval of user inactivity*]
- User inactivity at the control panel lasting for the specified period of time.

FTA_SSL.3(rui) TSF-initiated termination

Hierarchical to: **No other components.**

Dependencies: **No dependencies.**

FTA_SSL.3.1(rui) The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

[assignment: *time interval of user inactivity*]
- User inactivity at the remote UI lasting for 15 minutes.

6.1.2 Function Use Restriction Function

FMT_MSA.1(exec-job) 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(exec-job) 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]*]
- query, modify, delete, insert

[assignment: *list of security attributes*]
- Role

[assignment: *the authorised identified roles*]
- U.ADMINISTRATOR

FMT_MSA.3(exec-job) 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(exec-job) 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]*]
- Restrictive

[refinement]
- TOE Function Access Control Policy -> TOE Function Access Control SFP

FMT_MSA.3.2(exec-job) 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

FDP_ACC.1(exec-job) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(exec-job) 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**.

FDP_ACF.1(exec-job) 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(exec-job) 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***]

- objects controlled under the TOE Function Access Control SFP in Table 20, and for each, the indicated security attributes in Table 20.

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

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

- [**assignment:** ***other conditions***]

[**assignment: other conditions**]

- rules specified in the TOE Function Access Control SFP in Table 20 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects

FDP_ACF.1.3(exec-job) 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(exec-job) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of*

subjects to objects]
- None

Table 20—TOE Function Access Control SFP

Object	Attribute	Operation(s)	Subject	Attribute	Access control rule
[Secured Print]	+PRT	Use of the function, using pointer to the Object.	U.USER	Role	For the attribute of the Object, the role associated with the Subject, must be authorized to perform the Operation.
[Copy]	+CPY +DSR	Use of the function, using pointer to the Object.	U.USER	Role	For the attribute of the Object, the role associated with the Subject, must be authorized to perform the Operation.
[Scan]	+SCN +DSR	Use of the function, using pointer to the Object.	U.USER	Role	For the attribute of the Object, the role associated with the Subject, must be authorized to perform the Operation.
[Fax]	+FAXOUT	Use of the function, using pointer to the Object.	U.USER	Role	For the attribute of the Object, the role associated with the Subject, must be authorized to perform the Operation.
[Fax/I-Fax Inbox]	+FAXIN	Use of the function, using pointer to the Object.	U.USER	Role	For the attribute of the Object, the role associated with the Subject, must be authorized to perform the Operation.
[Access Stored Files]	+DSR	Use of the function, using pointer to the Object.	U.USER	Role	For the attribute of the Object, the role associated with the Subject, must be authorized to perform the Operation.
Remote UI [Access Stored Files]	+DSR +FAXIN	Use of the function, using pointer to the Object.	U.USER	Role	If the role associated with the Subject is Administrator, the Operation is permitted.

6.1.3 Job Output Restriction Functions

6.1.3.1 Delete Job

FMT_MSA.1(delete-job) 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(delete-job) The TSF shall enforce the **Common Access Control SFP in Table 22,** [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)*]
- **PRT Access Control SFP in Table 23**
- **BOX Access Control SFP in Table 24**

[selection: *change_default, query, modify, delete, [assignment: other operations]*]
- Refer to **"Operation"** in Table 21.

[assignment: *list of security attributes*]
- Refer to **"Security Attributes"** in Table 21.

[assignment: *the authorised identified roles*]
- Refer to **"Role"** in Table 21.

Table 21—Management of security attributes

Security Attributes	Operation	Role
User name	modify, delete, create, query, insert	U.ADMINISTRATOR
Box PINs	modify, delete, create	U.ADMINISTRATOR
PIN of own Mail Box	modify	U.NORMAL

APPLICATION NOTE 1. This Protection Profile does not define any mandatory security attributes, but some may be defined by SFR packages or by the ST Author. The ST Author should define how security attributes are managed. Note that this Protection Profile allows the ST Author to instantiate "Nobody" as an authorized identified role, which makes it possible for the ST Author to state that some management actions (e.g., deleting a security attribute) may not be performed by any User.

FMT_MSA.3(delete-job) 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(delete-job) The TSF shall enforce the **Common Access Control SFP in Table 22,** [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*]
- **Common Access Control SFP in Table 22**
- **PRT Access Control SFP in Table 23**
- **BOX Access Control SFP in Table 24**

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

FMT_MSA.3.2(delete-job) 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

FDP_ACC.1(delete-job)Subset access control

Hierarchical to: **No other components.**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1(delete-job) The TSF shall enforce the **Common Access Control SFP in Table 22** on **the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 22**.

FDP_ACF.1(delete-job) 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(delete-job) The TSF shall enforce the **Common Access Control SFP in** Table 22 to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 22, and for each, the indicated security attributes in Table 22**.

FDP_ACF.1.2(delete-job) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the Common Access Control SFP in Table 22 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects**.

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

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
- U.ADMINISTRATOR is authorized to delete any D.DOC/D.FUNC.
- U.ADMINISTRATOR is authorized to modify any +FAXOUT D.FUNC.

FDP_ACF.1.4(delete-job) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
- None

Table 22—Common Access Control SFP

Object	Attribute	Operation(s)	Subject	Access control rule
D.DOC	+PRT,+SCN,+CPY, +FAXOUT, +DSR,+NVS,+SMI	Delete	U.NORMAL	Denied, except for his/her own documents
D.DOC	+FAXIN	Delete	U.NORMAL	Denied
D.FUNC	+PRT,+SCN,+CPY, ＋FAXOUT +DSR,+NVS,+SMI	Modify; Delete	U.NORMAL	Denied, except for his/her own function data

Object	Attribute	Operation(s)	Subject	Access control rule
D.FUNC	+FAXIN	Modify	U.USER	Denied
D.FUNC	+FAXIN	Delete	U.NORMAL	Denied

6.1.3.2 Temporarily Stored Print Jobs

FDP_ACC.1(prt) Subset access control

Hierarchical to: **No other components.**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1(prt) The TSF shall enforce the **PRT Access Control SFP in Table 23** on **the list of subjects, objects, and operations among subjects and objects covered by the PRT Access Control SFP in Table 23**.

