Security Target for RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000, version JE-1.00-H

Author: RICOH COMPANY, LTD.

Date: 2019-12-19
Version: 1.0

Table of Contents

List of Figures

List of Tables

1 ST Introduction (ASE_INT)

1.1 ST Reference

The following are the identification information of this ST.

- Title: Security Target for RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000 version JE-1.00-H
- Version: 1.0
- Date: 2020-01-05
- Author: RICOH COMPANY, LTD.
- Keywords: multifunction, hardcopy, MFD, MFP, HCD, printer, copier, scanner, facsimile, print, copy, scan, fax, document server

1.2 TOE Reference

The identification information of the TOE is shown below.

TOE Name: RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000

TOE Version: JE-1.00-H

TOE Type: Digital Multi-Function Printer (hereafter "MFP")

Target MFP models:

- RICOH IM C2000, IM C2000A, IM C2000F, and IM C2000G
- RICOH IM C2500, IM C2500A, IM C2500F, and IM C2500G
- RICOH IM C3000, IM C3000A, IM C3000F, and IM C3000G
- RICOH IM C3500, IM C3500A, IM C3500F, and IM C3500G
- RICOH IM C4500, IM C4500A, IM C4500F, and IM C4500G
- RICOH IM C5500, IM C5500A, and IM C5500F
- RICOH IM C6000, IM C6000F, and IM C6000G

All of the above MFPs are equipped with Printer, Scanner, and Copy functions, support an optional Fax function, and are upgraded to version JE-1.00-H software.

Additional options such as document feeders and finishers are available, but none affects the TSF.

The versions of the firmware and hardware corresponding to this version of the TOE are shown below. When using an MFP, you can display the firmware and hardware versions. The machine’s serial number plate indicates which Type the model belongs to:

Type 1: MFPs for “-27”, “-65”, “-17”, “-18” or “-29” models:

- RICOH IM C2000, RICOH IM C2000A, RICOH IM C2000G,
  RICOH IM C2500, RICOH IM C2500A, RICOH IM C2500G,
  RICOH IM C3000, RICOH IM C3000A, RICOH IM C3000G,
  RICOH IM C3500, RICOH IM C3500A, RICOH IM C3500G,
- SAVIN IM C2000, SAVIN IM C2000G,
  SAVIN IM C2500, SAVIN IM C2500G,
  SAVIN IM C3000, SAVIN IM C3000G,

SAVIN IM C3500, SAVIN IM C3500G,

- LANIER IM C2000, LANIER IM C2000G,
  LANIER IM C2500, LANIER IM C2500G,
  LANIER IM C3000, LANIER IM C3000G,
  LANIER IM C3500, LANIER IM C3500G,
- nashuatec IM C2000, nashuatec IM C2000A,
  nashuatec IM C2500, nashuatec IM C2500A,
  nashuatec IM C3000, nashuatec IM C3000A,
  nashuatec IM C3500, nashuatec IM C3500A,
- Rex Rotary IM C2000, Rex Rotary C2000A,
  Rex Rotary C2500, Rex Rotary C2500A,
  Rex Rotary C3000, Rex Rotary C3000A,
  Rex Rotary C3500, Rex Rotary C3500A,
- Gestetner IM C2000, Gestetner IM C2000A,
  Gestetner IM C2500, Gestetner IM C2500A,
  Gestetner IM C3000, Gestetner IM C3000A,
  Gestetner IM C3500, Gestetner IM C3500A,

Type 2: MFPs for “-27”, “-65”, “-17”, “-18”, “-57” or “-29” models

- RICOH IM C4500, RICOH IM C4500A, RICOH IM C4500G,
  RICOH IM C5500, RICOH IM C5500A,
  RICOH IM C6000, RICOH IM C6000G,
- SAVIN IM C4500, SAVIN IM C4500G,
  SAVIN IM C6000, SAVIN IM C6000G,
- LANIER IM C4500, LANIER IM C4500G,
  LANIER IM C6000, LANIER IM C6000G,
- nashuatec IM C4500, nashuatec IM C4500A,
  nashuatec IM C5500, nashuatec IM C5500A,
  nashuatec IM C6000,
- Rex Rotary C4500, Rex Rotary C4500A,
  Rex Rotary C5500, Rex Rotary C5500A,
  Rex Rotary C6000,
- Gestetner IM C4500, Gestetner IM C4500A,
  Gestetner IM C5500, Gestetner IM C5500A,
  Gestetner IM C6000

Type 3: MFPs for “-00” or “-01” models

- RICOH IM C2000, RICOH IM C2000F
  RICOH IM C2500, RICOH IM C2500F
  RICOH IM C3000, RICOH IM C3000F
  RICOH IM C3500, RICOH IM C3500F

Type 4: MFPs for “-00”, “-01” or “-04” models

- RICOH IM C4500, RICOH IM C4500A, RICOH IM C4500F
  RICOH IM C5500, RICOH IM C5500A, RICOH IM C5500F
  RICOH IM C6000, RICOH IM C6000F

306

307 Machine firmware and hardware for Type 1

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.21
	Network Support	18.56
	Web Support	2.17
	Fax	02.02.00
	RemoteFax	02.01.00
	Scanner	02.02
	Web Uapl	2.01
	NetworkDocBox	2.01
	animation	2.01
	Printer	2.13
	RPCS	3.23.13
	Font EXP	1.00
	PCL	1.01
	IRIPS PS3	1.00
	IRIPS PDF	1.06
	IRIPS Font	1.15
	GraphicData	2.00
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-22(WW)	04.00.00
	PowerSaving Sys	F.L3.23.1
	M2a_System	2.03
	M2a_BLEPlugin	4.0.1

Primary Classification	Secondary Classification	Version
	M2a_BluetoothSe	1.01
	M2a_cspf	3.00.00
	M2a_DeviceHub	2.01
	M2a_HelpService	6.01
	M2a_ICCdDisptch	3.07.00
	M2a_InstSetting	2.01
	M2a_iWnn	2.8.201
	M2a_iWnn_Hang	2.8.2
	M2a_iWnn_Hans	2.8.2
	M2a_iWnn_Hant	2.8.2
	M2a_KrbServ	1.07.01
	M2a_MeidaPrtScn	1.04
	M2a_NFCPlugin	3.03.00
	M2a_PrinterInfo	1.04
	M2a_PrinterSJob	1.03
	M2a_ProgramInfo	1.21
	M2a_QRCode_SDC	4.0.3
	M2a_QuickCdAuth	3.05.00
	M2a_RemAssist	1.1
	M2a_RemPnlOpe	1.2
	M2a_RemSptSvc	1.2
	M2a_SimpleWFD	1.17
	M2a_SmartCopy	1.07
	M2a_SmartFAX	5.08
	M2a_SmartScan	1.06
	M2a_SmartScanEx	2.02
	M2a_USBCdPlugin	3.03.00

Primary Classification	Secondary Classification	Version
	M2a_VoiceServ	2.01
	M2a_WEcoInfo	2.01
	M2a_WFaxInfo	2.00
	M2a_WLanguage	2.01
	M2a_WStopKey	2.00
	M2a_WTonner	2.00
	M2a_WTray	2.00
	M2a_zoo	3.02.00
	Engine	1.10:04
	ADF	01.000:03 (*1) 01.030:02 (*2) Blank (*3)
Hardware	Ic Ctlr	03
	Ic Key	01024704

308 (*1): When the MFP includes Auto Reverse Document Feeder

309 (*2): When the MFP includes One-Pass Duplex Scanning ADF

310 (*3): When the MFP includes Exposure Glass Cover

311

312 Machine firmware and hardware for Type 2

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.21
	Network Support	18.56
	Web Support	2.17
	Fax	02.02.00
	RemoteFax	02.01.00
	Scanner	02.02
	Web Uapl	2.01
	NetworkDocBox	2.01

Primary Classification	Secondary Classification	Version
	animation	2.01
	Printer	2.13
	RPCS	3.23.13
	Font EXP	1.00
	PCL	1.01
	IRIPS PS3	1.00
	IRIPS PDF	1.06
	IRIPS Font	1.15
	GraphicData	2.00
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-22(WW)	04.00.00
	PowerSaving Sys	F.L3.23.1
	M2a_System	2.03
	M2a_BLEPlugin	4.0.1
	M2a_BluetoothSe	1.01
	M2a_cspf	3.00.00
	M2a_DeviceHub	2.01
	M2a_HelpService	6.01
	M2a_ICCdDisptch	3.07.00
	M2a_InstSetting	2.01
	M2a_iWnn	2.8.201
	M2a_iWnn_Hang	2.8.2
	M2a_iWnn_Hans	2.8.2
	M2a_iWnn_Hant	2.8.2

Primary Classification	Secondary Classification	Version
	M2a_KrbServ	1.07.01
	M2a_MeidaPrtScn	1.04
	M2a_NFCPlugin	3.03.00
	M2a_PrinterInfo	1.04
	M2a_PrinterSJob	1.03
	M2a_ProgramInfo	1.21
	M2a_QRCode_SDC	4.0.3
	M2a_QuickCdAuth	3.05.00
	M2a_RemAssist	1.1
	M2a_RemPnlOpe	1.2
	M2a_RemSptSvc	1.2
	M2a_SimpleWFD	1.17
	M2a_SmartCopy	1.07
	M2a_SmartFAX	5.08
	M2a_SmartScan	1.06
	M2a_SmartScanEx	2.02
	M2a_USBCdPlugin	3.03.00
	M2a_VoiceServ	2.01
	M2a_WEcoInfo	2.01
	M2a_WFaxInfo	2.00
	M2a_WLanguage	2.01
	M2a_WStopKey	2.00
	M2a_WTonner	2.00
	M2a_WTray	2.00
	M2a_zoo	3.02.00
	Engine	1.10:04

Primary Classification	Secondary Classification	Version
	ADF	01.000:03 (*1) 01.030:02 (*2) Blank (*3)
Hardware	Ic Ctlr	03
	Ic Key	01024704

(*1): When the MFP includes Auto Reverse Document Feeder

(*2): When the MFP includes One-Pass Duplex Scanning ADF

(*3): When the MFP includes Exposure Glass Cover

Machine firmware and hardware for Type 3

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.21
	Network Support	18.56
	Web Support	2.17
	Fax	02.02.00
	RemoteFax	02.01.00
	Scanner	02.02
	Web Uapl	2.01
	NetworkDocBox	2.01
	animation	2.01
	Printer	2.13
	RPCS	3.23.13
	RPCS Font	1.00
	IRIPS PS3	1.00
	IRIPS PDF	1.06
	IRIPS Font	1.21
	PSFont JIS2004	1.04
	Option MSIS	0.38

Primary Classification	Secondary Classification	Version
	GraphicData	2.00
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-22(WW)	04.00.00
	PowerSaving Sys	F.L3.23.1
	M2a_System	2.03
	M2a_BLEPlugin	4.0.1
	M2a_BluetoothSe	1.01
	M2a_cspf	3.00.00
	M2a_DeviceHub	2.01
	M2a_HelpService	6.01
	M2a_ICCdDisptch	3.07.00
	M2a_InstSetting	2.01
	M2a_iWnn	2.8.201
	M2a_iWnn_Hang	2.8.2
	M2a_iWnn_Hans	2.8.2
	M2a_iWnn_Hant	2.8.2
	M2a_KrbServ	1.07.01
	M2a_MeidaPrtScn	1.04
	M2a_NFCPlugin	3.03.00
	M2a_PrinterInfo	1.04
	M2a_PrinterSJob	1.03
	M2a_ProgramInfo	1.21
	M2a_QRCode_SDC	4.0.3
	M2a_QuickCdAuth	3.05.00

Primary Classification	Secondary Classification	Version
	M2a_RemAssist	1.1
	M2a_RemPnlOpe	1.2
	M2a_RemSptSvc	1.2
	M2a_SimpleWFD	1.17
	M2a_SmartCopy	1.07
	M2a_SmartFAX	5.08
	M2a_SmartScan	1.06
	M2a_SmartScanEx	2.02
	M2a_USBCdPlugin	3.03.00
	M2a_VoiceServ	2.01
	M2a_WEcoInfo	2.01
	M2a_WFaxInfo	2.00
	M2a_WLanguage	2.01
	M2a_WStopKey	2.00
	M2a_WTonner	2.00
	M2a_WTray	2.00
	M2a_zoo	3.02.00
	Engine	1.10:04
	ADF	01.000:03 (*1) 01.030:02 (*2) Blank (*3)
Hardware	Ic Ctlr	03
	Ic Key	01024704

318

319 Machine firmware and hardware for Type 4

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.21
	Network Support	18.56

Primary Classification	Secondary Classification	Version
	Web Support	2.17
	Fax	02.02.00
	RemoteFax	02.01.00
	Scanner	02.02
	Web Uapl	2.01
	NetworkDocBox	2.01
	animation	2.01
	Printer	2.13
	RPCS	3.23.13
	RPCS Font	1.00
	IRIPS PS3	1.00
	IRIPS PDF	1.06
	IRIPS Font	1.21
	PSFont JIS2004	1.04
	Option MSIS	0.38
	GraphicData	2.00
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-22(WW)	04.00.00
	PowerSaving Sys	F.L3.23.1
	M2a_System	2.03
	M2a_BLEPlugin	4.0.1
	M2a_BluetoothSe	1.01
	M2a_cspf	3.00.00
	M2a_DeviceHub	2.01

Primary Classification	Secondary Classification	Version
	M2a_HelpService	6.01
	M2a_ICCdDisptch	3.07.00
	M2a_InstSetting	2.01
	M2a_iWnn	2.8.201
	M2a_iWnn_Hang	2.8.2
	M2a_iWnn_Hans	2.8.2
	M2a_iWnn_Hant	2.8.2
	M2a_KrbServ	1.07.01
	M2a_MeidaPrtScn	1.04
	M2a_NFCPlugin	3.03.00
	M2a_PrinterInfo	1.04
	M2a_PrinterSJob	1.03
	M2a_ProgramInfo	1.21
	M2a_QRCode_SDC	4.0.3
	M2a_QuickCdAuth	3.05.00
	M2a_RemAssist	1.1
	M2a_RemPnlOpe	1.2
	M2a_RemSptSvc	1.2
	M2a_SimpleWFD	1.17
	M2a_SmartCopy	1.07
	M2a_SmartFAX	5.08
	M2a_SmartScan	1.06
	M2a_SmartScanEx	2.02
	M2a_USBCdPlugin	3.03.00
	M2a_VoiceServ	2.01
	M2a_WEcoInfo	2.01
	M2a_WFaxInfo	2.00

Primary Classification	Secondary Classification	Version
	M2a_WLanguage	2.01
	M2a_WStopKey	2.00
	M2a_WTonner	2.00
	M2a_WTray	2.00
	M2a_zoo	3.02.00
	Engine	1.10:04
	ADF	01.000:03 (*1) 01.030:02 (*2) Blank (*3)
Hardware	Ic Ctlr	03
	Ic Key	01024704

(*1): When the MFP includes Auto Reverse Document Feeder

(*2): When the MFP includes One-Pass Duplex Scanning ADF

(*3): When the MFP includes Exposure Glass Cover

1.3 TOE Variants

The models listed in Section 1.2 correspond to differences in print speed, and regional markets / localization. In addition, some models are also marketed under different Ricoh Family Group brand names. A complete list of all certified models is provided in the Notes for Administrators document identified in section 1.6.7.

All variants use the same hardware and the same versions of firmware for TOE security functions. All are included in the scope of this Common Criteria certification, but only one representative model is tested (see Section 1.4).

1.3.1 Print speed variants

The first two numeric digits correspond to copy speed, e.g. C2000 performs 20 copies per minute, C2500 performs 25, and so on. Differences between models with different printing speeds are limited to print engine components that do not affect the TSF.

1.3.2 Regional variants

An alphabetic suffix corresponds to regional variations for default user interface languages and other localization settings, and regional fonts and printer languages. There are no security-relevant differences between regional variants.

1.3.3 Branding variants

In addition to RICOH models (with no suffix or “A”, “F”, or “G” suffix), some models are marketed under the following brand names; however, they have not been tested as part of the certification:

- SAVIN and LANIER (with no suffix or with "G" suffix)
- nashuatec, RexRotary, and Gestetner (with no suffix or with "A" suffix).

Differences between branding variants are limited to labels, displays, packaging materials, and documentation. None of these differences affects the TSF.

1.4 Evaluated and tested configurations

The evaluated configuration comprises all of the required and optional TOE and non-TOE components listed in the first two columns of the tables in subsections below. The specific components used for testing are identified in the third column.

The tested configuration is equivalent to evaluated configurations because none of the variants for branding, marketing region, paper speed, or paper feed, affects the TSF, and all variants employ the same TSF-enforcing hardware and software.

The representative model selected for Common Criteria evaluation is a RICOH IM C4500, fitted with Fax Option M37 for testing of fax-related security functions. The IM C4500 model was chosen because it is a high-speed model that is marketed in all regions.

1.4.1 Required TOE components

The following TOE components are required to perform basic security functions of a hardcopy device.

Function	Required TOE component(s)	Tested TOE components
Hardware	Any of the models specified in Section 1.2 and 1.3	RICOH IM C4500 D0BN-17
Software	Version JE-1.00-H software upgrade	Version JE-1.00-H software upgrade

Table 1 Required TOE components

1.4.2 Optional TOE components

Optional security functions require additional TOE components, listed in Table 2:

Security function	Optional TOE components	Tested TOE components
Fax-network separation	Fax Control Unit (FCU)	Fax Control Unit Type M37

Table 2 Optional TOE components

1.4.3 Required non-TOE components

The following non-TOE components are required for the TOE to perform basic security functions of a hardcopy device.

Security function	Required non-TOE component(s)	Tested TOE components
Trusted communications	Connection to a local area network	Yes
Audit log collection	Connection to an audit log server on the LAN	syslog server

Table 3 Required non-TOE components

1.4.4 Optional non-TOE components

Optional security functions require additional non-TOE components, listed in Table 4:

Security function	Optional non-TOE component(s)	Tested TOE components
Fax-network separation, fax-related security functions	Connection to a telephone line	PSTN emulator, PC with fax driver for sending, fax machine for receiving

Security function	Optional non-TOE component(s)	Tested TOE components
Network-based identification and authentication	Connection to an authentication server on the LAN	LDAP server
Protection of scanner output on network	Connection to an SMTP server on the LAN	SMTP server

Table 4 Optional non-TOE components

1.5 TOE Overview

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

1.5.1 TOE Type

This TOE is a Digital Multi-Function Printer (MFP), which is an IT device that inputs, stores, and outputs electronic and hardcopy documents.

1.5.2 TOE Usage

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

As shown in Figure 1, the TOE is connected to its operational environment through a local area network (hereafter "LAN") and the public switched telephone network (PSTN). Other elements of the TOE's operational environment include a remote fax machine, an SMTP server, an Audit Server, and a user's client computer. Users can operate the TOE from the Operation Panel of the TOE or through LAN communications. Each element is described in this section.

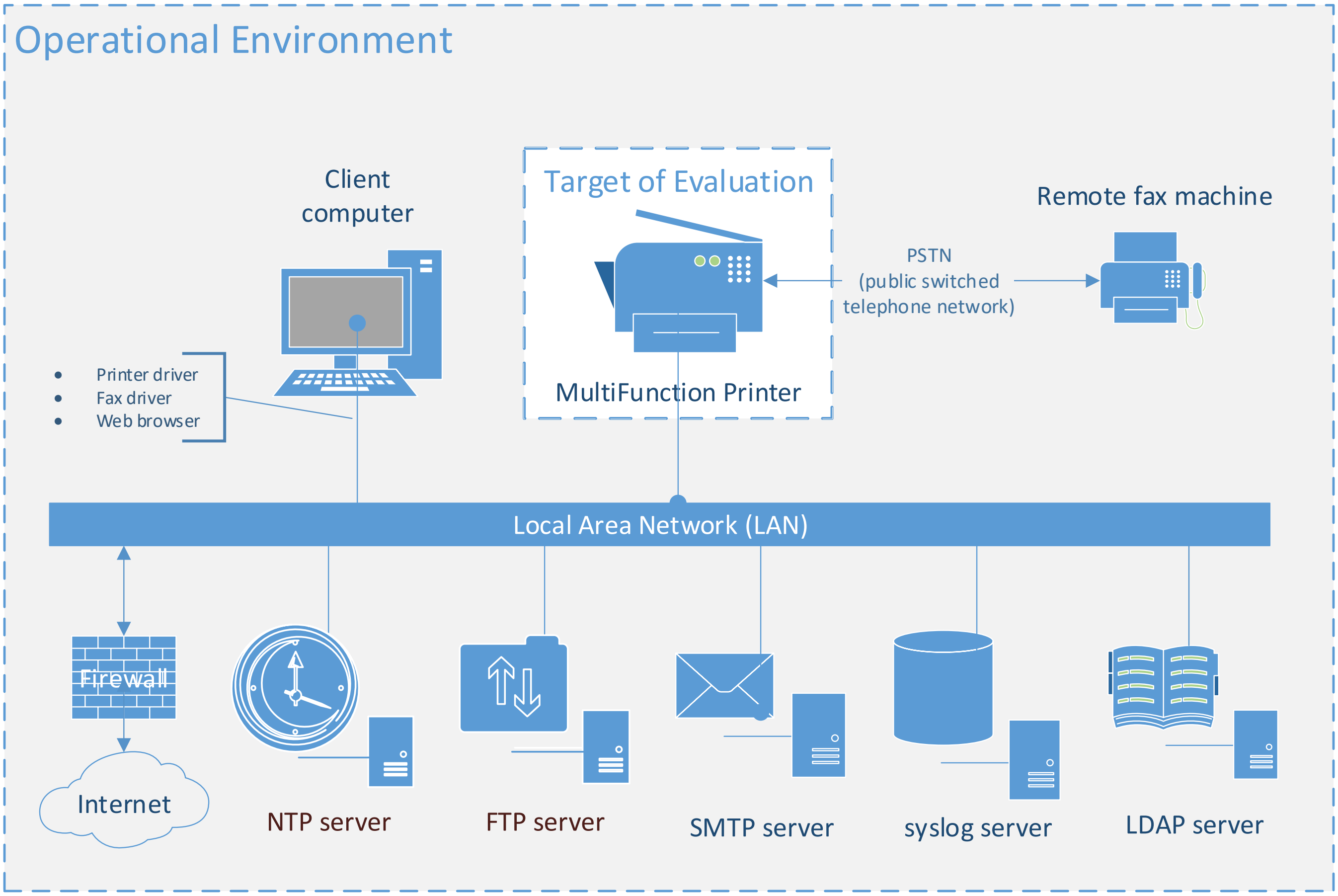


Figure 1 Example of TOE Environment

1.5.2.1 Multifunction Printer (MFP)

It is the TOE. Users can perform the following operations from the Operation Panel of the MFP:

- Configuration of the MFP,
- Copying, faxing, storage, and network transmission of paper documents,
- Printing, faxing, network transmission, and deletion of the stored documents.
- Receiving fax documents via telephone lines and storing them as documents.

1.5.2.2 LAN

Network used in the TOE environment.

1.5.2.3 Client computer

A computer that performs as a client of the TOE via the LAN. Users can remotely operate the MFP from the client computer:

- Various settings for the MFP using a Web browser installed on the client computer,
- Operation of stored documents using a Web browser installed on the client computer,
- Storage and/or printing of documents using the printer driver installed on the client computer,
- Faxing documents using the fax driver installed on the client computer.

1.5.2.4 PSTN line

A connection to a public switched telephone network for the TOE to communicate with external fax machines.

1.5.2.5 Firewall

A device to protect the LAN from Internet threats.

1.5.2.6 SMTP Server

An external IT entity used by the TOE for e-mail transmission.

1.5.2.7 syslog Server

An external IT entity used by the TOE for audit log storage.

1.5.2.8 LDAP server

An external IT entity used by the TOE for network authentication of users.

1.5.2.9 FTP server

An external IT entity used by the TOE to receive and store user documents.

1.5.3 Major Security Features of TOE

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

- Identification and Authentication
- Use-of-Feature Authorization
- Access Control
- Stored Data Encryption
- Trusted Communications

- Administrative Roles
- Auditing
- Trusted Operation
- PSTN Fax-Network Separation

1.6 TOE Description

This section describes the Physical Boundary of TOE, Hardware components, Logical Boundary of TOE, TOE Functions, and Guidance Documents.

1.6.1 Physical Boundary of TOE

The physical boundary of the TOE is the MFP, which consists of the following hardware components (shown in Figure 2): Operation Panel Unit, Engine Unit, (optional) Fax Controller Unit, Controller Board, HDD, Ic Ctlr, Network Unit, USB Port, and SD Card Slot. The MFP also consists of software components. These components comprise a physically large product that is delivered at once by a delivery company to users, and it is often set up with the assistance of a customer engineer.

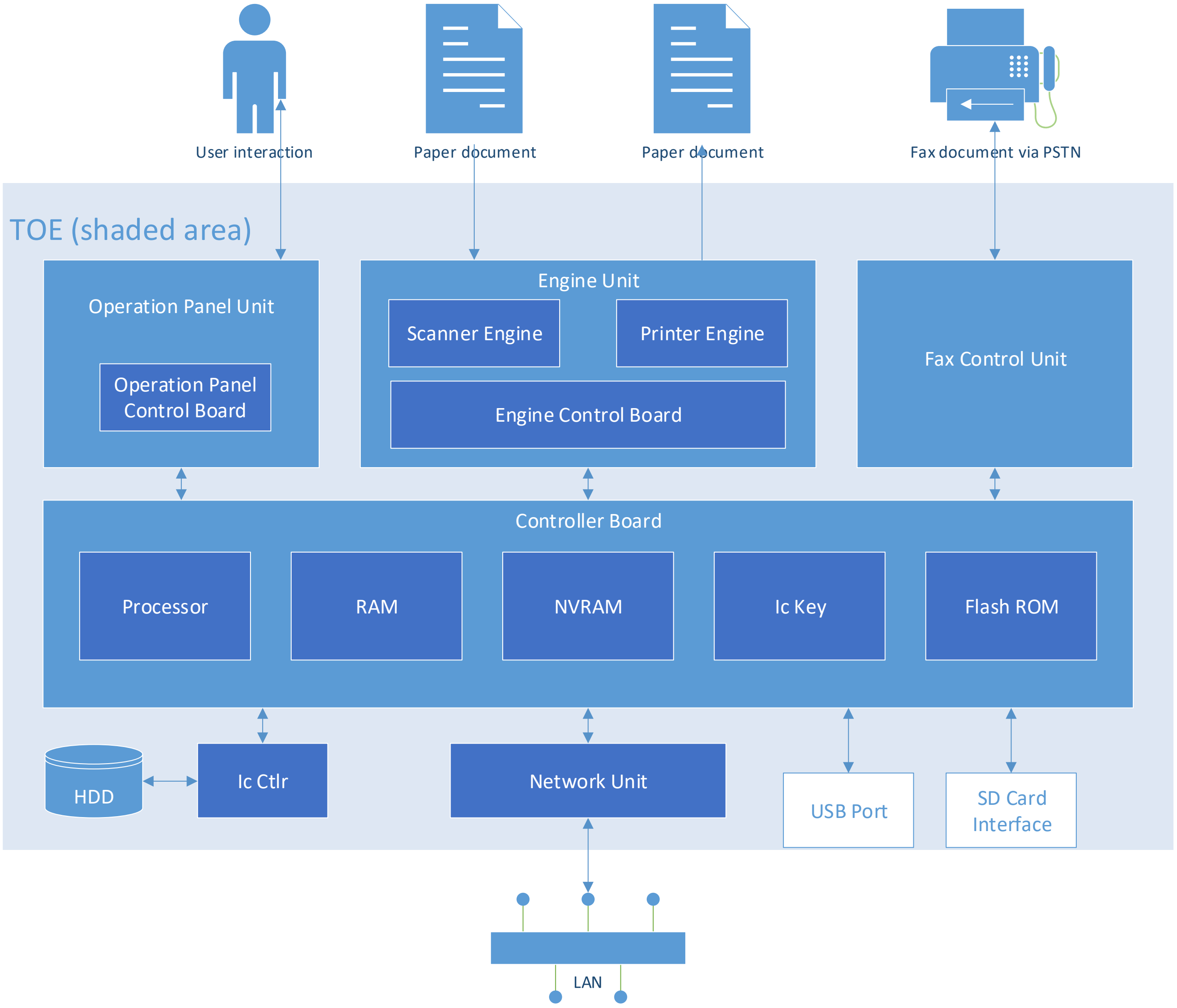


Figure 2 Hardware Configuration of the TOE

1.6.2 Hardware components

1.6.2.1 Controller Board

The Controller Board is a device that contains Processors, RAM, NVRAM, Ic Key, and FlashROM. The Controller Board sends and receives information to control the MFP. The information is processed by the MFP Control Software. The following describes the components of the Controller Board:

1.6.2.1.1 Processor

A semiconductor chip that performs basic computer processing for MFP operations.

1.6.2.1.2 RAM

A volatile memory medium which is used as a working area for image processing such as compressing/decompressing the image data. It is also used to temporarily read and write internal information.

1.6.2.1.3 NVRAM

A non-volatile memory medium in which TSF data for configuring MFP operations is stored. The NVRAM is a field-replaceable non-volatile storage device, and is claimed as such in this document.

1.6.2.1.4 Ic Key

A hardware security module which provides true random number generation and protected storage.

1.6.2.1.5 FlashROM

A non-volatile memory medium in which the MFP Control Software is installed.

1.6.2.2 Operation Panel

The Operation Panel consists of an LCD touch screen user interface and LED indicators that are controlled by Operation Panel Control Software installed on the Operation Panel Control Board. The Operation Panel Control Software performs the following:

1. Transfers operation instructions from the LCD touch screen to the Controller Board.
2. Controls the LED indicators and displays information on the LCD touch screen according to display instructions from the MFP Control Software.

The Operation Panel utilizes Linux 3.18 on an ARM Cortex-A9 Quad Core processor.

1.6.2.3 Engine Unit

The Engine Unit consists of a Scanner Engine which scans paper documents, and a Printer Engine that prints and ejects paper documents, both controlled by the Engine Control Software installed on the Engine Control Board. The Engine Control Software sends status information about the Scanner Engine and Printer Engine to the Controller Board, and operates the Scanner Engine or Printer Engine according to instructions from the MFP Control Software.

1.6.2.4 Fax Controller Unit (FCU)

The Fax Controller Unit consists of a modem which sends and receives fax data to and from other fax devices using the G3 standard for communication. FCU Control Software is installed on the Fax Controller Unit operates the modem and exchanges fax data according to instructions from the MFP Control Software. The Fax Controller Unit type M37 utilizes the RU30 processor in its operation.

1.6.2.5 HDD

The HDD is a hard disk drive that is a non-volatile memory medium. It stores documents, login user names and login passwords of Normal Users. The HDD is a field-replaceable non-volatile storage device, and is claimed as such in this document.

1.6.2.6 Ic Ctlr

The Ic Ctlr is a board that implements data encryption and decryption functions for data stored on the HDD.

1.6.2.7 Network Unit

The Network Unit is an external interface to an Ethernet LAN.

1.6.2.8 USB Port

The USB Port is an external interface to connect a client computer to the TOE for printing directly from the client computer. During installation, this interface is disabled.

1.6.2.9 SD Card Slot

There are two SD Card Slots, one for customer engineers and one for users.

The SD Card Slot for customer engineer is used when the customer engineer installs the TOE. A cover is placed on the SD Card Slot during the TOE operation so that an SD Card cannot be inserted into or removed from the slot.

The SD Card Slot for users is used by users to print documents in the SD Card. The slot is set to disabled at the installation.

1.6.3 Logical Boundary of the TOE

The Basic Functions and Security Functions are described as follows:

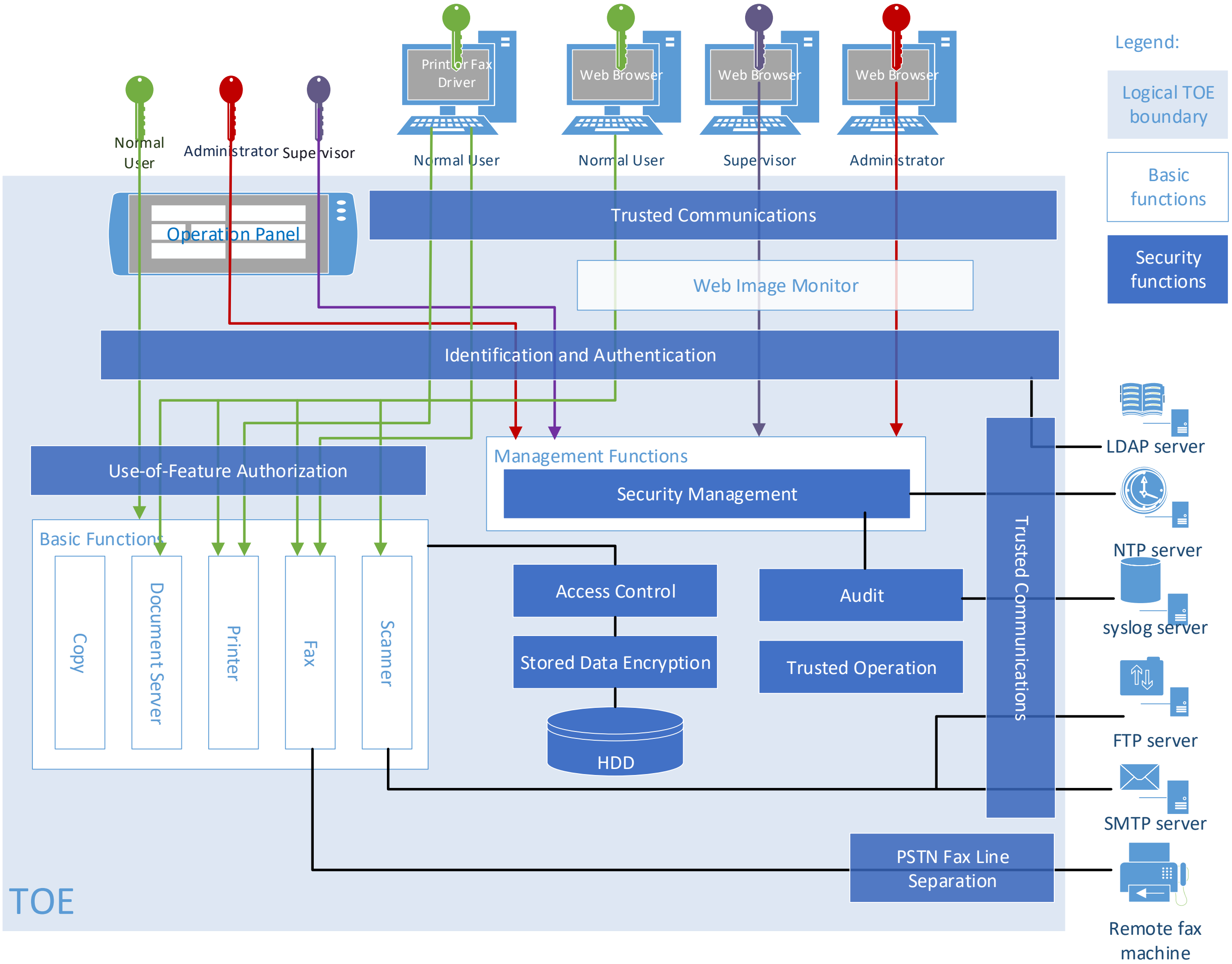


Figure 3 Logical Boundary of the TOE

1.6.4 Basic Functions

1.6.4.1 Copy Function

The Copy Function scans paper documents to be printed.

1.6.4.2 Printer Function

The Printer Function prints or stores documents received from a printer driver installed on the client computer, and prints or deletes previously-stored documents from commands from the Operation Panel or the client computer's web browser.

1.6.4.3 Scanner Function

The Scanner Function scans paper documents and then transmits and deletes the scanned images, on command from the Operation Panel.

1.6.4.4 Fax Function

The Fax Function consists of a Fax Transmission Function and a Fax Reception Function. Both functions exchange documents according to the Group 3 standard over a Public Switch Telephone Network (PSTN).

The Fax Transmission Function sends scanned images of paper documents, or images of electronic documents from a client computer, to external fax devices.

The Fax Reception Function receives documents from external fax devices, and stores them in the TOE.

1.6.4.5 Document Server Function

The Document Server Function is to perform operations on persistently-stored documents in the TOE.

From the Operation Panel, users can store, print and delete Document Server documents.

From a client computer, users can print and delete Document Server documents.

1.6.4.6 Management Function

The Management Function allows authorized users to configure the TOE's operation. The management function can be accessed from the Operation Panel or a client computer. Security Management functions can be accessed only by Administrators.

1.6.4.7 Web Image Monitor Function

The Web Image Monitor Function (hereafter "WIM") allows authorized users to remotely control the TOE from a web browser on a client computer.

1.6.5 Security Functions

The Security Functions are described as follows:

1.6.5.1 Identification and Authentication

User identification, authentication, and authorization ensure that functions of the TOE are accessible only to Users who have been authorized by an Administrator. User identification and authentication is also used as the basis for access control and administrative roles and helps associate security-relevant events and TOE use with specific Users. Identification and authentication is performed by the TOE. User's credentials can be entered locally on the Operation Panel, through WIM login, through print or fax drivers, or using network authentication services.

1.6.5.2 Use-of-Feature Authorization

The Use-of-Feature Restriction Function authorizes authenticated users to perform the operations of Copy Function, Printer Function, Scanner Function, Document Server Function and Fax Function, based on the user role and the permissions set by an Administrator for each user.

1.6.5.3 Access Control

Access controls ensure that documents, document processing job information, and security-relevant data, are accessible only to authenticated users who have appropriate access permissions.

1.6.5.4 Stored Data Encryption

The Stored Data Protection Function encrypts data on the HDD and in NVRAM to protect documents and confidential system information if those devices are removed from the TOE. Keychains for both devices are described in this document.

1.6.5.5 Trusted Communications

Trusted communication paths are established to ensure that communications with the TOE are performed with known endpoints. Data encryption ensures that data assets cannot be accessed while in transit on the LAN.

1.6.5.6 Administrative Roles

Role-based access controls ensure that the ability to configure the security settings of the TOE is available only to Users who have been authorized with an Administrator role.

1.6.5.7 Auditing

Audit logs are generated by the TOE to ensure that security-relevant events and TOE use can be monitored by authorized personnel. The TOE generates audit logs and securely transmits them to an External IT entity for storage. While stored in the TOE, audit logs are protected from unauthorized access and modification.

1.6.5.8 Trusted Operation

The Software Verification Function verifies the integrity and authenticity of MFP Control Software, FCU Control Software, and Operation Panel Control Software, before applying updates. Power-on self-tests are performed to ensure that TOE operation is not disrupted by detectable malfunction.

1.6.5.9 PSTN Fax-Line Separation

The Fax Line Separation Function restricts information received from or transmitted to the telephone network to only fax data and fax protocols. It ensures that the fax modem cannot be used to bridge to the LAN.

1.6.5.10 Image Overwrite

The Image Overwrite Function actively overwrites residual image data stored on the HDD after a Document Processing job has been completed or cancelled.

1.6.6 Functions supported but not evaluated

The following functions supported by the TOE are not included in this evaluation:

- Fax over IP
- Store while copying documents
- Store while sending documents by fax
- Menu Protect
- PDF Group Passwords
- SMTP Authentication
- File Transfer Authentication
- Erase All Memory

1.6.7 Guidance Documents

A common set of guidance documents is provided for the TOE. Selection of a particular guidance document set depends on the print speed and sales region, and they are identified in the Notes for Administrators document.

Paper manuals supplied with the TOE:

- Safe Use of This Machine
- For Users of This Product
- Notes for Users
- Software License Agreement

Online manuals available for the TOE:

- Safety Information
- User Guide
  - Setup
  - Introduction and Basic Operations
  - Copy
  - Document Server
  - Fax
  - Scan
  - Printer
  - Maintenance
  - Troubleshooting
  - Settings
  - Specifications
  - Security
  - Driver Installation Guide
- Security Reference
- Notes for Administrators v1.0: Using This Machine in a Network Environment Compliant with Protection Profile for Hardcopy Devices PP_HCD_V1.0

A complete list of manuals as they apply to all TOE variants is provided in the Notes for Administrators document. URLs for online manuals are provided in the paper manual, Safe Use of This Machine, which is supplied with the TOE.