FDP_ACF.1(prt) 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(prt) The TSF shall enforce the **PRT Access Control SFP in Table 23** to objects based on the following: **the list of subjects and objects controlled under the PRT Access Control SFP in Table 23, and for each, the indicated security attributes in Table 23**.

FDP_ACF.1.2(prt) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the PRT Access Control SFP in Table 23 governing access among Users and controlled objects using controlled operations on controlled objects**.

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

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
- None

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

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
- None

Table 23—PRT Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+PRT	Read	U.NORMAL	Denied, except for his/her own documents

6.1.3.3 Document Data Stored in Mail Box

FDP_ACC.1(box) Subset access control

Hierarchical to: **No other components.**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1(box) The TSF shall enforce the **BOX Access Control SFP in Table 24** on **the list of subjects, objects, and operations among subjects and objects covered by the BOX Access Control SFP in Table 24**.

FDP_ACF.1(box) 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(box) The TSF shall enforce the **BOX Access Control SFP in Table 24** to objects based on the following: **the list of subjects and objects controlled under the BOX Access Control SFP in Table 24, and for each, the indicated security attributes in Table 24**.

FDP_ACF.1.2(box) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the BOX Access Control SFP in Table 24 governing access among Users and controlled objects using controlled operations on controlled objects**.

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

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
- None

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

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
- None

Table 24—BOX Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+SCN, +CPY, +DSR, +FAXOUT	Read	U.NORMAL	Denied, except for his/her own documents
D.DOC	+FAXIN	Read	U.NORMAL	Denied

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+SCN, +CPY, +DSR,+FAXIN, +FAXOUT	Read	U.ADMINISTRATOR	Denied, except (1) for his/her own documents, or (2) if authorized by mechanism if such functions are provided by a conforming TOE

6.1.4 Forward Received Jobs Function

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components.

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

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

6.1.5 HDD Data Erase Function

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

6.1.6 HDD Data Encryption Function

6.1.6.1 Encryption/Decryption Function

FCS_COP.1(h) Cryptographic operation

Hierarchical to: No other components.

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

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

meet the following: [assignment: *list of standards*].

[assignment: *list of cryptographic operations*]
- Encryption of data written to the HDD
- Decryption of data read out from the HDD

[assignment: *cryptographic algorithm*]
- AES

[assignment: *cryptographic key sizes*]
- 256 bit

[assignment: *list of standards*]
- FIPS PUB 197

FPT_CIP_EXP.1 Confidentiality and integrity of stored data

Hierarchical to: **No other components.**

Dependencies: **No dependencies**

FPT_CIP_EXP.1.1 The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data when either is written to [assignment: ***a Removable Nonvolatile Storage device***].

[assignment: ***a Removable Nonvolatile Storage device***]
- HDD

FPT_CIP_EXP.1.2 The TSF shall provide a function that detects and performs [assignment: *list of actions*] when it detects alteration of user and TSF data when either is written to [assignment: ***a Removable Nonvolatile Storage device***].

[assignment: *list of actions*]
- no action

[assignment: ***a Removable Nonvolatile Storage device***]
- HDD

APPLICATION NOTE 2. Today many manufacturers are looking at hardware solutions such as fully encrypting disks to meet disk encryption requirements. Some of these drives will not allow data to be written to the drive unless the correct credentials (either the key itself or credentials required to unlock the key stored in a secure area of the drive) are presented. Assuming that this functionality can not be bypassed, detection of modifications is not a useful function within the TOE and therefore it should be possible to instantiate "no action" in the assignment for the "list of actions" in FPT_CIP_EXP.1.2, arguing that unauthorized modification is prevented by the design of the system.
Quote from [PP Guide]

6.1.6.2 Device Identification and Authentication Function

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: **No other components.**

Dependencies: **No dependencies.**

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

[refinement] physical tampering → Physical replacement of the HDD and HDD Data Encryption & Mirroring Board

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

[refinement] physical tampering → Physical replacement of the HDD and HDD Data Encryption & Mirroring Board

6.1.7 LAN Data Protection Function

6.1.7.1 IP Packet Encryption Function

FCS_COP.1(n) Cryptographic operation

Hierarchical to: No other components.

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

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

[assignment: *list of cryptographic operations*]
- Encryption of IP packets sent to the LAN
- Decryption of IP packets received from the LAN

[assignment: *cryptographic algorithm*]
- Refer to "Cryptographic Algorithm" in Table 25.

[assignment: *cryptographic key sizes*]
- Refer to "Cryptographic Key Sizes" in Table 25.

[assignment: *list of standards*]
- Refer to "List of Standards" in Table 25.

Table 25— IPSec cryptographic algorithm, key sizes and standards

cryptographic algorithm	cryptographic key sizes	list of standards
3DES-CBC	168 bit	FIPS PUB 46-3
AES-CBC	128 bit, 192bit, 256 bit	FIPS PUB 197
AES-GCM	128 bit, 192bit, 256 bit	SP800-38D

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**.

6.1.8 Self-Test Function

FPT_TST.1 TSF testing

Hierarchical to: **No other components.**

Dependencies: **No dependencies.**

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up*, *periodically during normal operation*, *at the request of the authorised user*, *at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

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

[selection: [assignment: *parts of TSF*], *the TSF*]
- Cryptographic algorithms used with the LAN Data Protection Function (AES, 3DES)

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

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

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.9 Audit Log Function

FAU_GEN.1 Audit data generation

Hierarchical to: **No other components.**

Dependencies: **FPT_STM.1 Reliable time stamps**

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;

- All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and
- **all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 26;** [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 26: (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 26—Audit data requirements

Auditable event	Relevant SFR	Audit level	Additional information
Job completion	FDP_ACF.1	Not specified	Type of job
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1	Basic	None required
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1	Basic	Attempted user identity, if available
Use of the management functions	FMT_SMF.1	Minimum	None required
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required
Changes to the time	FPT_STM.1	Minimum	None required
Termination of an interactive session by the session locking mechanism[3]	FTA_SSL.3	Minimum	None required
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required

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] See "Section 14.1 IEEE Std 2600.1 Errata" in the PP Guide.
In IEEE Std 2600.1, this is indicated as "Locking of an interactive session by the session locking mechanism" but notes that this is a transcription error.

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.

FAU_SAR.1 Audit review

Hierarchical to: **No other components.**

Dependencies: **FAU_GEN.1 Audit data generation**

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

[assignment: authorised users]
- U.ADMINISTRATOR

[assignment: list of audit information]
- Refer to the audit logs listed in Table 26.

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

FAU_SAR.2 Restricted audit review

Hierarchical to: **No other components.**

Dependencies: **FAU_SAR.1 Audit review**

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

FAU_STG.1 Protected audit trail storage

Hierarchical to: **No other components.**

Dependencies: **FAU_GEN.1 Audit data generation**

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

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

6.1.10 Management Function

6.1.10.1 User Management Function

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*]
- Use a password 4 to 32 characters in length
- Prohibit the use of 3 or more consecutive characters
- Use at least one uppercase character (A to Z)
- Use at least one lowercase character (a to z)
- Use at least one number (0-9)
- Use at least one non-alphabet characters (^-@[]:;,./¥!"#$%&'()=~|{`+*}_?><)
- Allowed characters
  - All characters other than control characters

FMT_MTD.1(user-mgt) 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 (user-mgt) 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 "Operation" in Table 27.

[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 "TSF Data" in Table 27.

[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR, the U.NORMAL to whom such TSF data areassociated*]]
- Refer to "Role" in Table 27.

Table 27— User information management

TSF data	Role	Operation
User name, role	U.ADMINISTRATOR	modify, delete, create, query, insert
Passwords	U.ADMINISTRATOR	modify, delete, create, insert
Own password	U.NORMAL	modify

FMT_SMR.1 Security roles

Hierarchical to: **No other components.**

Dependencies: **FIA_UID.1 Timing of identification**

FMT_SMR.1.1 The TSF shall maintain the roles **U.ADMINISTRATOR, U.NORMAL, [selection: *Nobody*,** [assignment: *the authorised identified roles*]].

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

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

6.1.10.2 Cryptographic Key Management Function

FCS_CKM.1 Cryptographic key generation

Hierarchical to: **No other components.**

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

[assignment: *cryptographic key generation algorithm*]
- Cryptographic key generation algorithm according to FIPS PUB 186-2

[assignment: *cryptographic key sizes*]
- 128bit, 168bit, 192bit, 256 bit

[assignment: *list of standards*]
- FIPS PUB 186-2

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

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

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].

[assignment: *cryptographic key distribution method*]
- DH (Diffie Hellman) and ECDH (Elliptic Curve Diffie Hellman)

[assignment: *list of standards*]
- SP800-56A

6.1.10.3 Device Management Function

FMT_MTD.1(device-mgt) 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(device-mgt) 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 "Operation" in Table 28.

[assignment: *list of TSF data*]
- Refer to "TSF Data Table 28.

[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*, [assignment: *the authorized identified roles* ***except U.NORMAL***]]]
- Refer to "Role" in Table 28.

Table 28— Device management function

TSF Data	Role	Operation
Date/Time settings	U.ADMINISTRATOR	modify
HDD Data Erase settings	U.ADMINISTRATOR	query, modify
IPSec settings	U.ADMINISTRATOR	query, modify
Auto Reset settings	U.ADMINISTRATOR	query, modify

TSF Data	Role	Operation
Lockout policy settings	U.ADMINISTRATOR	query, modify
Password policy settings	U.ADMINISTRATOR	query, modify
Audit log	U.ADMINISTRATOR	query, delete

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 "Management Function" in Table 29.

Table 29—The management of security requirements

Management Function	Operation
Date/Time settings	modify
HDD Data Erase settings	query, modify
IPSec settings	query, modify
Auto Reset settings	query, modify
Lockout policy settings	query, modify
Password policy settings	query, modify
Audit log	query, delete
Username, role	modify, delete, create, query, insert
Password	modify, delete, create, insert
Box PIN	modify, delete, create, insert
Own password	modify
PIN of own Mail Box	modify

6.2 Security assurance requirements

This section defines the security assurance requirements for the TOE.

Table 30 lists the security assurance requirements for 2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A, and related SFR packages, EAL 3 augmented by ALC_FLR.2.

Table 30— 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 Authorisation 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

6.3 Security functional requirements rationale

6.3.1 The completeness of security requirements

Table 31 provides a mapping of TOE Security Objectives and security functional requirements. This shows how each of the security functional requirements corresponds to at least one TOE Security Objective.
Bold typeface items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 31—The 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.HDD.ACCESS.AUTHORISED
FIA_AFL.1							S				
FIA_ATD.1							S				
FIA_UAU.1							**P**	**P**			
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S	
FIA_USB.1							**P**				
FTA_SSL.3(lui)							**P**	**P**			
FTA_SSL.3(rui)							**P**	**P**			
FMT_MSA.1(exec-job)							S				
FMT_MSA.3(exec-job)							S				
FDP_ACC.1(exec-job)							**P**				
FDP_ACF.1(exec-job)							S				
FMT_MSA.1(delete-job)	S	S	S								
FMT_MSA.3(delete-job)	S	S	S								
FDP_ACC.1(delete-job)	**P**	**P**	**P**								
FDP_ACF.1(delete-job)	S	S	S								
FDP_ACC.1(prt)	**P**										
FDP_ACF.1(prt)	S										
FDP_ACC.1(box)	**P**										
FDP_ACF.1(box)	S										
FPT_FDI_EXP.1								**P**			
FDP_RIP.1	**P**										
FPT_CIP_EXP.1	**P**	**P**	**P**	**P**	**P**	**P**					
FCS_COP.1(h)	S	S	S	S	S	S					
FPT_PHP.1											**P**
FCS_COP.1(n)	S	S	S	S	S	S					
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					
FCS_CKM.1	S	S	S	S	S	S					
FCS_CKM.2	S	S	S	S	S	S					
FPT_TST.1									**P**		
FAU_GEN.1										**P**	
FAU_GEN.2										**P**	
FAU_SAR.1										**P**	
FAU_SAR.2										**P**	
FAU_STG.1										**P**	
FAU_STG.4										**P**	
FPT_STM.1										S	
FIA_SOS.1							S				
FMT_MTD.1(user-mgt)				**P**	**P**	**P**					
FMT_SMR.1	S	S	S	S	S	S	S				
FMT_MTD.1(device-mgt)				**P**	**P**	**P**					

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.HDD.ACCESS.AUTHORISED
FMT_SMF.1	S	S	S	S	S	S					

6.3.2 The sufficiency of security requirements

This section provides the rationale on how the security functional requirements are sufficient to satisfy the Security Objectives.