2 ST Conformance Claims (ASE_CCL)

2.1 Common Criteria (CC) conformance claims

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

- Part 1: Introduction and general model Version 3.1 Revision 5 CCMB-2017-04-001
- Part 2: Security functional components Version 3.1 Revision 5 CCMB-2017-04-002 extended
- Part 3: Security assurance components Version 3.1 Revision 5 CCMB-2017-04-003 conformant (EAL1)

2.2 Protection Profile (PP) conformance claims

The PP to which this ST and TOE are strictly conformant and exactly compliant is:

- PP Name: Protection Profile for Hardcopy Devices
- PP Version: 1.0, dated 2015-09-11

The ST and TOE also address all of the NIAP Technical Decisions that apply to the PP:

TD0074	FCS_CKM.1(a) Requirement in HCD PP v1.0
TD0157	FCS_IPSEC_EXT.1.1 - Testing SPDs
TD0176	FDP_DSK_EXT.1.2 - SED Testing
TD0219	NIAP Endorsement of Errata for HCD PP v1.0 (Errata #1, June 2017)
TD0253	Assurance Activities for Key Transport
TD0261	Destruction of CSPs in flash
TD0299	Update to FCS_CKM.4 Assurance Activities
TD0393	Require FTP_TRP.1(b) only for printing
TD0474	Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1

Hereafter, the PP and applicable Technical Decisions are referred to collectively as “HCD PP v1.0”.

The TOE claims conformance with the following essential, additional, and optional uses as specified in the PP:

Category	Features	Conformance
Essential Uses	Scanning	Claimed
	Printing	Claimed
	Copying	Claimed
	Network Communications	Claimed
	Administration	Claimed
Additional Uses	PSTN Faxing	Claimed
	Storage and Retrieval	Claimed
	Field-Replaceable Nonvolatile Storage	Claimed
Optional Uses	Internal Audit Log Storage	Claimed
	Image Overwrite	Claimed
	Purge Data	Not Claimed

Table 5 Protection Profile claims

2.3 Conformance Claim Rationale

2.3.1.1 Consistency Claim with TOE Type in this PP

In this PP, a conforming product must support at least one of the job functions printing, scanning, or copying and must support the functions network communications and administration.

The TOE is a product that supports printing, scanning, copying, network communications, and administration functions, as required by the PP.

2.3.2 Consistency Claim with Security Problems and Security Objectives in PP

The TOE is exactly compliant with the Security Problems and Security Objectives in this PP.

2.3.3 Consistency Claim with Security Requirements in PP

The TOE is exactly compliant with the Security Requirements in this PP.

3 Security Problem Definitions (ASE_SPD)

This section describes Threats, Organizational Security Policies and Assumptions.

3.1 Users

There are two categories of Users defined in this ST, Normal and Admin. There are two Admin sub-roles.

Designation	Name	Definition
U.NORMAL	Normal User	A User who has been identified and authenticated and does not have an administrative role
U.ADMIN	Administrator	A User who has been identified and authenticated and has an administrative role
U.ADMIN.SUP	MFP Supervisor	
U.ADMIN.MFP	MFP Administrator	

Table 6 User categories

A pseudo-user role, Customer Engineer, can be enabled by an Administrator for use by an authorized service representative. It is normally disabled, as it is in the evaluated configuration.

3.2 Assets

Assets are passive entities in the TOE that contain or receive information. In this PP, Assets are Objects (as defined by the CC). There are two categories of Assets defined in this PP:

Designation	Asset category	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

Table 7 Asset categories

There are no additional Asset categories defined in this ST.

3.2.1 User Data

User Data are composed of two types:

Designation	User Data type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job

Table 8 User Data types

There are no additional types of User Data defined in this ST. Attributes associate documents and document processing jobs with the document processing functions of the TOE:

Document processing function	Attribute
Printing	+PRT
Copying	+CPY
Scanning	+SCN
Document Storage/Retrieval	+DSR
Fax (reception)	+FAXIN
Fax (transmission)	+FAXOUT

Table 9 Document and Job Attributes

650 3.2.2 TSF Data

651 TSF Data are composed of two types:

Designation	TSF Data type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

652 *Table 10 TSF Data types*

653 There are no additional types of TSF Data defined in this ST.

654 *3.2.2.1 Protected TSF Data*

655 D.TSF.PROT is composed of the following data:

Data item
Login user name
Number of Attempts before Lockout
Settings for Lockout Release Timer
Lockout time
Date settings (year/month/day)
Time settings
Minimum Character No.
Password Complexity Setting
Operation Panel auto logout time
WIM auto logout time
Stored Reception File User
Document user list
Available function list
User authentication method
Device Certificate
Network settings
Audit transfer settings
TOE Software

656 *Table 11 Data in D.TSF.PROT*

657 *3.2.2.2 Confidential TSF Data*

658 In this ST, D.TSF.CONF is composed of the following data:

Data item
Login password
Audit log
HDD cryptographic key

659 *Table 12 Data in D.TSF.CONF*

660 3.3 Threat definitions

661 The following threats are mitigated by this TOE:

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

Table 13 Threats

3.4 Organizational Security Policies

The following Organizational Security Policies (OSPs) are enforced by this TOE:

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION (conditionally mandatory)	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL (conditionally mandatory)	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW (conditionally mandatory)	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Device.

Table 14 Organizational Security Policies

3.5 Assumptions

The following assumptions must be satisfied in order for the Security Objectives and Security Functional Requirements to be effective:

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

Table 15 Assumptions

670 4 Security Objectives (ASE_OBJ)

671 4.1 Security Objectives for the TOE

672 The following Security Objectives are satisfied by this TOE:

Designation	Definition
O.USER_I&A	The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles.
O.ACCESS_CONTROL	The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
O.USER_AUTHORIZATION	The TOE shall perform authorization of Users in accordance with security policies.
O.ADMIN_ROLES	The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.
O.UPDATE_VERIFICATION	The TOE shall provide mechanisms to verify the authenticity of software updates.
O.TSF_SELF_TEST	The TOE shall test some subset of its security functionality to help ensure that subset is operating properly.
O.COMMS_PROTECTION	The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.
O.AUDIT	The TOE shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the TOE.
O.STORAGE_ENCRYPTION (conditionally mandatory)	If the TOE stores User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices.
O.KEY_MATERIAL (conditionally mandatory)	The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material.
O.FAX_NET_SEPARATION (conditionally mandatory)	If the TOE provides a PSTN fax function, then the TOE shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function.
O.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data in its Field-Replaceable Nonvolatile Storage Devices.

673 *Table 16 Security Objectives for the TOE*

674 4.2 Security Objectives for the Operational Environment

675 The following Security Objectives must be satisfied by the TOE's Operational Environment.

Designation	Definition
OE.PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE.NETWORK_PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.
OE.ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.
OE.ADMIN_TRAINING	The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly.

676 *Table 17 Security Objectives for the Operational Environment*

677 ## 4.3 Security Objectives rationale

678 The following table maps threats, OSPs, and assumptions, to their respective Security Objectives.

Threat/Policy/Assumption	Rationale
T.UNAUTHORIZED_ACCESS *An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.*	O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_COMPROMISE *An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.*	O.ACCESS_ CONTROL restricts access to TSF Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_FAILURE *A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.*	O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected.
T.UNAUTHORIZED_UPDATE *An attacker may cause the installation of unauthorized software on the TOE.*	O.UPDATE_VERIFICATION verifies the authenticity of software updates.
T.NET_COMPROMISE *An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.*	O.COMMS_PROTECTION protects LAN communications from sniffing, replay, and man-in-the-middle attacks.
P.AUTHORIZATION *Users must be authorized before performing Document Processing and administrative functions.*	O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users. O.USER_I&A provides the basis for authorization. O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators.
P.AUDIT *Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.*	O.AUDIT requires the generation of audit data. O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users. O.USER_AUTHORIZATION provides the basis for authorization.
P.COMMS_PROTECTION *The TOE* must be able to identify itself to other devices *on the LAN.*	O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks.
P.STORAGE_ENCRYPTION (conditionally mandatory) *If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.*	O.STORAGE_ENCRYPTION protects User Document Data and Confidential TSF Data stored in Field-Replaceable Nonvolatile Storage Devices from exposure if a device has been removed from the TOE and its Operational Environment.
P.KEY_MATERIAL (conditionally mandatory) *Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.*	O.KEY_MATERIAL protects keys and key materials from unauthorized access and ensures that they any key materials are not stored in cleartext on the device that uses those materials for its own encryption.
P.FAX_FLOW (conditionally mandatory) *If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.*	O.FAX_NET_SEPARATION requires a separation between the PSTN fax line and the LAN.

Threat/Policy/Assumption	Rationale
P.IMAGE_OVERWRITE (optional) *Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Device.*	O.IMAGE_OVERWRITE overwrites residual image data from Field-Replaceable Nonvolatile Storage Devices after Document Processing jobs are completed or cancelled.
A.PHYSICAL *Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.*	OE.PHYSICAL_PROTECTION establishes a protected physical environment for the TOE.
A.NETWORK *The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.*	OE.NETWORK_PROTECTION establishes a protected LAN environment for the TOE.
A.TRUSTED_ADMIN *TOE Administrators are trusted to administer the TOE according to site security policies.*	OE.ADMIN_TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.TRAINED_USERS *Authorized Users are trained to use the TOE according to site security policies.*	OE.ADMIN_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Administrators. OE.USER_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Users.

679 *Table 18 Security Objectives rationale*

5 Extended Component Definitions (ASE_ECD)

This ST uses extended components that are defined in HCD PP v1.0 and in the claimed Technical Decisions and Errata. No additional extended components are defined for this ST.

6 Security Functional Requirements (ASE_REQ)

6.1 Notational conventions

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

Italic typeface indicates the portion of an SFR that has been completed for this Security Target.

Bold italic typeface indicates the portion of an SFR that has been partially completed or refined in the Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition, and which also has been completed for this Security Target.

SFR components that are followed by a letter in parentheses, e.g., (a), (b), …, represent required iterations. This Security Target uses the iteration identifiers that are used in the Protection Profile; therefore, they may not be sequential in this Security Target.

SFR components that are followed by an identifier in square brackets, e.g., [1], [2]…, represent iterations that have been added for this Security Target. In some cases, they may be combined with the (letter) designation of required iterations, e.g., FCS_COP.1 (d)[1], FCS_COP.1 (d)[2], … .

Extended components are identified by "_EXT" following the SFR name.

6.2 Class FAU: Security Audit

6.2.1 FAU_GEN.1 Audit data generation

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;

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

c) **All auditable events specified in Table 19**, [*no other specifically defined auditable events*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 19**, [*no other audit relevant information*].

Auditable event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None

Auditable event	Relevant SFR	Additional information
Failure to establish session.	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure.

Table 19 Auditable Events

Application Note:

In cases where user identification events are inseparable from user authentication events, they may be considered to be a single event for audit purposes.

Regarding FMT_SMR.1, if the relationship between users and roles is not modifiable, its auditable event cannot be generated and the requirement to generate an audit record can be ignored.

The ST author can include other auditable events directly in the table; they are not limited to the list presented.

Assurance Activity:

TSS:

The evaluator shall check the TOE Summary Specification (TSS) to ensure that auditable events and its recorded information are consistent with the definition of the SFR.

Operational Guidance:

The evaluator shall check the guidance documents to ensure that auditable events and its recorded information are consistent with the definition of the SFRs.

Test:

The evaluator shall also perform the following tests:

The evaluator shall check to ensure that the audit record of each of the auditable events described in Table 19 is appropriately generated.

The evaluator shall check a representative sample of methods for generating auditable events, if there are multiple methods.

The evaluator shall check that FIA_UAU.1 events have been generated for each mechanism, if there are several different I&A mechanisms.

6.2.2 FAU_GEN.2 User identity association

(for O.AUDIT)

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.

Assurance Activity:

The Assurance Activities for FAU_GEN.1 address this SFR.

6.2.3 FAU_SAR.1 Audit review

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

Assurance Activity:

The following assurance activities are required when storing audit records inside the TOE.

TSS:

The evaluator shall check to ensure that the TSS contains a description that audit records can be viewed only by authorized users and functions to view audit records.

The evaluator shall check to ensure that the TSS contains a description of the methods of using interfaces that retrieve audit records (e.g., methods for user identification and authentication, authorization, and retrieving audit records).

Operational Guidance:

The evaluator shall check to ensure that the operational guidance appropriately describes the ways of viewing audit records and forms of viewing.

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that the forms of audit records are provided as specified in the operational guidance by retrieving audit records in accordance with the operational guidance.
2. The evaluator shall check to ensure that no users other than authorized users can retrieve audit records.
3. The evaluator shall check to ensure that all audit records are retrieved by the operation of retrieving audit records.

6.2.4 FAU_SAR.2 Restricted audit review

(for O.AUDIT)

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.

Assurance Activity:

Test:

The evaluator shall include tests related to this function in the set of tests performed in FMT_SMF.1.

6.2.5 FAU_STG.1 Protected audit trail storage

(for O.AUDIT)

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 prevent unauthorised modifications to the stored audit records in the audit trail.

Assurance Activity:

The following assurance activities are required when storing audit records inside the TOE.

TSS:

The evaluator shall check to ensure that the TSS contains a description of the means of preventing audit records from unauthorized access (modification, deletion).

Operational Guidance:

The evaluator shall check to ensure that the TSS and operational guidance contain descriptions of the interfaces to access to audit records, and if the descriptions of the means of preventing audit records from unauthorized access (modification, deletion) are consistent.

Test:

The evaluator shall also perform the following test:

1. The evaluator shall test that an authorized user can access the audit records.
2. The evaluator shall test that a user without authorization for the audit data cannot access the audit records.

6.2.6 FAU_STG_EXT.1 Extended: External Audit Trail Storage

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation,
FTP_ITC.1 Inter-TSF trusted channel.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

Assurance Activity:

TSS:

The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism.

The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

Operational Guidance:

The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.

Test:

The evaluator shall perform the following test for this requirement:

Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.

6.2.7 FAU_STG.4 Prevention of audit data loss

(for O.AUDIT)

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 Refinement: The TSF shall [***overwrite the oldest stored audit records***] and [***no other actions***] if the audit trail is full.

Assurance Activity:

The following assurance activities are required when storing audit records inside the TOE.

TSS:

The evaluator shall check to ensure that the TSS contains a description of the processing performed when the capacity of audit records becomes full, which is consistent with the definition of the SFR.

Operational Guidance:

The evaluator shall check to ensure that the operational guidance contains a description of the processing performed (such as informing the authorized users) when the capacity of audit records becomes full.

Test:

The evaluator shall also perform the following tests:

1. The evaluator generates auditable events after the capacity of audit records becomes full by generating auditable events in accordance with the operational guidance.

2. The evaluator shall check to ensure that the processing defined in the SFR is appropriately performed to audit records.

6.3 Class FCO: Communication

There are no class FCO requirements.

6.4 Class FCS: Cryptographic Support

6.4.1 FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(b) Cryptographic Operation (for signature generation/ verification)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_CKM.1.1(a) Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with [*NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes*] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.**

Application Note:

The ST author selects the key generation scheme used for key establishment and device authentication. If multiple schemes are supported, then the ST author should iterate this component to capture this capability. When key generation is used for device authentication, the public key is expected to be associated with an X.509v3 certificate. If the TOE acts as a receiver in the RSA key establishment scheme, the TOE does not need to implement RSA key generation.

Since the domain parameters to be used are specified by the requirements of the protocol in this PP, it is not expected that the TOE will generate domain parameters, and therefore there is no additional domain parameter validation needed when the TOE complies with the protocols specified in this PP.

SP 800-56B references (but does not mandate) key generation according to FIPS 186-3. For purposes of compliance in this version of the HCD PP, RSA key pair generation according to FIPS 186-4 is allowed in order for the TOE to claim conformance to SP 800-56B.

The generated key strength of 2048-bit DSA and rDSA keys need to be equivalent to, or greater than, a symmetric key strength of 112 bits. See NIST Special Publication 800-57, "Recommendation for Key Management" for information about equivalent key strengths.

Assurance Activity:

TSS:

The evaluator shall ensure that the TSS contains a description of how the TSF complies with 800-56A and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement.

Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described in the TSS.

The TSS may refer to the Key Management Description (KMD), described in Appendix F , that may not be made available to the public.

Test:

The evaluator shall use the key pair generation portions of "The FIPS 186-4 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and “The 186-4 RSA Validation System (RSA2VS)” as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

6.4.2 FCS_CKM.1(b)[DAR] Cryptographic key generation (Symmetric Keys) [Data At Rest]

(for O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(f) Cryptographic Operation (Key Encryption)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_CKM.1.1(b)[DAR] Refinement: The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [*256 bit*] that meet the following: No Standard**.

Application Note:

Symmetric keys may be used to generate keys along the key chain.

Assurance activity:

TSS:

The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.

KMD:

If the TOE is relying on random number generation from a third-party source, the KMD needs to describe the function call and parameters used when calling the third-party DRBG function. Also, the KMD needs to include a short description of the vendor's assumption for the amount of entropy seeding the third-party DRBG. The evaluator uses the description of the RBG functionality in FCS_RBG_EXT or the KMD to determine that the key size being requested is identical to the key size and mode to be used for the encryption/decryption of the user data (FCS_COP.1(d)).

6.4.3 FCS_CKM.1(b)[DIM] Cryptographic key generation (Symmetric Keys) [Data In Motion]

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_CKM.1.1(b)[DIM] Refinement: The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [*128 bit, 256 bit*] that meet the following: No Standard**.

Application Note:

Symmetric keys may be used to generate keys along the key chain.

Assurance activity:

TSS:

The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.

KMD:

If the TOE is relying on random number generation from a third-party source, the KMD needs to describe the function call and parameters used when calling the third-party DRBG function. Also, the KMD needs to include a short description of the vendor's assumption for the amount of entropy seeding the third-party DRBG. The evaluator uses the description of the RBG functionality in FCS_RBG_EXT or the KMD to determine that the key size being requested is identical to the key size and mode to be used for the encryption/decryption of the user data (FCS_COP.1(d)).

6.4.4 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],
FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy **all plaintext secret and private cryptographic keys and cryptographic critical security parameters** when no longer needed.

Application Note:

"Cryptographic Critical Security Parameters" are defined in FIPS 140-2 as "security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module".

Keys, including intermediate keys and key material that are no longer needed are destroyed by using an approved method, FCS_CKM.4.1. Examples of keys are intermediate keys, submasks, and BEV. There may be instances where keys or key material that are contained in persistent storage are no longer needed and require destruction. Based on their implementation, vendors will explain when certain keys are no longer needed. There are multiple situations in which key material is no longer necessary, for example, a wrapped key may need to be destroyed when a password is changed. However, there are instances when keys are allowed to remain in memory, for example, a device identification key.

Assurance activity:

TSS:

The evaluator shall verify the TSS provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.

KMD:

The evaluator shall verify the Key Management Description (KMD) includes a description of the areas where keys and key material reside and when the keys and key material are no longer needed.

The evaluator shall verify the KMD includes a key lifecycle, that includes a description where key material reside, how the key material is used, how it is determined that keys and key material are no longer needed, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM.4 for the destruction.

6.4.5 FCS_CKM.4 Cryptographic key destruction

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**For volatile memory, the destruction shall be executed by *[removal of power to the memory]*; For nonvolatile storage, the destruction shall be executed by a *[single]* overwrite of key data storage location consisting of *[a new value of a key of the same size]***] that meets the following: [***no standard***].

Application Note:

In the first selection, the ST Author is presented options for destroying disused cryptographic keys based on whether they are in volatile memory or non-volatile memory within the TOE.

The selection of block erase for non-volatile memory applies only to flash memory.

Within the selections is the option to overwrite the memory location with a new value of a key. The intent is that a new value of a key (as specified in another SFR within the PP) can be used to "replace" an existing key.

Several selections allow assignment of a 'value that does not contain any CSP'. This means that the TOE uses some other specified data not drawn from a source that may contain key material or reveal information about key material, and not being any of the particular values listed as other selection options. The point of the phrase 'does not contain any CSP' is to ensure that the overwritten data is carefully selected, and not taken from a general 'pool' that might contain current or residual data that itself requires confidentiality protection.