O.DOC.NO_DIS is the security objective that ensures user document data is protected from unauthorized disclosure. O.DOC.NO_DIS is addressed by the following:
Based on user identification information resulting from FIA_UID.1, roles managed by FMT_SMR.1 are assigned for access control.
The identified users are allowed to operate only his/her own job according to FMT_MSA.1(delete-job)/FMT_MSA.3(delete-job), FDP_ACC.1(delete-job)/FDP_ACF.1(delete-job).
The identified users are allowed to print or preview only his/her own job, according to FDP_ACC.1(prt)/FDP_ACF.1(prt), FDP_ACC.1(box)/FDP_ACF.1(box).
Furthermore, by FDP_RIP.1, complete deletion of residual information of user document data created as a result of job processing is ensured. By FPT_CIP_EXP.1, FCS_COP.1(h), and FCS_CKM.1, user data and TSF data in the HDD are protected from unauthorized alteration and disclosure. By FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, and FCS_CKM.2, user data and TSF data sent over the LAN are protected from unauthorized alteration and disclosure. By FMT_SMF.1, management functions related to these actions, are provided.

O.DOC.NO_ALT is the security objective that ensures protection of user document data from unauthorized alteration. O.DOC.NO_ALT is addressed by the following:
Based on user identification information resulting from FIA_UID.1, roles managed by FMT_SMR.1 are assigned for access control.
The identified users are allowed to operate only his/her own job according to FMT_MSA.1(delete-job)/FMT_MSA.3(delete-job), FDP_ACC.1(delete-job)/FDP_ACF.1(delete-job).
Furthermore, by FPT_CIP_EXP.1, FCS_COP.1(h), and FCS_CKM.1, user data and TSF data in the HDD are protected from unauthorized alteration and disclosure. By FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, and FCS_CKM.2, user data and TSF data sent over the LAN are protected from unauthorized alteration and disclosure. By FMT_SMF.1, management functions related to these actions, are provided.

O.FUNC.NO_ALT is the security objective that ensures protection of user function data from unauthorized alteration. O.FUNC.NO_ALT is addressed by the following:
Based on user identification information resulting from FIA_UID.1, roles managed by FMT_SMR.1 are assigned for access control.
The identified users are allowed to operate only his/her own job according to FMT_MSA.1(delete-job)/FMT_MSA.3(delete-job), FDP_ACC.1(delete-job)/FDP_ACF.1(delete-job).
Furthermore, by FPT_CIP_EXP.1, FCS_COP.1(h), and FCS_CKM.1, user data and TSF data in the HDD are protected from unauthorized alteration and disclosure. By FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, and FCS_CKM.2, user data and TSF data sent over the LAN are protected from unauthorized alteration and disclosure. By FMT_SMF.1, management functions related to these actions, are provided.

O.PROT.NO_ALT is the security objective that ensures protection of TSF protected data from unauthorized

alteration. O.PROT.NO_ALT is addressed by the following:
Based on user identification information managed by FMT_MTD.1(user-mgt) and resulting from FIA_UID.1, roles managed by FMT_SMR.1 are assigned for the Device Management function as specified by FMT_SMR.1, FMT_MTD.1(device-mgt), and FMT_SMF.1.
Furthermore, by FPT_CIP_EXP.1, FCS_COP.1(h), and FCS_CKM.1, user data and TSF data in the HDD are protected from unauthorized alteration and disclosure. By FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, and FCS_CKM.2, user data and TSF data sent over the LAN are protected from unauthorized alteration and disclosure.

O.CONF.NO_DIS is the security objective that ensures protection of TSF confidential data from unauthorized disclosure. O.CONF.NO_DIS is addressed by the following:
Based on user identification information managed by FMT_MTD.1(user-mgt) and resulting from FIA_UID.1, roles managed by FMT_SMR.1 are assigned for the Device Management function as specified by FMT_SMR.1, FMT_MTD.1(device-mgt), and FMT_SMF.1.
Furthermore, by FPT_CIP_EXP.1, FCS_COP.1(h), and FCS_CKM.1, user data and TSF data in the HDD are protected from unauthorized alteration and disclosure. By FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, and FCS_CKM.2, user data and TSF data sent over the LAN are protected from unauthorized alteration and disclosure.

O.CONF.NO_ALT is the security objective that ensures protection of TSF confidential data from unauthorized alteration. O.CONF.NO_ALT is addressed by the following:
Based on user identification information managed by FMT_MTD.1(user-mgt) and resulting from FIA_UID.1, roles managed by FMT_SMR.1 are assigned for the Device Management function as specified by FMT_SMR.1, FMT_MTD.1(device-mgt), and FMT_SMF.1.
Furthermore, by FPT_CIP_EXP.1(h), FCS_COP.1, and FCS_CKM.1, user data and TSF data in the HDD are protected from unauthorized alteration and disclosure. By FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, and FCS_CKM.2, user data and TSF data sent over the LAN are protected from unauthorized alteration and disclosure.

O.USER.AUTHORIZED is the security objective that ensures user identification and authentication. O.USER.AUTHORIZED is addressed by the following:
Users authenticated by the identification and authentication mechanism specified by FIA_UAU.1, FIA_UID.1, FIA_UAU.7, and FIA_AFL.1, with user sessions managed by FIA_ATD.1, FIA_USB.1, and FTA_SSL.3(lui)/FTA_SSL.3(rui), are granted use of the function, as determined by access control specified by FDP_ACC.1(exec-job)/FDP_ACF.1(exec-job).
Furthermore, authorized user information are managed by FIA_SOS.1, FMT_MSA.1(exec-job), FMT_MSA.3(exec-job), FMT_SMR.1.

O.INTERFACE.MANAGED is the security objective that ensures control of operations of the I/O interfaces in accordance with security policy. O.INTERFACE.MANAGED is addressed by the following:
By FIA_UAU.1, FIA_UID.1, FTA_SSL.3(lui)/FTA_SSL.3(rui), the user interface is managed.
By FPT_FDI_EXP.1, restricted forwarding of data to the LAN is specified.

O.SOFTWARE.VERIFIED is addressed by providing the self-test procedures specified by FPT_TST.1.

O.AUDIT.LOGGED is addressed by providing the Audit Log function as specified by FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, and FAU_STG.4. FIA_UID.1 and FPT_STM.1 provide the means for user information and timestamps generated on audit logs.

O.HDD.ACCESS.AUTHORISED is addressed by the Device Identification and Authentication function as specified by FPT_PHP.1, prior to permitting access to the HDD.

6.3.3 The dependencies of security requirements

This section provides the justification for any dependencies not met.

Table 32—The dependencies of security requirements

Functional Requirement	Dependencies required by CC	Dependencies satisfied by ST	Reason for not meeting dependencies
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	N/A (dependencies are satisfied)
FIA_ATD.1	No dependencies.	No dependencies.	N/A (dependencies are satisfied)
FIA_UAU.1	FIA_UID.1	FIA_UID.1	N/A (dependencies are satisfied)
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	N/A (dependencies are satisfied)
FIA_UID.1	No dependencies.	No dependencies.	N/A (no dependencies)
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	N/A (dependencies are satisfied)
FTA_SSL.3(lui)	No dependencies.	No dependencies.	N/A (no dependencies)
FTA_SSL.3(rui)	No dependencies.	No dependencies.	N/A (no dependencies)
FMT_MSA.1(exec-job)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(exec-job) FMT_SMR.1 FMT_SMF.1	N/A (dependencies are satisfied)
FMT_MSA.3(exec-job)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(exec-job) FMT_SMR.1	N/A (dependencies are satisfied)
FDP_ACC.1(exec-job)	FDP_ACF.1	FDP_ACF.1(exec-job)	N/A (dependencies are satisfied)
FDP_ACF.1(exec-job)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(exec-job) FMT_MSA.3(exec-job)	N/A (dependencies are satisfied)
FMT_MSA.1(delete-job)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(delete-job) FMT_SMR.1 FMT_SMF.1	N/A (dependencies are satisfied)
FMT_MSA.3(delete-job)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	N/A (dependencies are satisfied)
FDP_ACC.1(delete-job)	FDP_ACF.1	FDP_ACF.1(delete-job)	N/A (dependencies are satisfied)
FDP_ACF.1(delete-job)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(delete-job) FMT_MSA.3(delete-job)	N/A (dependencies are satisfied)
FDP_ACC.1(prt)	FDP_ACF.1	FDP_ACF.1(prt)	N/A (dependencies are satisfied)
FDP_ACF.1(prt)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(prt) FMT_MSA.3(delete-job)	N/A (dependencies are satisfied)
FDP_ACC.1(box)	FDP_ACF.1	FDP_ACF.1(box)	N/A (dependencies are satisfied)
FDP_ACF.1(box)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(box) FMT_MSA.3(delete-job)	N/A (dependencies are satisfied)
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	N/A (dependencies are satisfied)
FDP_RIP.1	No dependencies.	No dependencies.	N/A (no dependencies)
FPT_CIP_EXP.1	No dependencies.	No dependencies.	N/A (no dependencies)
FCS_COP.1(h)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4 is not claimed because: Cryptographic keys are stored in RAM, and disappear when power is shut off. Also, extraction of cryptographic keys is prevented by the design of the system. As such, cryptographic keys are managed securely enough not to require any method for their destruction.
FPT_PHP.1	No dependencies.	No dependencies.	N/A (no dependencies)
FTP_ITC.1	No dependencies.	No dependencies.	N/A (no dependencies)

Functional Requirement	Dependencies required by CC	Dependencies satisfied by ST	Reason for not meeting dependencies
FCS_COP.1(n)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4 is not claimed because: Cryptographic keys are stored in RAM, and disappear when power is shut off. Also, extraction of cryptographic keys is prevented by the design of the system. As such, cryptographic keys are managed securely enough not to require any method for their destruction.
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1(n) FCS_COP.1(h)	FCS_CKM.4 is not claimed because: Cryptographic keys are stored in RAM, and disappear when power is shut off. Also, extraction of cryptographic keys is prevented by the design of the system. As such, cryptographic keys are managed securely enough not to require any method for their destruction.
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4 is not claimed because: Cryptographic keys are stored in RAM, and disappear when power is shut off. Also, extraction of cryptographic keys is prevented by the design of the system. As such, cryptographic keys are managed securely enough not to require any method for their destruction.
FPT_TST.1	No dependencies.	No dependencies.	N/A (no dependencies)
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A (dependencies are satisfied)
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	N/A (dependencies are satisfied)
FPT_STM.1	No dependencies.	No dependencies.	N/A (no dependencies)
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	N/A (dependencies are satisfied)
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	N/A (dependencies are satisfied)
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	N/A (dependencies are satisfied)
FAU_STG.4	FAU_STG.1	FAU_STG.1	N/A (dependencies are satisfied)
FIA_SOS.1	No dependencies.	No dependencies.	N/A (dependencies are satisfied)
FMT_MTD.1(user-mgt)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A (dependencies are satisfied)
FMT_SMR.1	FIA_UID.1	FIA_UID.1	N/A (dependencies are satisfied)
FMT_MTD.1(device-mgt)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A (dependencies are satisfied)
FMT_SMF.1	No dependencies.	No dependencies.	N/A (no dependencies)

6.4 Security assurance requirements rationale

This Protection Profile has been developed for Hardcopy Devices used in restrictive commercial information processing environments that require a relatively high level of document security, operational accountability and information assurance. The TOE environment will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE except for removable nonvolatile storage devices, where protection of User and TSF Data are provided when such devices are removed from the TOE environment. Agents have limited or no means of infiltrating the TOE with code to effect a change and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 3 is appropriate.