Assurance activity:

TSS:

The evaluator shall verify the TSS provides a high level description of how keys and key material are destroyed.

If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify that the pattern does not contain any CSPs.

The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.

KMD:

The evaluator examines the KMD to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how they are overwritten.

The evaluator shall check to ensure the KMD lists each type of key that is stored in non-volatile memory, and identifies the memory type (volatile or non-volatile) where key material is stored.

The KMD identifies and describes the interface(s) that is used to service commands to read/write memory. The evaluator examines the interface description for each different media type to ensure that the interface supports the selection(s) made by the ST Author.

Test:

For these tests the evaluator shall utilize appropriate development environment (e.g. a Virtual Machine) and development tools (debuggers, simulators, etc.) to test that keys are cleared, including all copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

Test 1: Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator shall:

1. Record the value of the key in the TOE subject to clearing.
2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
3. Cause the TOE to clear the key.
4. Cause the TOE to stop the execution but not exit.
5. Cause the TOE to dump the entire memory of the TOE into a binary file.
6. Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.

Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.

Test 2: Applied to each key help in non-volatile memory and subject to destruction by the TOE, except for replacing a key using the selection *[a new value of a key of the same size]*. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended.

1. Identify the purpose of the key and what access should fail when it is deleted. (e.g. the data encryption key being deleted would cause data decryption to fail.)
2. Cause the TOE to clear the key.
3. Have the TOE attempt the functionality that the cleared key would be necessary for. The test succeeds if step 3 fails.

Test 3: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

1. Record the value of the key in the TOE subject to clearing.
2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
3. Cause the TOE to clear the key.
4. Search the non-volatile memory the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.

Test 4: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

1. Record the storage location of the key in the TOE subject to clearing.
2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
3. Cause the TOE to clear the key.
4. Search the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.

The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.

6.4.6 FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(a) Refinement: The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [CBC]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **[*NIST SP 800-38A*]**

Application Note:

For the assignment, the ST author should assign the mode or modes in which AES operates to support the cryptographic protocols chosen for FTP_ITC and FTP_TRP.

For the selection, the ST author should choose the standards that describe the modes specified in the assignment.

Assurance Activity:

Test:

The evaluator shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

6.4.7 FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(b) Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [2048 bits]] that meets the following FIPS PUB 186-4, "Digital Signature Standard"***].

Application Note:

The ST Author should choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement (and the corresponding FCS_CKM.1 requirement) should be iterated to specify the functionality. For the algorithm chosen, the ST author should make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm.

For elliptic curve-based schemes, the key size refers to the log2 of the order of the base point.

Assurance Activity:

Test:

The evaluator shall use the signature generation and signature verification portions of "The Digital Signature Algorithm Validation System" (DSA2VS), "The Elliptic Curve Digital Signature Algorithm Validation System" (ECDSA2VS), and "The RSA Validation System" RSA2VS as a guide in testing the requirement above. The Validation System used shall comply with the conformance standard identified in the ST (i.e., FIPS PUB 186-4). This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

6.4.8 FCS_COP.1(c)[L1] Cryptographic operation (Hash Algorithm)

(selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_COP.1.1(c)[L1] Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [***SHA-1***] that meet the following: [**ISO/IEC 10118-3:2004**].

Application Note (for O.STORAGE_ENCRYPTION):

The hash selection should be consistent with the overall strength of the algorithm used for FCS_COP.1(d). (SHA 256 should be chosen for AES 128-bit keys, SHA 512 should be chosen for AES-256-bit keys) The selection of the standard is made based on the algorithms selected.

Vendors are strongly encouraged to implement updated protocols that support the SHA-2 family; until updated protocols are supported, this PP allows support for SHA-1 implementations in compliance with SP 800-131A.

Assurance activity:

TSS:

The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

Operational Guidance:

The evaluator checks the operational guidance documents to determine that any configuration that is required to be done to configure the functionality for the required hash sizes is present.

Test:

The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.

Short Messages Test - Bit-oriented Mode

The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Short Messages Test - Byte-oriented Mode

The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test - Bit-oriented Mode

The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test - Byte-oriented Mode

The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Pseudorandomly Generated Messages Test

This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of The Secure Hash Algorithm Validation System (SHAVS). The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

6.4.9 FCS_COP.1(c) [L2] Cryptographic operation (Hash Algorithm)

(selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_COP.1.1(c)[L2] Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [***SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].

Application Note (for O.STORAGE_ENCRYPTION):

The hash selection should be consistent with the overall strength of the algorithm used for FCS_COP.1(d). (SHA 256 should be chosen for AES 128-bit keys, SHA 512 should be chosen for AES-256-bit keys) The selection of the standard is made based on the algorithms selected.

Vendors are strongly encouraged to implement updated protocols that support the SHA-2 family; until updated protocols are supported, this PP allows support for SHA-1 implementations in compliance with SP 800-131A.

Assurance activity:

TSS:

The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

Operational Guidance:

The evaluator checks the operational guidance documents to determine that any configuration that is required to be done to configure the functionality for the required hash sizes is present.

Test:

The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.

<u>Short Messages Test - Bit-oriented Mode</u>

The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

<u>Short Messages Test - Byte-oriented Mode</u>

The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test - Bit-oriented Mode

The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test - Byte-oriented Mode

The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Pseudorandomly Generated Messages Test

This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of The Secure Hash Algorithm Validation System (SHAVS). The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

6.4.10 FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

(for O. STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [*CBC*] mode and cryptographic key sizes [*256 bits*] that meet the following: AES as specified in ISO/IEC 18033-3, [*CBC as specified in ISO/IEC 10116*]**.

Application Note:

This PP allows for software encryption or hardware encryption.

If XTS Mode is selected, a cryptographic key of 256-bit or of 512-bit is allowed as specified in IEEE 1619. XTS-AES key is divided into two AES keys of equal size - for example, AES-128 is used as the underlying algorithm, when 256-bit key and XTS mode are selected. AES-256 is used when a 512-bit key and XTS mode are selected.

The intent of this requirement is to specify the approved AES modes that the ST Author may select for AES encryption of the appropriate information on the Field-Replaceable Nonvolatile Storage Device. For the first selection, the ST author should indicate the mode or modes supported by the TOE implementation. The second selection indicates the key size to be used, which is identical to that specified for FCS_CKM.1(b). The third selection must agree with the mode or modes chosen in the first selection. If multiple modes are supported, it may be clearer in the ST if this component was iterated.

Assurance activity:

TSS:

The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for encryption.

Operational Guidance:

If multiple encryption modes are supported, the evaluator examines the guidance documentation to determine that the method of choosing a specific mode/key size by the end user is described.

Test:

The following tests are conditional based upon the selections made in the SFR.

AES-CBC Tests

AES-CBC Known Answer Tests

There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

KAT-1. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key.

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption.

KAT-2. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys.

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AES-CBC decryption.

KAT-3. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N].

To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.

KAT-4. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost 128-i bits be zeros, for i in [1,128].

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.

AES-CBC Multi-Block Message Test

The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation.

The evaluator shall also test the decrypt functionality for each mode by decrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.

AES-CBC Monte Carlo Tests

The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:

```
# Input: PT, IV, Key
for i = 1 to 1000:
    if i == 1:
        CT[1] = AES-CBC-Encrypt(Key, IV, PT)
        PT = IV
```

```
else:
    CT[i] = AES-CBC-Encrypt(Key, PT)
    PT = CT[i-1]
```

The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.

6.4.11 FCS_COP.1(f) Cryptographic operation (Key Encryption)

(selected from FCS_KYC_EXT.1.1)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(f) Refinement: The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [[*CBC*] mode]** and cryptographic key sizes **[*256 bits*]** that meet the following: **AES as specified in ISO /IEC 18033-3, [*CBC as specified in ISO/IEC 10116*]**.

Application Note:

This requirement is used in the body of the ST if the ST Author chooses to use AES encryption/decryption for protecting the keys as part of the key chaining approach that is specified in FCS_KYC_EXT.1.

Assurance activity:

TSS:

The evaluator shall verify the TSS includes a description of the key encryption function(s) and shall verify the key encryption uses an approved algorithm according to the appropriate specification.

KMD:

The evaluator shall review the KMD to ensure that all keys are encrypted using the approved method and a description of when the key encryption occurs is provided.

Test:

The evaluator shall use tests in FCS_COP.1(d) to verify encryption.

6.4.12 FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

(selected with FCS_IPSEC_EXT.1.4)

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(b) Cryptographic key generation (Symmetric Keys)]

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(g) Refinement: The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **Hash-**[***SHA-256, SHA-384, SHA-512***], key size [**64 (when using SHA-256), 128 (when using SHA-384 or SHA-512)**], and message digest sizes [***256, 384, 512***] bits that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**

Assurance Activity:

Test:

The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

6.4.13 FCS_HTTPS_EXT.1 Extended: HTTPS selected

(selected in FTP_TRP.1.1)

Hierarchical to: No other components.

Dependencies: FCS_TLS_EXT.1 Extended: TLS selected.

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

Application Note:

The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

Assurance Activity:

TSS:

The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack.

Test:

Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.

6.4.14 FCS_IPSEC_EXT.1 Extended: IPsec selected

(selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to: No other components.

Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

FCS_COP.1(c)[L2] Cryptographic Operation (Hash Algorithm)

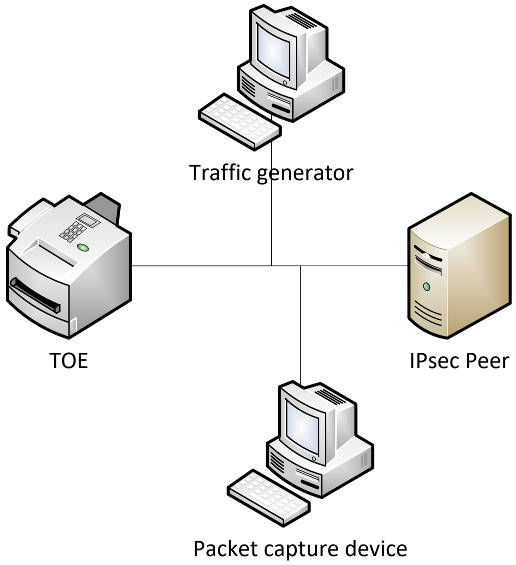
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

Application Note:

In order to show that the TSF implements the RFCs in accordance with the requirements of this PP, the evaluator shall perform the assurance activities listed below.

The TOE is required to use the IPsec protocol to establish connections used to communicate with an IPsec Peer.



The evaluators shall minimally create a test environment equivalent to the test environment illustrated above. It is expected that the traffic generator is used to construct network packets and will provide the evaluator with the ability manipulate fields in the ICMP, IPv4, IPv6, UDP, and TCP packet headers. The evaluators must provide justification for any differences in the test environment.

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

Application Note:

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet). The SPD can be implemented in various ways, including router access control lists, firewall rulesets, a “traditional” SPD, etc. Regardless of the implementation details, there is a notion of a “rule” that a packet is “matched” against and a resulting action that take place.

While there must be a means to order the rules, a general approach to ordering is not mandated, as long as the SPD can distinguish the IP packets and apply the rules accordingly. There may be multiple SPDs (one for each network interface), but this is not required.

Assurance Activity:

TSS:

The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet) and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.

As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.

Operational Guidance:

The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

Test:

The evaluator uses the guidance documentation to configure the TOE to carry out the following tests:

a) Test 1: The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and (if configurable) allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.

b) Test 2: The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.

FCS_IPSEC_EXT.1.2 The TSF shall implement [**transport mode**].

Assurance Activity:

TSS:

The evaluator checks the TSS to ensure it states that the VPN can be established to operate in tunnel mode and/or transport mode (as selected).

Operational Guidance:

The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.

Test:

The evaluator shall perform the following test(s) based on the selections chosen:

1. (conditional): If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in tunnel mode and also configures an IPsec Peer to operate in tunnel mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the client to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.

2. (conditional): If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec Peer to operate in transport mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

Assurance Activity:

TSS:

The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no "rules" are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.

Operational Guidance:

The evaluator checks that the operational guidance provides instructions on how to construct the SPD and uses the guidance to configure the TOE for the following tests.

Test:

The evaluator shall perform the following test:

The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a "TOE created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that the packet was not permitted to flow to any of the TOE's interfaces.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [***the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC***].

Assurance Activity:

TSS:

The evaluator shall examine the TSS to verify that the symmetric encryption algorithms selected (along with the SHA-based HMAC algorithm, if AES-CBC is selected) are described. If selected, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(g) Cryptographic Operations (for keyed-hash message authentication).

Operational Guidance:

The evaluator checks the operational guidance to ensure it provides instructions on how to configure the TOE to use the algorithms selected by the ST author.

Test:

The evaluator shall also perform the following tests:

The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to using each of the selected algorithms, and attempt to establish a connection using ESP. The connection should be successfully established for each algorithm.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [***IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109***, [***no other RFCs for extended sequence numbers***], and [***RFC 4868 for hash functions***];].

Application Note:

Either IKEv1 or IKEv2 support must be provided, although conformant TOEs can provide both; the first selection is used to make this choice. For IKEv1, the requirement is to be interpreted as requiring the IKE implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109. RFC 4304 identifies support for extended sequence numbers, which compliant TOEs can specify using the second selection. RFC 4868 identifies additional hash functions for use with both IKEv1 and IKEv2; if these functions are implemented, the third (for IKEv1) and fourth (for IKEv2) selection can be used.

Assurance Activity:

TSS:

The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.

Operational Guidance:

The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the following test if IKEv2 is selected.

Test:

(conditional): If IKEv2 is selected, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [***IKEv1***] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [***no other algorithm***].

Assurance Activity:

TSS:

The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.

Operational Guidance:

The evaluator ensures that the operational guidance describes the configuration of the mandated algorithms, as well as any additional algorithms selected in the requirement. The guidance is then used to configure the TOE to perform the following test for each ciphersuite selected.

Test:

The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

Assurance Activity:

TSS:

The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.

Operational Guidance:

If the mode requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure that instructions for this configuration are contained within that guidance.

Test:

The evaluator shall also perform the following test:

(conditional): The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported. This test is not applicable if IKEv1 is not selected above in the FCS_IPSEC_EXT.1.5 protocol selection.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [***IKEv1 SA lifetimes can be established based on*** [***length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs***]].

Application Note:

The ST Author is afforded a selection based on the version of IKE in their implementation. If the lifetime limitations are configurable, then the evaluator verifies that the appropriate instructions for configuring these values are included in the operational guidance.

As far as SA lifetimes are concerned, the TOE can limit the lifetime based on the number of bytes transmitted, or the number of packets transmitted. Either packet-based or volume-based SA lifetimes are acceptable; the ST author makes the appropriate selection to indicate which type of lifetime limits are supported.

Assurance Activity:

Operational Guidance:

The evaluator verifies that the values for SA lifetimes can be configured and that the instructions for doing so are located in the operational guidance. If time-based limits are supported, the evaluator ensures that the values allow for Phase 1 SAs values for 24 hours and 8 hours for Phase 2 SAs. Currently there are no values mandated for the number of packets or number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.

When testing this functionality, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered."

Test:

Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

1. (Conditional): The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is renegotiated.

2. (Conditional): The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.

3. (Conditional): The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [[**DH groups 1 and 2**]].

Application Note:

The above requires that the TOE support DH Group 14. If other groups are supported, then those should be selected (for groups 24, 19, 20, and 5) or specified in the assignment above; otherwise "no other DH groups" should be selected. This applies to IKEv1/IKEv2 exchanges.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.

Test:

The evaluator shall also perform the following test (this test may be combined with other tests for this component, for instance, the tests associated with FCS_IPSEC_EXT.1.1):

For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [***RSA***] algorithm and Pre-shared Keys.

Application Note:

The selected algorithm should correspond to an appropriate selection for FCS_COP.1(b). If IPsec is included in the TOE, the ST author also includes FIA_PSK_EXT from Appendix D.2.6.

Assurance Activity:

TSS:

The evaluator shall check that the TSS contains a description of the IKE peer authentication process used by the TOE, and that this description covers the use of the signature algorithm or algorithms specified in the requirement.

Test:

The evaluator shall also perform the following test:

For each supported signature algorithm, the evaluator shall test that peer authentication using that algorithm can be successfully achieved and results in the successful establishment of a connection.

6.4.15 FCS_KYC_EXT.1 Extended: Key Chaining

(for O.STORAGE_ENCRYPTION)

Hierarchical to:	No other components.
Dependencies:	[FCS_COP.1(e) Cryptographic operation (Key Wrapping),
	FCS_SMC_EXT.1 Extended: Submask Combining,
	FCS_COP.1(f) Cryptographic operation (Key Encryption),
	FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or
	FCS_COP.1(i) Cryptographic operation (Key Transport)]

Application Note:

This SFR forms a keychain that terminates either with a DEK or a BEV to unlock a self-encrypting drive. If passwords are not used, it can be a keychain of one, with no intermediate keys forming the DEK or BEV, provided that key is protected. For example, if the DEK for an SED is not stored on the SED and is released on power-up, a keychain of one is allowed.

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [***intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s)****:* [***key encryption as specified in FCS_COP.1(f)***]] while maintaining an effective strength of [***256 bits***].

Application Note:

Key Chaining is the method of using multiple layers of encryption keys to ultimately secure the BEV (Border Encryption Value). The number of intermediate keys will vary – from one (e.g., taking the conditioned password authorization factor and directly using it as the BEV) to many. This applies to all keys that *contribute to the ultimate wrapping or derivation of the BEV; including those in areas of protected storage (e.g. TPM stored keys, comparison values).*

Multiple key chains to the BEV are allowed, as long as all chains meet the key chain requirement.

Once the ST Author has selected a method to create the chain (either by unwrapping or encrypting keys), they pull the appropriate requirement out of this appendix. It is allowable for an implementation to use for any or all methods.

The method the TOE uses to chain keys and manage/protect them is described in the Key Management Description; see Key Management Description for more information.

Assurance activity:

TSS:

The evaluator shall verify the TSS contains a high-level description of the BEV sizes – that it supports BEV outputs of no fewer 128 bits for products that support only AES-128, and no fewer than 256 bits for products that support AES-256.

KMD:

The evaluator shall examine the KMD to ensure that it describes a high level description of the key hierarchy for all accepted BEVs. The evaluator shall examine the KMD to ensure it describes the key chain in detail. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap, submask combining, or key encryption.

The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the Key Chain.

The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.

6.4.16 FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

(for O.STORAGE_ENCRYPTION and O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1: The TSF shall perform all deterministic random bit generation services in accordance with [***NIST SP 800-90A***] using [***Hash_DRBG (refinement: SHA-256)***].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[***one (1)***] hardware-based noise source(s)] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

Application Note:

ISO/IEC 18031:2011 contains different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used and include the specific underlying cryptographic primitives used in the requirement. While any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CTR_DRBG are allowed. Table C.2 in ISO/IEC 18031:2011 provides an identification of Security strengths, Entropy and Seed length requirements for the AES-128 and 256 Block Cipher.

The CTR_DRGB in ISO/IEC 18031:2011 requires using derivation function, whereas NIST SP 800-90A does not. Either model is acceptable. In the first selection in FCS_RBG_EXT.1.1, the ST Author chooses the standard with which they are compliant.

The first selection in FCS_RBG_EXT.1.2 the ST author fills in how many entropy sources are used for each type of entropy source they employ. It should be noted that a combination of hardware and software based noise sources is acceptable.

*It should be noted that the entropy source is considered to be a part of the RBG and if the RBG is included in the TOE, the developer is required to provide the entropy description outlined in Appendix E. The documentation *and tests* required in the Evaluation Activity for this element necessarily cover each source indicated in FCS_RBG_EXT.1.2.*

Assurance activity:

TSS:

For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator shall verify that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG. If the ST specifies more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each DRBG mechanism.

Entropy Description:

The evaluator shall ensure the Entropy Description provides all of the required information as described in Appendix E. The evaluator assesses the information provided and ensures the TOE is providing sufficient entropy when it is generating a Random Bit String.

Operational Guidance:

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected DRBG mechanism(s), if necessary.

Test:

The evaluator shall perform 15 trials for the RBG implementation. If the RBG is configurable by the TOE, the evaluator shall perform 15 trials for each configuration. The evaluator shall verify that the instructions in the operational guidance for configuration of the RBG are valid.