EAL 3 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

7 TOE Summary specification

This section describes the TOE summary specifications.

7.1 User Authentication Function

- **Supported functional requirements: FIA_UAU.1, FIA_UID.1, FIA_UAU.7, FIA_ATD.1, FIA_USB.1, FIA_AFL.1, FTA_SSL.3(lui), FTA_SSL.3(rui)**

When the control panel or a remote UI is used to operate the MFP, before permitting such operations, the TOE requires user authentication in order to identify and authenticate valid users. However, the submission of print jobs, fax jobs, and I-fax jobs is always permitted. [**FIA_UAU.1, FIA_UID.1**]

Two methods of user authentication are supported:

- External Authentication

  Authentication is based on user information registered in the authentication server. This may be an Active Directory server that uses Kerberos authentication, or LDAP server that uses LDAP authentication.

- Internal Authentication

  Authentication is based on user information registered in the device.

For user authentication, the TOE prompts input of the user name, password, and the login destination. User authentication succeeds only if the user name and password matches the one at the specified destination. For security, note that the password is masked by asterisks in the text field. [**FIA_UAU.7**]

The TOE issues an Access Control Token (ACT) to each user successfully authenticated.

The ACT is an object that contains the user's name and role, as well as the access permissions to the application functions that are specified for each user role. [**FIA_ATD.1, FIA_USB.1**]

The TOE provides a lockout function in order to minimize invalid login attempts. [**FIA_AFL.1**]

- This function locks out any user that fails to login successfully within the maximum number of failed authentication attempts. A value from 1 to 10 can be specified as the number of attempts before lockout (Initial value: 3).
- Any user that is locked out will not be able to login until the lockout time passes. A value from 1 to 60 minutes can be specified as the lockout time (Initial value: 3 minutes).

The TOE terminates an interactive session when there is no user activity at the control panel or remote UI lasting for a specified period of time. [**FTA_SSL.3(lui), FTA_SSL.3(rui)**]

- At the control panel, session timeout occurs after a specified period of user inactivity. A value from 10 seconds to 9 minutes can be specified (Initial value: 2 minutes).
- At a remote UI, session timeout occurs after 15 minutes of user inactivity.

7.2 Function Use Restriction Function

- **Supported functional requirements: FDP_ACC.1(exec-job), FDP_ACF.1(exec-job), FMT_MSA.1(exec-job), FMT_MSA.3(exec-job), FMT_SMF.1**

For each UI, the TOE provides Function Use Restriction, which controls access based on the contents of the ACT issued to authenticated users. Any queries, modifications, deletions, and additions to the role contained in the ACT, are performed by U.ADMINISTRATORs only. For Function Use Restriction, the attribute of the Object is the functions itself, and is therefore fixed.

When the control panel is used, Function Use Restriction Function permits or denies use of functions depending on the settings in "Application Restrictions", which are based on the role contained in the ACT.

When a remote UI is used, Function Use Restriction Function permits or denies use of functions based on attribute values associated with the role in the ACT.

Only U.ADMINISTRATORs are allowed use of all functions.

Table 33— Function Use Restriction Policy

UI	Object	Condition	Operation
Control panel	Pointer to [Secured Print]	The role associated with U.USER must have permission to the [Secured Print] function.	Executed by activating the Object.
	Pointer to [Copy]	The role associated with U.USER must have permission to the [Copy] function	Executed by activating the Object.
	Pointer to [Scan and Send]	The role associated with U.USER must have permission to the [Scan and Send] function	Executed by activating the Object.
	Pointer to [Fax]	The role associated with U.USER must have permission to the [Scan and Send] function	Executed by activating the Object.
	Pointer to [Fax/I-Fax Inbox]	The role associated with U.USER must have permission to the [Access Stored Files] function	Executed by activating the Object.
	Pointer to [Access Stored Files]	The role associated with U.USER must have permission to the [Access Stored Files] function	Executed by activating the Object.
	Pointer to [Scan and Store]	The role associated with U.USER must have permission to the [Scan and Store] function	Executed by activating the Object.
Remote UI	Pointer to [Access Stored Files]	The role associated with U.USER is anything other than Administrator.	Cannot be executed.

7.3 Job Output Restriction Functions

- **Supported Functional Requirements: FMT_MSA.1(delete-job), FMT_MSA.3(delete-job), FMT_SMF.1**

For Print, Copy, Scan, and Fax TX jobs, the TOE provides the following security functions. Job Output Restriction restricts access to submitted jobs, to the user that executed the job. The user name can be

registered, acquired, modified, deleted, or added by U.ADMINISTRATORs only. For a submitted job, the user name is initialized with the name of the user that generated the job. For PINs associated with Mail Boxes or the Memory RX Inbox, these are initialized by U.ADMINISTRATOR.

7.3.1 Temporarily Stored Print Jobs

- **Supported functional requirements: FDP_ACC.1(delete-job), FDP_ACF.1(delete-job)、FDP_ACC.1(prt), FDP_ACF.1(prt)**

If a print job with a PIN is submitted, the job is temporarily stored in the machine without being output. Additionally, it uses the user name associated with the print job to determine its owner, in order to realize access restriction as described below.

For temporarily stored jobs, the following operations are available to U.USERs, only if the user's name matches the user name associated with the desired job.

- Print
- Change priority for printing
- Delete

Printing starts when the PIN for the print job is entered from the control panel of the machine.

For all temporarily stored jobs, U.ADMINISTRATOR is allowed to execute the following:

- Delete

7.3.2 Temporarily Stored FAX TX Jobs

- **Supported functional requirements: FDP_ACC.1(delete-job), FDP_ACF.1(delete-job)**

When the TOE receives a FAX TX job with transmission time specified, it is first stored temporarily, until sending at the specified time.

For temporarily stored FAX TX jobs, the following operations are available to U.NORMALs, only if the user's name matches the user name associated with the desired job.

- Change destination

For all temporarily stored FAX TX jobs, U.ADMINISTRATOR is allowed to execute the following:

- Change destination

7.3.3 Document Data Stored in Mail Box

- **Supported functional requirements: FDP_ACC.1(delete-job), FDP_ACF.1(delete-job)、FDP_ACC.1(box), FDP_ACF.1(box), FMT_MSA.1(delete-job), FMT_SMF.1**

For Copy, Scan, or Send jobs, the TOE provides Mail Boxes where these jobs may be stored as document data, to be printed or sent at a later time. Since these are stored in Mail Boxes, access control to Mail Boxes, is equivalent to access control to the stored document data.

A seven digit PIN can be assigned to a Mail Box, to help prevent unauthorized access by a user.

No PIN is required when storing document data in a Mail Box. The TOE realizes access restriction, by determining the U.USER that enters the correct PIN, to be the owner of the stored document data.

For document data stored in a Mail Box, the following operations are made available to U.NORMAL only by entering the correct PIN.

- Print
- Change print settings
- Preview
- Send
- Delete

If the control panel is used, U.ADMINISTRATOR is allowed access to the following operations without entering any PIN.

- Print
- Change print settings
- Preview
- Send
- Delete

If a remote UI is used, U.ADMINISTRATOR is allowed access to the following operations only by entering the correct PIN.

- Print
- Change print settings
- Preview
- Send
- Delete

For documents received by fax/I-fax, the TOE provides the Memory RX Inbox where these jobs may be stored as files, to be output at a later time. Since these are stored in the Memory RX Inbox, access control to this inbox, is equivalent to access control to the stored document data. A seven digit PIN can be assigned to the Memory RX Inbox, to prevent unauthorized access by a user.
Only U.ADMINISTRATORs are authorized to initialize, set, modify, or delete the PIN on the Memory RX Inbox, which means only U.ADMINISTRATORS are allowed access to the stored document data. The TOE realizes access restriction, by determining the U.ADMINISTRATOR that enters the correct PIN to be the owner of the stored document data, preventing any U.NORMAL from executing print or send operations on the document data.

If the control panel is used, U.ADMINISTRATOR is allowed access to the following operations without entering any PIN.

- Print
- Send
- Delete

If a remote UI is used, U.ADMINISTRATOR is allowed access to the following operations only by entering the correct PIN.

- Print
- Send

- Delete

For documents received by fax/I-fax, these jobs are printed using the settings in effect when the job was received.
Therefore, the TOE does not allow any user to make any changes to the document data.

[Box PIN]
For the PIN set on Mail Boxes/Memory RX Inbox, only U.ADMINISTRATORs assigned the Administrator role are allowed to set, change, or delete any PIN. Note however, that U.NORMALs are allowed to change the PIN for the Mail Box they use.

7.4 Forward Received Jobs Function

- **Supported functional requirements: FPT_FDI_EXP.1**

The design of the TOE prevents received data from being forwarded directly to a server or computer. This function enables the user to restrict forwarding of received jobs to the LAN.

7.5 HDD Data Erase Function

- **Supported functional requirements: FDP_RIP.1**

By overwriting with random data, the TOE permanently erases document data (including temporary image files) in the HDD, to ensure that no trace of the document data remains on the HDD.

The user can choose one of the following erasure methods:

- Overwrite using the DoD standard
- Overwrite with random data three times
- Overwrite once with random data
- Overwrite once with null data

The timing in which data are erased is specified below.

- Image files temporarily stored in the HDD as a result of job processing is completely erased during or after processing of the job.
- Document data are completely erased from the HDD, immediately after being deleted from Mail Box/Memory RX Inbox.
- Residual information that remained unerased due to a sudden power shutdown, are completely erased from the HDD upon startup of the TOE.

7.6 HDD Data Encryption Function

- **Supported functional requirements: FPT_CIP_EXP.1**

The security functions provided by the TOE's "HDD Data Encryption & Mirroring Board" are described below.

The encryption/decryption function together with the Device Identification and Authentication function provide confidentiality and integrity protection for user data and TSF data stored in the HDD.

7.6.1 Encryption/Decryption Function

- **Supported functional requirements: FCS_COP.1(h)**

To protect the confidentiality and integrity of user data and TSF data stored in the HDD, the TOE performs the following cryptographic operations to encrypt all data stored in the HDD.

- Encryption of data written to the HDD.
- Decryption of data read out from the HDD.

The cryptographic algorithm and cryptographic key size are specified below:

- AES algorithm (FIPS PUB 197)
- 256 bit key length

7.6.2 Cryptographic Key Management Function

- **Supported functional requirements: FCS_CKM.1**

The TOE uses the following specifications for generating the cryptographic key that is used by the HDD data encryption function.

- Uses a cryptographic key generation algorithm according to FIPS PUB 186-2
- Generates a cryptographic key with 256 bit key length

The cryptographic key is managed as follows.

- Upon startup, the TOE reads the seed information stored in FlashROM and generates a cryptographic key.
- After generating the cryptographic key, the TOE stores the key in RAM.

No method is available for acquiring the seed from the encryption board. Note also, that because the cryptographic key is stored in volatile RAM memory, it disappears when power is shut off.

7.6.3 Device Identification and Authentication Function

- **Supported functional requirements: FPT_PHP.1**

The HDD Data Encryption & Mirroring Board identifies the MFP at each startup, and permits access to the HDD only if it is identified as the correct MFP. This function helps prevent unauthorized access to the contents of the HDD, even if the HDD and HDD Data Encryption & Mirroring Board are physically removed and connected to a different MFP.

[Registration of the Authentication ID]

The HDD Data Encryption & Mirroring Board, when it is initially mounted, acquires the device authentication ID from the MFP device, and stores it in FlashROM.