If the RBG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "Generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP800-90A).

If the RBG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

Entropy input: the length of the entropy input value must equal the seed length.

Nonce: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.

Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.

Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

6.4.17 FCS_TLS_EXT.1 Extended: TLS selected

(selected in FTP_TRP.1.1)

Hierarchical to:	No other components.
Dependencies:	FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
	FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
	FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
	FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [***TLS 1.2 (RFC 5246)***] supporting the following ciphersuites:

[TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384].

Application Note:

The ST author must make the appropriate selections and assignments to reflect the TLS implementation.

The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the ciphersuites that are supported. If administrative steps need to be taken so that the suites negotiated by the implementation are limited to those in this requirement, the appropriate instructions need to be contained in the guidance called for by AGD_OPE.

The Suite B algorithms (RFC 5430) listed above are the preferred algorithms for implementation. The TLS requirement may be changed in the next version of the HCD PP to comply with CNSSP 15 and NIST SP 800-131A.

Assurance Activity:

TSS:

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

Test:

The evaluator shall also perform the following test:

1. The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

2. The evaluator shall setup a man-in-the-middle tool between the TOE and the TLS Peer and shall perform the following modifications to the traffic:

a. [Conditional: TOE is a server] Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the server denies the client's Finished handshake message.

b. [Conditional: TOE is a client] Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.

c. [Conditional: TOE is a client] If a DHE or ECDHE ciphersuite is supported, modify the signature block in the Server's KeyExchange handshake message, and verify that the client rejects the connection after receiving the Server KeyExchange.

d. [Conditional: TOE is a client] Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data.

6.5 Class FDP: User Data Protection

Application Note:

The User Data Access Control SFP is composed of Table 20, Table 21, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, and FMT_MSA.3.

		"Create"	"Read"	"Modify"	"Delete"
Print (+PRT)	***Operation:***	***Submit a document to be printed***	***View image or Release printed output***	***Modify stored document***	***Delete stored document***
	Job owner	*Allowed* (note 1)	*View: no function* *Release: allowed*	*No function*	*Allowed*
	U.ADMIN	*No function*	*View: no function* *Release: allowed*	*No function*	*Allowed*
	U.NORMAL	*Allowed*	Denied	Denied	Denied
	Unauthenticated	(condition 1)	Denied	Denied	Denied
Scan (+SCN)	***Operation:***	***Submit a document for scanning***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	*Allowed* (note 2)	*No function*	*No function*	*Allowed*
	U.ADMIN	*No function*	*No function*	*No function*	*Allowed*
	U.NORMAL	*Allowed*	Denied	Denied *(No function)*	Denied *(No function)*
	Unauthenticated	Denied	Denied	Denied *(No function)*	Denied *(No function)*

		"Create"	"Read"	"Modify"	"Delete"
Copy (+CPY)	***Operation:***	***Submit a document for copying***	***View scanned image or Release printed copy output***	***Modify stored image***	***Delete stored image***
	Job owner	*Allowed* (note 2)	*View: no function* *Release: no function*	*No function*	*Allowed*
	U.ADMIN	*No function*	*View: no function* *Release: no function*	*No function*	*Allowed*
	U.NORMAL	*Allowed*	Denied	Denied *(No function)*	Denied *(No function)*
	Unauthenticated	Denied	Denied	Denied *(No function)*	Denied *(No function)*
Fax send (+FAXOUT)	***Operation:***	***Submit a document to send as a fax***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	*Allowed* (note 2)	*No function*	*No function*	*Allowed*
	U.ADMIN	*No function*	*No function*	*No function*	*Allowed*
	U.NORMAL	*Allowed*	Denied	Denied *(No function)*	Denied *(No function)*
	Unauthenticated	Denied	Denied	Denied *(No function)*	Denied *(No function)*
Fax receive (+FAXIN)	***Operation:***	***Receive a fax and store it***	***View fax image or Release printed fax output***	***Modify image of received fax***	***Delete image of received fax***
	Fax owner	*Allowed* (note 3)	*View: allowed* *Release: allowed*	*No function*	*Allowed*
	U.ADMIN	*Allowed* (note 4)	*View: no function* *Release: no function*	*No function*	*No function*
	U.NORMAL	*Allowed* (note 4)	Denied	Denied	Denied
	Unauthenticated	*Allowed*	Denied	Denied	Denied
Storage / retrieval (+DSR)	***Operation:***	***Store document***	***Retrieve stored document***	***Modify stored document***	***Delete stored document***
	Job owner	*Allowed* (note 1)	*Allowed*	*Allowed*	*Allowed*
	U.ADMIN	*No function*	*Denied*	*Allowed*	*Allowed*
	U.NORMAL	*Allowed*	Denied	Denied	Denied
	Unauthenticated	(condition 1)	Denied	Denied	Denied

Table 20 D.USER.DOC Access Control SFP

		"Create" *	"Read"	"Modify"	"Delete"
Print (+PRT)	***Operation:***	***Create print job***	***View print queue / log***	***Modify print job***	***Cancel print job***
	Job owner	(note 1)	*Allowed*	*No function*	*Allowed*
	U.ADMIN	*No function*	*Allowed*	*No function*	*Allowed*
	U.NORMAL	*Allowed*	*Allowed*	Denied	Denied
	Unauthenticated	*Allowed*	*Allowed*	Denied	Denied
Scan (+SCN)	***Operation:***	***Create scan job***	***View scan status / log***	***Modify scan job***	***Cancel scan job***
	Job owner	(note 2)	*Allowed*	*No function*	*Allowed*
	U.ADMIN	*No function*	*Allowed*	*No function*	*Allowed*
	U.NORMAL	*Allowed*	*Allowed*	Denied	Denied
	Unauthenticated	Denied	*Denied*	Denied	Denied
Copy (+CPY)	***Operation:***	***Create copy job***	***View copy status / log***	***Modify copy job***	***Cancel copy job***
	Job owner	(note 2)	*Allowed*	*No function*	*Allowed*
	U.ADMIN	*No function*	*Allowed*	*No function*	*Allowed*
	U.NORMAL	*Allowed*	*Allowed*	Denied	Denied
	Unauthenticated	Denied	*Denied*	Denied	Denied
Fax send (+FAXOUT)	***Operation:***	***Create fax send job***	***View fax job queue / log***	***Modify fax send job***	***Cancel fax send job***
	Job owner	(note 2)	*Allowed*	*Allowed*	*Allowed*
	U.ADMIN	*No function*	*Allowed*	*No function*	*Allowed*
	U.NORMAL	*Allowed*	*Allowed*	Denied	Denied
	Unauthenticated	Denied	*Denied*	Denied	Denied
Fax receive (+FAXIN)	***Operation:***	***Create fax receive job***	***View fax receive status / log***	***Modify fax receive job***	***Cancel fax receive job***
	Fax owner	(note 3)	*Allowed*	*No function*	*Allowed*
	U.ADMIN	(note 4)	*Allowed*	*No function*	*Allowed*
	U.NORMAL	(note 4)	*Allowed*	Denied	Denied
	Unauthenticated	*Allowed*	*Denied*	Denied	Denied
Storage / retrieval (+DSR)	***Operation:***	***Create storage / retrieval job***	***View storage / retrieval log***	***Modify storage / retrieval job***	***Cancel storage / retrieval job***
	Job owner	(note 1)	*Allowed*	*No function*	*No function*
	U.ADMIN	*No function*	*Allowed*	*No function*	*No function*
	U.NORMAL	*Allowed*	*Allowed*	Denied	Denied
	Unauthenticated	(condition 1)	*Denied*	Denied	Denied

Table 21 D.USER.JOB Access Control SFP

Application note:

In general, the ST Author may modify this SFP provided that any changes are more restrictive. As examples, the ST Author may: remove the rules related to Document Processing functions that are not present in a TOE, add or modify rules to further deny access, or subdivide User Data to further restrict access for some data (e.g., D.USER.JOB.PROT and D.USER.JOB.CONF). Empty cells in the table indicate that the operation may be permitted, but it is not required to be permitted.

In particular, referring to Table 20 and Table 21:

A cell marked "Denied" indicates that the user (row) must not be permitted to perform the operation (column). The ST Author cannot override this.

A cell that is blank indicates that the user may be permitted to perform the operation. However, the ST author may add conditions or restrictions, or deny permission entirely.

A cell that is marked with a Condition means that the user can be permitted to perform the operation, provided that it meets that Condition as specified below. As with blank cells, the ST author can make it more restrictive.

***Condition 1**: Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.*

See also the following Notes that are referenced in Table 20 and Table 21:

***Note 1**: Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.*

***Note 2**: Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.*

***Note 3**: Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of received faxes is assigned to a specific user or U.ADMIN role.*

***Note 4**: PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.*

6.5.1 FDP_ACC.1 Subset access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** on **subjects, objects, and operations among subjects and objects specified in *Table 20 and Table 21***.

Application note:

Refer to the Application Note associated with Table 20 and Table 21.

Assurance Activity:

It is covered by assurance activities for FDP_ACF.1.

6.5.2 FDP_ACF.1 Security attribute based access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: **subjects, objects, and attributes specified in *Table 20 and Table 21***.

FDP_ACF.1.2 Refinement: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 20 and Table 21***].

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***all controlled operations on controlled objects specified in Table 20 and Table 21 are explicitly denied to U.ADMIN.SUP***].

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS describes the functions to realize SFP defined in Table 20 and Table 21 by providing specific details so that ST readers can understand without being misunderstood.

Operational Guidance:

The evaluator shall check to ensure that the operational guidance contains a description of the operation to realize the SFP defined in Table 20 and Table 21, which is consistent with the description in the TSS.

Test:

The evaluator shall perform tests to confirm the functions to realize the SFP defined in Table 20 and Table 21 with each type of interface (e.g., operation panel, Web interfaces) to the TOE.

The evaluator testing should include the following viewpoints:

- representative sets of the operations against all the object types defined in Table 20 and Table 21 (including some cases where operations are either permitted or denied)
- representative sets for the combinations of the setting for security attributes that are used in access control

6.5.3 FDP_DSK_EXT.1 Extended: Protection of Data on Disk

(for O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption).

FDP_DSK_EXT.1.1 The TSF shall [***perform encryption in accordance with FCS_COP.1(d)***], such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext Confidential TSF Data.

Application Note:

If the self-encrypting device option is selected, the device must be certified in conformance to the current Full Disk Encryption Protection Profile. The ST Author should consult with a CC Scheme for advice on approved Protection Profiles.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

Application Note:

The intent of this requirement is to specify that encryption of any confidential data will not depend on a user electing to protect that data. The encryption specified in FDP_DSK_EXT.1 occurs transparently to the user and the decision to protect the data is outside the discretion of the user.

Assurance activity:

In the assurance activities, below, “Device” refers to the Field-Replaceable Nonvolatile Storage Device from FDP_DSK_EXT.1. If the TOE contains more than one applicable Device, then the assurance activities are performed as necessary on each such Device.

TSS:

The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the Device and the point at which the encryption function is applied.

For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes the interface(s) used by the TOE to invoke this functionality.

The evaluator shall verify that the TSS describes the initialization of the Device at shipment of the TOE, or by the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the Device. The evaluator shall verify the TSS describes areas of the Device that it does not encrypt (e.g., portions that do not contain confidential data boot loaders, partition tables, etc.). If the TOE supports multiple Device encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all Devices.

Operational Guidance:

The evaluator shall review the AGD guidance to determine that it describes the initial steps needed to enable the Device encryption function, including any necessary preparatory steps. The guidance shall provide instructions that are sufficient to ensure that all Devices will be encrypted when encryption is enabled or at shipment of the TOE.

KMD:

The evaluator shall verify the KMD includes a description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device’s main SOC or separate co-processor, for software: initialization of the Device, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions that do not contain confidential data, partition tables, etc.)). The evaluator shall verify the KMD provides a functional (block) diagram showing the main components (such as memories and processors) and the data path between, for hardware, the Device's interface and the Device's persistent media storing the data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the storage device entirely when a user or administrator first provisions the product. The hardware encryption diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the hardware encryption diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine.

The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is enabled, the TOE encrypts all applicable Devices. The evaluator shall verify that the KMD describes the data flow from the interface to the Device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted area).

The evaluator shall verify that the KMD provides a description of the boot initialization, the encryption initialization process, and at what moment the product enables the encryption. If encryption can be enabled and disabled, the evaluator shall validate that the product does not allow for the transfer of confidential data before it fully initializes the encryption. The evaluator shall ensure the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key.

Test:

The evaluator shall perform the following tests:

Test 1. Write data to Storage device: Perform writing to the storage device with operating TSFI which enforce write process of User documents and Confidential TSF data.

Test 2. Confirm that written data are encrypted: Verify there are no plaintext data present in the encrypted range written by Test 1; and, verify that the data can be decrypted by proper key and key material.

All TSFIs for writing User Document Data and Confidential TSF data should be tested by above Test 1 and Test 2.

6.5.4 FDP_FXS_EXT.1 Extended: Fax separation

(for O.FAX_NET_SEPARATION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

Application note:

FDP_FXS.EXT.1 is required if fax-net separation is performed by the TSF.

Assurance Activity:

The following assurance activities are required when the TOE has a fax communication function to transmit and receive via PSTN.

TSS:

The evaluator shall check the TSS to ensure that it describes:

1. The fax interface use cases
2. The capabilities of the fax modem and the supported fax protocols
3. The data that is allowed to be sent or received via the fax interface
4. How the TOE can only be used transmitting or receiving User Data using fax protocols

Operational Guidance:

The evaluator shall check to ensure that the operational guidance contains a description of the fax interface in terms of usage and available features.

Test:

The evaluator shall test to ensure that the fax interface can only be used transmitting or receiving User Data using fax protocols. Testing will be dependent upon how the TOE enforces this requirement. The following tests shall be used and supplemented with additional testing or a rationale as to why the following tests are sufficient:

1. Verify that the TOE accepts incoming calls using fax carrier protocols and rejects calls that use data carriers. For example, this may be achieved using a terminal application to issue modem commands directly to the TOE from a PC modem (issue terminal command: ‘ATDT <TOE Fax Number>’) – the TOE should answer the call and disconnect.
2. Verify TOE negotiates outgoing calls using fax carrier protocols and rejects negotiation of data carriers. For example, this may be achieved by using a PC modem to attempt to receive a call from the TOE (submit a fax job from the TOE to <PC modem number>, at PC issue terminal command: ‘ATA’) – the TOE should disconnect without negotiating a carrier.

6.5.5 FDP_RIP.1(a) Subset residual information protection

(for O.IMAGE_OVERWRITE)

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1(a) Refinement: The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting data** upon the **deallocation of the resource from** the following objects: **D.USER.DOC**.

Assurance activity:

TSS:

The evaluator shall examine the TSS to ensure that the description is comprehensive in describing where image data is stored and how and when it is overwritten.

Operational Guidance:

The evaluator shall check to ensure that the operational guidance contains instructions for enabling the Image Overwrite function.

Test:

The evaluator shall include tests related to this function in the set of tests performed in FMT_SMF.1.

6.6 Class FIA: Identification and Authentication

6.6.1 FIA_AFL.1 Authentication failure handling

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within*** [***1 to 5***]] unsuccessful authentication attempts occur related to [***list of authentication events shown in Table 22***].

Authentication Events
User authentication using the Operation Panel
User authentication using WIM from the client computer
User authentication when printing from the client computer
User authentication when using LAN Fax from the client computer

Table 22 Authentication Events

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [***perform actions shown in Table 23***].

Unsuccessfully Authenticated Users	Actions for Authentication Failure
Normal user	The lockout for the Normal User is released by the lockout time set by the MFP Administrator, or release operation by the MFP Administrator.
MFP Supervisor	The lockout for a MFP Supervisor is released by the lockout time set by the MFP Administrator, release operation by the MFP Administrator, or elapse of a given time after the TOE's restart.
MFP Administrator	The lockout for the MFP Administrator is released by the lockout time set by the MFP Administrator, release operation by a MFP Supervisor, or elapse of a given time after the TOE's restart.

Table 23 List of Actions for Authentication Failure

Application note:

This SFR applies only to internal identification and authentication.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS contains a description of the actions in the case of authentication failure (types of authentication events, the number of unsuccessful authentication attempts, actions to be conducted), which is consistent with the definition of the SFR.

Operational Guidance:

The evaluator shall check to ensure that the administrator guidance describes the setting for actions to be taken in the case of authentication failure, if any are defined in the SFR.

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that the subsequent authentication attempts do not succeed by the behavior according to the actions defined in the SFR when unsuccessful authentication attempts reach the status defined in the SFR.
2. The evaluator shall check to ensure that authentication attempts succeed when conditions to re-enable authentication attempts are defined in the SFR and when the conditions are fulfilled.
3. The evaluator shall perform the tests 1 and 2 described above for all the targeted authentication methods when there are multiple Internal Authentication methods (e.g., password authentication, biometric authentication).
4. The evaluator shall perform the tests 1 and 2 described above for all interfaces when there are multiple interfaces (e.g., operation panel, Web interfaces) that implement authentication attempts.

6.6.2 FIA_ATD.1 User attribute definition

(for O.USER_AUTHORIZATION)

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: [***Login User Name, User Role, Available Functions List***].

Application note:

The list of security attributes should be the union of all attributes for each of the supported authentication methods.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS contains a description of the user security attributes that the TOE uses to implement the SFR, which is consistent with the definition of the SFR.

6.6.3 FIA_PMG_EXT.1 Extended: Password Management

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”***, [**“"", “'", “+", “,", “-", “.", “/", “:", “;", “<", “=", “>", “?", “[", “\", “]", “_", “`", “{", “|", “}", “~"**]];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

Application Note:

This SFR applies only to password-based single-factor Internal Authentication.

Assurance Activity:

Operational Guidance:

The evaluator shall examine the operational guidance to determine that it provides guidance to security administrators on the composition of passwords, and that it provides instructions on setting the minimum password length.

Test:

The evaluator shall also perform the following test:

The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.

6.6.4 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

(selected with FCS_IPSEC_EXT.1.4)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

Application Note:

The TOE must support pre-shared keys for use in the IPsec protocol. There are two types of pre-shared keys--text-based (which are required) and bit-based (which are optional)--supported by the TOE, as specified in the requirements below. The first type is referred to as “text-based pre-shared keys”, which refer to pre-shared keys that are entered by users as a string of characters from a standard character set, similar to a password. Such pre-shared keys must be conditioned so that the string of characters is transformed into a string of bits, which is then used as the key.

The second type is referred to as “bit-based pre-shared keys” (for lack of a standard term); this refers to keys that are either generated by the TSF on a command from the administrator, or input in "direct form" by an administrator. "Direct form" means that the input is used directly as the key, with no "conditioning" as was the case for text-based pre-shared keys. An example would be a string of hex digits that represent the bits that comprise the key.

The requirements below mandate that the TOE must support text-based pre-shared keys and optionally support bit-based pre-shared keys, although generation of the bit-based pre-shared keys may be done either by the TOE or in the Operational Environment.

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [[**1-32 characters**]];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [***SHA-256***] and be able to [***use no other pre-shared keys***].

Application Note:

For the length of the text-based pre-shared keys, a common length (22 characters) is required to help promote interoperability. If other lengths are supported they should be listed in the assignment; this assignment can also specify a range of values (e.g., "lengths from 5 to 55 characters") as well.

In the second selection for FIA_PSK_EXT.1.3, the ST author fills in the method by which the text string entered by the administrator is “conditioned” into the bit string used as the key. This can be done by using one of the specified hash functions, or some other method through the assignment statement. If “bit-based pre-shared keys” is selected, the ST author specifies whether the TSF merely accepts bit-based pre-shared keys, or is capable of generating them. If it generates them, the requirement specified that they must be generated using the RBG specified by the requirements. If the use of bit-based pre-shared keys is not supported, the ST author chooses “use no other pre-shared keys”.

Assurance Activity:

Operational Guidance:

The evaluator shall examine the operational guidance to determine that it provides guidance on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.

TSS:

The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22 characters are supported, and that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by IPsec, and that this conditioning is consistent with the first selection in the FIA_PSK_EXT.1.3 requirement. If the assignment is used to specify conditioning, the evaluator will confirm that the TSS describes this conditioning.