[Procedure for identification and authentication]

Upon startup, the HDD Data Encryption & Mirroring board generates a pseudo-random number which it passes to the MFP device as a random number to a challenge. The MFP device makes a computation using its device authentication ID and the received random number, and passes the resulting hash value (SHA-1) to the encryption board. The HDD Data Encryption & Mirroring Board performs the same computation in order to verify the response.

Access to the HDD is denied, unless the HDD Data Encryption & Mirroring Board confirms successfully that it is mounted on the correct MFP device.

7.7 LAN Data Protection Function

LAN Data Protection Function encrypts/decrypts all IP packets that are used in communication with an IT device.

7.7.1 IP Packet Encryption Function

- **Supported functional requirements: FCS_COP.1(n), FTP_ITC.1**

To ensure confidentiality and integrity of user data and TSF data communicated to and from an IT device, the TOE uses IPSec to encrypt/decrypt all IP packets.

- Encryption of IP packets sent to the LAN
- Decryption of IP packets received from the LAN

The following cryptographic algorithm and cryptographic key sizes are used.

- See Table 25

7.7.2 Cryptographic Key Management Function

- **Supported functional requirements: FCS_CKM.1, FCS_CKM.2**

The TOE uses the following specifications for generating the cryptographic key that is used by the IP packet encryption function.

- Uses a cryptographic key generation algorithm according to FIPS PUB 186-2
- Generates a cryptographic key with 128/168/192/256 bit key length

The following method is used by the TOE, to transmit the cryptographic key used by the IP Packet Encryption Function, to the other party

- ECDH (Elliptic Curve Diffie Hellman) and DH (Diffie Hellman) according to SP800-56A

7.8 Self-Test Function

- **Supported functional requirements: FPT_TST.1**

At startup, the TOE performs the following self-test.

- Checks whether cryptographic algorithms are running properly (AES、3DES)
- Checks the integrity of the cryptographic key
- Checks the integrity of the executable code of the cryptographic algorithm

Since executable code is first encrypted by the HDD Data Encryption & Mirroring Board before being stored in the HDD, a self-test on the cryptographic algorithm confirms that a whole set of functions are operating properly.

7.9 Audit Log Function

- **Supported functional requirements: FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4**

The TOE generates logs for the following events.

- Startup
- Shutdown
- Job completion
- User authentication success/failure
- Logout
- Use of device management functions
- Use of user management functions
- Changes to the date/time setting
- IPSec connection failures

The items that are recorded on each log, are listed below. The date/time is provided by the TOE. The TOE's date/time information is set by the Management Function, or is set by time synchronization when the accurate time is obtained from the Time Server.

- Date/Time, User Name, Event Type, Outcome (Success/Failed)

Other log events may have additional items as described below.

- Job type (job completion)
- Name of the user that failed authentication (authentication failure)

Also, export of audit logs can be performed from a remote UI, in order to read out log records, although use of this function is restricted to U.ADMINISTRATORs only.

Users other than U.ADMINISTRATOR are not allowed to export audit logs when logged in to the TOE from a remote UI.

When accessing the TOE from a remote UI, another capability restricted to U.ADMINISTRATORs only is the deletion of log records from the [Deleting Collected Logs] menu.

Users other than U.ADMINISTRATOR are not allowed access to this capability when logged in to the TOE from a remote UI, thus preventing unauthorized alterations from occurring.

A maximum of 20,000 audit records can be maintained. Once this becomes full, the oldest audit record is overwritten with the newest.

7.10 Management Functions

7.10.1 User Management Function

- **Supported functional requirements: FIA_SOS.1 , FMT_MTD.1(user-mgt) , FMT_SMR.1, FMT_SMF.1**

In the TOE, only U.ADMINISTRATORs assigned the Administrator role can set, change, or delete user, role, and access restriction information and box PINs.

General users or U.NORMAL, can only change their own passwords and the PIN for the Mail Box they use.

[Setting/Changing/Deleting User, Role, and Access Restriction Information]

New users are registered by setting the user name and password, and assigning a role to the user. Registered user information can be modified by changing the user name, password, or the assigned role, or the user's registration can be deleted altogether. User specified passwords are checked to see that they are consistent with the password policy.

Five roles exist, which are called "Base Roles": Administrator, Power User, General User, Limited User, and Guest User. To create a new "Custom Role" different than these, any one of four base roles excluding Guest User, is used as a template for the new role, which can then be registered.

The Administrator role is a role whose base role is "Administrator", and has administrative privileges.

The initial value for "Base Role" can be changed to any one of four base roles except Guest User.

The access restriction information that determines whether use of certain functions is permitted or denied, is specified by the "Application Restrictions" setting, which depends on what role is assigned. Although the initial value for "Application Restrictions" is fixed for base roles, the initial value of "Application Restrictions" can be changed for custom roles.

[Types of Users]

There are two types of users: U.ADMINISTRATOR and U.NORMAL.

- U.ADMINISTRATOR

  User assigned the Administrator role and has administrative privileges.

- U.NORMAL

  General user assigned a role other than Guest User role or Administrator role.

7.10.2 Device Management Function

- **Supported functional requirements: FMT_MTD.1(device-mgt), FMT_SMF.1, FMT_SMF.1**

To provide for the effective enforcement of security functions, the TOE allows only U.ADMINISTRATORs to set the device management settings in Table 28.

The following settings are also provided.

[Password Policy Settings]

To encourage the use of strong passwords, the following password policy may be set.

- Use a password 4 to 32 characters in length
- Prohibit the use of 3 or more consecutive characters
- Use at least one uppercase characters (A to Z)
- Use at least one lowercase characters (a to z)
- Use at least one number (0-9)
- Use at least one non-alphabet characters (^-@[]:;,./¥!"#$%&'()=~|{`+*}_?><)
- Allowed characters:
  - All characters other than control characters

[Lockout Policy Settings]

The number of attempts before lockout and the lockout time can be set.

- Number of attempts before lockout

  Select a value from 1 to 10 (Initial value: 3)

- Lockout time

  Select a value from 1 to 60 minutes (Initial value: 3 minutes)

END