If “bit-based pre-shared keys” is selected, the evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall compose at least 15 pre-shared keys of 22 characters that cover all allowed characters in various combinations that conform to the operational guidance, and demonstrates that a successful protocol negotiation can be performed with each key.

2. [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.

3. [conditional]: If the TOE supports bit-based pre-shared keys but does not generate such keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

4. [conditional]: If the TOE supports bit-based pre-shared keys and does generate such keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

6.6.5 FIA_UAU.1 Timing of authentication

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 Refinement: The TSF shall allow [***the viewing of the list of user jobs, WIM Help, system status, counter and information of inquiries, and creation of fax reception and print jobs***] on behalf of the user to be performed before the user is authenticated.

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

Application note:

User authentication may be performed internally by the TOE or externally by an External IT Entity.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS describes all the identification and authentication mechanisms that the TOE provides (e.g., Internal Authentication and authentication by external servers).

The evaluator shall check to ensure that the TSS identifies all the interfaces to perform identification and authentication (e.g., identification and authentication from operation panel or via Web interfaces).

The evaluator shall check to ensure that the TSS describes the protocols (e.g., LDAP, Kerberos, OCSP) used in performing identification and authentication when the TOE exchanges identification and authentication with External Authentication servers.

The evaluator shall check to ensure that the TSS contains a description of the permitted actions before performing identification and authentication, which is consistent with the definition of the SFR.

Operational Guidance:

The evaluator shall check to ensure that the administrator guidance contains descriptions of identification and authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces), which are consistent with the ST (TSS).

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that identification and authentication succeeds, enabling the access to the TOE when using authorized data.

2. The evaluator shall check to ensure that identification and authentication fails, disabling the access to the TOE afterwards when using unauthorized data.

The evaluator shall perform the tests described above for each of the authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces).

6.6.6 FIA_UAU.7 Protected authentication feedback

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [***displaying dummy characters as authentication feedback on the Operation Panel and through WIM***] to the user while the authentication is in progress.

Application note:

FIA_UAU.7 applies only to authentication processes in which the User interacts with the TOE.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS contains a description of the authentication information feedback provided to users while the authentication is in progress, which is consistent with the definition of the SFR.

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that only the information defined in the SFR is provided for feedback by attempting identification and authentication.
2. The evaluator shall perform the test 1 described above for all the interfaces that the TOE provides (e.g., operation panel, identification and authentication via Web interface).

6.6.7 FIA_UID.1 Timing of identification

(for O.USER_I&A and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 Refinement: The TSF shall allow [***the viewing of the list of user jobs, WIM Help, system status, counter and information of inquiries, creation of fax reception jobs, and creation of print jobs***] on behalf of the user to be performed before the user is identified.

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

Application note:

User identification may be performed internally by the TOE or externally by an External IT Entity.

Assurance Activity:

It is covered by assurance activities for FIA_UAU.1.

6.6.8 FIA_USB.1 User-subject binding

(for O.USER_I&A)

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: [***login user name of Normal User, login user name of MFP Administrator, login user name of MFP Supervisor, available function list, and user role***].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***rules for the initial association of attributes listed in Table 24***].

Users	Subjects	User Security Attributes
Normal user	Normal user process	Login user name of Normal User User role Available functions list
MFP Administrator	MFP Administrator process	Login user name of MFP Administrator User role Available functions list (none for Administrators)
MFP Supervisor	MFP Supervisor process	Login user name of MFP Supervisor User role Available functions list (none for Administrators)

Table 24 Rules for Initial Association of Attributes

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [***none***].

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS contains a description of rules for associating security attributes with the users who succeed identification and authentication, which is consistent with the definition of the SFR.

Test:

The evaluator shall also perform the following test:

The evaluator shall check to ensure that security attributes defined in the SFR are associated with the users who succeed identification and authentication (it is ensured in the tests of FDP_ACF) for each role that the TOE supports (e.g., User and Administrator).

6.7 Class FMT: Security Management

6.7.1 FMT_MOF.1 Management of security functions behavior

(for O.ADMIN_ROLES)

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

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to [***determine the behavior of, enable, disable, modify the behavior of***] the functions [***listed in Table 26***] to U.ADMIN.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS contains a description of the management functions that the TOE provides as well as user roles that are permitted to manage the functions, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the TSS identifies interfaces to operate the management functions.

Operational Guidance:

The evaluator shall check to ensure that the administrator guidance describes the operation methods for users of the given roles defined in the SFR to operate the management functions.

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that users of the given roles defined in the SFR can operate the management functions in accordance with the operation methods specified in the administrator guidance.
2. The evaluator shall check to ensure that the operation results are appropriately reflected.
3. The evaluator shall check to ensure that U.NORMAL is not permitted to operate the management functions.

6.7.2 FMT_MSA.1 Management of security attributes

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 Refinement: The TSF shall enforce the User Data Access Control SFP to restrict the ability to [[***perform operations specified in Table 25***]] the security attributes [***listed in Table 25***] to [***the roles identified in Table 25***].

Security Attribute(s)	Operation(s)	User Role
Document data attribute	No operation permitted	None
Document user list [when document data attributes are (+PRT), (+SCN), (+CPY), and (+FAXOUT)]	No operation permitted	None
Document user list [when document data attribute is (+DSR)]	Query, modify	MFP Administrator, applicable Normal User who created the document data
Document user list [when document data attribute is (+FAXIN)]	Query, modify	MFP Administrator

Table 25 User Roles for Security Attributes

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR.

Operational Guidance:

The evaluator shall check to ensure that the administrator guidance contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the administrator guidance describes the timing of modified security attributes.

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to the security attributes in accordance with the operation methods specified in the administrator guidance.

2. The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.

3. The evaluator shall check to ensure that a user that is not part of an authorized role defined in the SFR is not permitted to perform operations on the security attributes.

6.7.3 FMT_MSA.3 Static attribute initialization

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 Refinement: The TSF shall enforce the User Data Access Control SFP to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

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

Application note:

FMT_MSA.3.2 applies only to security attributes whose default values can be overridden.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS describes mechanisms to generate security attributes which have properties of default values, which are defined in the SFR.

Test:

If U.ADMIN is selected, then testing of this SFR is performed in the tests of FDP_ACF.1.

6.7.4 FMT_MTD.1 Management of TSF data

(for O.ACCESS CONTROL)

Hierarchical to: No other components.

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

FMT_MTD.1.1 Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 26 and Table 27**.

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
Access control	Document user list for stored document types +DSR and +FAXIN	D.TSF.PROT	OperationPanel, Webbrowser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Default values of the document user list	D.TSF.PROT	OperationPanel, Webbrowser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Available function list	D.TSF.PROT	Operation Panel, Web browser	Modify	MFP Administrator
Audit function	Audit log	D.TSF.CONF	Web browser	Query, delete, export	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Audit transfer settings	D.TSF.PROT	Operation Panel, Web browser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Date settings (year/month/day), Time	D.TSF.PROT	Operation Panel, Web browser	Modify	MFP Administrator
Identification and Authentication	Minimum character number of password	D.TSF.PROT	Operation Panel	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Password complexity setting	D.TSF.PROT	Operation Panel	Modify	MFP Administrator
	Operation Panel auto logout time	D.TSF.PROT	Operation Panel	Modify	MFP Administrator
	WIM auto logout time	D.TSF.PROT	Web browser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Login user names of Normal Users	D.TSF.PROT	Operation Panel, Web browser	Create, modify, delete	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Login user name of MFP Supervisor	D.TSF.PROT	Operation Panel, Web browser	Modify	MFP Supervisor

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Login user name of MFP Administrator	D.TSF.PROT	Operation Panel, Web browser	Modify	MFP Administrator (Owner)

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Login passwords of Normal Users	D.TSF.CONF	Operation Panel, Web browser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Login password of MFP Supervisor	D.TSF.CONF	Operation Panel, Web browser	Modify	MFP Supervisor

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Login password of MFP Administrator	D.TSF.CONF	Operation Panel, Web browser	Modify	MFP Supervisor

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Login password of MFP Administrator	D.TSF.CONF	Operation Panel, Web browser	Modify	MFP Administrator (Owner)

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Login password of MFP Administrator	D.TSF.CONF	Operation Panel, Web browser	Modify	MFP Administrator
	Number of Attempts before Lockout	D.TSF.PROT	Web browser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Settings for Lockout Release Timer	D.TSF.PROT	Webbrowser	Modify	MFP Administrator
	Lockout time	D.TSF.PROT	Webbrowser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
PSTN Fax-Line Separation	Stored Reception File User	D.TSF.PROT	Operation Panel, Web browser	Modify	MFP Administrator
Stored Data Encryption	HDD cryptographic key	D.TSF.CONF	Operation Panel	Create, delete	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
Trusted communications	Network Settings	D.TSF.PROT	Operation Panel, Web browser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
	Device Certificate	D.TSF.CONF	OperationPanel, Webbrowser	Create, query, modify, delete	MFP Administrator
Trusted operations	TOE Software	D.TSF.PROT	Webbrowser	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
Multiple areas	TOE configuration data	D.TSF.PROT	Webbrowser	Export, import	MFP Administrator

Table 26 List of Administrator-only TSF Data, Operations, and Roles

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
Access control	Document user list for stored document type +DSR	D.TSF.PROT	Operation Panel, Web browser	Modify	MFP Administrator, Normal User (Owner) who stored the document
	Available function list	D.TSF.PROT	Web browser	Query	Normal User (Owner)

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
Identification and Authentication	Login passwords of Normal Users	D.TSF.CONF	Operation Panel, Web browser	Modify	Normal User (Owner)

Table 27 List of Additional TSF Data, Operations, and Roles

Note for Evaluators: *If a +PRT or +SCN document is stored in the document server, the act of storing is a +DSR job and the attribute of the stored document becomes +DSR.*

Assurance Activity:

Operational Guidance:

The evaluator shall check to ensure that the administrator guidance identifies the management operations and authorized roles consistent with the SFR.

The evaluator shall check to ensure that the administrator guidance describes how the assignment of roles is managed.

The evaluator shall check to ensure that the administrator guidance describes how security attributes are assigned and managed.

The evaluator shall check to ensure that the administrator guidance describes how the security-related rules (e.g., access control rules, timeout, number of consecutive logon failures,) are configured.

Test:

The evaluator shall perform the following tests:

- The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to TSF data in accordance with the operation methods specified in the administrator guidance.
- The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.
- The evaluator shall check to ensure that no users other than users of the given roles defined in the SFR can perform operations to TSF data.

6.7.5 FMT_SMF.1 Specification of Management Functions

(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [***management functions listed in Table 26***].

Application note:

Regarding "management functions provided by the TSF", the ST Author should consider management functions that support the security objectives of this protection profile.

The management functions should be restricted to the authorized identified role in FMT_MOF.1, FMT_MTD.1, FMT_MSA.1.

The ST Author may identify cases where a security objective is fulfilled without explicit manageability.

For example, the following management functions are categorized by security objectives:

For O.USER_AUTHORIZATION, O.USER_I&A, O.ADMIN_ROLES, O.ACCESS_CONTROL:

- *User management (e.g., add/change/remove local user)*
- *Role management (e.g., assign/deassign role relationship with user)*
- *Configuring identification and authentication (e.g., selecting between local and external I&A)*
- *Configuring authorization and access controls (e.g., access control lists for TOE resources)*

Configuring communication with External IT Entities

For O.UPDATE_VERIFICATION:

- *Configuring software updates*

For O.COMMS_PROTECTION:

- *Configuring network communications*
- *Configuring the system or network time source*

For O.AUDIT:

- *Configuring data transmission to audit server*
- *Configuring the system or network time source*
- *Configuring internal audit log storage*

For O.STORAGE_ENCRYPTION, O.KEY_MATERIAL:

- *Configuring and invoking encryption of Field-Replaceable Nonvolatile Storage Devices*

(Optional) For O.IMAGE_OVERWRITE, O.PURGE DATA:

- *Configuring and/or invoking image overwrite functions*
- *Configuring and/or invoking data purging functions*

Assurance Activity:

TSS:

The evaluator shall check the TSS to ensure that the management functions are consistent with the assignment in the SFR.

Operational Guidance:

The evaluator shall check the guidance documents to ensure that management functions are consistent with the assignment in the SFR, and that their operation is described.

6.7.6 FMT_SMR.1 Security roles

(for O.ACCESS_CONTROL, O.USER_AUTHORIZATION, and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 Refinement: The TSF shall maintain the roles U.ADMIN, U.NORMAL.

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

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS contains a description of security related roles that the TOE maintains, which is consistent with the definition of the SFR.

Test:

As for tests of this SFR, it is performed in the tests of FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.

6.8 Class FPR: Privacy

There are no class FPR requirements.

6.9 Class FPT: Protection of the TSF

6.9.1 FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

(for O.KEY_MATERIAL)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KYP_EXT.1.1 Refinement: The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

Assurance Activity:

KMD:

The evaluator shall examine the Key Management Description (KMD) for a description of the methods used to protect keys stored in nonvolatile memory.

The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in nonvolatile memory.

6.9.2 FPT_SKP_EXT.1 Extended: Protection of TSF Data

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Application Note:

The intent of the requirement is that an administrator is unable to read or view the identified keys (stored or ephemeral) through "normal" interfaces. While it is understood that the administrator could directly read memory to view these keys, doing so is not a trivial task and may require substantial work on the part of an administrator. Since the administrator is considered a trusted agent, it is assumed they would not engage in such an activity.

Assurance Activity:

TSS:

The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

6.9.3 FPT_STM.1 Reliable time stamps

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application note:

The time may be set by a trusted administrator or by a network service (e.g., NTP) from a trusted External IT Entity.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS describes mechanisms that provide reliable time stamps.

Operational Guidance:

The evaluator shall check to ensure that the guidance describes the method of setting the time.

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that the time is correctly set up in accordance with the guidance or external network services (e.g., NTP).

2. The evaluator shall check to ensure that the time stamps are appropriately provided.

6.9.4 FPT_TST_EXT.1 Extended: TSF testing

(for O.TSF_SELF_TEST)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

Application note:

Power-on self-tests may take place before the TSF is operational, in which case this SFR can be satisfied by verifying the TSF image by digital signature as specified in FCS_COP.1(b), or by hash specified in FCS_COP.1(c).

Assurance Activity:

TSS:

The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

Operational Guidance:

The evaluator shall also ensure that the operational guidance describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.

6.9.5 FPT_TUD_EXT.1 Extended: Trusted Update

(for O.UPDATE_VERIFICATION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), or
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)].

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [***no other functions***] prior to installing those updates.

Application note:

FPT_TUD_EXT.1.2 may be interpreted to allow an administrator to "pre-authorize" automatic updates, provided that they are verified according to FPT_TUD_EXT.1.3.

The digital signature mechanism is specified in FCS_COP.1(b). The published hash is generated by one of the functions specified in FCS_COP.1(c). It is acceptable to implement both mechanisms.

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software for update when performing updates, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.

Operational Guidance:

The evaluator shall check to ensure that the administrator guidance contains descriptions of the operation methods to obtain the TOE version as well as the operation methods to start update processing, which are consistent with the description of the TSS.

Test:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure the current version of the TOE can be appropriately obtained by means of the operation methods specified by the administrator guidance.

2. The evaluator shall check to ensure that the verification of the data for updates of the TOE succeeds using authorized data for updates by means of the operation methods specified by the administrator guidance.

3. The evaluator shall check to ensure that only administrators can implement the application for updates using authorized data for updates.

4. The evaluator shall check to ensure that the updates are correctly performed by obtaining the current version of the TOE after the normal updates finish.

5. The evaluator shall check to ensure that the verification of the data for updates of the TOE fails using unauthorized data for updates by means of the operation methods specified by the administrator guidance. (The evaluator shall also check those cases where hash verification mechanism and digital signature verification mechanism fail.)

6.10 Class FRU: Resource Utilization

There are no class FRU requirements.

6.11 Class FTA: TOE Access

6.11.1 FTA_SSL.3 TSF-initiated termination

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [***lapse of Operation Panel auto logout time, lapse of WIM auto logout time, completion of document data reception from the printer driver, and completion of document data reception from the fax driver***].

Assurance Activity:

TSS:

The evaluator shall check to ensure that the TSS describes the types of user sessions to be terminated (e.g., user sessions via operation panel or Web interfaces) after a specified period of user inactivity.

Operational Guidance:

The evaluator shall check to ensure that the guidance describes the default time interval and, if it is settable, the method of setting the time intervals until the termination of the session.

Test:

The evaluator shall also perform the following tests:

1. If it is settable, the evaluator shall check to ensure that the time until the termination of the session can be set up by the method of setting specified in the administrator guidance.
2. The evaluator shall check to ensure that the session terminates after the specified time interval.
3. The evaluator shall perform the tests 1 and 2 described above for all the user sessions identified in the TSS.

6.12 Class FTP: Trusted Paths/Channels

6.12.1 FTP_ITC.1[IPsec] Inter-TSF trusted channel

(for O.COMMS_PROTECTION, O.AUDIT)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_ITC.1.1[IPsec] Refinement: The TSF shall **use [*IPsec*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [*LDAP, FTP, NTP, syslog, and SMTP*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2[IPsec] Refinement: The TSF shall permit **the TSF, or the authorized IT entities,** to initiate communication via the trusted channel

FTP_ITC.1.3[IPsec] Refinement: The TSF shall initiate communication via the trusted channel for [***communication via the LAN of document data, function data, protected data, and confidential data***].

Application note:

The assignment in FTP_ITC.1.3 should address the confidentiality and/or integrity requirements for communication of User and TSF Data between the TOE and another IT entity. FTP_TRP.1 is intended to be used for interactive communication between the TOE and remote users.

The intent of the above requirement is to use a cryptographic protocol to protect external communications with authorized IT entities that the TOE interacts with to perform its functions. Protection (by one of the listed protocols) is required at least for communications with the server that collects the audit information. If it communicates with an authentication server (e.g., RADIUS), then the ST author chooses "authentication server" in FTP_ITC.1.1 and this connection must be protected by one of the listed protocols. If other authorized IT entities (e.g., NTP server) are protected, the ST author makes the appropriate assignments (for those entities) and selections (for the protocols that are used to protect those connections). After the ST author has made the selections, they are to select the detailed requirements in Appendix D.2 of HCD PP v1.0 corresponding to their protocol selection to put in the ST. To summarize, the connection to an external audit collection server is required to be protected by one of the listed protocols. If an External Authentication server is supported, then it is required to protect that connection with one of the listed protocols. For any other external server, external communications are not required to be protected, but if protection is claimed, then it must be protected with one of the identified protocols.

While there are no requirements on the party initiating the communication, the ST author lists in the assignment for FTP_ITC.1.3 the services for which the TOE can initiate the communication with the authorized IT entity.

The requirement implies that not only are communications protected when they are initially established, but also on resumption after an outage. It may be the case that some part of the TOE setup involves manually setting up tunnels to protect other communication, and if after an outage the TOE attempts to re-establish the communication automatically with (the necessary) manual intervention, there may be a window created where an attacker might be able to gain critical information or compromise a connection.

Assurance Activity:

TSS:

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Test:

The evaluator shall also perform the following tests:

1. The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

2. For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.

3. The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext.

4. The evaluator shall ensure, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

Further assurance activities are associated with the specific protocols.

6.12.2 FTP_TRP.1(a) Trusted path (for Administrators)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(a) Refinement: The TSF shall **use [*TLS/HTTPS*] to** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

FTP_TRP.1.2(a) Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path

FTP_TRP.1.3(a) Refinement: The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

Application Note:

This requirement ensures that authorized remote administrators initiate all communication with the TOE via a trusted path, and that all communications with the TOE by remote administrators is performed over this path. The data passed in this trusted communication path are encrypted as defined the protocol chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the TOE, and then ensures the detailed requirements in Appendix D.2 of HCD PP v1.0 corresponding to their selection are copied to the ST if not already present.

Assurance Activity:

TSS:

The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.

Operational Guidance:

The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.

Test:

The evaluator shall also perform the following tests:

1. The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
2. For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.
3. The evaluator shall ensure, for each method of remote administration, the channel data are not sent in plaintext.

Further assurance activities are associated with the specific protocols.

6.12.3 FTP_TRP.1(b) Trusted path (for Non-administrators)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(b) Refinement: The TSF shall **use [*TLS/HTTPS*] to** provide **a trusted** communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

FTP_TRP.1.2(b) Refinement: The TSF shall permit [***the TSF, remote users***] to initiate communication via the trusted path

FTP_TRP.1.3(b) Refinement: The TSF shall require the use of the trusted path for **initial user authentication and all remote user actions**.

Application Note:

This requirement ensures that authorized remote users initiate all communication with the TOE via a trusted path, and that all communications with the TOE by remote users is performed over this path. The data passed in this trusted communication path are encrypted as defined the protocol chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the TOE, and then ensures the detailed requirements in Appendix D.2 of HCD PP v1.0 corresponding to their selection are copied to the ST if not already present.

Assurance Activity:

TSS:

The evaluator shall examine the TSS to determine that the methods of remote TOE access for non-administrative users are indicated, along with how those communications are protected.

The evaluator shall also confirm that all protocols listed in the TSS in support of remote TOE access are consistent with those specified in the requirement, and are included in the requirements in the ST.

Operational Guidance:

The evaluator shall confirm that the operational guidance contains instructions for establishing the remote user sessions for each supported method.

Test:

The evaluator shall also perform the following tests:

1. The evaluators shall ensure that communications using each specified (in the operational guidance) remote user access method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
2. For each method of remote access supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote user session without invoking the trusted path.
3. The evaluator shall ensure, for each method of remote user access, the channel data are not sent in plaintext.

Further assurance activities are associated with the specific protocols.

7 Security Assurance Requirements (APE_REQ)

This section describes Security Assurance Requirements (SARs) in the evaluations performed by the evaluator based on the CC. These are all common to the Security Functional Requirements (SFRs) in Section 5. Assurance activities to the individual SFRs are described in their respective sections.

After the ST has been approved for evaluation, the Common Criteria IT Security Evaluation Facilities (ITSEF) will obtain the TOE, necessary IT environment, and the TOE guidance documents. The assurance activities described in the ST (which will be refined by the ITSEF to be TOE-specific, either within the ST or in a separate document) will be performed by the ITSEF. Although these activities were performed under the control of the ITSEF, it is allowed to obtain supports from the developer as well. The results of these activities will be documented and presented (along with the administrative guidance used) for validation.

For each assurance family, “Developer Notes” are provided on the developer action elements to clarify what, if any, additional documentation/activity needs to be provided by the developer.

The TOE security assurance requirements specified in Table 28 provides evaluative activities required to address the threats identified in Section 0 of this PP.

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

Table 28 TOE Security Assurance Requirements

7.1 Class ASE: Security Target evaluation

The ST is evaluated as per ASE activities defined in the CEM. In addition, there may be Assurance Activities specified within the PP that call necessary descriptions to be included in the TSS that are specific to the TOE technology type.

Appendix E of HCD PP v1.0 provides a description of the information expected to be provided regarding the quality of entropy in the random bit generator.

Given the criticality of the key management scheme, this PP requires the developer to provide a detailed description of their key management implementation. This information can be submitted as an appendix to the ST and marked proprietary, as this level of detailed information is not expected to be made publicly available. See Appendix F of HCD PP v1.0 for details on the expectation of the developer’s Key Management Description.

7.2 Class ADV: Development

For TOEs conforming to this PP, the information about the TOE is contained in the guidance documentation available to the end user as well as the TOE Summary Specification (TSS) portion of the ST. While it is not required that the TOE developer write the TSS, the TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The Assurance Activities contained in Section 5 should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

7.2.1 ADV_FSP.1 Basic functional specification

The functional specification describes the TSF Interfaces (TSFIs). At the level of assurance provided by this PP, it is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly invokable by TOE users (to include administrative users), at this assurance level there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. The activities for this family for this PP should focus on understanding the interfaces presented in the TSS in response to the functional requirements, and the interfaces presented in the AGD documentation. No additional "functional specification" document should be necessary to satisfy the assurance activities specified. The interfaces that need to be evaluated are characterized through the information needed to perform the assurance activities listed, rather than as an independent, abstract list.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Developer Note: The developer shall provide appropriate TSS description and guidance documents as the functional specification. The TSS description identifies TSFIs associated with each SFR in order to confirm the validity of interface design. The developer is required to provide a description at least at a confirmable level in which TSS description and contents of guidance documents are consistent with each other. In case of insufficient information for evaluation in TSS description and contents of guidance documents, additional documentation can be requested. For the SFRs that cannot be directly operated/confirmed from external interfaces, the developer may be requested to provide additional information.

Content and presentation elements:

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Assurance activity:

TSS:

The evaluator shall confirm identifiable external interfaces from guidance documents and examine that TSS description identifies all the interfaces required for realizing SFR.

The evaluator shall confirm identification information of the TSFI associated with the SFR described in the TSS and confirm the consistency with the description related to each interface.

The evaluator shall check to ensure that the SFR defined in the ST is appropriately realized, based on identification information of the TSFI in the TSS description as well as on the information of purposes, methods of use, and parameters for each TSFI in the guidance documents

The assurance activities specific to each SFR are described in Section 5 and the evaluator shall perform evaluations by adding to this assurance component.

7.3 Class AGD: Guidance Documents

The guidance documents will be provided with the developer's security target. Guidance must include a description of how the administrator verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by an administrator.

Guidance must be provided for every Operational Environment that the product supports as claimed in the ST. This guidance includes

- instructions to successfully install the TOE in that environment; and
- instructions to manage the security of the TOE as a product and as a component of the larger Operational environment.

Guidance pertaining to particular security functionality is also provided; requirements on such guidance are contained in the assurance activities specified in Section 5.

7.3.1 AGD_OPE.1 Operational user guidance

Developer action elements:

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

Developer Note: The developer should review the assurance activities for this component to ascertain the specifics of the guidance that the evaluators will be checking for. This will provide the necessary information for the preparation of acceptable guidance.

Content and presentation elements:

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

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

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

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

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

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

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

Evaluator action elements:

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

Assurance activity:

Operational Guidance:

The contents of operational guidance are confirmed by the assurance activities in Section 5 and the TOE evaluation in accordance with the CEM.

The evaluator shall check to ensure that the following guidance is provided:

Procedures for administrators to confirm that the TOE returns to its evaluation configuration after the transition from the maintenance mode to the normal Operational Environment.

Application note:

During evaluation, the TOE returns to its evaluation configuration. In the field, the TOE may return to the configuration that was in force prior to entering maintenance mode.

7.3.2 AGD_PRE.1 Preparative procedures

Developer action elements:

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

Developer Note: As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to preparative procedures.

Content and presentation elements:

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

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

Evaluator action elements:

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

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

7.4 Class ALC: Life-cycle Support

At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation at this assurance level.

7.4.1 ALC_CMC.1 Labelling of the TOE

This component is targeted at identifying the TOE such that it can be distinguished from other products or version from the same vendor and can be easily specified when being procured by an end user.

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labeled with its unique reference.

Evaluator action elements:

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

Assurance activity:

Operational Guidance:

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. The evaluator shall ensure that this identifier is sufficient for an acquisition entity to use in procuring the TOE (including the appropriate administrative guidance) as specified in the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

7.4.2 ALC_CMS.1 TOE CM coverage

Given the scope of the TOE and its associated evaluation evidence requirements, this component's assurance activities are covered by the assurance activities listed for ALC_CMC.1.

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

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

Assurance activity:

Operational Guidance:

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

7.5 Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces as constrained by the availability of design information presented in the TSS. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

7.5.1 ATE_IND.1 Independent testing - Conformance

Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operation) documentation provided. The focus of the testing is to confirm that the requirements specified in Section 5 are being met, although some additional testing is specified for SARs in Section 7. The Assurance Activities identify the minimum testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the product models combinations that are claiming conformance to this PP.

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Assurance activity:

Test:

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.

The Test Plan identifies the product models to be tested, and for those product models not included in the test plan but included in the ST, the test plan provides a justification for not testing the models. This justification must address the differences between the tested models and the untested models, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. In case the ST describes multiple models (product names) in particular, the evaluator shall consider the differences in language specification as well as the influences, in which functions except security functions such as a printing function, may affect security functions when creating this justification. If all product models claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each product model to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each model either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE.

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include the goal of the particular procedure, the test steps used to achieve the goal, and the expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a “fail” and “pass” result (and the supporting details), and not just the “pass” result.

7.6 Class AVA: Vulnerability Assessment

For the first generation of this protection profile, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, evaluators will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing tools and for the development of future protection profiles.

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing basic attack potential.

Assurance activity:

Test:

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in printing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report.

For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability.

For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

7.7 Security Assurance Requirements rationale

The rationale for choosing these security assurance requirements is that they define a minimum security baseline that is based on the anticipated threat level of the attacker, the security of the Operational Environment in which the TOE is deployed, and the relative value of the TOE itself. The assurance activities throughout the PP are used to provide tailored guidance on the specific expectations for completing the security assurance requirements.

8 TOE Summary Specification (ASE_TSS)

This section provides a summary specification for each TOE security function. The security functions are described for each corresponding security functional requirement.

8.1 Identification and Authentication, Use-of-Feature Authorization (TSF_FIA)

The Identification and Authentication Function verifies that users are authorized to operate the TOE and access the TOE's protected information.

8.1.1 FIA_UAU.1 and FIA_UID.1

The TOE identifies and authenticates a user by checking credentials entered by the user.

User credentials are checked against user authentication data stored in the TOE, or against an external network authentication service (LDAP).

Users can be identified and authenticated through several interfaces:

- Locally, manually entering a username and password using the Operation Panel.
- Remotely, manually entering credentials using a client computer's web browser to access the Web Image Monitor (WIM).
- Remotely, using a client computer's print driver or fax driver which has been configured to submit credentials on behalf of the user.

When users are identified and authenticated via remote interfaces, their credentials are protected in transit using trusted paths.

Certain functions may be performed without user identification and authentication:

- Viewing user job lists, WIM Help, system status, the counter and information of inquiries, repair request notifications, and eco information of system.
- Creation of fax reception jobs.
- Creation of print jobs.

8.1.2 FIA_PMG_EXT.1

For authentication within the TOE, login passwords for users can be registered only if these passwords meet the conditions specified by the selections in FIA_PMG_EXT.1.

8.1.3 FIA_UAU.7

When users enter their passwords using the Operation Panel or using WIM from the client computer, the TOE displays a sequence of dummy characters whose length is the same as that of the entered password.

8.1.4 FIA_AFL.1

The TOE counts consecutive login failures for a given login name and locks out that user until the lockout is released. The TOE can lock out any user.

Authentication events that are subject to lockout are listed with the SFR FIA_AFL.1.1 in Table 22, and the actions to release lockout are listed with the SFR FIA_AFL.1.2 in Table 23.

8.1.5 FIA_USB.1 and FIA_ATD.1

After successful identification and authentication, users are authorized to perform functions according to the user role (Normal User, MFP Administrator, or MFP Supervisor) that is associated with their user registration. The user security attributes associated with each role are:

- Login User Name
- User Role
- Available Functions List

The User Role assigned to the user at login is maintained until the user is logged out. If user identification and authentication fails, use of the TOE is denied according to FIA_UAU.1 and FIA_UID.1.

An Available Functions List is associated with each Normal User. It lists the basic hardcopy functions that the user is permitted to perform.

8.1.6 FTA_SSL.3

User sessions are terminated according to the type of user session:

Operation Panel: the user is logged out of the TOE when inactivity reaches the Operation Panel auto logout time (settable from 10 to 999 seconds).

WIM: the user is logged out of the TOE when inactivity reaches the WIM auto logout time (settable from 3 to 60 minutes).

Printer driver: the user is logged out of the TOE immediately after receiving the print data from the printer driver.

Fax driver: the user is logged out of the TOE immediately after receiving the transmission information from the fax driver.

Network login: the user is logged out of the TOE when inactivity reaches the Operation Panel auto logout time (settable from 10 to 999 seconds).

8.2 Access Control (TSF_FDP)

The Access Control Function permits authorized TOE users to operate document data and user jobs in accordance with the privileges allowed by their user role.

8.2.1 FDP_ACC.1 and FDP_ACF.1

The TOE controls user operations for document data and user jobs as specified in Table 20 and Table 21.

8.2.1.1 Access control rule on document data

The TOE provides users with the ability to perform operations on document data that are stored in the TOE.

Normal Users are permitted to operate on document data if the ID of the user corresponds to the Document User List for that document (i.e., the user is the “Job Owner”). A Normal User is not permitted to operate on document data for which it is not the Job Owner. The privileges that allow users to edit the Document User List are described in section 8.5.

As described in Table 29, a Normal User who is a Job Owner may print, download to client computers, send by fax, send by e-mail as attachments, and delete stored documents, using the Operation Panel or a web browser.

The TOE allows only the Job Owner to view and delete the document data handled as a user job while Copy Function, Printer Function, Scanner Function, Fax Function, or Document Server Function is being used.

While no interface to change job owners is provided, an interface to cancel user jobs is provided. If a user job is cancelled, any document the cancelled job operates will be deleted.

Function	User interface	Type of document	Operations permitted for authorized users
Printer	Operation Panel	+PRT	Print Delete
Printer	Web browser	+PRT	Print Delete
Scanner	Operation Panel	+SCN	E-mail transmission
Fax	Operation Panel	+FAXIN	Print Delete
Fax	Web browser	+FAXIN	Print Download Delete (Operations above are permitted only if Normal Users are authorized to use Document Server Function)
Document Server	Operation Panel	+DSR	Print Delete
Document Server	Operation Panel	+FAXOUT	Print Delete
Document Server	Web browser	+DSR	Print Delete
Document Server	Web browser	+FAXOUT	Fax transmission Download Print Delete (Fax transmission is permitted for Normal Users who are authorized to use Fax Function)

Table 29 Stored Documents Access Control Rules for Normal Users

MFP Administrators are not permitted to print, download, or send stored documents. MFP Administrators may delete stored documents, using the Operation Panel, web browser, or indirectly by cancelling a job.

The MFP Supervisor is not permitted to perform any document operations.

8.2.1.2 Access control rule on user jobs

The TOE displays on the Operation Panel a menu to cancel a user job only if the user who logs in from the Operation Panel is a Job Owner or MFP Administrator and a cancellation of a user job is attempted by the Job Owner or an MFP Administrator. Other users are not allowed to operate user jobs.

When a user job is cancelled, any documents operated by the cancelled job will be deleted. However, if the document data operated by the cancelled user job is a stored document, the data will not be deleted and remain stored in the TOE.

8.3 Stored Data Encryption (TSF_FCS)

The Stored Data Protection Function encrypts data on the HDD and in NVRAM.

8.3.1 FCS_KYC_EXT.1, FPT_KYP_EXT.1, and FCS_COP.1(f)

The keychain for encrypting field-replaceable non-volatile storage devices begins with a common Root Encryption Key (REK). The plaintext REK is stored in a hardware security module, Ic Key.

The REK is used to encrypt and decrypt a Key Encryption Key (KEK). The KEK is used to encrypt and decrypt Device Encryption Keys (DEKs) for the HDD and NVRAM. All such operations use 256-bit AES keys to protect 256-bit AES data encryption on the target devices.

Key	En/decrypts	Algorithm	Length	SFR	Validation
Root Encryption Key (REK)	Key Encryption Key	AES CBC	256	FCS_COP.1(f)	CAVP AES #5364
Key Encryption Key (KEK)	HDD Key NVRAM Key DevCert Key	AES CBC	256	FCS_COP.1(f)	CAVP AES #5364

Table 30 Keychain encryption

Additional details about the keychain and device encryption are provided in the Key Management Description.

8.3.2 FCS_CKM.1(b)[DIM], FCS_CKM.1(b)[DAR], and FCS_RBG_EXT.1

The REK, KEK, HDD Key, and NVRAM Key, are created using a software-based DRBG that has been seeded by a third-party hardware-based TRNG and DRBG.

RNG	Method	Standard	Validation
Hardware TRNG	True RNG + DRBG	AIS31 Class 2	CC #ANSSI-CC-2012/84
Software DRBG	Hash_DRBG_SHA256	SP 800-90A	CAVP HMAC #3552 CAVP SHS #4306 CAVP DRBG #2075

Table 31 Random Number Sources

Additional details about key creation, the TRNG, and the DRBG, are provided in the Key Management Description and Entropy Description documents.

8.3.3 FCS_CKM.4 and FCS_CKM_EXT.4

Key destruction details are provided in the Key Management Description.

8.3.4 FDP_DSK_EXT.1 and FCS_COP.1(d)

Two field-replaceable non-volatile storage devices employ encryption: the HDD, and NVRAM.

The entire HDD is encrypted. All HDD data is encrypted with AES 256 CBC encryption by a hardware component, Ic Ctrl. HDD encryption is enabled and initialized in the evaluated configuration, as described in the Notes for Administrators guidance document.

Partition 3 of NVRAM is encrypted a software component, LPUX NVRAM Encryption Driver, with AES 256-bit encryption. It is enabled and initialized during manufacturing and cannot be disabled. Other partitions of NVRAM do not contain confidential User or TSF Data.

The following algorithms are used:

Function	SFR	Algorithm	Validation
HDD encryption	FCS_COP.1(d)	AES 256 CBC	AES #3921
NVRAM encryption	FCS_COP.1(d)	AES 256 CBC	AES #4560

Table 32 Storage encryption cryptographic functions

Keychain, key management, and other details are provided in the Key Management Description.

8.4 Trusted Communications (TSF_FTP)

The Trusted Communications Function provides trusted paths for communications between the TOE and remote users / external IT entities.

8.4.1 FTP_TRP.1 (a), FTP_TRP.1 (b), FCS_HTTPS_EXT.1, and FCS_TLS_EXT.1

The TOE employs TLS 1.2 to protect communications between the TOE and remote users' client computers (print drivers, fax drivers, and WIM HTTPS sessions).

The TOE supports these ciphersuites:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

8.4.2 FCS_CKM.1 (a), FCS_RBG_EXT.1, FCS_COP.1 (a), FCS_COP.1(b)[DIM], FCS_COP.1(c) , and FCS_COP.1(g)

The TOE generates a self-signed Device Certificate according to FCS_CKM.1(a). Administrators may import a Device Certificate that is generated outside of the TOE.

To establish a session key for TLS communications, the TOE employs a Diffie-Hellman-based key establishment scheme conforming to NIST SP 800-56A, and a Hash DRBG. The session key is used to encrypt communications with AES 128 or AES 256 CBC:

Function	SFR	Algorithm	Validation

Key establishment	FCS_CKM.1(a)
	FCS_COP.1(b)[DIM]
	FCS_COP.1(c)
		DSA KeyGen 186-4
		KAS-FFC
			DSA #1385
			Comp #1826

Random number generation	FCS_RBG_EXT.1	Hash_DRBG_SHA256	HMAC #3552 DRBG #2075 SHS #4306
Encryption / decryption	FCS_COP.1(a)	AES 128 CBC AES 256 CBC	AES #5364

Table 33 TLS/HTTPS cryptographic functions

Per IG D.8, Scenario 6 – non-approved primitive only, a partial DH key agreement scheme is allowed in an approved FIPS mode of operation. No keys are established into the module using DH. Key establishment methodology provides 112 bits of encryption strength.

8.4.3 FPT_SKP_EXT.1, FCS_CKM.4 and FCS_CKM_EXT.4

All pre-shared keys, symmetric keys, and private keys are protected in storage and are not accessible to any user through TOE interfaces. A root encryption key is securely stored in IcKey (a Trusted Platform Module). No other plaintext keys are stored in non-volatile storage. The root encryption key is used to decrypt a key encryption key which is used to decrypt symmetric keys for encrypted storage and the Device Certificate. The IPsec PSK is stored in an encrypted partition of NVRAM. Key destruction is described in the Key Management Description.

8.4.4 FCS_ITC.1[IPsec], FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, and FCS_COP.1(g)

The TOE employs IPsec to protect communications between the TOE and external IT entities in the operational environment. In the evaluated configuration, it is used for communications with LDAP, syslog, NTP, SMTP, and FTP servers.

IPsec is operated in transport mode, as set by the administrator.

IPsec supports automatic key exchange or automatic key exchange by IKEv1.

In Phase 1, peer authentication supports two types of authentication: pre-shared key authentication and digital certificate authentication.

The pre-shared key can be any length from 1 to 32 characters, and composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

An administrator can select whether to use main mode or aggressive mode. In the evaluated configuration, only main mode is used.

In IKEv1, supported DH groups are 1,2 and 14. The value set by the administrator is used.

IKEv1 key lifetimes can be set by the administrator, from 300 seconds to 172,800 seconds. In the evaluated configuration, Phase 1 key lifetime is set to 86,400 seconds (24 hours), and Phase 2 lifetime is set to 28,800 seconds (8 hours).

As an SPD, four individual entries and one default entry can be set by an administrator. Beginning with the first entry the packet is compared, and if it matches the entry, IPsec communication is performed. If the packet does not match the first entry, subsequent entries are tested until there is a match. If no entries match the packet, the default entry will be compared, and if it does not match, the packet is discarded.

The TOE supports these cryptographic algorithms:

Function	SFR	Algorithm	Validation

IKEv1	FCS_CKM.1(a)
	FCS_COP.1(a)
	FCS_COP.1(b)[DIM]
	FCS_COP.1(g)
	FCS_RBG_EXT.1
		RSA 186-4
		AES 128 CBC
		AES 256 CBCHMAC-SHA256
		HMAC-SHA384
		HMAC-SHA512
			RSA #2869
			AES #5364
			HMAC #3552
			SHS #4306

ESP	FCS_COP.1(a)
	FCS_COP.1(b)[DIM]
	FCS_COP.1(g)
	FCS_RBG_EXT.1
		AES 128 CBC
		AES 256 CBC
		HMAC-SHA256
		HMAC-SHA384
		HMAC-SHA512
			AES #5315
			HMAC #3515
			SHS #4269

Table 34 IPsec cryptographic functions

8.5 Administrative Roles (TSF_FMT)

The Security Management Function consists of functions to 1) control operations for TSF data, 2) maintain user roles assigned to Normal Users, MFP Administrator, or MFP Supervisor to operate the Security Management Function, and 3) set appropriate default values to security attributes, all of which accord with user role privileges or user privileges that are assigned to Normal Users, MFP Administrator, or MFP Supervisor.

8.5.1 FMT_SMR.1

The TOE maintains U.NORMAL and U.ADMIN roles as described in Table 6. Normal Users are permitted to use document processing functions TOE and access their own data. Administrators do not initiate document processing jobs: the sub-role MFP Administrator can manage Normal Users' jobs and data and configures the TOE, and the sub-role MFP Supervisor sets MFP Administrators' passwords.

8.5.2 FMT_SMF.1, FMT_MOF.1, and FMT_MTD.1

The TOE provides management functions listed in Table 26 and the TOE restricts operations on TSF Data according to the rules described in Table 26.

8.5.3 FMT_MSA.1 and FMT_MSA.3

The TOE restricts operations on security attributes according to the rules described in Table 25.

The TOE sets default values for objects/subjects according to the rules described in Table 35 when those objects/subjects are generated.

Objects	Security attributes	Default values
Document data	Document data attribute	**+PRT**: Documents printed from the client computer with direct print, locked print, hold print, and sample print. **+SCN**: Documents sent by e-mail as attachments from the MFP. **+CPY**: Documents copied using the MFP. **+FAXOUT**: Documents sent by fax from the MFP or client computer. **+FAXIN**: Documents received from a telephone line. **+DSR**: Documents stored in the TOE by using Copy Function, Scanner Function, Document Server Function and Fax Data Storage Function. Documents printed using Document Server printing or stored print from the client computer.
Document data (stored document types are Document Server document, scanner document and fax transmission document)	Document user list	Default values of a document user list assigned to a Normal User who created the document data.
Document data (stored document type is printer document)	Document user list	Login user name of a Normal User who stored the document data.
Document data (stored document type is fax reception document)	Document user list	Login user name of a Normal User included in the Stored Reception File User list.

Objects	Security attributes	Default values
User jobs	Login user name of Normal User	Login user name of a Normal User who newly creates a user job.
Each MFP application (Copy Function, Printer Function, Scanner Function, Document Server Function and Fax Function)	Function type	The values specified for each function type is as follows: For Copy Function, values to identify Copy Function. For Document Server Function, values to identify Document Server Function. For Printer Function, values to identify Printer Function. For Scanner Function, values to identify Scanner Function. For Fax Function, values to identify Fax Function.

Table 35 List of Static Initialization for Security Attributes of Document Access Control SFP

The attributes which may be overridden are restricted to U.ADMIN, as described in Table 36

Object	Attribute	Role that can override default value
Document data when attribute is +DSR or +FAXIN	Document user list	MFP Administrator

Table 36 Roles allowed to override default values

8.6 Audit Function (TSF_FAU)

The Audit Function is to generate the audit log of TOE use and security-relevant events (hereafter, "audit events"). This function provides the recorded audit log in a legible fashion for users to audit (audit log review). The recorded audit log can be accessed and deleted only by the MFP Administrator.

8.6.1 FAU_GEN.1 and FAU_GEN.2

The TOE records an audit log of events listed in Table 37.

Auditable event requirements	Auditable events satisfied
Start-up and shutdown of the audit functions	Start-up of the Audit Function
	Shutdown of the Audit Function
Job completion	Printing via networks
	LAN Fax via networks
	Scanning documents
	Copying documents
	Receiving incoming faxes
	Creating document data (storing)
	Reading document data (print, download, fax transmission)
	Deleting document data
Unsuccessful User authentication, Unsuccessful User identification	Failure of login operations
Use of management functions	Use of functions identified in FMT_SMF.1
Modification to the group of Users that are part of a role	Modification of MFP Administrator roles
Changes to the time	Date settings (year/month/day), time settings (hour/minute)
Failure to establish session	Failure of communication with the audit server
	Failure of communication with the authentication server
	Failure of communication with the FTP server
	Failure of communication with the NTP server
	Failure of communication with print driver
	Failure of communication with fax driver
	Failure of communication with WIM

Table 37 List of Audit Events

Audit log entries record the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Additionally Job Completion events record the type of job, and Failure to Establish Session events record the reason for such failure.

The complete list of audit log items, attributes, and content, can be found in the guidance documentation in “Logs That Can Be Managed Using Web Image Monitor”.

8.6.2 FAU_STG.1, FAU_STG_EXT.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2

The TOE stores audit log data in a dedicated storage area of the HDD. Audit records are buffered in that storage area before transfer to an audit server or retrieval by an Administrator.

Audit data is Confidential TSF Data. Audit records can be retrieved by:

- An Administrator, using the WIM to initiate transfer of audit records.
- An Administrator-configured transfer over a trusted channel (IPSec) to the Audit Server in the Operational Environment.

Administrator-configuration can initiate transfers on a time schedule, when the log storage area is reaching its capacity, or whenever events are logged.

There are three types of audit logs: Job logs, Access logs, and Ecology logs. The maximum number of records that can be stored in the TOE are:

- Job log: 4,000 records
- Access log: 12,000 records
- Ecology log: 4,000 records

If a maximum is reached, records are overwritten by new records according to the following order:

1. Records that have been transferred and records that are not set for transfer, oldest first
2. Records for completed events that are set for transfer but not yet transferred, oldest first
3. Records that are in process, oldest first

8.6.3 FPT_STM.1

The date (year/month/day) and time (hour/minute/second) the TOE records for the audit log are derived from the system clock of the TOE. The system clock is also used for other time-related functions, including user lockout timing, idle session timeouts, and SA lifetimes.

The system clock may be set locally or configured to use a network time server. Only an MFP Administrator can configure the system clock.

8.7 Trusted Operation (TSF_FPT)

The Software Verification Function is to verify the integrity of the executable codes of the MFP Control Software, FCU Control Software and Operation Panel Control Software, and confirm that these codes can be trusted.

8.7.1 FPT_TST_EXT.1, FCS_COP.1(b), FCS_COP.1(c)[L1], and FCS_COP.1(c)[L2]

During start-up, the TOE verifies the integrity of the TSF through a series of integrity tests, using the cryptographic functions listed below.

Integrity test	SFR	Algorithm	Validation

TPM	FCS_COP.1(c)[L1]	SHA-1	SHS #C715
MFP Control Software	FCS_COP.1(b) FCS_COP.1(c)[L2]	RSA 186-4 SHA-256	RSA #2002 SHS #3231
Fax Control Unit	FCS_COP.1(c)[L1]	SHA-1	SHS #2363
Operation Panel Software	FCS_COP.1(b) FCS_COP.1(c)[L1]	RSA 186-4 SHA-1	RSA #C582 SHS #C582
Operation Panel Applications	FCS_COP.1(b) FCS_COP.1(c)[L1]	RSA 186-4 SHA-1	RSA # C582 SHS # C582

Table 38 Start-up integrity tests

TOE also performs Entropy testing as described in a separate Entropy Description document.

Testing the BIOS, MFP and Operation Panel operating systems, applications, and entropy source, demonstrates that the entire TSF is operating correctly.

If any of these steps fails, the TOE displays a Service Call (SC) error code on the Operator Panel and the TOE becomes unavailable. In such cases, the Administrator should contact a Customer Engineer to service the TOE.

If all steps succeed, then the TOE becomes available.

8.7.2 FPT_TUD_EXT.1, FCS_COP.1(b), FCS_COP.1(c)[L1], and FCS_COP.1(c)[L2]

TOE allows only the MFP Administrator to read the version of the MFP Control Software, Operation Panel Control Software, and FCU Control Software. The MFP Administrator can read these versions using the Operation Panel or WIM from the client computer.

The MFP Administrator can prepare for installation of updated MFP Control Software, Operation Panel Software, or FCU Control Software, by uploading an installation package from the client computer using WIM. The package contains the TOE Software and a digital signature (DS) that was created using the SERES private key. Digital signatures for trusted updates are generated outside of the TOE, by the manufacturer.

For MFP Control or FCU Software, the TOE performs the following verifications before the installing the package:

1. Identifies the type of software (e.g., MFP Control, Operation Panel, FCU);
2. Verifies that the software model name matches the TOE;
3. Creates a SHA256 message digest (MD1) of the software, uses the SERES public key to decrypt DS (MD2), and then verifies that MD1 = MD2.

For Operation Panel software, the TOE performs the following verifications before the installing the package:

1. Identifies the type of software (e.g., MFP Control, Operation Panel, FCU);
2. Verifies that the software model name matches the TOE;
3. Creates a SHA256 message digest (MD1) of the index file, uses the SERES public key to decrypt DS (MD2), and then verifies that MD1 = MD2.
4. Creates a SHA256 message digest (MD3) of the software image, uses an internal key to decrypt DS (MD4), and then verifies that MD3 = MD4.

The TOE performs the signature verification of the software to be updated using the encryption functions listed below when updating the software.

Integrity test	SFR	Algorithm	Validation
MFP Control Software	FCS_COP.1(b) FCS_COP.1(c)[L2]	RSA 186-4 SHA-256	RSA #2002 SHS #3231
Operation Panel Software	FCS_COP.1(b) FCS_COP.1(c)[L2]	ECDSA SigVar 186-4 SHA-256	ECDSA # C629 SHS # C629
Operation Panel Applications	FCS_COP.1(b) FCS_COP.1(c)[L2]	RSA 186-4 ECDSA SigVar 186-4 SHA-256	RSA # C582 ECDSA # C582 SHS # C582

8.8 PSTN Fax-Line Separation (TSF_FXS)

The Fax Line Separation Function permits only fax transmissions as input information from telephone lines so that unauthorized intrusion from telephone lines can be prevented.

8.8.1 FDP_FXS_EXT.1

The fax interface use cases are below.

- Sending faxes
  - The TOE receives documents from client PCs via the LAN, and using the fax interface, transmits them as fax documents via the PSTN line using the ITU-T T.30 protocol.
  - The TOE can transmit stored documents as faxes.
- Receiving faxes
  - A remote fax machine establishes a connection to the TOE through the PSTN line using the ITU-T T.30 protocol, through which the TOE receives fax documents.
- Fax-Line Separation
  - The fax modem accepts connections through the PSTN only if they conform to the ITU-T T.30 protocol.
  - Data that is transmitted or received through the PSTN is fax-format, image data.

8.9 Image Overwrite

8.9.1 FDP_RIP.1(a)

During the processing of jobs, image data is stored on the HDD. When such data is no longer needed by the user or the TOE, residual data can be overwritten using the Auto Erase Memory function.

When enabled, the Auto Erase Memory function automatically overwrites the residual image data after each completion of the following processing jobs:

- Copy jobs

- Print jobs
- Sample Print/Locked Print/Hold Print
- Stored Print jobs (after deletion of the job)
- Spool printing jobs
- LAN-Fax print data
- Faxes sent/received using remote machines
- Scanned files sent by e-mail
- Files sent by Scan to Folder
- Documents sent using Web Image Monitor
- Documents deleted from the Document Server using the Copier, Printer, Fax or Scanner functions

When the Auto Erase Memory function is enabled, such data is actively overwritten with values and repetition selected by the Administrator:

- NSA: Temporary data is overwritten twice with random numbers and once with zeros.
- DoD: Each item of data is overwritten by a random number, then by its complement, then by another random number, and is then verified.
- Random Numbers: Temporary data is overwritten multiple times with random numbers. The number of overwrites can be selected from 1 to 9, default 3.

3150 A Terminology

3151 A.1 Glossary

Term	Definition	Source
Address Book	Electronic storage mechanism that equates names of persons or physical locations with machine-usable destinations (e.g., fax telephone numbers, email addresses, Uniform Resource Locators).	
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 security policies of the TOE. Administrators may possess special privileges that provide capabilities to override portions of security policies.	[2600.1]
Asset	Entities that the owner of the TOE presumably places value upon.	[CC]
Assumption	Physical, technical, and administrative conditions or requirements of the Operational Environment that must be upheld in order for the TOE to provide security functionality.	
Border Encryption Value	A secret value passed to a storage encryption component such as a self-encrypting storage device.	[CPP_FDE_EE_V2.0]
Commercial Off-The-Shelf	Products that are both commercial and sold in substantial quantities in the commercial marketplace, and that can be procured or utilized under government contract in the same precise form as available to the general public.	[FAR]
Confidential (TSF) Data	Assets for which either disclosure or alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE.	[2600.1]
Create	Assigning a value or content to data in a storage device. Note that in the case of document processing jobs, the outcome is that the job is initiated	
Credentials	A form of authentication data that specifies basic identifying information about a User or application. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer Credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization.	[2600]
Decommission	The act of retiring an HCD from active use in the Operational Environment. It may also involve a change in geographic location and/or ownership.	
Delete	Dereferencing or otherwise making unavailable data in a storage device. Note that in the case of document processing jobs, the outcome is that the job is terminated.	
Document	A medium and the information recorded on it that generally has permanence and can be read by a person or a machine.	[610.12]
Document Processing	Printing, scanning, or copying a Document.	
Document Processing Job	A User request to the TOE to perform a Document Processing operation on a Document.	
Entropy Description	A non-public document that is part of CC evaluation	[HCDPP]
External IT Entity	An External Entity that is an IT device (not a human).	[CC] defines "External Entity"

Term	Definition	Source
Field-Replaceable (Unit)	The smallest subassembly that can be swapped in the field to repair a fault.	[IEEE]
Intermediate key	A key used in a point between the initial user authorization and the DEK	[CPP_FDE_EE_V2.0]
Job Owner	A User who initiates or creates a document processing job. It may also refer to a User to whom ownership of a document or job has been delegated or otherwise permitted by the Job Owner.	
Hardcopy Device	A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), “all-in-ones” and other similar products.	[2600]
Internal Authentication	Identification and authentication function that is wholly contained within the TOE.	
Key Management Description	A non-public document that is part of CC evaluation	[HCDPP]
Local Area Network	A non-public data network in which serial transmission is used without store and forward techniques for direct data communication among data stations located on the User's premises.	[8802-6]
Local User	A User who is physically present at the HCD.	
MFP Administrator	An administrative user with control of one or more aspects of MFP operations.	
MFP Supervisor	An administrative user with control of MFP Administrators	
Modify	Changing the value / content of data in a storage device. Note that in the case of document processing jobs, the outcome is that the instructions or other parameters of the job are changed.	
Multifunction Printer	A device that performs Document printing, scanning, and copying. It may also send and receive Documents over the PSTN using facsimile protocols.	
Network Printing	Printing operation that has been initiated by a Network User.	
Network User	A User who interacts with the HCD over a network.	
Nonvolatile Storage Device	A device that provides computer storage of data that is not cleared when the power is turned off.	
Normal User	A User who is authorized to perform functions that process User Document Data in the TOE.	
Operational Environment	Environment in which the TOE is operated.	[CC]
Organizational Security Policy	Set of security rules, procedures, or guidelines for an organization.	[CC]
Output Tray	A receptacle for the TOE's printed output.	
Protected (TSF) Data	Assets for which alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.	[2600.1]
Protection Profile	Implementation-independent statement of security needs for a TOE type.	[CC]
Read	To access data from a storage device or data medium. (Note that in this case, the data medium may be a printed output, and therefore, release of a print job is a “read” operation)	[610.12]
Redeploy	The act of moving an HCD from one Operational Environment to another Operational Environment.	

Term	Definition	Source
Security Assurance Requirement	A description of how assurance is to be gained that the TOE meets the SFRs.	[CC]
Security Functional Requirement	A translation of the Security Objectives for the TOE into a standardized language.	[CC]
Security Objective	Statement of an intent to counter identified Threats and/or satisfy identified organization security policies and/or Assumptions.	[CC]
Security Target	Implementation-dependent statement of security needs for a specific identified TOE.	[CC]
Servicing	Performing repairs or preventative maintenance on the HCD.	
Standard Protection Profile	A Protection Profile that is developed according to processes defined by NIAP.	
Submask	A submask is a bit string that can be generated and stored in a number of ways, such as passphrases, tokens, etc.	[CPP_FDE_EE_V2.0]
Target of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance.	[CC]
Temporary Storage	Storage of data that is not intentionally retained by the TOE after the completion of a Document Processing Job.	
Threat	Capabilities, intentions, and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.	[2600.1]
TOE Owner	A person or organizational entity responsible for protecting TOE Assets and establishing related security policies.	[2600.1]
TOE Security Functionality	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.	[CC]
TSF Data	Data for the operation of the TOE upon which the enforcement of the SFR relies.	[CC]
Unauthorized Access	Access to a resource that a User is not permitted to access.	
User	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary.	[CC]
User Data	Data for the User that does not affect the operation of the TSF.	[CC]
User Document Data	The Asset that consists of the information contained in a User's Document. This includes the original Document itself in either hardcopy or electronic form, image data, or residually stored data created by the hardcopy device while processing an original Document and printed hardcopy output	[2600.1]
User Job Data	The Asset that consists of the information about a User's Document or job to be processed by the TOE.	[2600.1]

Table 39 Glossary of Terms

Sources:

[2600] IEEE Std. 2600™-2008 "IEEE Standard for Information Technology: Hardcopy Device and System Security"

[2600.1] IEEE Std. 2600.1™-2009 "IEEE Standard for a Protection Profile in Operational Environment A"

[610.12] IEEE Std 610.12-1990 "IEEE Standard Glossary of Software Engineering Terminology"

[8802-6] ISO /IEC 8802-6:1994 "Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 6"

[CC] ISO/IEC 15408-1:2009 "Information technology – Security techniques – Evaluation criteria for IT security – Part 1"

[CPP_FDE_EE_V2.0] collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0, September 09, 2016

[FAR] United States Federal Acquisition Regulations

[HCDPP] "Protection Profile for Hardcopy Devices v1.0"

[IEEE] IEEE Standards Dictionary (ISBN 973-0-7381-2601-2)

A.2 Acronyms

Acronym	Definition
BEV	Border Encryption Value
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Service
COTS	Commercial Off-The-Shelf
EAL	Evaluation Assurance Level
HCD	Hardcopy Device
IPA	Information-technology Promotion Agency
I&A	Identification and Authentication
IT	Information Technology
JISEC	Japan Information technology Security Evaluation and Certification scheme
KMD	Key Management Description
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MFP	Multifunction Printer
NIAP	National Information Assurance Partnership
OSP	Organizational Security Policy
PP	Protection Profile
PSTN	Public Switched Telephone Network
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SPP	Standard Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification

Table 40 Acronyms